HistoCrypt 2018

Proceedings of the
1st International Conference on
Historical Cryptology

June 18–20, 2018
Uppsala University
Uppsala, Sweden

Proceedings of the 1st International Conference on Historical Cryptology

HistoCrypt 2018

Editor
Beáta Megyesi

June 18-20, 2018
Department of Linguistics and Philology
Uppsala University
Sweden

Published by

NEALT Proceedings Series 34
Linköping University Electronic Press, Sweden
Linköping Electronic Conference Proceedings No. 149
ISSN: 1650-3686
eISSN: 1650-3740
ISBN: 978-91-7685-252-1
URL: http://www.ep.liu.se/ecp/contents.asp?issue=149

Sponsors

UPPSALA
UNIVERSITET

RIKSBANKENS
JUBILEUMSFOND

STIFTELSEN FÖR HUMANISTISK OCH
SAMHÄLLSVETENSKAPLIG FORSKNING

cryptography

an Open Access Journal by MDPI

Preface: Program Chair

We are very pleased to introduce the proceedings of the International Conference on Historical Cryptology (HISTOCRYPT 2018), held at the Department of Linguistics and Philology on the English Park Campus, Uppsala University, Sweden, between June 18 and 20, 2018.

HISTOCRYPT addresses all aspects of historical cryptology/cryptography including work in closely related disciplines (such as history, history of ideas, computer science, AI, computational linguistics, linguistics, or image processing) with relevance to historical ciphertexts and codes. The subjects of the conference include, but are not limited to the use of cryptography in military, diplomacy, business, and other areas, analysis of historical ciphers with the help of modern computerized methods, unsolved historical cryptograms, the Enigma and other encryption machines, the history of modern (computer-based) cryptography, linguistic aspects of cryptology, the influence of cryptography on the course of history, or teaching and promoting cryptology in schools, universities, and the public.

HISTOCRYPT represents a continuation of the friendly events of European Historical Ciphers Colloquiums (EuroHCC) held in Heusenstamm (2012), Kassel (2016), and Smolenice (2017) to discuss on-going research in historical cryptology in Europe. Considering EuroHCC's growing popularity among the crypto-historians and cryptographers and the established HICRYPT network on historical cryptology with over 90 members from 20 countries around the world, our aim is to establish HISTOCRYPT as an annual, world-wide event. The first event in the series takes place in 2018 at Uppsala University, Sweden. We are very happy that the conference has been internationally recognized outside Europe as well, and submissions are received from all over the world. It is a great honor to serve as the Program Chair for HISTOCRYPT 2018, to be held in Uppsala for the first time.

The scientific program was carefully planned by an international scientific program committee, consisting of researchers in cryptology, history, intelligence and language technology. The program committee invited paper submissions in two distinct tracks: *regular papers* up to 10 pages on substantial, original, and unpublished research, including empirical evaluation results, where appropriate; *short papers* up to 4 pages on smaller, focused contributions, work in progress, negative results, surveys, tutorials, or opinion pieces; or summarizing a software system to be accompanied by a live demonstration at the conference.

The conference received 24 submissions from all over Europe (Czechia, Denmark, France, Germany, Hungary, Italy, Netherlands, Poland, Slovakia, Sweden, and the UK) as well as from Ghana, Israel, New Zealand, Russia, the United States, and Uruguay.

Our primary goal in the program committee was to achieve a high quality program using a double-blind, rigorous review process. All papers were reviewed by at least three experts invited by the program committee members for reviewing. After dis-

cussion among the reviewers to synchronize recommendations, the final selection of the papers was made by the program committee. The decision was not an easy task due to many submissions with high scores and overall positive reviews, and the time and space constraints of the two day long main conference. Our goal was to include papers dealing with a wide variety of topics from various scientific areas of relevance to historical cryptology. We aimed at achieving balance between regular and short papers, and chose to accept papers—being regular or short—with high scores as oral talks, while we were more lenient with poster presentations. 66% of the regular papers and 33% of the short papers were accepted for oral presentations, while 22% of the regular papers and 50% of the short papers were accepted as posters and/or demos. In the final program, there are 16 regular, and 5 short papers, all collected in this volume, thematically structured, in the same order as they are presented during the conference.

In addition to the accepted papers, we are proud to present six invited keynote speakers, distinguished researchers from France, Germany, Israel, and the US. They cover different areas of the conference. Craig Bauer (York College of Pennsylvania) presents highlights from his book on the world's greatest ciphers. Katherine Ellison (Illinois State University) talks about the central role of cryptology in the history of reading. Rémi Géraud tells us about his and David Naccache's work (École normale supérieure) on a French code from the late 19th century. Ephraim Lapid (Bar-Ilan University and IDC Herzliya) presents the thrilling story behind the British "Israeli Enigma".

Given the location of HISTOCRYPT at Uppsala University, special attention is given to the heritage of Prof. Arne Beurling and his role in breaking the German teletype ciphers. Therefore, we invited Kjell-Ove Widman, professor emeritus in applied mathematics (University of Linköping) to talk about Arne Beurling as a mathematician and code breaker, and George Lasry (University of Kassel) to tell us about his very new methods to solve the "completely hopeless" T52, which Arne Beurling worked on and which can be found in the archives of the Swedish National Defence Radio Establishment (FRA). And in connection to the poster and demo session, we organize an exhibition to show four Enigma machines, usually hidden in the FRA archive.

Lastly, the conference program also includes two workshops, organized by their own committees. The workshop on *(Automated) Cryptanalysis of Classical Ciphers with CrypTool 2* demonstrates the open-source e-learning tool consisting of several classical and modern cryptographic algorithms where participants can learn and practice how to use CrypTool. The workshop *Solving codes rather than ciphers. Is there a software challenge?* focuses on the fascinating codes, encrypted messages word by word, aiming at finding solutions for breaking these.

These proceedings will provide a permanent record of the program. The conference proceedings are published by the Northern European Association for Language Technology (NEALT) Proceedings Series by Linköping University Electronic Press, as freely available Gold Open Access. The proceedings are indexed in the DBLP com-

puter science bibliography and also published in the anthology of the Association of Computational Linguistics (ACL Anthology) in parallel.

Organizing a conference with an interesting and diverse program in a highly cross-disciplinary field is far from easy and relies on the goodwill of many researchers involved in the various scientific areas, all with their own traditions. I would like to express my gratitude and appreciation to my great fellows on the program committee for their invaluable work, for fruitful discussions, and for sharing the effort of creating the program. A special thank goes to the steering committee, especially Arno Wacker, for his support and generous advice. I would also like to record my appreciation for the work of the 23 reviewers and 4 subreviewers for their time and effort to contribute to the reviewing, give constructive and collegial feedback, and help the program committee in the selection of papers. Wholehearted thanks go to the six keynote speakers, and the workshop organizers, as well as Anders H. Wik and Åsa Ljungqvist for bringing to light the Enigma machines and arranging the exhibition in connection to the demo session. I would also like to thank all authors without whom this conference would not have taken place! Nils Blomqvist deserves a huge and special thank for professionally serving as the proceedings co-manager. My greatest debt goes to the local organization, Eva Pettersson, for carrying the burden of the local organization, and Bengt Dahlqvist, for helping out with the on-line registration and the conference website. We are also extremely pleased to have received generous sponsorship from the Swedish Foundation for Humanities and Social Sciences allowing free registration and covered accommodation and travel costs for many conference participants. Lastly, I am grateful to my nearest and dearest—my twins, bonus kids, and partner—for generously giving me the space to disappear into our world of hidden secrets from the past.

I wish you all a fruitful conference and hope you will enjoy HISTOCRYPT 2018!

Beáta Megyesi (Program Chair)

Program Committee

- Beáta Megyesi (Program Chair), Uppsala University, Sweden
- Bernhard Esslinger, University of Siegen, Germany
- Otokar Grošek, Slovak University of Technology, Slovakia
- Benedek Láng, Budapest University of Technology and Economics, Hungary
- Mark Phythian, University of Leicester, UK
- Anne-Simone Rous, Saxon Academy of Sciences and Humanities, Germany
- Gerhard F. Straßer, Emeritus, Pennsylvania State University, USA

Local Organizing Committee

- Eva Pettersson (Local Chair), Uppsala University, Sweden
- Bengt Dahlqvist, Uppsala University, Sweden
- Beáta Megyesi, Uppsala University, Sweden

Steering Committee

- Arno Wacker, University of Kassel, Germany
- Joachim von zur Gathen, Emeritus, Bonn-Aachen International Center for Information Technology, Germany
- Marek Grajek, Poland
- Klaus Schmeh, Private researcher, Germany

Extended Program Committee: Reviewers

- Eugen Antal, Slovak University of Technology in Bratislava, Slovakia
- Leopold Auer, Emeritus, Austria
- Charlotte Backerra, TU Darmstadt, Germany
- Nicolas Courtois, University College London, UK
- Karl de Leeuw, University of Amsterdam, Netherlands

- Camille Desenclos, Université de Haute-Alsace, France
- Mans Hulden, University of Colorado Boulder, USA
- Ioanna Iordanou, Oxford Brookes University, UK
- Pascal Junod, Snap, Switzerland
- Kevin Knight, University of Southern California, USA
- Jozef Kollár, Slovak University of Technology in Bratislava, Slovakia
- Grzegorz Kondrak, University of Alberta, Canada
- Nils Kopal, University Kassel/Applied Information Security, Germany
- George Lasry, University of Kassel, Germany
- Sjouke Mauw, University of Luxembourg, Luxemburg
- Jakub Mirka, The State Regional Archives in Pilsen, Czech Republic
- Michal Musilek, University of Hradec Kralove, Czech Republic
- Valerie Nachef, University of Cergy-Pontoise, France
- Stefan Porubsky, Academy of Sciences, Czech Republic
- Klaus Schmeh, Cryptovision, Germany
- Shlomo Shpiro, Bar-Ilan University, Israel
- Serge Vaudenay, Ecole Polytechnique Fédérale de Lausanne, Switzerland
- Pavol Zajac, Slovak University of Technology in Bratislava, Slovakia

Subreviewers

- Bradley Hauer, University of Alberta, Canada
- Saeed Najafi, University of Alberta, Canada
- Matteo Scarlata, University College London, UK
- Peter Spacek, Slovak University of Technology in Bratislava, Slovakia

INVITED TALK:

Updates on the World's Greatest Unsolved Ciphers

Craig Bauer

York College of Pennsylvania, USA

Abstract

Craig's book, *Unsolved! The History and Mystery of the World's Greatest Ciphers from Ancient Egypt to Online Secret Societies*, saw print a little over a year ago. Many updates can now be made. The talk includes highlights from the book, progress that has been made on several ciphers contained therein, and images of more historic unsolved ciphers, as challenges for conference attendees.

Bio

Craig P. Bauer is professor of mathematics at York College of Pennsylvania and the editor-in-chief of Cryptologia. He was the 2011-2012 Scholar-in-Residence at the National Security Agency (NSA) Center for Cryptologic History and is the author of two books: *Secret History: The Story of Cryptology* and *Unsolved!: The History and Mystery of the World's Greatest Ciphers from Ancient Egypt to Online Secret Societies*. His television appearances include the mini-series *The Hunt for the Zodiac Killer* and two episodes of *Codes and Conspiracies*.

INVITED TALK:

Cryptology and the Fantasy of Reading

Katherine Ellison
Illinois State University, USA

Abstract

This presentation will explore the central role of cryptology in the history of reading, when literacy became a goal of the masses rather than a special skill reserved only for the educated elite. Beginning in the seventeenth century, instructional cryptography manuals established the foundational terms and methodologies of literacy training. Cryptologers including John Wilkins, Gustavus Selenus, Gasparis Schotti, Noah Bridges, and John Falconer sought not only to educate the public in ciphering and deciphering but to establish multimodal habits of everyday literacy; they had a vision of the future of citizen literacy that resisted the dominance of alphabetic reading and insisted that literacy must encompass alphabets as well as mathematics, algorithms, scientific symbols, musical notation, visual images, and digital technologies (and they did use the term "digital", as in requiring the use of the digits). Cryptology also provided the framework for teaching audiences how to see the ways in which the habits of printing, page layout, and the physical materiality of books and paper all make meaning in relation to the symbols on the page. Though their methods did not heavily influence eighteenth- and nineteenth-century educational theorists, the revival of cryptologic curiosity during World War I, in particular, brought the seventeenth-century methods to the attention of figures like John Matthews Manly, Edith Rickert, the Friedmans, and others. Riverbank Laboratory even began publishing primers for teaching kindergarteners how to read – by teaching them the bilateral cipher of Francis Bacon.

Bio

Katherine Ellison is co-editor of *A Material History of Medieval and Early Modern Ciphers: Cryptography and the History of Literacy* (2017) and author of *A Cultural History of Early Modern English Cryptography Manuals* (2016) and *Fatal News: Reading and Information Overload in Early Eighteenth-Century Literature* (2006). Professor of English at Illinois State University, she has published widely on cryptology, media history, and literacy in *Games and War*, *Early Modern Trauma*, *Literature Compass*, the *Journal for Early Modern Cultural Studies*, the *Journal of the Northern Renaissance*, *Book History*, *Eighteenth-Century Fiction*, *Educational Research*, *Academic Exchange Quarterly*, *Maternal Pedagogies*, and *Sex and Death in Eighteenth-Century Literature*. She is beginning a new collection with Medievalist Dr. Susan Kim on John Matthews Manly and Edith Rickert and a monograph on *Fop Intelligence*, an investigation of cryptology and gender identity.

INVITED TALK:

A French Code from the Late 19th Century

David Naccache and Rémi Géraud

École normale supérieure, Paris, France

Abstract

The Franco-Prussian war (1870-1871) was the first major European conflict during which extensive telegraph use enabled fast communication across large distances. Field officers would therefore have to learn how to use secret codes. But training officers also raises the probability that defectors would reveal these codes to the enemy. Practically all known secret codes at the time could be broken if the enemy knew how they worked.

Under Kerckhoffs' impulsion, the French military thus developed new codes, meant to resist even if the adversary knows the encoding and decoding algorithms, but simple enough to be explained and taught to military personnel.

Many of these codes were lost to history. One of the designs however, due to Major H. D. Josse, has been recovered and this article describes the features, history, and role of this particular construction. Josse's code was considered for field deployment and underwent some experimental tests in the late 1800s, the result of which were condensed in a short handwritten report. During World War II, German forces got hold of documents describing Josse's work, and brought them to Berlin to be analysed. A few years later these documents moved to Russia, where they have resided since.

Bio

David Naccache heads the ENS' ISG. His research areas are code security, forensics, the automated and the manual detection of vulnerabilities. Before joining ENS Paris (PSL) he was a professor during 10 years at the Université Paris 2 (Sorbonne Universités). He previously worked for 15 years for Gemplus (now Gemalto), Philips (now Oberthur) and Thomson (now Technicolor). He is a forensic expert by several courts, and the incumbant of the Law and IT forensics chair at EOGN. David is the inventor of 170 patent families and the author of 200 publications in information security and cryptography.

Dr. Rémi Géraud is cryptologist, security researcher, member of the Information Security Group of École normale supérieure. His research interests include the mathematics of public-key cryptographic protocols, information security, physical and network intrusion, defensive design, and on a broader scale the economics and geopolitics of information.

INVITED TALK:

The Israeli Enigma

Ephraim Lapid
Bar-Ilan University and IDC Herzliya, Israel

Abstract

From its early days, the Israeli military has developed a Signals Corp to provide effective and secure communication to the needs of the defense establishment. From the start, there was good cooperation between the functions of cyphering and deciphering, although they were conducted by different organizations, to assure the security and reliability of military communications.

As soon as Israel gained its independence, it became a key target for British intelligence collection. British espionage activities on Israel were coordinated from the Security Intelligence Middle East (SIME) headquarters near Cairo, and later from Cyprus. The nascent Israeli cryptography was of special interest for British intelligence, as Britain still maintained a substantial military presence in the region, especially at the Suez Canal in Egypt and in Jordan. In the early 1950s, British intelligence embarked on a covert operation aimed at giving them access to Israel's most secret communications. The Israeli Defense Forces (IDF) looked for an advanced cypher machine to replace the hand-cypher, which caused bottlenecks of huge numbers of messages. Israel succeeded in purchasing from the United Kingdom 50 Enigmas in good order, and believing in the Enigma's invincibility, invested substantial effort and cost to transform them in great secrecy into Hebrew. However, before these Enigmas were put to operational use, a warning was received from several Israelis, who were former members of Bletchley Park's staff, on British successes in cracking the Enigma during WWII. A decision was made to abandon the Israeli Enigmas. Most of the Hebrew Enigmas were sadly destroyed, only one example was retained and is today on display at the IDF heritage center.

In the British Bletchley Park team were several persons who later immigrated to Israel, including Prof. Joseph Gilis, who founded the Department of Mathematics at the Weizmann Institute and Dr. Walter Eytan, the First Director-General of Israel's Ministry of Foreign Affairs. Two other Jewish experts from South Africa, Shaul Bar-Levav and Meir Shapira, were the founders of the IDF units of ciphering at the Signal Corp and deciphering in the Sigint unit. Colonel Shaul Shamai, a prodigious decoder of Arabic codes, was the only soldier who was decorated by an IDF Chief of Staff who had not fought on the battlefield, a testimony to his crucial contribution to deciphering key Arab cyphers.

Bio

Brigadier General (Res.) Dr. Ephraim Lapid is a lecturer at Bar-Ilan University and IDC Herzliya Israel. He served as a Senior Intelligence officer in the Israel Defense Forces (I.D.F) and was the I.D.F. Spokesperson and Instructor in the Israeli National Defense College. After retiring from the Israeli Military, he was a senior official in the Jewish Agency.

INVITED TALK:
SPECIAL SESSION ON ARNE BEURLING

Arne Beurling: Mathematician and Code Breaker

Kjell-Ove Widman

Professor Emeritus, Sweden

Abstract

Arne Beurling was a 34-year old professor of mathematics at Uppsala University when the Second World War broke out in 1939. He reported immediately to the Swedish SIGINT service and was first entrusted with Soviet military codes which he helped solve, partly in cooperation with Finnish colleagues. After the occupation of Norway in 1940, a hitherto unknown type of encrypted traffic was picked up from telegraph cables running from Norway to Germany through Sweden. Given the task of analysing the traffic, Beurling took the collected material from two days in May and retreated to his office. Two weeks later he reappeared, having diagnosed the type of the transmission, deduced the ciphering algorithm, and found a way to attack it. Special machines were built, and over a three-year period, more than 250 000 messages sent between Berlin and the occupying forces in Norway were deciphered and forwarded to the relevant Swedish authorities.

Beurling's achievement is surely one of the more remarkable ones in the history of cryptography, in particular since he worked with ciphered messages only and had no á priori knowledge of the system. This talk will try to give a hint of his cryptanalytic work and the Swedish code breaking effort during the war, as well as touch on his personality and his career as a mathematician.

Bio

Kjell-Ove Widman has been professor of applied mathematics at the University of Linköping, director of The Mittag-Leffler Institute of the Royal Swedish Academy of Science, and guest professor at universities in Germany, Italy, Poland and the US. He became interested in cryptology while doing his national service, and has worked on and off in the field since then, consulting for governmental and private organisations and companies. He has also translated books in mathematics and related fields.

INVITED TALK:
SPECIAL SESSION ON ARNE BEURLING

Modern Codebreaking of T52

George Lasry
University of Kassel, Germany

Abstract

The Siemens and Halske T52 is a family of teleprinter encryption systems, used in WWII by the Luftwaffe, the German Navy and Army, and German diplomatic services. Codenamed "Sturgeon" by the Allied, it was designed to provide enhanced security, compared to the other German teleprinter encryption system, the Lorenz SZ42 ("Tunny"). In one of the most impressive feats of cryptographic genius, the first model, the T52a/b, was reconstructed by Arne Beurling only from encrypted traffic. It was also reconstructed at Bletchley Park. Until the end of 1942, Sweden was able to read current T52 traffic that passed through its teleprinter lines, taking advantage of errors by German operators (e.g., messages sent in depth). At the beginning of 1943, Germany increased their security measures, also introducing a new model, the T52d. The T52d was a much more secure system, featuring an irregular movement of the wheels, and a "Klartext" (autokey) function. Sweden could not read its traffic, and a Bletchley Park report from 1944 considers the T52d problem to be "completely hopeless".

The T52 problem (when no depth is available) is still daunting today, even with modern computing. Since WWII, no new methods for the cryptanalysis of the T52 have been published. The machine complexity, and its huge keyspace size, 10^{27}, prohibit any brute-force attack. In this presentation, George will describe how he applied a novel statistical approach, to decipher rare original telegrams from 1942, encrypted using the T52a/b, and found in FRA archives. Also, he will present a first-ever practical attack on the T52d and its successor, the T52e, which takes advantage of a subtle weakness in the design of their stepping mechanism.

Bio

George Lasry specializes in the codebreaking of historical ciphers using modern optimization techniques. He has developed state-of-the-art attacks for a series of challenging cipher machines and systems. In 2013, he deciphered a collection of 600 original ADFGVX ciphertexts from 1918, which provide new insights into key events in the Eastern Front of WWI. In 2017, he also reconstructed German diplomatic and naval codebooks and deciphered hundreds of encoded messages from 1910 to 1915. Also, George has solved several public challenges, including the Double Transposition challenge, Chaocipher Exhibit 6, the M-209 Challenge and the 2015 Enigma Challenge. George Lasry regularly writes about his findings in Cryptologia. The subject of his Ph.D. thesis is the *Cryptanalysis of Classical Ciphers with Search Metaheuristics*.

Contents

WORLD WAR I

WORLD WAR II

POSTER AND DEMO

CONFERENCE PROGRAM

Sunday, June 17, 2018

Welcome Reception 18:00-21:00 at the Linnaeus Garden[1], Sweden's oldest botanic garden.

Monday, June 18, 2018 MAIN CONFERENCE

09:00 – 09:30 **Opening**

Arno Wacker Chair of the Steering Committee
Beáta Megyesi Chair of the Program Committee
Eva Pettersson Chair of the Local Organizing Committee

09:30 – 10:15 **Keynote**
Chair: Beáta Megyesi

Craig Bauer
Updates on the World's Greatest Unsolved Ciphers

10:15-11:00 **Historical Ciphers/Codes**
Chair: Gerhard Strasser

Ekaterina Domnina
Nicodemo Tranchedini's Diplomatic Cipher: New Evidence

Camille Desenclos.
Unsealing the Secret: Rebuilding the Renaissance French Cryptographic Sources (1530-1630)

11:00-11:30 Coffee Break

11:30-12:30 **Cryptanalysis of Classical Algorithms**
Chair: Anne-Simone Rous

Juan José Cabezas, Joachim von zur Gathen, and Jorge Tiscornia
Uruguayan Cryptographic Carpet

Nils Kopal
Solving Classical Ciphers with CrypTool 2

Mark Stamp, Fabio Di Troia, Miles Stamp and Jasper Huang
Hidden Markov Models for Vigenère Cryptanalysis

[1] http://www.botan.uu.se/our-gardens/the-linnaeus-garden/visit-the-garden/

12:30-13:30 Lunch

13.30-14.15 **Keynote**
Chair: Bernhard Esslinger

David Naccache and Rémi Géraud
A French Code from the Late 19th Century

14:15-14:45 Coffee break

14:45-16.15 **WW1**
Chair: Marek Grajek

Karl de Leeuw
The Solving of a Fleissner Grille during an Exercise by the Royal Netherlands Army in 1913

George Lasry
Deciphering German Diplomatic and Naval Attaché Messages from 1914-1915

Ingo Niebel
Learning Cryptanalysis the Hard Way: A Study on German Culture of Cryptology in World War I

Paolo Bonavoglia
New Findings in a WWI Notebook of Luigi Sacco

16:15-16:45 Coffee break

16:45-17.30 **Keynote**
Chair: Benedek Láng

Katherine Ellison
Cryptology and the Fantasy of Reading

18:30-00:00 Conference Dinner at Norrlands Nation[2]

[2] http://www.norrlandsnation.se/

Tuesday, June 19, 2018 MAIN CONFERENCE

09:00-09:45 **Keynote**
Chair: Otokar Grošek

Ephraim Lapid
The Israeli Enigma

09:45-10:15 Coffee break

10:15-12:00 **WW2**
Chair: Karl de Leeuw

Anders Wik
The First Classical Enigmas. Swedish Views on Enigma Development 1924-1930

Marek Grajek
Inventory of Early Inter-Allied Enigma Cooperation

Dermot Turing
The Poles and Enigma after 1940: le voile se lève-t-il?

Magnus Ekhall and Fredrik Hallenberg
US Navy Cryptanalytic Bombe – A Theory of Operation and Computer Simulation

Carola Dahlke
What We Know about Cipher Device "Schlüsselgerät SG-41" so far

12:00-13:00 Lunch

13:00–15:00 **Business meeting**

15:00-15.30 Coffee break

15:30-16:30 **Keynote: Special Theme on Arne Beurling**
Chair: Anders H. Wik

Kjell-Ove Widman
Arne Beurling: Mathematician and Code Breaker

George Lasry
Modern codebreaking of T52

16:30-18:00 **Poster and demo session with exhibition and coffee**

Posters

Noor R. Al-Kazaz, Sean A. Irvine and William J. Teahan
An Automatic Cryptanalysis of Playfair Ciphers Using Compression

Niels O. Faurholt
Willard's System

Anna Lehofer
The Application of Hierarchical Clustering to Homophonic Ciphers

Michal Musílek and Štěpán Hubálovský
Teaching and Promoting Cryptology at Faculty of Science University of Hradec Králové

Klaus Schmeh
Examining the Dorabella Cipher with Three Lesser-Known Cryptanalysis Methods

Jaap van Tuyll
Design and Strength of a Feasible Electronic Ciphermachine from the 1970s

Demos

Eugen Antal and Pavol Zajac
ManuLab System Demonstration

Magnus Ekhall and Fredrik Hallenberg
US Navy Cryptanalytic Bombe - A Theory of Operation and Computer Simulation

Nils Kopal
Solving Classical Ciphers with CrypTool 2

Extra demo by the organizers: Beáta Megyesi, Nils Blomqvist and Eva Pettersson
The DECODE database

Exhibition by FRA[3]: Anders H. Wik and Åsa Ljungqvist
Enigma machines

18:00-18:15 **Closing**

19:00-00:00 Conference Dinner at Restaurant Borgen[4]

[3] http://www.fra.se/snabblankar/english.10.html
[4] https://www.borgenuppsala.se/

Wednesday, June 20, 2018 WORKSHOPS

09:00-12:00 **(Automated) Cryptanalysis of Classical Ciphers with CrypTool 2**

Workshop organizers: Nils Kopal, Armin Krauss, Bernhard Esslinger
Room: 22-1017

12:00-13:00 Lunch

13:00-17:00 **Solving Codes rather than Ciphers. Is there a Software Challenge?**

Workshop organizer: Karl de Leeuw
Room: 22-1017

HISTORICAL CIPHERS/CODES

Nicodemo Tranchedini's Diplomatic Cipher: New Evidence

Ekaterina Domnina
Department of Area Studies
Faculty of Foreign Languages and Area Studies
Moscow State Lomonosov University
ekaterina.domnina@ffl.msu.ru

Abstract

This paper discusses a newly identified letter, written by Francesco Sforza's diplomatic agent Nicodemo Tranchedini da Pontremoli (1413-1481). The aim of this paper is to establish the date and purpose of this document and to offer a partial reconstruction of the code Tranchedini used for it.

1 Introduction

In 1902 Nikolay Petrovich Likhachev (1862–1936), a Russian historian and antiquary, bought an encrypted fragment (a postscript) of a diplomatic letter. Judging by the signature, a certain Nicodemus wrote it from Florence on 23 February of an unknown year (The Scientific and Historical Archive of the Russian Institute of History, Russian Academy of Sciences, Saint Petersburg, Coll. 48, Box 585, no. 35, f. 1). Thus, Likhachev added one more artefact to his large assemblage of cuneiforms, papyri and paper documents, which was one of the largest private collections in Russia at the time (Figure 1).

The sellers of this particular letter, the Charavet family from Paris or some other auction catalogue contributor, advertised it as a rare find to cast an additional light on the late medieval diplomatic practice. Since the document bore only the day and month (23 February), but not the year, they dated it to the reign of the French king Louis XI (1423–1483). They alleged that it reported on the diplomatic congress in Mantua, which was organised in 1460 by the pope Pius II to promote the idea of a new crusade (Figure 2).

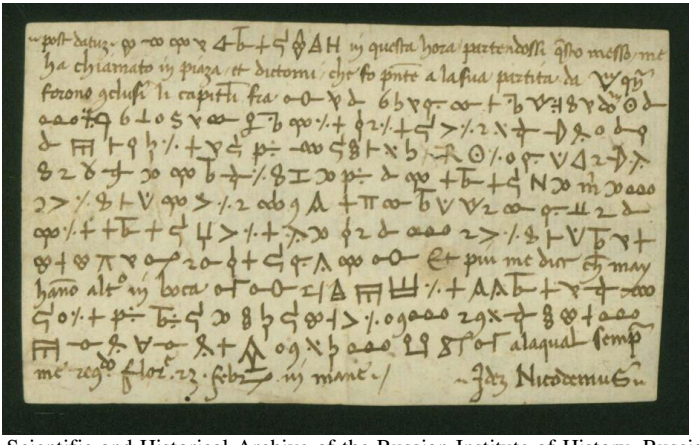


Figure 1. The Scientific and Historical Archive of the Russian Institute of History, Russian Academy of Sciences, Saint Petersburg, Coll. 48, Box 585, no. 35, f. 1r (with permission)

Proceedings of the 1st Conference on Historical Cryptology, pages 3– 7,
Uppsala, Sweden, 18-20 June, 2018

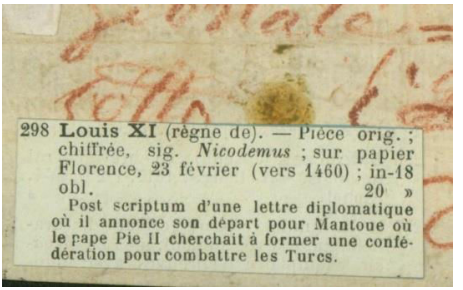

298 **Louis XI** (règne de). — Pièce orig. ; chiffrée, sig. *Nicodemus* ; sur papier Florence, 23 février (vers 1460) ; in-18 obl. 20 »
Post scriptum d'une lettre diplomatique où il annonce son départ pour Mantoue où le pape Pie II cherchait à former une confédération pour combattre les Turcs.

Figure 2. The Scientific and Historical Archive of the Russian Institute of History, Russian Academy of Sciences, Saint Petersburg, Coll. 48, Box 585, no. 35, f. 1v, detail (with permission)

Such an intriguing description definitely worked well to sparkle collectors' interest in this document, but at the same time did not cite any credible source for such an attribution. Indeed the early twentieth century witnessed a rise of interest towards medieval and Renaissance cryptology. It was at that period that Aloys Meister published his research on Italian ciphers (Meister, 1902). In this sense Likhachev was in a good company when he purchased this encoded document from the Charavet antiquaries. At the same time, he evidently never seriously attempted to decode this letter.

Today the study of this encoded letter could add to the discussion on how Italian Renaissance cryptology evolved and, most importantly, whether there was any difference between the codes devised by scholars and those employed in the daily diplomatic practice (Buonafalce, 2008:64). When trying to find answers to these questions one should definitely take a closer look at this encoded letter from the Likhachev collection and establish its author, contents, receiver and purpose.

2 The author of the letter

On a wrapper of this document Likhachev left a note, suggesting that it was written by Nicodemo Tranchedini da Pontremoli (Figure 3). However, during later cataloguing of the Likhachev's collection this attribution was not taken into consideration. Throughout the Soviet era, when the majority of Russian scholars working with this collection had no access to the foreign archives, it was impossible to check whether Likhachev's attribution of this letter to Tranchedini was correct or not. Now this can be done by studing Tranchedini's holographs from the Italian archives.

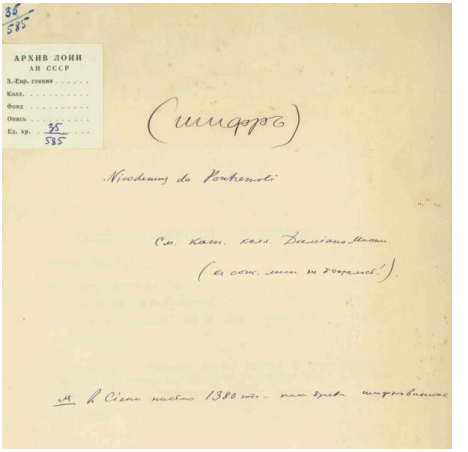

35
585
АРХИВ ЛОИИ
АН СССР
Nicodemus da Pontremoli

Figure 3. The Scientific and Historical Archive of the Russian Institute of History, Russian Academy of Sciences, Saint Petersburg, Coll. 48, Box 585, no. 35, wrapper (with permission)

Nicodemo Tranchedini da Pontremoli (1413-1481) was one of the most faithful and long-standing diplomatic agents of Francesco Sforza (1401-1466), both before the latter rose into power and afterwards. He received a humanistic education, taking keen interest in collecting and studying Latin and Greek manuscripts. A Florentine by birth, Tranchedini worked for Sforza in his home city-state, enjoying continuous favour of the Medici family. As Sforza's representative, he also resided in Rome and Genoa, among other places (Sverzellati, 1998). Famous for his impact on the formation of the diplomatic letter *per se*, Tranchedini left behind a large amount of correspondence, currently preserved primarily in the State Archives of Milan (Archivio di Stato di Milano, Carteggio Visconteo Sforzesco, *passim*).

Comparing Tranchedini's alleged signature from the document in question to his signatures on his letters in the Milanese State Archives I was able to conclude that it was indeed his own, but not from the 1460s or even later, contrary to the Charavet attribution. Further study of Tranchedini's correspondence showed that in the

1450s he primarily resided at the papal court, and thus the letter should be attributed to the 1440s, when he visited Florence as Sforza's agent.

3 Tranchedini's diplomatic cipher

In order to prove this hypothesis one should look at the code itself and search for its key. The most obvious starting point would be the cipher collection of his son Francesco Tranchedini (c.1441–c.1496), preserved in several copies. Mentored by Cicco Simonetta (1410-1480), the ducal secretary, Francesco served the Sforza family alongside his father. He listed Nicodemo's cipher on fol. 3r of his treaty (Cerioni. 1970, II; Hoeflechner, 1970). As L. Cerioni established (1970, I:6-7), it was employed from about 1471 until 1478. This particular nomenclator consisted of 253 signs, 55 – for letters, 12 – for double letters, 8 – for nulls, 65 – for syllables, 113 – for words.

When compared to the code of the letter in question, it did not match. This means that the encoded postscript belonged to the earlier date. After that I could only hope for some good luck, combined with thoroughly check through Nicodemo's letters from the 1440-1450s. The search through Tranchedini's correspondence from the 1440s returned neither similar encoded letters of his, nor the original letter to which this postscript belonged.

However, the search through Nicodemo's letters from 1450s bore some fruit. Not only did I find a document with a cipher identical to the letter in question but also a partical deciphering of the code (Archivio di Stato di Milano, Carteggio Visconteo Sforzesco, 41, no. 106, fol. 1, 11 March 1454, Rome). Judging by the handwriting, it is evident that Cicco Simonetta deciphered this passage himself. Then his addition was glued with wax over the ciphered text. (Figure 4). Taking this fragment as a starting point and using simple substitution analysis, I was able to reconstruct the code (Figure 5).

This nomenclator consisted of 81 signs: 36 for letters, 4 for double letters, 1 for nulls, 30 for syllables, 11 for words. It is incomplete since no other extant examples of this code seem to have survived in Tranchedini's correspondence from the 1450s in the State Archives of Milan. It is also important to underline that certain signs from the 1453 letter had a different meaning compared to that in the postscript. This means that the code was evolving over the time. However, since no other pieces of this code are available now, it is not possible to establish how often Simonetta changed Tranchedini's nomenclator.

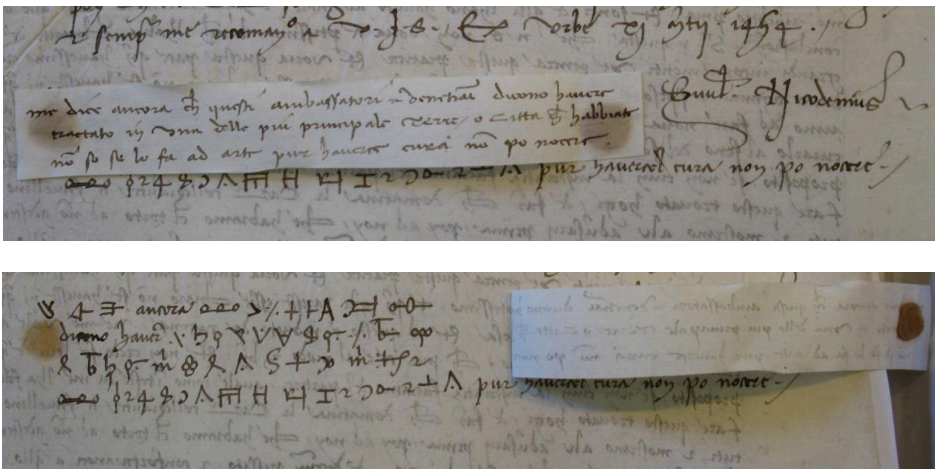


Figure 4. Archivio di Stato di Milano, Carteggio Visconteo Sforzesco, 41, no. 106, fol. 1v, 11 March 1454, Rome, a fragment (permission no. 4218/28.13.11/13, 24/2017 issued on 18.07.2017)

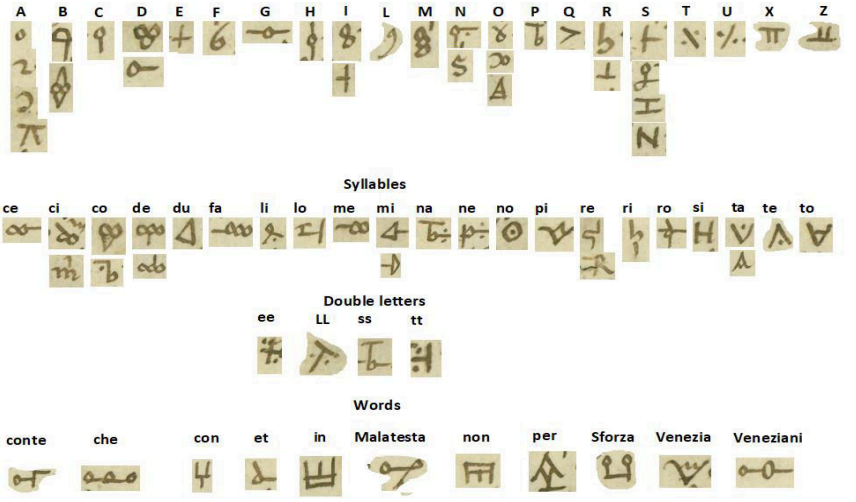


Figure 5. A reconstructed nomenclator for Tranchedini's cipher from the Likhachev's collection

4 Contents and dating of the document

When analysing the reconstructed contents of this postscript one could easily conclude that the key figure to understand and interpret it is condottiere Francesco Piccinino (or Pitticino) (c.1407– 16 October 1449) (See Appendix 1).

When on 13 August 1447 Filippo Maria Visconti, the Duke of Milan, died and the Ambrogian republic was proclaimed, it continued its rivalry with Venice for the control of the river Po valley. Condottieri Jacopo and Francesco Piccinini, as well as others, used these adversities to enrich themselves by constantly switching sides in return for lucrative payments from Milan and Venice. Francesco Sforza also participated in this worrisome diplomacy, awaiting an opportunity to seize power from the republicans in Milan. On 18 October 1448 he and Venice concluded an alliance at Rivoltella, which upset Francesco Piccinino's plan to get employment from Venice. Instead, in late autumn 1448 Piccinino allied himself with Sforza to make him pay for his troops' winter expenses, but then, in the following spring he defected to Milan (Ferrente, 2005:28).

It is most probable that this postscript belonged to the letter that Tranchedini wrote to Simonetta in February of 1449 as he witnessed these events. At least, there is firm evidence that in January of this year he negotiated with the Florentines to win their support for Sforza and succeeded in this endeavour, providing him with 20.000 florins on their behalf (Zaccaria, 2015:33-34, 371).

5 Conclusions

Firstly, the letter should be dated 23 February 1449 and was almost certainly intended for Simonetta, who stood behind Tranchedini's mission to Florence in January 1449. Secondly, it is not yet clear where the main part of this letter is, if indeed it is preserved. Thirdly, the document adds new data to the discussion about how Sforza prepared to conquer Milan, which he did in early 1450. Finally, Tranchedini's cipher in this postscript differs from the sophisticated ciphers presented by his son in his cryptologic collection, which could indicate that there might have been a significant difference between cryptologic theory and its practical implementation in Renaissance Italy. The study of these differences could help to establish the way the cryptographic methodology evolved not only in Italian states, but also in other European countries, which followed their example.

Acknowledgments

I would like to thank the wonderful staff of the Scientific and Historical Archive of the Russian Institute of History, Russian Academy of Sciences, Saint Petersburg and Archivio di Stato di Milano for helping me with my research and for granting me permission to reproduce images from their collections. I am also grateful to the anonymous reviewers of the HistoCrypt 2018 team for their comments on this paper and to Dr Justine Roehmel for her continuous support of my research work.

References

Archivio di Stato di Milano, Carteggio Visconteo Sforzesco, 41, no. 106.

The Scientific and Historical Archive of the Russian Institute of History, Russian Academy of Sciences, Saint Petersburg, Coll. 48, Box 585, no. 35.

Augusto Buonafalce 2008. Cicco Simonetta's cipher-Breaking rules. *Cryptologia*, 32(1):62-70.

Lydia Cerioni. 1970. *La Diplomazia sforzesca nella seconda metà del Quattrocento e i suoi cifrari segreti*. Vol. I-II. Il centro di ricerca, Roma.

Serena Ferente. 2005. *La sfortuna di Jacopo Piccinino. Storia dei bracceschi in Italia (1423-1465).* Olschki, Firenze.

Walter Hoeflechner. 1970. Hg. *Diplomatische Geheimschriften. Codex Vindobonensis 2398 der Oesterreichischen Nationalbibliothek.* Akad. Druck- u. Verl.-Anst., Graz.

Aloys Meister. 1902. *Die Anfaenge der modern diplomatischen Geheimschrift: Beitraege zur Geschichte der italienischen Kryptographie des XV. Jahrhunderts*. F. Schöning, Paderborn

Paola Sverzellati. 1998. Per la biografia di Nicodemo Tranchedini da Pontremoli, ambasciatore sforzesco. *Aevum*, 72(2):485-557.

Raffaella Maria Zaccaria. 2015. Ed. *Il carteggio della Signoria fiorentina all'epoca del cancellierato di Carlo Marsuppini (1444-1453). Inventario e regesti. Pubblicazioni degli archivi di Stato di Firenze. Strumenti CXCIX*. Edifir-Edizioni, Firenze.

Appendix 1. [Nicodemo Tranchedini a Cicco Simonetta]

Post datuz come de missere Bossi?[1] in questa hora partendossi questo messo me, ha chiamato in piaza et dictomi, che fo pronte a la sua partita da Venezia, quando forono gelusi li capitoli fra veneziani et Frncesco Pitticino et che ebe Francesco deve havere quatro milla etc et non scrivere?, ne fare mostrare novanta dua millia d'oro o de provisone et de essere socio, che aquista de qua delta, excepta Piacenza, et deve essere con? quello ha et che aquista pe[r] di da Malatesta? adherente de venetiani. Et più me dice, che may hanno altro in boca conte? venetiani lo o non invetatessero[sic] fare avenenare o morire di qualche altro modi che non gli toglie per? altro che Sforza, ill. conte, ala qual semper me racommando. Florentiae, 23 febr. in mane ides? Nicodemus

The Scientific and Historical Archive of the Russian Institute of History, Russian Academy of Sciences, Saint Petersburg, Coll. 48, Box 585, no. 35. f. 1r

Translation

[Nicodemo Tranchedini to Cicco Simonetta]

P.S. From mister Bossi?, leaving at this hour, he sent for me, called me in the square and told me he was ready to leave Venice when the agreement between the Venetians and Francesco Pitticino was stalled and that Francesco had and should have four thousand etc. In addition, neither he should sign? [an agreement], nor demonstrate ninety two thousand in gold or under condition to be an ally, that he obtained at this delta [of Po], save for Piacenza, and he should keep those [lands] he already has, which he has just conquered from Malatesta?, the Venetians' ally. In addition, he told me that never did the Venetians plot to poison or kill the count? by any other means and that they would not change Sforza, the illustrious count, for anyone else, to whom I always commend myself. Florence, 23 Febr. In the hand of Nicodemus

[1] Question mark indicates the signs, the meaning of which is not 100 per cent certain.

Unsealing the Secret: Rebuilding the Renaissance French Cryptographic Sources (1530-1630)

Camille Desenclos
CRÉSAT (EA-3436)
Université de Haute-Alsace
camille.desenclos@uha.fr

Abstract

Neither political nor diplomatic historians can avoid working with enciphered sources. However, we mostly study their content and not their writing processes. In the wake of a new history of political information, ciphers and, more broadly, cryptographic usages, practices and cultures should be embraced by historians. By considering cryptographic sources as significant witnesses of a culture of political information, we can no longer look at them as information repositories or instances for cryptanalysis but as complex scientific and political objects.

In that respect, Renaissance French ciphers form perfect study objects. They are not yet as complex and technical as in the mid-seventeenth or eighteenth century and show a representative variety of goals (political or diplomatic), systems (jargon, simple substitution, homophonic substitution, …) and usages. As any other early modern source, however, cryptographic sources are dispersed, incomplete and, sometimes, hardly understandable at first sight. By studying many ciphering tables, by observing encryption and decipherment practices within a correspondence, by matching the enciphered letters and the related ciphering table, by comparing cryptographic systems, we hope to rebuild, at least partly, the Renaissance French cryptographic practices.

1 Introduction

Anyone who works on Renaissance political or diplomatic correspondences has faced, at least once, ciphers or enciphered letters. The Kingdom of France, as any other European state, has provided favorable conditions to the rise of a wide, diverse and frequent cryptographic practice. The implementation of permanent diplomatic representations all over Europe – there were twelve French permanent diplomatic agents at the beginning of the 17th century – has entailed the development of new strategies and tools for the protection of information. The more the circulation of diplomatic correspondences increased, the more ciphers became essential. During the 16th century, enciphered letters thus progressed from an extraordinary use to common practice by the French diplomacy. In addition to this increased usage in diplomatic correspondence, the political and religious disorders within the French Kingdom during the second half of the 16th century led high-ranking but rebellious noblemen to make use of ciphers, too, in order to cover up their intentions and plots to their King and his spies.

Although ciphers cannot be distinguished from epistolary writing nor from the political or diplomatic writing usages, they have been neglected by French historians for a long time. The importance of ciphers for the protection of information was recognized, but their functioning as well as their writing processes are still ignored, as ciphers were studied only in an intellectual and not material perspective. By studying them only for their content rather than considering them as significant objects, ciphers could not be entirely understood and were narrowed to their ability to protect information and secrets (Tallon, 2010). Thus studies dedicated at most a few pages, nay a couple of lines, to ciphers and cryptographic usages and practices, mostly in addition to a presentation of the various ways of transmission: postal routes, special couriers … (Martin, 2010). Ciphers were not only exclusively associated with the protection of information but with diplomacy also, at the expense of a wider analysis of the cryptographic practices and usages within the French administration and high nobility, especially during political, social and/or religious disorders. However, French history, with its wars of religion, provides significant examples to be analyzed by historians.

Proceedings of the 1st Conference on Historical Cryptology, pages 9– 17,
Uppsala, Sweden, 18-20 June, 2018

While historians have not yet seized on the subject, historical cryptography and even more historical cryptanalysis (Nachef et al., 2016) arouse more interest. The history of cryptography has been clearly studied more than once. However, those noteworthy but international studies embrace its whole history. Yet the main focus relies on the modern era (Kahn, 1996) and/or on cryptographic theoretical treatises. Although this global perspective allows for the better understanding of each step of the cryptographic evolution, French cryptographic practices during the 16th century until Rossignol's works are, at best, briefly mentioned in these global analyses. These studies do not present the cryptographic patterns in detail and thus cannot meet the needs of historians. If some studies have indeed been devoted to Renaissance practical cryptography (Devos, 1950; Monts-de-Savasse, 1997), they only describe the ciphers and cipher-text characters and/or focus on very specific case studies. They certainly promote a better knowledge of general processes and cryptographic semantics. This remains nevertheless technical and narrowly focused knowledge, far from the expectations and needs of historians. The impact of encrypting letters on the writing and circulation of information does not seem to have been noticeable in diplomatic or political history. Nevertheless, some historians (Ribera, 2007; Hugon, 2004) proceed from diplomatic history to an early modern history of political information. They analyze indeed ciphers in relation to their concrete uses as ways to write and protect political information. By considering both their technical and political dimensions, ciphers can become a new object of study within a new field cutting across boundaries: the history of information. The presence of cipher-text and plain-text in one and a same letter reveals the essential balance between public and private spheres, public decisions and secret actions. Beyond secrecy, elaborating stronger ciphers as well as encrypting a portion of text resulted from the same decision: protecting what could be valuable information. But what caused the French cryptographic practices to evolve? The increasing circulation of information? The structuring of diplomatic and intelligence systems? Was secrecy more needed? Or did the political writing process itself evolve? The aim of this paper will thus be to demonstrate the methodological and historical benefits of matching the history of cryptography with the history of information and to reposition Renaissance cryptography as a significant practice in French political writing.

2 French Cryptographic Treatises

A study of Renaissance French cryptographic uses and practices faces some difficulties in regard to the absence and/or dispersion of sources. Many enciphered letters, even some ciphering tables, have been preserved, but without their related documentation. Ciphering tables[1] did not document the way they were used, and neither did diplomatic instructions describe the way ciphers had to be employed. The basic principles appear to be obvious. In most cases, ciphers rely on homophonic substitutions. But when a plain-text letter could be represented by two or three cipher-text characters, how was the cipher-text character chosen? Their concrete functioning stays unclear as it was probably explained orally before the correspondence or the embassy started. Moreover, we cannot find any recommendation about the nature of information which had to be enciphered, the required proportion of cipher-text within letters, and so on. Cryptographic practice relied certainly on a subjective interpretation by each user, but many aspects were common to Renaissance political and diplomatic society.

Moreover, no secondary sources have apparently been preserved in the French archives or libraries. The diplomatic treatises, which have become the main sources about the process of political writing, never describe the cryptographic uses and practices nor the influence of encryption on diplomatic writing. As a technical process, which belonged to the daily diplomatic routine, encryption was apparently not considered as part of the art of diplomacy. Some general recommendations were expressed in later works only (Callières, 1716). Callière's treatise dedicated almost two pages to cryptography, even if the main concern remained the diverse and general ways to protect information. Neither the purpose of encryption nor the functioning of ciphers were mentioned. Only the strategies to protect information were introduced. François de Callières did not mention the encryption process and its technical implementation. In addition to the technical aspects of cryptographic practices that were not

[1] A few ciphering tables present a quick documentation, mostly about the use of specific cipher-text characters. However, they are more the exception to the rule than actual documentation.

part of the art of diplomacy, this information needed to remain secret. Otherwise it would help other countries to break the French ciphers. That can easily – though only partly – explain the silence of these theoretical works.

Cryptographic treatises could therefore be useful sources both to learn how Renaissance people understood the encryption process and how and why they used it. The first such work, written in French, was nevertheless published only at the very end of the 16th century (Vigenère, 1586). Blaise de Vigenère – like François Viète a few years after him – was in the service of the French King for several years. Their proximity to centers of power suggests an influence or even a participation in the conception of ciphering tables. However, these treatises seem to have remained strictly theoretical, even though some rare implementations could be observed, at least in the 17th century (De Leeuw 2015). They conceived complex cryptographic systems, but they cannot be considered as practical encryption manuals. Vigenère's work did indeed describe theoretical cryptographic mechanisms and tried to conceive of a perfect, unbreakable, and thus almost ideal cipher[2]. Although Vigenère's work was clearly not intended for regular users but only for other scholars or scientists, noblemen and diplomats could not use Vigenère's proposals, anyway, because of their lacks of mathematical skills and their restricted writing time. Yet if these works strictly remained theoretical and had no influence on the cryptographic practice, Vigenère or Viète knew real-life cryptography though not as authors of cryptographic treatises but rather by working directly with the regular creators of ciphers while decrypting enciphered letters for the Duke of Nevers (Vigenère) or for the French King (Viète).

Several technical diplomatic treatises, however, such as *Traicté des chiffres* by Charles Brulart de Léon (circa 1630)[3] intended to provide practical solutions to the issues of daily cryptographic writing, which needed to be fast and simple, after all. Through its many examples[4] Brulart de Léon's treatise describes cryptographic mechanisms, recommended cipher-text characters, and so on. Following Cicco Simonetta's work, this treatise went further. It presents practical encryption processes which should enhance the protection of information such as not leaving any space within the cipher-text; frequently using cipher-text characters without any value (so-called nulls) so that rarely used characters would not lead to their value or nature; disguising the frequency of cipher-text characters, and so on. Brulart de Léon thus proposed concrete rules for encryption. By following these recommendations, the writer could hide the origin of his letter and prevent any interception. Brulart de Léon, as Cicco Simonetta before him, probably dedicated his work to the state office. As a former diplomat, Brulart de Léon[5] claimed to take advantage of his own diplomatic experience and to propose various solutions to the main issues of the daily encryption practice that he himself has been faced. But even if Brulart de Léon's recommendations paid better heed to the concrete diplomatic needs, they remained complex, constraining and hardly compatible with the speed requested by diplomatic writing. Whatever its initial or real goal, Brulart de Léon's work has stayed off the record. Only the original handwritten version has been preserved, and no written or printed copy has apparently been produced. Furthermore, its form looks more like a personal memorandum: there is no introduction and no inscription; the work has been preserved in the same manuscript along with other personal notes and memorandums. If Brulart de Léon's work was used by the state office, it would have been preserved with the state office archives. Anyway, just like any other theoretical cryptographic treatise, Brulart de Léon's manuscript highlights only one aspect of cryptographic practice. It describes the technical aspects (how to choose cipher-text characters

[2] Blaise de Vigenère explained it quite clearly in his dedicace to Antoine Séguier: "Ce traicté donques sera de semblables usages de chiffres, diversifiez en plusieurs manieres; tant pour incidemment parcourir ce qui se presentera à propos de ces beaux et cachez mysteres, adombrez sous l'escorce de l'escriture; que pour à l'imitation de cela en trasser beaucoup de rares et à peu de gens divulguez artifices […] et la plus grand' part provenans de nostre forge et meditation; non encore que nous scachions touchez jusques icy d'aucun" (Vigenère, 1586, page 4).

[3] French National Library, fr. 17538, fol. 48sq.

[4] Brulart de Léon's treatise, however, does not only present standard methods but also rare systems like a ciphering wheel.

[5] Brulart de Léon has been ambassador to the Republic of Venice from 1611 to 1620, then extraordinary ambassador to the city of Avignon (1625) and to Switzerland (1628-1630).

while conceiving ciphering tables, how to write cipher-text while drafting a letter) and tried to improve them in order to increase the protection of information. But it never questions general aspects: what kind of information has to be enciphered? Why? According to which principles? How were the ciphering tables used and how were encryption and decipherment operated?

3 What About Primary Sources?

Unlike their contemporary documentation about the cryptographic uses and practices, a substantial amount of Renaissance French enciphered letters has been preserved. By chance, most of them have survived with their deciphered text (in margins, between the lines or on a separate sheet). However, even if letters, like no other sources, transcribe perfectly the Renaissance cryptographic culture and practices, enciphered letters present to historians a major issue. Not all letters contain a decipherment or, at least, their separate deciphered text has been lost. That can prevent the reading and understanding of the content of such sources.

Upon receipt the state office systematically wrote the decipherment on the letter so that the state secretary could more easily read the whole piece. But if the recipient deciphered the letter himself, there was no need to rewrite the deciphered text on the original letter. The separate sheet on which the recipient processed the decipherment could easily be lost, deleted or even integrated into another set of documents. The original enciphered letter thus becomes unreadable for historians without the ciphering table or cryptanalytic skills. Many letters still have kept their secrets[6].

For several letters, however, their related ciphering tables still exist. Although they should be deleted at the end of each embassy or long-term correspondence, they have often been preserved, sometimes by the state office itself, and are now one of the most reliable sources of cryptographic uses and mechanisms. More than enciphered letters, ciphering tables make the understanding of the cryptographic systems and their contextual or structural adaptations easier. However, the ciphering tables have faced different fates and their identification can be tricky. They are rarely preserved within the same manuscript (or box) along with the related enciphered letters. For example, the cipher of Jean Hotman, the French resident to the Holy Roman Empire between 1609 and 1614, can be found in the French National Library within the manuscript fr. 4030. On the other hand, his enciphered correspondence with the French King is now kept in manuscripts fr. 15924 to fr. 15930. Moreover, the manifold Renaissance denominations for the ciphering tables ("jargon"[7], "cipher"[8], "key"[9]...) and the absence of any name and/or date on the verso or on the top of the ciphering tables seem to prevent historians from identifying the origins and usages of these tables. Even more, the Renaissance designations often mix tables and enciphered letters. Both can be designated as ciphers ("chiffres")[10]. Thus identifying the right typology of the cryptographic sources and matching enciphered letters to their related ciphering tables are real issues for historians.

We have counted the cryptographic sources which were already described and identified at the French National Library. In 2014, the catalog mentioned only 60 ciphering tables, a great deal less than their actual holdings. In fact, only one fifth of the manuscripts are fully described in the catalog. In addition to cursory descriptions of the other manuscripts, some mistakes and omissions (some bibliographic records were written in the 19th century) have distorted these results, which do not represent the diversity of political and diplomatic sources. Most of the diplomatic correspondences, for example, are only described in a few words[11]. As usual, primary

[6] No letter from Henri IV to François Savary de Brèves, French ambassador to the Ottoman Empire, can be read, as the decipherment has not been written directly on the enciphered letters (French National Library, fr. 3541).

[7] French National Library, Cinq-Cent Colbert 474, fol. 1: "Jargon au deschifre" [Deciphering jargon].

[8] French National Library, fr. 4053, fol. 57: "Chiffre de monseigneur le marechal" [Cipher of M. the marshal].

[9] French National Library, fr. 3629, fol. 42: "Clef pour deschiffrer les lettres de Madame de Raiz" [Deciphering key for the letters of Ms. de Raiz].

[10] French National Library, fr. 3634, fol. 5: "Chiffre reçu le dernier octobre à Meun par le duc de Nevers" [Cipher which was received the last day of October in Meun by the duke of Nevers]. This cipher is thus a fully enciphered letter written to the Duke of Nevers.

[11] The manuscript fr. 16113, for example, is labelled "Dépêches originales adressées à la Cour par divers ambassadeurs et agents français en Espagne" [Original letters from several French ambassadors and agents in Spain

cryptographic sources are widely dispersed, poorly described or identified, or even completely missing.

Because of the need to access and analyze cryptographic primary sources materially and intellectually, a long-term research project is currently conducted in collaboration with the French National Library in order to re-establish a direct contact with Renaissance French cryptographic sources. The French National Library counts as the main repository for political and diplomatic sources (until the mid-1620's). According to the Renaissance archival practices, almost all diplomatic correspondences and reports before 1626 have made their way to the French National Library, along with several political correspondences from the second half of the 16th century. Both kinds of sources are now preserved in the collections of "manuscrits français" [French manuscripts] and "nouvelles acquisitions françaises" [French new acquisitions]. The "collection d'érudits" [scholars' collection] presents exceptional documents, too[12]. In fact, a major part of the French cryptographic sources (before the 1630's) is kept at the French National Library and forms a vast and representative corpus of Renaissance cryptographic uses and practices, even if further research in the French National Archives and in the French Diplomatic Archives will be mandatory. By studying the remaining ciphering tables, by observing actual encryption practices, by analyzing additions on the verso or top of ciphering tables, by comparing cryptographic systems, we hope to rebuild, at least partly, the Renaissance French cryptographic practices, uses and cultures. In that perspective, comparisons with other European cryptographic practices through case studies or similar projects such as the one conducted by Benedek Lang (2018) on Hungarian Early Modern cryptographic practices, could lead to a useful, if not essential, distinction between European, "national" and contextual cryptographic patterns.

As a first step in this ongoing project, we are locating, identifying and dating every preserved ciphering table and enciphered letter. Every manuscript whose description suggests cryptographic documents (mention of original correspondences or reports) is systematically checked. So far, 179 ciphering tables and more than 2 100 enciphered letters (including circa 200 non-deciphered letters) have been found and described. At this stage, we presume that 50 non-deciphered letters, and probably more in the future, could be deciphered. Wherever possible, this identification work leads to the correction of some incomplete bibliographic records. In addition we mention the presence of cipher-text and/or decipherment, add dates and names if they can be restored, and so on. Nevertheless, only the bibliographic records which already present a full description will be corrected. The aim of this project is not to completely describe the political and diplomatic collections at the French National Library but to re-connect the cryptographic sources to each other.

Thanks to this identification work, we should be able to cross-check ciphering tables and enciphered letters and link the letters to their related tables. Each enciphered letter whose ciphering table has not yet been found, will be compared to the anonymous ciphering tables. The cross-checking (through cryptographic systems and no more by names) will not be successful for each enciphered letter. More enciphered letters from different writers than ciphering tables have been preserved. Nevertheless, some ciphering tables, if still missing, could be reconstructed thanks to the decipherment in the letters. By comparing the cipher-text and the deciphered text, the cryptographic patterns could be understood and restored to a great extent.

4 First Results

Our first results, though still incomplete, have confirmed the real necessity to embrace cryptographic sources as material objects and to look at them in a broader perspective. They are not only the implementation of cryptographic patterns, which could interest the history of sciences or technology, but a true testimony of a culture of political information. Facing only the technical mechanisms is not enough. Of course, both the history of technology and the history of sciences are essential to the understanding of the technical mechanisms and their evolutions. The cryptographic sources, however, deserve to be subjected to different approaches and methodologies in order to merely surpass political history or the history of technology. More than any other political source,

to the French Court]. However, it contains a ciphering table of André de Cochefilet, baron of Vaucelas, ambassador to Spain from 1609 to 1615.

[12] The manuscript Clairambault 360 for example preserves the ciphering table of Henri IV and Maurice of Hesse.

cryptographic ones do indeed involve political, diplomatic, scientific, social and cultural history.

Identifying cryptographic sources at the French National Library has required prior research. In order to prevent hypotheses based on better known, but modern, practices and uses, we first needed to reassess the Renaissance patterns: which words referred to ciphers and cryptographic practices? Did these denominations possess any specific value? Specific words can already be highlighted: “jargon”, “chiffre” [cipher], “clef” [key], “deschiffre” [deciphered text], “table”. The word “jargon” especially referred systematically to the same object and practice: a ciphering table using a substitution system, by words and not by characters (for example: the word rose for the French King). Such tables were never called anything else but “jargon”. On the contrary, the word “chiffre” had many uses. If the main use, according to our modern practice, concerned ciphering tables, fully enciphered reports or anonymous letters were sometimes designated (on the verso) as “chiffres”, too. The origin of this confusion could be related to the use, by diplomats mostly, of the expression “en chiffre” [with cipher]. Moreover, if “deschiffre” is an early modern word for both decipherment and deciphered text, the cipher-text was hardly ever designated by “chiffre” but by “en chiffre” [with cipher/enciphered]. The denominations of cryptographic tools and productions were not yet standardized: marginal mentions rarely described the typology of documents in detail but provided names or dates[13]. These mentions aimed to make the identification of the document easier and quicker for the state office, the diplomats or more generally its recipient. Ciphering tables were often sent as attachment or handed over in person; there was then no need for any additional mentions. At last, the expression “ciphering table” comes from modern usages. Renaissance cryptography was not yet practiced as an applied science. It still relied on a spontaneous approach as shown by the alphabetical and thematic organization within ciphering tables. Everyone had to be able to use such tables, even without any cryptographic or algorithmic knowledge. Thus the distinction between ciphering tables and deciphering tables was probably spontaneous; both were indeed designated as “chiffre” only. In the future, however, we must find out if both ciphering and deciphering tables were conceived and written systematically, as they will be beginning with Rossignol, or if the existence of one or the other relied on specific uses or users.

Beyond the denominations, defining similarities between the cryptographic processes is essential for the upcoming cross-checks. If the French cryptographic systems were mostly based on substitution, they became more complex and rational during the 16th century. At the beginning of the 16th century, ciphers only presented few cipher-text characters (simple substitution and limited nomenclator). In the second half of the 16th century, though, especially from the 1580's, homophonic substitution was introduced (two to five cipher-text characters for one single plain-text letter), nomenclators were extended (around one hundred words on an average) and new cipher-text characters appeared: characters without any value, canceling characters, repeating characters[14]. These improvements, however, did not go as far as the theoretical recommendations of cryptographers were concerned. A large majority of ciphers, even in the 1620's, still relied on homophonic substitution, much simpler for diplomats and noblemen.

The fast technical evolution of French cryptographic practices makes the identification of ciphering tables easier and confers to our study an extra historical perspective. For each ciphering table, its main features are highlighted and analyzed: enciphering pattern (simple substitution, homophonic substitution, jargon, nomenclators), type of cipher-text characters (Latin and/or Greek alphabet and/or numbers and/or symbols). Most of the time, a careful analysis can lead to a precise dating (to within one or two decades at most). In addition to this first analysis, we get a closer look at the cipher-text characters as they give us the best clues for the cross-checking stage. In the same way that encryption patterns have been improved, the form of the cipher-text characters has become more and more rational and easy to generate so that they can be written and read faster. From symbols or highly-modified Latin characters[15],

[13] French National Library, fr. 3462, n.f.: “Chiffre reformé pour Levant duquel a esté envoyé un double à Monsieur de Breves ambassadeur en avril 1604” [Modified cipher for the Levant whose duplicate has been sent to M. de Breves, ambassador in April 1604].

[14] See for example, French National Library, fr. 3668, fol. 72: Cipher of the count of Tillières and the French King, 1625.

[15] See, for example, French National Library, fr. 3329, fol. 2: Cipher of Jacques d'Humières and François de Balzac.

cipher-text characters were increasingly transformed into numbers. Symbolic characters, which are easy to spot, are thus a specific feature of the first half of the 16th century, even if, until the 1580's, some examples, mostly in political ciphers, can still be found. From the 1560's on, however, symbols gradually disappeared and were replaced by numbers or Latin or Greek characters. Therefore the presence of symbols within a cipher is a significant clue about the date or, for ciphers after 1590, a real specific feature. Nomenclators finally help dating the ciphering tables. The names within the nomenclators represented indeed the main noblemen, ministers, clergymen or diplomats from a specific time. For example, the anonymous ciphering table in the manuscript fr. 3329 can be dated from 1574-1577 as the nomenclator includes the marshal of Montluc. Blaise de Montluc had been appointed marshal in 1574 and died in 1577. Such a precise dating is of course not always possible, especially for the oldest ciphers which did not use large nomenclators. A date range can still be defined in those cases. At last, nomenclators, as well as the improvements of the cryptographic patterns and characters, inform on the circumstances of their usage. A high proportion of foreign names reveals a diplomatic use, and if a country, for instance Spain, is more represented, it is highly likely the cipher was used by a French ambassador to Spain.

But whatever its rise, cryptography is not used in every Renaissance correspondence. The operation remained arduous both for writers and readers and was limited to what was considered as crucial or secret information. Thus the presence and amount of cipher-text reveal the significant political value of the text. However, this was not representative of a specific time. Fully enciphered letters were already written in the first half of the 16th century, and an integral encryption never became a standard. In addition to their long and arduous writing, ciphers did not need to be systematical but, on the contrary, had to adapt themselves as much as possible to the evolving contextual needs: diplomatic conflict, war, insecure postal routes, and so on. Information was not by nature secret; only the collecting of information and/or its use within a given context made its veiling inevitable. In the future, these usage hypotheses will require broader statistics, but the persistent general writing patterns seem logical for now. Moreover, the amount of cipher-text within a given letter (few lines, one page or the whole letter) will help to better understand the needs for writing secret information.

Diplomacy was obviously the main, and by the way first, user of ciphers. The oldest enciphered letter which so far we have found in the French National Library, dates from 1526 and comes from a French diplomatic agent in Rome[16]. A vast majority of enciphered letters from the first half of the 16th century and beyond that from the first decades of the 17th century comes from the diplomatic practice. However, if ciphers were an essential tool for diplomacy, they were not used systematically and on a daily basis. Not every diplomatic agent was provided with a ciphering table. Only the high-ranking diplomats possessed one or several such instruments. In fact, ciphering tables replicated the diplomatic hierarchy. On the contrary, the political use of ciphers was not based on hierarchy but only on needs, as it was not linked to professional or temporary tenure. Although ciphers were only used by the French diplomacy during the first half of the 16th century, the French nobility started to also use ciphers during the second half of the 16th century. Noblemen did not yet use ciphers for personal matters (Lang, 2014) but only for political purposes. Far from being anecdotal this use increased from the end of the 1570's and became more diversified in its practices and the origin of its users. That reveals how deeply ciphers were interwoven with the custom of political writing. The agitated political context in France substantially explains this evolution: noblemen were watched by the royal power, French or foreign factions were watching each other …. Thus ciphers became essential to the political correspondence: they protected information, reputation and sometimes physical integrity. Further counts and identifications will insert these examples from the 1580's in a broader perspective. The corpus that is finally expected should provide some more information about the proportion of each use (political or diplomatic). We hope thereby to be able to predict more precisely the motivations for the political use of ciphers and confirm, or invalidate, the current example of the 1580's. The political use of ciphers could be permanent or strictly limited to momentary needs (mostly during disorders).

[16] French National Library, fr. 2984: letters from Nicolas Raincé to Anne de Montmorency. Nicolas Raincé was the secretary of Jean du Bellay, cardinal and French representative in Rome.

Anyway, political ciphers were not as advanced as their diplomatic counterparts. The needs were very different: users were not "professional" agents; they had not been trained and this political use was still rather new. Above all the main need remained speed, before safety. Except in some rare cases like Vigenère who served the Duke of Nevers in the 1580's, cryptographers served the French King, not other noblemen. The reduced complexity of their ciphering tables was completely logical: there were more symbols; nomenclators were shorter, and homophonic substitution was less advanced. The differences between political ciphers, mostly the ones during the Catholic League, and diplomatic ciphers reveal how French diplomacy mastered the cryptographic practice and did its best to meet the agents' daily needs by constantly improving the protection of information and facilitating the encryption and decipherment operations. Renaissance French diplomacy acted like a laboratory in which ciphers and their implementation were constantly tested and improved. Its practices and patterns were then reused in wider circles, few years or decades after their conception by the French diplomacy.

5 Conclusion

Two essential elements have been highlighted during these first years of our research project: the need for a methodology which is adapted to the cryptographic features (in order to proceed successfully to the identification, analysis and cross-checking of our ongoing corpus) as well as the need for studying not only the ciphers but the general context in which they were employed. If this research project is far from completion, some hypotheses can be stated about the general uses and issues of cryptography within the political and diplomatic society of the French Renaissance. Building on these first results and future findings, we aim to study the encryption mechanisms and their improvements until cryptography became an applied science. We will thus be able to observe the intellectual evolution of French cryptography: its increased use in political and diplomatic correspondences; the dichotomy between the practiced cryptography and its theory; the variations between the diplomatic or political cryptographic uses. We hope to highlight the adaptation of ciphers to geographical locations and/or to political and diplomatic context and finally to understand the refinement and complexity of cryptography as practiced in Renaissance France. We aim to bridge a substantial divide between the production and collect of information and the decision-making process: the material process of the writing of political information. From then we could re-build a history of Renaissance French cryptography, not only in the perspective of the history of sciences but also as part of a global history of information.

Acknowledgments

Part of the project has been supported by a Mark Pigott Research Grant (2015). We would like to thank Gerhard F. Straßer and the anonymous reviewers for their valuable comments, suggestions and help with grammatical and lexical issues.

References

François de Callières. 1716. *De la manière de négocier avec les souverains*. La Compagnie, Amsterdam.

Jean-Pierre Devos. 1950. *Les chiffres de Philippe II (1555-1598) et du Despacho universal durant le XVII^e siècle*. Académie royale de Belgique, Bruxelles.

Alain Hugon. 2004. *Au service du Roi Catholique, "honorables ambassadeurs" et "divins espions": représentations diplomatiques et service secret dans les relations hispano-françaises de 1598 à 1635*. Casa de Velasquez, Madrid.

David Kahn. 1996. *The Codebreakers*. Simon and Schuster, New York.

Benedek Lang. 2014. "People's Secrets: Towards a Social History of Early Modern Cryptography". In *The Sixteenth Century Journal*. 45.2: 291-308.

Benedek Lang. 2018. "Real-Life Cryptology: Enciphering Practice in Early Modern Hungary". In Katherine Ellison and Susan Kim (eds), *A Material History of Medieval and Early Modern Ciphers: Cryptography and the History of Literacy*. Routledge, New York/London, pages 223-240.

Karl de Leeuw. 2014. "Books, Science, and the Rise of the Black Chambers in Early Modern Europe". In Anne-Simone Rous and Martin Mulsow (dir.), *Geheime Post: Kryptologie und Steganographie der diplomatischen Korrespondenz europaïscher Höfe während der Frühen Neuzeit*. Duncker & Humblot, Berlin, pages 87-99.

Claire Martin. 2010. *Mémoires de Benjamin Aubéry du Maurier, ambassadeur protestant de Louis XIII (1566-1636)*. Droz, Genève.

Jacques de Monts-de-Savasse, “Les chiffres de la correspondance diplomatique des ambassadeurs d'Henri IV en l'année 1590”. In Pierre Albert (dir.). 1997. *Correspondance jadis et naguère: congrès national des sociétés historiques et scientifiques*. Comité des travaux historiques et scientifiques. Paris, pages 219-228.

Valérie Nachef, Jacques Patarin and Armel Dubois-Nayt. 2016. “Mary of Guise's Enciphered Letters”. In Peter Y. A. Ryan, David Naccache and Jean-Jacques Quisquater (eds.). *The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday.* Springer, Berlin, pages 3-24.

Jean-Michel Ribera. 2007. *Diplomatie et espionnage: les ambassadeurs du roi de France auprès de Philippe II du traité du Cateau-Cambrésis (1559) à la mort de Henri III (1589)*. Honoré Champion, Paris.

Alain Tallon. 2010. *L'Europe au XVIe siècle: États et relations internationales*. Presses universitaires de France, Paris.

Blaise de Vigenère. 1586. *Traicté des chiffres ou secretes manieres d'escrire*. Abel L'Angelier, Paris.

Cryptanalysis of Classical Algorithms

Uruguayan cryptographic carpet

Juan José Cabezas
Instituto de Computación
Facultad de Ingeniería
Universidad de la República
Montevideo, Uruguay
jcabezas@fing.edu.uy

Joachim von zur Gathen
B-IT, Universität Bonn
Germany
gathen@
bit.uni-bonn.de

Jorge Tiscornia
Presidencia Uruguay
Montevideo, Uruguay
jtiscornia@
presidencia.gub.uy

Abstract

We present a unique item in the history of cryptography: a woollen carpet woven in a Uruguayan penitentiary in 1980 during the dictatorship in that country. The colors of a pair of horizontally adjacent knots encrypt a single letter. The carpet is in moderately good shape, with loss of colors and some damage by moths. We had obtained the original code and here report on the deciphering. The plaintext is a political message destined to comrades outside, with a description of the political situation and directives for actions.

The cryptosystem is a simple substitution. Breaking such codes is trivial. The real task here is to translate the knots into a machine-readable representation of their colors, in the presence of unclear colors and damage to parts of the carpet.

The encrypted carpet is an important document from the dark times of the Uruguayan dictatorship, manufactured by prisoners from the guerrilla movement *Tupamaros*. Two of the present authors (JJC and JT) were active members of this group. Their personal memories were essential for our successful reconstruction of the plaintext.

1 Introduction

Uruguay (*República Oriental del Uruguay*) borders on Brazil, Argentina, and the Atlantic Ocean with the estuary of the Río de la Plata. It was known as the *Switzerland of South America* because of its wealth, safety, and democratic governance. An economic downturn started in the 1960s. In its wake, militant groups arose.

On the extreme right side, the JUP (*Juventud Uruguaya de Pie*, Uruguayan youth standing up) aimed at the unions and other leftists, and their death squads killed some of their enemies.

On the left side was the MLN (*Movimiento de Liberación Nacional*, Movement for national liberation). Its members were known as the *Tupamaros*, after the leader Túpac Amaru II of an anticolonial uprising in Perú around 1780.

By 1973, the Tupamaros were essentially defeated by the government forces, their leaders killed, imprisoned, or refugees abroad. Many of them were held at a penitentiary with the unlikely name of *penal de Libertad*. The town of Libertad (Liberty) is located 51 km from Montevideo, the capital of Uruguay, and was founded by European refugees in the 19th century, happy to find their religious liberty. *Penal* is prison or penitentiary.

The Tupamaro inmates composed, in discussions over three years, a lengthy text to their companions outside, still in liberty (with small l). How to get it out of prison?

They were allowed to produce handicraft articles, receiving the materials at 8 am and handing them back at 4.30 pm. Ricardo García wove the carpet in several months' work in 1980. The carpet successfully left the prison.

A relative of Ricardo García received the carpet but it never reached its destination, an MLN group in Sweden. When the relative went into exile in Germany, he had the cipher table (Table 2), but lost it and remembered it only years later. The carpet was never decrypted in its time.

Uruguay regained democracy in 1985 and the prisoners of Libertad were freed. 29 years later, Jorge Tiscornia found the carpet in Ricardo García's home, and he was also given the cipher table. At the end of 2014, he told Juan José Cabezas about the carpet (Figure 1) who then set out to decipher it.

The carpet is unique in several aspects; it shows an imaginative use of simple cryptography under the dire circumstances of prison, and it is a unique

Proceedings of the 1st Conference on Historical Cryptology, pages 21– 27,
Uppsala, Sweden, 18-20 June, 2018

Figure 1: The carpet.

testimony of its type concerning this historic period.

The only other encryption methods by weaving or knotting that we are aware of are the Inca quipus and the encrypted quilts on the underground railway for black slaves fleeing from the USA to Canada in the 19th century (see Tobin (1999)).

The Tupamaros were inspired by Dickens' *Tale of Two Cities* (Dickens, 1859). It distills the atmosphere in pre-revolutionary France around 1789. A tough tavern owner, a central character in the book, works as the eyes and ears of the pre-revolution. She knits diligently accounts into her knitware, of evil persons, their deeds, and of spies, dreaming of future vengeance. "Knitted, in her own stitches and her own symbols, it will always be as plain to her as the sun." For any malefactor, it would be easier "to erase himself from existence, than to erase one letter of his name or crimes from the knitted register of Madame Defarge." Dickens says nothing about her encryption method, but these words were enough to fire the penitentiary inmates' imagination and inspire the idea of their carpet. Dickens' poetic introductory sentence refers to the French Revolution, but it describes the Tupamaros' situation as well: "It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness, it was the epoch of belief, it was the epoch of incredulity, it was the season of Light, it was the season of Darkness, it was the spring of hope, it was the winter of despair, we had everything before us, we had nothing before us, we were all going direct to Heaven, we were all going direct the other way.".

2 The encryption method

In the following, we distinguish typographically between `ciphertext` and *plaintext*.

The coding method, communicated by Ricardo García to us, uses a simple substitution on 18 letters. Each letter is encoded by a pair of horizontally adjacent colors, allowing six colors for the first item and three for the second one.

The encoding goes as follows:

O	G	B	L	W	P	color
M	*A*	*R*	*K*	*O*	*S*	O
D	*I*	*N*	*T*	*E*	*L*	G
J	*U*	*P*	*V*	*H*	*F*	B

Table 1: The code.

using the following six colors:

color	abbr
orange, yellow	O
dark green	G
beige, pink, ochre	B
light green	L
white, light gray	W
purple	P

Table 2: The colors.

The lines stand for Marcos, (door) lintel, and JUP (see above). VHF presumably is a filler with the remaining letters and unlikely to refer to *very high frequency*. The system thus employs a reduced alphabet of 18 letters: *A, D, E, F, H, I, J, K, L, M, N, O, P, R, S, T, U, V*. Taking into account the phonetics and orthography of the Latin American Spanish language, some of them represent more than one letter:

- *K* represents the letter k, and qu, and also c when pronounced like k.
- *V* represents v and b.
- *S* represents s, and also c when pronounced like s.
- *J* represents j and g.
- *I* represents i and y.

It was not meant as a simplified orthography of Spanish, but can be taken as such. (In today's text messages in Spanish, K is often used for qu.) For example, the list of color pairs

```
(W,O),(P,G),(G,O),(L,O),
(W,G),(L,G),(G,O),(P,G)
```

encrypts the text *OLAKETAL*. Interword spaces, the (silent) initial H, and punctuation marks are not present, and the list represents the phrase *Hola que tal* (Hi, how are you?).

The absence of spaces, accents, and punctuation marks means that a string of colors may represent more than one grammatically and semantically valid text. In our decipherment, such ambiguities were an obstacle, and this might be worse if this method was used elsewhere without the a priori knowledge we had about the context.

3 The current state of the carpet

The carpet measures 55.3×36.8 cm and contains almost 13 000 knots for about 6400 encrypted letters, arranged in a matrix of 67 rows and 96 columns. Moths have totally or partially damaged about 10% of the color pairs, and the borders are frayed, as is visible in the figures.

We distilled from a high-resolution digital image of the carpet a machine-readable matrix of colors. Our software then transformed the resulting RGB values to one of the six colors. This had to be done in a robust way so that similar colors were transformed to the same value, but distinct colors were properly distinguished. Then adjacent pairs of knots were deciphered as individual letters, proper word separations introduced, and the final decipherment produced. This was less than straightforward, and we encountered the following problems.

1. Damage to the carpet.
2. About 5% of the colors ran into adjacent knots, affecting their (automatic) legibility.
3. After 35 years, colors have degraded. In some parts, it is difficult to distinguish between white and ochre, and between light and dark green.
4. The reading ambiguities mentioned above sometimes make interpretation difficult. For example, the string *AKNTPERONOA* is to be read as *a CNT pero no a* ... (to CNT but not to ...) where CNT is the *Convención Nacional de Trabajadores* (National Convention of Workers).

4 Decryption

The digitized image is presented in Postscript, which is then converted to plaintext. We illustrate the process on the carpet's second line, magnified in Figures 3 through 5 and its decryption in Figure 6.

Each dot of color is given as an RGB (Newman and Sprouil, 1983) triple of red, green, and blue values, each ranging from 0 to 25.

We took samples from various sections of the carpet and determined the range of RGB values for each color, and also the fractions of these values, in order to be able to account for dark or light sections. That is, 6 7 8 and 7 8 9 represent the same hue, the latter slightly lighter than the former. Overlap of these values and fractions occurred mainly for G (dark green) and L (light green), and for B (beige) and W (white). Since G and B occur more frequently in the carpet than L

Figure 2: The bottom left shows moth damage and lost material on the fringes.

Figure 3: The second line, left part. It starts at top left and ends at bottom right.

Figure 4: The second line, middle part.

Figure 5: The second line, right part.

GO	BO	GO	PB	GO	PG	WG	BO	WO	PG	GB	WG	OB	WO	GG	OG
a	*r*	*a*	*f*	*a*	*l*	*e*	*r*	*o*	*l*	*u*	*e*	*j*	*o*	*i*	*d*
GO	LB	GG	WG	OB	WO	PO	PO	WG	BB	BO	WO	OG	GB	PO	WG
a	*v*	*i*	*e*	*j*	*o*	*s*	*s*	*e*	*p*	*r*	*o*	*d*	*u*	*s*	*e*
GO	BG	G?	??	LO	GG	GO	OG	GB	BO	GO	BG	LG	WG		
a	*n*	*a*	*r*	*k*	*i*	*a*	*d*	*u*	*r*	*a*	*n*	*t*	e		

Figure 6: Part of the second line transcribed (upper line) and decrypted (lower line).

and W, respectively, we opted to use the former in ambiguous cases.

The next step was to convert these color values into text. We covered each knot in the carpet by small horizontal rectangles, whose width was about that of the whole knot. Our matrix algorithm (James D. Foley and Hughes, 1990) scanned each rectangle and looked for a dominant color among the rectangles of each knot. If a dominant color was found, it was considered the color of the knot. In a pair of adjacent knots starting in an "even" position, there are six possible colors for its first member and three for its second one. Invalid dominant colors, damaged areas, and the absence of a dominant color are also reported.

In cases of doubt, we also employed a vector search using vertical vectors in the middle of the knot. If two or more occurrences of a valid color were detected, then four vertical vectors determined its dominance in the knot.

In the end, we obtained a sequence of knot colors, with numerous unresolved cases.

Bypassing the intermediate steps explained below, we take the carpet's second line as an example in Figures 3 through 6.

5 Recovering the plaintext

In another example, from the carpet's third line, we illustrate some of the steps from the raw identification of letters, with many unclear positions, into plaintext. This was no easy task and required substantial manual intervention. We first discovered some obvious plaintext snippets, then searched for valid words before and after such pieces, and in the case of damaged knots, had to visually inspect the carpet.

Letters without parenthesis or bracket are considered correct by the software. * is an unrecognized letter, *(MARKOS)*, *(DINTEL)*, and *(JUPVHF)* show six possible choices, and similarly *(MDJ)*, *(AIU)*, *(RNJ)*, *(KTV)*, *(OEH)*, and *(SLF)* correspond to three possibilities. These indicate that the first or second color of a pair, respectively, may be damaged. $[c1|c2$ means that letter c1 seems more likely than letter c2 in this place, and $< c >$ indicates the letter c, but with low probability.

So here are the steps from the original letters to plaintext. Lower case letters in the fourth text present guessed corrections of the automatic color readings.

*N[U|*L(SLF)ARD(DINTEL)SARROLLOIDAR*
*ESPLIKASION[I|*K[D|*EP*OTA*
TRESTENDENSIAAN<I>TIM<D>
LN[a|(KTV)J[N|*FALSO**

*N[U|*L(SLF)AR DESARROLLO I DAR*
*ESPLIKASION [I|*K[D|*EP*OTA*
TRES TENDENSIA AN<I>TIM<D>LN[a|
(KTV)J[N| FALSO*

*N[U|*L(SLF)AR DESARROLLO I DAR*
*ESPLIKASION [I|*K[D|*EP*OTA*
TRES TENDENSIA ANTI MLN [a|
(KTV)J[N| FALSO*

pULSAR DESARROLLO I DAR
ESPLIKASION DErrOTA
TRES TENDENSIA ANTI MLN
KoN FALSO

... pulsar desarrollo y dar explicación derrota. Tres - tendencia anti-MLN con falso ... (... further the development and give an explanation of [our] defeat. Third—anti-MLN tendency with false...)

A translation into plaintext would have been hard without the personal acquaintance of Tiscornia with the situation and political context of the MLN and the penitentiary at Libertad around 1980.

6 Conclusions

We have recovered the plaintext of about 95% of the carpet; only small parts of it are damaged beyond recognition. The carpet is now becoming a valuable testimony of Uruguayan and Latin American history.

From a cryptographical point of view, the following aspects are particularly interesting:

- The inmates have succeeded in encrypting a substantial amount of information by means of material accessible to prisoners in the penitentiary.
- The construction of the carpet presumably involved a large number of hours, but then, time is the one thing that is abundant in prison.
- The prisoners used a simple coding mechanism in a clever way which even fooled the exit checks at the prison.

In terms of cryptanalytic techniques, our task was trivial once the sequence of colors was established. However, given just that sequence with its many errors and ambiguities, it is not clear how easy this task would have been without the knowledge of the encryption in Table 2.

In synthesis, we have an original piece of cryptography, well conceived and well implemented. It was secure, efficient, and economic under the dire circumstances of the penitentiary. The fact that we could decipher it 35 years later shows the success of their method.

7 The first lines of the computer generated transcription.

The first four lines of the transcription read as follows:

*(DINTEL)MD[A|*FA(DINTEL)*E*OLUEJO*
IDAVIEJO(MARKOS)SP<M>RODUSE
ANUJKIAD(AIU)RA(DINTEL)TETRESA(RNP)
(DINTEL)OSPORKAUSASUNO(SLF)

[|*E(MARKOS)II<*>DI(KTV)*
(JUPVHF)(DINTEL)FIATS
APO<>LITIKAI<P>UER*
SONA(DINTEL)AT(JUPVHF)
DONI(KTV)E(DINTEL)
*I[I|*O<*>SINKANASDI<A>RIJE<*
T>ITESN<>EIM(SLF)*

*N[U|*L(SLF)ARD(DINTEL)SARROLLOIDAR*
*ESPLIKASION[I|*K[D|*EP*OTATR*
ESTENDENSIAAN<I>TIM<D>L
N[a|(KTV)J[N|*FALSO**

*DP[R|*SLE<I>NINDESTRUIENDO*
ENVE(MARKOS)
*DEELEV[N|*V[R|*T<*>ODOESTOK*
ON(JUPVHF)OKAKOM<>UNIA<I>D*
*[A|*SIONITE(DINTEL)SIO**

Distilling cleartext from this is not always obvious.

8 Parts of the carpet's cleartext.

We present the initial part of the cleartext. The opinions and political points of view expressed in this document do not, in any way, reflect necessarily those of the authors or their institutions. Comments between brackets are the authors'.

A complete version of the cleartext (in Spanish) can be found at `https://www.fing.edu.uy/~jcabezas/papers/ElTapizMLN2015.pdf`.

[First line.] *...ona: sólo tu debe conocer vía y forma. Traduce esto, al final te aclaro. Hazlo llevar ...ama Falero.*

[Introduction.] *Luego ida viejos se produce anarquía durante tres años por causas:*

1. *pérdida confianza política y personal a todo nivel,*
2. *incapacidad dirigentes de impulsar desarrollo y dar explicación derrota y*
3. *tendencia anti-MLN con falso marxismo-leninismo, destruyendo en vez de elevar, todo esto con poca comunicación y tensión represiva.*

Arriba hay confianza y crece, fierreros y divisionistas retroceden.

El correcto marxismo-leninismo va mas lento, dirección autocrítica MLN, un paso necesario y defectuoso.

[Previous events.] *Luego del año 55, la izquierda marxista será determinada por dos hechos:*

1. *lucha de clases desatada por crisis económica*
2. *discusión ideológica internacional entre vía violenta o pacífica al socialismo.*[1]

Acknowledgements

Alfredo "Tuba" Viola brought the authors together during a course given by the second author in Montevideo. Without his support, this paper would not have come into being, and we thank him for it.

About the authors. JJC is a professor of computer science at the Instituto de Computación in the Universidad de la República, Uruguay. He was

[1] [M]ona: only you must know the method and form. Translate this, at the end I explain it. Take it [... ama] Falero.
After the older leaders left, we had anarchy during three years for various reasons: 1. loss of political and personal confidence at all levels, 2. inability of the leaders to further development and explain our defeat, 3. anti-MLN tendency with false marxism-leninism, destroying rather than elevating, all this with little communication and repressive tension.
On the higher floors [where the leaders were housed, floors 3 to 5] we have growing confidence, [but] warriors [who want to continue the armed struggle] and divisionists [who prefer a political party for the struggle] retreat. The correct marxism-leninism goes more slowly, in the direction of MLN self-criticism, a necessary step that is missing.
Since 1955, the marxist left has been determined by two facts: 1. class struggle unleashed by the economic crisis, 2. international ideological discussion between violent and peaceful road to socialism.

severely injured in 1970 while manufacturing a bomb in his workshop and fled the country, hidden in the trunk of a car. JvzG is an emeritus professor of computer science at the Universität Bonn, Germany, and has no experience in building bombs. JT (Jorge Carlos Tiscornia Bazzi) is an Uruguayan writer and was a member of the Tupamaro *Colona 15*, together with JJC. He now works at the Presidencia Uruguay. During his 4646 days in the penitentiary of Libertad, from 1972 to 1985, he kept a secret diary on small slips of paper, normally used to roll cigarettes. He hid them in wooden clogs that he used in the shower. They are now published (Tiscornia (2012)) and provide moving insights into the (in)human conditions in prison, see also Tiscornia (2014). They were turned into a documentary movie (Charlo (2014)).

References

José Pedro Charlo. 2014. *El almanaque. Documentary movie.* Argentina, Spain, Uruguay.

Charles Dickens. 1859. *A Tale of Two Cities*. Chapman & Hall, London.

Steven K. Feiner James D. Foley, Andries van Dam and John F. Hughes. 1990. *Computer Graphics Principles and Practice*. Adisson Wesley.

William M. Newman and Robert F. Sprouil. 1983. *Principles of Interactive Computer Graphics*. Mc Graw Hill.

Jorge Tiscornia. 2012. *El almanaque*. Yaugurú, Montevideo, Uruguay.

Jorge Tiscornia. 2014. *Nunca en domingo. Relatos. Penal de Libertad 1972-1985*. Ediciones de la Banda Oriental, Montevideo, Uruguay.

Jacqueline Tobin. 1999. *Hidden in Plain View. A secret story of quilts and the underground railway*. Anchor Books, New York.

Solving Classical Ciphers with CrypTool 2

Nils Kopal
Applied Information Security – University of Kassel
Pfannkuchstr. 1, 34121 Kassel, Germany
nils.kopal@uni-kassel.de

Abstract

The difficulty of solving classical ciphers varies between very easy and very hard. For example, monoalphabetic substitution ciphers can be solved easily by hand. More complex ciphers like the polyalphabetic Vigenère cipher, are harder to solve and the solution by hand takes much more time. Machine ciphers like the Enigma rotor machine, are nearly impossible to be solved only by hand. To support researchers, cryptanalysts, and historians analyzing ciphers, the open-source software CrypTool 2 (CT2) was implemented. It contains a broad set of tools and methods to automate the cryptanalysis of different (classical and modern) ciphers. In this paper, we present a step-by-step approach for analyzing classical ciphers and breaking these with the help of the tools in CT2. The primary goals of this paper are: (1) Introduce historians and non-computer scientists to classical encryption, (2) give an introduction to CT2, enabling them to break ciphers by their own, and (3) present our future plans for CT2 with respect to (automatic) cryptanalysis of classical ciphers. This paper does not describe the used analysis methods in detail, but gives the according references.

1 Motivation

There are several historical documents containing text enciphered with different encryption algorithms. Such books can be found for instance in the secret archives of the Vatican. Often, historians who find such encrypted books during their research are not able to decipher and reveal the plaintext. Nevertheless, these books can contain secret information being of high interest for historians. In such cases, cryptanalysts and image-processing experts are needed to support deciphering the books, thus, enabling the historians to continue their research.

The ciphers used in historical books (from the early antiquity over the Middle Ages to the early modern times) include simple monoalphabetic substitution and transposition ciphers, codebooks and homophone ciphers.

With the open-source tool CrypTool 2 (CT2) (Kopal et al., 2014) historians and cryptanalysts have a powerful tool for the analysis as well as for the (automatic) decryption of encrypted texts. Throughout this paper, we present how CT2 can be used to actually break real world ciphertexts.

The following parts of this paper are structured as follows: The next section gives a short introduction to classical ciphers, as well as an overview of cryptanalysis. In Section 3, we briefly introduce the CT2. In Section 4, we present a general step-by-step approach for the analysis of ciphers with CT2. Section 5 shows real example analyses done with the help of CT2. Section 6 gives an overview of cryptanalysis components (for classical ciphers) already implemented in CT2 as well as components planned for the future. Finally, Section 7 summarizes the paper.

2 Foundations of Classical Ciphers and Cryptanalysis

After a brief introduction to classical ciphers we discuss the cryptanalysis of classical ciphers.

2.1 Classical Ciphers

Ciphers encrypt plaintext into ciphertext based on a set of rules, i.e. the encryption algorithm, and a secret key only known to the sender and intended receiver of a message.

Classical ciphers, as well as ciphers in general, can be divided into two different main classes: substitution ciphers and transposition ciphers. A

Proceedings of the 1st Conference on Historical Cryptology, pages 29– 38,
Uppsala, Sweden, 18-20 June, 2018

substitution cipher replaces letters or groups of letters of the plaintext alphabet with letters based on a ciphertext alphabet. Transposition ciphers do not change the letters themselves but their position in the text, i.e. plaintext alphabet and ciphertext alphabet are equal. There also exist ciphers that combine both, substitution and transposition, to create a composed cipher, e.g. the ADFGVX cipher (Lasry et al., 2017).

Substitution ciphers can be furthermore divided into monoalphabetic and polyalphabetic ciphers (Forsyth and Safavi-Naini, 1993). With monoalphabetic ciphers, only one ciphertext alphabet exists. Thus, every plaintext letter is always replaced with the same letter of the ciphertext alphabet. If there are more possibilities to choose from the ciphertext alphabet the substitution cipher is a homophone substitution cipher (Dhavare et al., 2013). If there are more than one ciphertext alphabet which are exchanged after each encrypted letter, the substitution is a polyalphabetic substitution, e.g. the Vigenère cipher (Schrödel, 2008). Substitution may also not only be based on single letters but on multiple letters, e.g. the Playfair cipher (Cowan, 2008). In history, for military and diplomatic communication, codebooks and nomenclatures were used. With a nomenclature, not only letters were substituted, but additionally, complete words were substituted. Codebooks contained substitutions for nearly all words of a language.

Transposition ciphers change the positions of each letter in the plaintext based on a pattern that is based on a key. The most used transposition cipher is the columnar transposition cipher (Lasry et al., 2016c). Here, a plaintext is written in a grid of columns. Then, the columns are reordered based on the lexicographical order of a keyword written above the columns. Finally, the ciphertext is read out of the transposed text column-wise. Decryption is done the same way but in the reverse order.

Composed ciphers execute different cipher types in a consecutive order to strengthen the encryption. One famous composed cipher is ADFGVX. Here in the first step, each plaintext character is substituted by a bigram only consisting of the 6 letters A,D,F,G,V, and X. After that, the intermediate ciphertext is encrypted with a columnar transposition cipher. ADFGVX was used by the Germans during World War I. It introduced a new concept, called fractionation. With fractionation, a plaintext symbol (here a bigram) is afterwards fractionated into two different symbols, making cryptanalysis even harder.

Ciphers based on codebooks were often super-enciphered, thus, first the words were substituted, for instance with numbers. Then, the resulted ciphertexts were additionally super-encrypted by changing them according to special rules.

Many encrypted historical books that survived history are available. Most of them are encrypted either with simple monoalphabetic substitutions or with homophone substitutions. For some books the type of cipher is unknown.

Many encrypted historical messages are encrypted with simple substitution ciphers, homophone substitution ciphers, polyalphabetic substitution ciphers, nomenclatures, or codebooks. Transposition ciphers were also used, but not as much as substitution ciphers since transpositions are more complex with respect to the encryption procedures. Additionally, performing a transposition cipher is more prone to errors. In modern times, transposition was used by the IRA (Mahon and Gillogly, 2008) and during World War II by the Germans and the British.

In World War II, rotor cipher machines like the German Enigma (Gillogly, 1995) performing polyalphabetic encryptions were introduced and widely used.

2.2 Cryptanalysis

Cryptanalysis is the science and art of breaking ciphers without the knowledge of the used key. Today, cryptanalysis is used to evaluate the security of modern encryption algorithms and protocols.

We divide the cryptanalysis of classical ciphers into two different approaches: the classical paper-based cryptanalysis and the modern computer-based cryptanalysis. In his paper we focus on modern computer-based cryptanalysis which can be done with CT2.

Substitution ciphers can be broken with the help of language and text statistics. Since every letter in a language as well as in the plaintext alphabet of a cipher has its unique frequency it can be used to guess and identify putative plaintext letters. With monoalphabetic substitutions, plaintext and ciphertext frequencies are identical, but the letters differ. For example an 'E' is substituted by an 'X' – 'X' has then the same frequency in ciphertext as 'E' has in plaintext. Thus, an algorithm

to break a substitution ciphers aims at recovering the original letter distribution.

Homophone substitutions as well as polyalphabetic substitutions flatten the distribution of letters, hence, aiming to destroy the possibility to break the cipher with statistics. Nevertheless, having enough ciphertext and using sophisticated algorithms, e.g. hill climbing and simulated annealing, it is still possible to break them.

Transposition ciphers can also be attacked with the help of statistics. Since transposition ciphers do not change the letters, the frequency of the unigrams in plaintext and ciphertext are exactly the same. Thus, to break transposition ciphers, text statistics of higher orders (bigrams, trigrams, tetragrams, or n-grams in general) are used to break them. Besides that, similar sophisticated algorithms, e.g. hill climbing and simulated annealing, are used to break transposition ciphers.

For breaking a classical cipher, it is useful to know the language of the plaintext. It is possible to break a cipher using a "wrong" language, but the correct one yields a higher chance of success. For cryptanalysis most of the algorithms implemented in CT2 contain a set of multiple languages, e.g. English, German, French, Spanish, Italian, Latin, and Greek. In many cases, the language of an encrypted book is known to the cryptanalyst or can be guessed by its (historical) context.

To identify the type of the cipher, whether it is a substitution cipher or a transposition cipher, cryptanalysts use the Index of Coincidence (IC) (Friedman, 1987). The IC, invented by William Friedman, is the probability of two randomly drawn letters out of a text to be identical. For English texts the IC is about 6.6% and for German texts about 7.8%. Simple monoalphabetic encryption, where a single letter is replaced by another letter, does not change the IC of the text. Same applies to all transposition ciphers, since these do not change the text frequencies. Polyalphabetic substitution aims at changing the letter distribution of a text to become the uniform distribution. Thus, the IC is about $\frac{1}{26} \approx 3.8\%$ (where 26 is the length of the ciphertext alphabet and all letters are used equally distributed). Homophone substitution also aims at changing the letter distribution of a text to become the uniform distribution, but here the IC is about $\frac{1}{n}$, where n is the amount of different symbols in the text.

Thus, having an IC close to 6.6% indicates that we have either a plaintext, a monoalphabetic substituted text, or a transposed text. And it is probably German. On the other hand, having an IC close to 3.8% indicates that we have a polyalphabetic encrypted text. Clearly, the IC is more accurate having long ciphertexts. Identification of homophone ciphers can be done by counting the number of different used letters or symbols. If the number is above the expected alphabet size, it is probably a homophone substitution.

State-of-the-art for breaking classical ciphers are search metaheuristics (Lasry, 2018). Because with classical ciphers, a "better guessed key" often yields a "better decryption" of a ciphertext, such algorithms are able to "improve" a key to come close to the correct key and often finally reveal the correct key. "Better" in this context means, that the putative plaintext that is obtained by decrypting a given ciphertext is rated higher by a so-called cost or fitness function. An example for such a function is the aforementioned IoC, which comes close to a value indicating natural language when the key comes closer to the original one. A common and very successfully used search metaheuristic is hill climbing. A hill climbing algorithm first randomly guesses a putative "start key". Then, it rates its cost value using a cost function. After that, it tries to "improve" the key by randomly changing elements of the key. With the Vigenère cipher for example, it would change the first letter of the keyword. After changing the letter, it again computes the cost function. If the result is higher than for the previous key, the new key is accepted. Otherwise, the new key is discarded and another modified one is tested. The algorithm performs these steps until no new modified key can be found that yields a higher cost value, i.e. the hill (= local maximum) of the fitness score is reached. Most of our classical cryptanalytic implementations in CT2 are based on such a hill climbing approach.

3 An Introduction to CrypTool 2

CrypTool 2 (CT2) is an open-source tool for e-learning cryptology. The CrypTool community aims to integrate into CT2 the best known and most powerful algorithms to automatically break (classical and modern) ciphers. Additionally, our goal is to make CT2 a tool that can be used by everyone who needs to break a classical cipher. Another well-known Windows analyzer for classical

ciphers is CryptoCrack (Pilcrow, 2018).

CT2 consists of a set of six main components: the Startcenter, the Wizard, the WorkspaceManager, the Online Help, the templates, and the CrypCloud, which we present in detail in the following.

The **Startcenter** is the first screen appearing when CT2 starts. From here, a user can come to every other component by just clicking an icon.

The **Wizard** is intended for CT2 users that are not yet very familiar with the topics cryptography or cryptanalysis. The user just selects step by step what he wants to do. The wizard displays at each step a small set of choices for the user.

The **WorkspaceManager** is the heart of CT2 since it enables the user to create arbitrary cascades of ciphers and cryptanalysis methods using graphical icons (components) that can be connected. To create a cascade, the user may drag&drop components (ciphers, analysis methods, and tools) onto the so-called workspace. After that, he has to connect the components using the connectors of each component. This can be done by dragging connection lines between the inputs (small triangles) and outputs (also small triangles) using the mouse. Data in CT2 can be of different types, e.g. text, numbers, binary data. The type of data is indicated by a unique color. A simple rule is, that connections between the same colors are always possible. Connections between different colors (data types) may also be possible, but then data has to be converted. CT2 can do this automatically in many cases, but sometimes special data converters are needed.

Figure 1 shows a sample workspace containing a so-called *Caesar cipher* (very simple monoalphabetic substitution) component, a *TextInput* component enabling the user to enter text, and a *TextOutput* component displaying the final encrypted text. The connectors are the small colored triangles. The connections are the lines between the triangles. The color of the connectors and connections indicate the data types (here text). When the user wants to execute the flow, he has to start it by hitting the *Play* button in the top menu of CT2. Currently, CT2 contains more than 160 different components for encryption, decryption, cryptanalysis, etc. Many components that can be put onto the workspace have a special visualization that can be viewed when opening the component by double clicking on it. Figure 2 shows such a maximized visualization of a standard component.

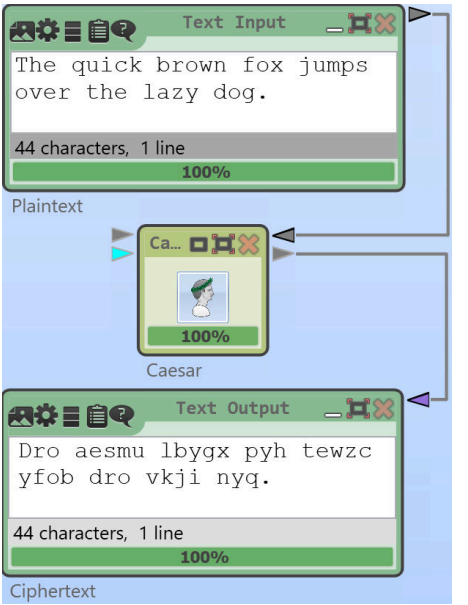


Figure 1: CT2 Workspace with Caesar Cipher

CT2 contains a huge **Online Help** describing each component. By pressing F1 on a selected component of the WorkspaceManager, CT2 automatically opens the online help of the corresponding component.

CT2 also contains a huge set of more than 200 so-called **Templates**. A template shows how to create a specific cipher or a cryptanalytic scenario using the graphical programming language and is ready to use. The Startcenter contains a search field that enables the user to search for specific templates using keywords.

Finally, the **CrypCloud** (Kopal, 2018) is a cloud framework built in CT2. We developed it as a real-world prototype for evaluating distribution algorithms for distributed cryptanalysis using a multitude of computers.

4 A Step-by-Step Approach for Analyzing Classical Ciphers in CrypTool 2

In this section, we show a step-by-step approach for analyzing classical ciphers in CT2. The first step is to make the cipher processable for CT2, so we create a digital transcription of the ciphertext. Then, we identify the type of the cipher. The third

step then finally breaks the cipher with CT2.

4.1 Create a Transcription

There are two ways to create a transcription of a ciphertext for CT2. The first method is to manually assign to each ciphertext symbol a letter by hand outside of CT2, e.g. with Windows Notepad. The transcription is saved as a simple text file. This file can be loaded into CT2 by using the *FileInput* component and then be processed further.

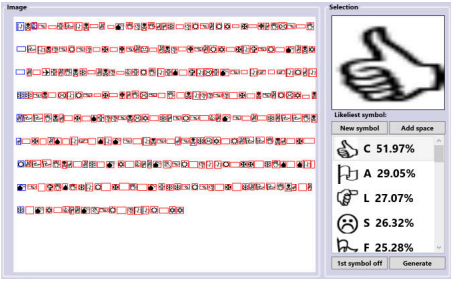


Figure 2: CT2 Transcriptor Component with Marked Symbols for Transcription

The second method to create a transcription uses the CT2 component *Transcriptor* (Figure 2). With the transcriptor, a user can load a picture, e.g. a scan of a document. Then, he can assign letters to the scanned symbols by marking them. Finally, the transcriptor is able to output the complete transcription. It supports the user in two different ways: (1) It automatically guesses, which symbol the user just had marked by showing the most likely symbols and (2) it can be set to semi-automatic mode. In semi-automatic mode, it automatically marks all other symbols that are similar to the one just marked by the user.

The DECODE project (Megyesi et al., 2017) already hosts a huge set of transcriptions of encrypted historical books done by experts. Within 2018 there will be an interface to call either CT2 from the DECODE website or to download DECODE records from within CT2.

4.2 Identify the Cipher

After creating the transcription of the cipher it is now possible to analyze its characteristics. A first analysis would be to create a text frequency analysis. For that, CT2 contains a *Frequency Test* component. It can be configured to show unigram distribution, bigram distribution, etc.

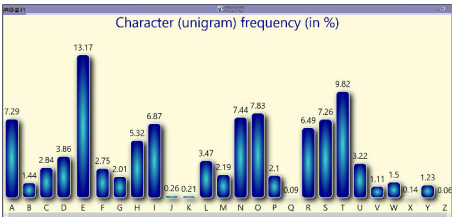


Figure 3: Frequency Test Component Showing Distribution of Plaintext

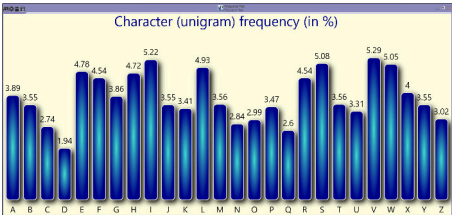


Figure 4: Frequency Test Component Showing Distribution of Ciphertext

In Figure 3 we show the distribution of a plaintext ("The Declaration of Independence" of the US). It can easily be seen, that the text follows the letter distribution of the English language, i.e. the 'E' is the most frequent letter, the letters 'X', 'Q', and 'Z' are very rare. In Figure 4 we show the distribution of a ciphertext ("The Declaration of Independence" of the US, encrypted with a Vigenère cipher). Here, all letters are more or less equally distributed, showing the cryptanalyst that it is possibly a polyalphabetic substitution cipher.

Another component that helps to analyze and identify a cipher is the *Friedman Test*, invented by William Friedman. With this test the key length (number of letters of a key word or phrase) of a polyalphabetic cipher can be calculated.

In Figure 5 we show the result of the Friedman test performed on plaintext ("The Declaration of Independence" of the US). It shows that the given text is possibly plaintext or a monoalphabetic substitution. Furthermore, the ciphertext could be transposed since the transposition does not change the letter distribution. In Figure 6 we show the result of the Friedman test performed on ciphertext ("The Declaration of Independence" of the US, encrypted with a Vigenère cipher). It shows that the given text is possibly ciphertext and polyalphabetic. Additionally, it shows that the estimated

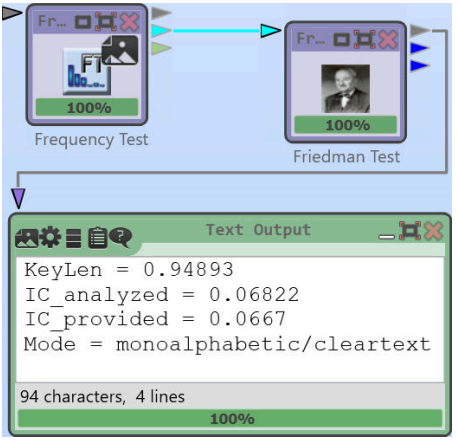


Figure 5: Friedman Test Component Showing Result of English Plaintext

key length is about 9. The component needs a provided IC (*IC_provided*) which is used as a reference value for the analyzed IC (*IC_analyzed*).

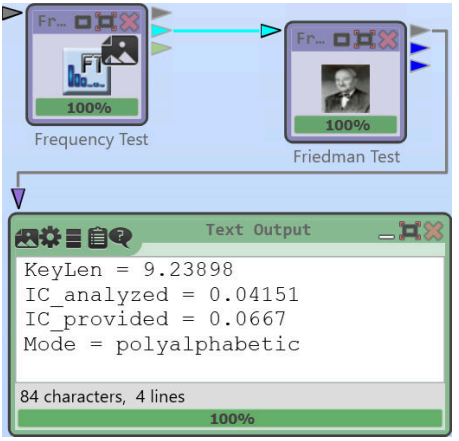


Figure 6: Friedman Test Component Showing Result of Ciphertext

4.3 Break the Cipher

After identifying the cipher type it can now be broken with the help of different cryptanalysis components. CT2 contains components for the automatic breaking of the monoalphabetic substitution cipher, the Vigenère cipher, and the columnar transposition cipher.

In Figure 7 we show the *Vigenère Analyzer* component which automatically solved a Vigenère cipher ("The Declaration of Independence" of the US, encrypted with a Vigenère cipher. The solver automatically tested every keylength between 5 and 20 using hill climbing. Only about ten seconds are needed for the component to automatically break the cipher. The decrypted text is automatically outputted by the component and can be displayed by an *TextOutput* component.

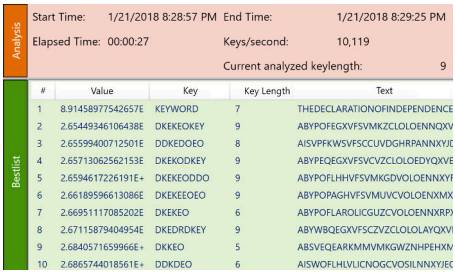


Figure 7: Vigenère Analyzer Solving a Cipher

All automatic cryptanalysis components have the same style of user interface. Besides start and end-time, the elapsed time for the analysis is shown. Furthermore, some components estimate the time for the remaining automatic analysis.

5 Example Cryptanalysis of Original Classical Ciphers

In this section we present two different real-world classical ciphers that can be broken with CT2.

5.1 Message in a Bottle Sent to General Pemberton in the US Civil War

The following message was sent in a bottle by a Confederate commander at the 4th of July 1863 in Vicksburg to General Pemberton. It was broken by the retired CIA codebreaker David Gaddy in 2010 (Daily Mail Reporter, 2010). We here use this message (221 letters) as our first real-world example for breaking classical ciphers with CT2.

In the first step, to automatically analyze the ciphertext, we had to create a transcription as shown in Section 4.1. We could have used the *Transcriptor* component or do it manually. Since the letters are written differently, the scanned image has only a low resolution, and the message contains ink spots, we did it manually. We show the result of the transcription of the ciphertext in Figure 9.

Now, we could analyze the text to identify the

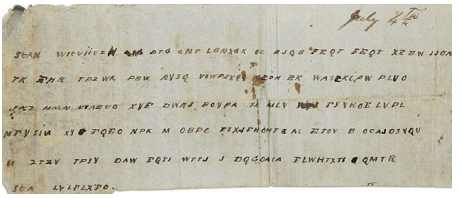


Figure 8: Encrypted Message in a Bottle Sent by General Johnston

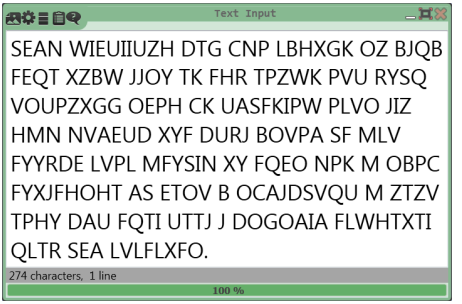


Figure 9: Transcription of Encrypted Message in a Bottle

type of the cipher. First, we created a letter frequency analysis (see Figure 10).

The distribution of letters indicated that the message is not encrypted with monoalphabetic substitution and possibly not transposed. Based on the more or less equal distribution of the letters we assume that the message is encrypted with a polyalphabetic cipher. To further strengthen our assumption, we applied the Friedman test and calculated the IC. In Figure 11 we show the results of the computation of the IC and the Friedman test.

The IC equal to 0.03834 indicated that the message is possibly encrypted with a polyalphabetic cipher. The estimated length of the key by the Friedman analysis is ≈ 5730, which is impossible for a text of only 221 letters. Thus, the message is either encrypted with a running key cipher, meaning the key length is infinity, or the Friedman test just fails because of the short length of the message. Since we know that in the Civil War the Vigenère cipher was often used, we assumed it could be encrypted with the Vigenère cipher. Other possibilities would be a codebook or a homophone cipher.

In the last step, we try to break the cipher. Since we assume it to be a Vigenère cipher, we used the *Vigenère Analyzer* component to break it.

We automatically test all key lengths between 1 and 20. Figure 12 shows the final result of the Vigenère Analyzer component. The component displays a toplist of "best" decryptions based on a cost function that rates the quality of the decrypted texts. The higher the cost value (sum of n-gram probabilities of English language) the higher the place in the toplist. Furthermore, the component shows the used keyword or pass phrase. With "MANCHESTERBLUFF" (15 letters), the message can be broken. The analysis run took 5 seconds on a standard desktop computer with 2.4 GHz. We present the final plaintext in Figure 13.

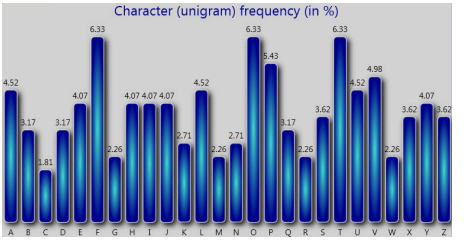


Figure 10: Letter Frequency Analysis of Encrypted Message in a Bottle

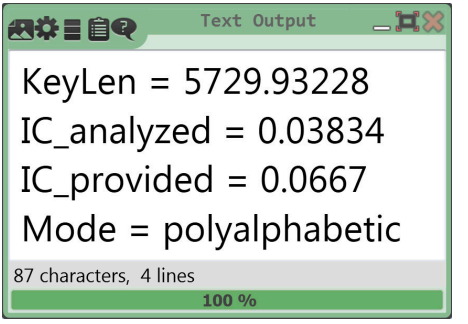


Figure 11: Friedman Test and IC of Encrypted Message in a Bottle

5.2 Borg Cipher – Encrypted Book from the 17th Century

The Borg cipher is a 408 pages manuscript, probably from the 17th century. The manuscript is located at the *Biblioteca Apostolica Vaticana* (Aldarrab et al., 2018). It is written using special ciphertext symbols. Figure 14 shows a small part of the Borg cipher. We here use the book as our

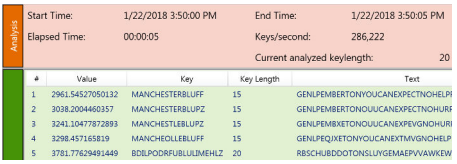


Figure 12: Breaking the Encrypted Message in a Bottle with the Vigenère Analyzer

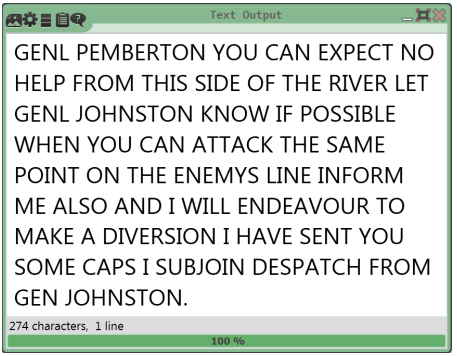


Figure 13: Message in a Bottle – Revealed Plaintext by Vigenère Analyzer

second real-world example for breaking classical ciphers with CT2. The cipher was already broken by (Aldarrab et al., 2018).

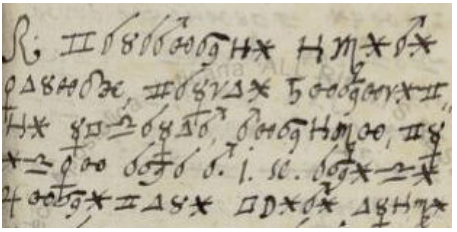


Figure 14: Picture Taken from the Borg Cipher

We took the complete transcription of the book from (Aldarrab et al., 2018).

First, we performed a frequency analysis of the text shown in Figure 15.

Then, we applied the Friedman test on the ciphertext and computed the IC (see the result in Figure 16). Both indicated, that the Borg cipher is encrypted using the monoalphabetic substitution.

Thus, we finally used the *Monoalphabetic Substitution Analyzer* component of CT2 to break the cipher, see Figure 17. We tested different languages to be used by the analyzer. Latin produced the best results, since the original text is Latin. The analysis run took 8 seconds.

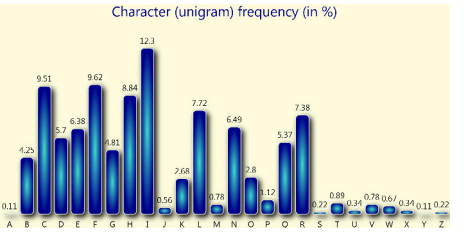


Figure 15: Letter Frequency Analysis of the Borg Cipher

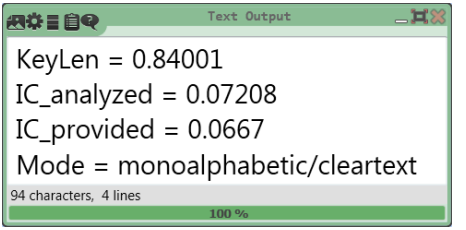


Figure 16: Friedman Test of the Borg Cipher

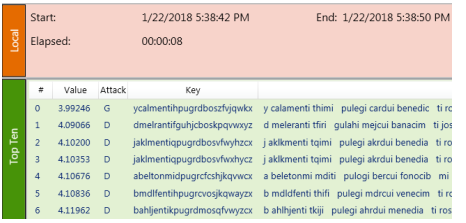


Figure 17: Breaking the Borg Cipher with the Monoalphabetic Substitution Analyzer

We present the first part of the finally decrypted Borg cipher in Figure 18.

6 Current Cryptanalysis Components in CrypTool 2 and Open Tasks

CT2 contains a set of different components for the automated cryptanalysis of classical ciphers. In Table 1 we show an overview of already implemented components for the cryptanalysis of classical ciphers. Green marked entries refer to components which we already implemented. Yellow marked entries refer to components that are not implemented yet. The monoalphabetic substitu-

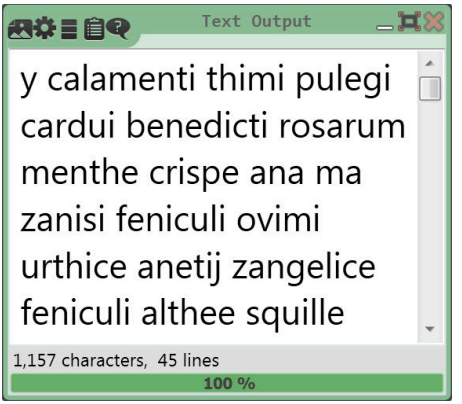


Figure 18: Borg Cipher – Revealed Plaintext by Monoalphabetic Substitution Analyzer

tion, the columnar transposition, the Vigenère cipher, and the Enigma machine are already breakable using CT2. We plan to implement homophone cipher analysis, codebook cipher analysis, grille analysis (a special transposition cipher), Playfair (a special substitution), strip and cylinder cipher analyzers, ADFGVX analyzer, analyzers for the Hagelin Machine (Lasry et al., 2016a) (Lasry et al., 2016b) (e.g. the M209 cipher machine), and a Hill cipher analyzer.

The currently implemented analysis tools, like frequency analysis, transcriptor, or Friedman test, were shown and used in Section 5. For the future, we also plan to implement a "Cipher Detector" component which is able to automatically detect the used type of cipher (with a high probability).

7 Conclusion

In this paper, we gave a brief introduction in the e-learning program CrypTool 2 (CT2) and how it can be used to automatically cryptanalyze classical ciphers. First, we gave an introduction to classical ciphers as well as to their cryptanalysis. Then, we shortly presented CT2 and its usage. After that, we showed an approach consisting of three steps (transcription, identification, and analyzing) for breaking classical ciphers using CT2. We showed two classical real-world ciphers ("Message in a Bottle Sent to General Pemberton in the US Civil War" and "Borg Cipher – Encrypted Book from the 17th Century") and described step-by-step how we broke them with components already implemented in CT2. Then,

Cipher	Component
Mono. Substitution	Mono. Subst. Analyzer
Homophone Subst.	Homophone Analyzer
Colum. Transposition	Transp. Analyzer
Codebook	Codebook Analyzer
Vigenère	Vigenère Analyzer
Grille	Grille Analyzer
Playfair	Playfair Analyzer
Enigma Machine	Enigma Analyzer
Strip/Cylinder Ciphers	Strip/Cylinder Analyzer
ADFGVX	ADFGVX Analyzer
Hagelin Machines	Hagelin Analyzer
Hill Cipher	Hill Cipher Analyzer
Analysis Tools	**Component**
Transcription	Transcriptor
Friedman Test	Friedman Test
Kasiski Test	Kasiski Test
Text Freq. Analysis	Text Freq. Analysis
Index of Coincedence	Cost Function
Autocorrelation	Autocorrelation
Cipher Detector	Cipher Detector

Table 1: Cryptanalysis Components for Classical Ciphers in CT2 – Overview

we gave an overview of methods for the automatic cryptanalysis already implemented in CT2 as well as an overview of cryptanalytic components that we plan to implement.

CT2 is a project that now runs for nearly 10 years. Within this time, we extended CT2 with state-of-the-art methods for the cryptanalysis for classical as well as for modern ciphers. CT2 contains possibilities to cryptanalyze ciphers by connecting different CT2 instances over the Internet (*CrypCloud*). In the future, we plan to extend CT2 in such a way that it becomes easier and more user-friendly, thus, non-computer scientists can more easily use it for breaking their classical ciphers. There are still a lot of open tasks besides the implementation of cryptanalytic methods. We plan to extend the existing components by a huge set of different languages (e.g. Latin, Greek, Hebrew, etc). Since many of the historical encrypted books are written in these languages, historians and cryptanalysts will benefit by the newly added languages. Furthermore, we will extend existing cryptanalytic components to be more robust and more general with respect to the used alpha-

bets. Currently, the monoalphabetic substitution analyzer needs (for the transcription) a specific input alphabet consisting of Latin letters. Till end of 2018 all kind of symbols a computer can process will be possible (e.g. a support of UTF-8 characters). Furthermore, new kinds of classical ciphers and cryptanalytic methods will be added. Examples are grilles and codebooks, which were extensively used in history.

The CT2 team highly welcomes suggestions, wishes, and ideas of historians, cryptanalysts, and everybody else for additional ciphers and automated cryptanalysis methods which should be included in CT2 in the future. The list shown in Table 1 is open for new entries proposed by everyone. Since CT2 is open-source software, we welcome everyone in contributing to the CT2 project (programmers, testers, etc). Finally, everyone interested in CT2 may download the software for free from https://www.cryptool.org/.

References

Nada Aldarrab, Kevin Knight, and Beata Megyesi. 2018. The Borg.lat.898 Cipher. `http://stp.lingfil.uu.se/~bea/borg/`.

Michael J Cowan. 2008. Breaking short playfair ciphers with the simulated annealing algorithm. *Cryptologia*, 32(1):71–83.

Daily Mail Reporter. 2010. CIA codebreaker reveals 147-year-old Civil War message about the Confederate army's desperation. `https://dailym.ai/2JkVFCu`.

Amrapali Dhavare, Richard M Low, and Mark Stamp. 2013. Efficient cryptanalysis of homophonic substitution ciphers. *Cryptologia*, 37(3):250–281.

William S Forsyth and Reihaneh Safavi-Naini. 1993. Automated cryptanalysis of substitution ciphers. *Cryptologia*, 17(4):407–418.

William Frederick Friedman. 1987. *The index of coincidence and its applications in cryptanalysis*. Aegean Park Press California.

James J Gillogly. 1995. Ciphertext-Only Cryptanalysis of Enigma. *Cryptologia*, 19(4):405–413.

Nils Kopal, Olga Kieselmann, Arno Wacker, and Bernhard Esslinger. 2014. CrypTool 2.0. *Datenschutz und Datensicherheit-DuD*, 38(10):701–708.

Nils Kopal. 2018. Secure Volunteer Computing for Distributed Cryptanalysis. `http://www.upress.uni-kassel.de/katalog/abstract.php?978-3-7376-0426-0`.

George Lasry, Nils Kopal, and Arno Wacker. 2016a. Automated Known-Plaintext Cryptanalysis of Short Hagelin M-209 Messages. *Cryptologia*, 40(1):49–69.

George Lasry, Nils Kopal, and Arno Wacker. 2016b. Ciphertext-only cryptanalysis of Hagelin M-209 pins and lugs. *Cryptologia*, 40(2):141–176.

George Lasry, Nils Kopal, and Arno Wacker. 2016c. Cryptanalysis of columnar transposition cipher with long keys. *Cryptologia*, 40(4):374–398.

George Lasry, Ingo Niebel, Nils Kopal, and Arno Wacker. 2017. Deciphering ADFGVX messages from the Eastern Front of World War I. *Cryptologia*, 41(2):101–136.

George Lasry. 2018. *A Methodology for the Cryptanalysis of Classical Ciphers with Search Metaheuristics*. kassel university press GmbH.

Thomas G Mahon and James Gillogly. 2008. *Decoding the IRA*. Mercier Press Ltd.

Beata Megyesi, Kevin Knight, and Nada Aldarrab. 2017. DECODE – Automatic Decryption of Historical Manuscripts. `http://stp.lingfil.uu.se/~bea/decode/`.

Phil Pilcrow. 2018. CryptoCrack. `http://www.cryptoprograms.com/`.

Tobias Schrödel. 2008. Breaking Short Vigenere Ciphers. *Cryptologia*, 32(4):334–347.

Hidden Markov Models for Vigenère Cryptanalysis

Mark Stamp* **Fabio Di Troia†**
Department of Computer Science
San Jose State University
San Jose, California
*mark.stamp@sjsu.edu
†fabioditroia@msn.com

Miles Stamp
Los Gatos High School
Los Gatos, California
milez000782@gmail.com

Jasper Huang
Lynbrook High School
San Jose, California
jhuang821@student.fuhsd.org

Abstract

Previous work has shown that hidden Markov models (HMM) can be effective for the cryptanalysis of simple substitution and homophonic substitution ciphers. Although computationally expensive, an HMM-based attack that employs multiple random restarts can offer a significant improvement over classic cryptanalysis techniques, in the sense of requiring less ciphertext to recover the key. In this paper, we show that HMMs are also applicable to the cryptanalysis of the well-known Vigenère cipher. We compare and contrast our HMM-based approach to recent research that uses Vigenère cryptanalysis to supposedly illustrate the strength of a type of neural network known as a generative adversarial network (GAN). In the context of Vigenère cryptanalysis, we show that an HMM can succeed with much less ciphertext than a GAN, and we argue that the model generated by an HMM is considerably more informative than that produced by a GAN.

1 Introduction

Hidden Markov models (HMMs) are a class of machine learning techniques that have proved useful in a wide variety of applications, ranging from speech analysis (Rabiner, 1989) to malware detection (Wong and Stamp, 2006). In the realm of classic ciphers, HMMs have been shown to perform well in the cryptanalysis of monoalphabetic substitution ciphers (Berg-Kirkpatrick and Klein, 2013; Lee, 2002; Vobbilisetty et al., 2017).

In this paper, we build on the work in (Vobbilisetty et al., 2017) to show that an HMM is a powerful and practical tool for the cryptanalysis of a Vigenère cipher. Furthermore, we show that an HMM trained on Vigenère ciphertext is informative, in the sense that the model enables us to clearly see which features contribute to the success of the technique. We compare our results to recent work in (Gomez et al., 2018), where a neural network is used to break Vigenère ciphertext messages.

The remainder of this paper is organized as follows. In Section 2, we discuss relevant background topics, with the emphasis on hidden Markov models. Experimental results obtain by applying HMMs to Vigenère ciphertexts are given in Section 3. Finally, in Section 4 we give our conclusions and briefly consider future work.

2 Background

2.1 Vigenère Cipher

A simple substitution cipher uses a fixed one-to-one mapping of the alphabet. It is a standard textbook exercise to break a simple substitution using frequency analysis. A homophonic substitution can be viewed as a generalization of a simple substitution, where a fixed many-to-one mapping is used. That is, in a homophonic substitution, more than one ciphertext symbol can map to a single plaintext letter. In contrast, for a polyalphabetic substitution, the "alphabet" (i.e., the mapping between plaintext and ciphertext) changes. As compared to a simple substitution, a homophonic substitution tends to flatten the ciphertext statistics, thereby making frequency analysis more difficult.

A Vigenère cipher is a simple polyalphabetic scheme, where a keyword is specified, and each letter of the keyword represents a shift of the alphabet. For example, suppose that the keyword is `CAT` and we want to encrypt `attackatdawn`. Then we have

keyword:	`CATCATCATCAT`
plaintext:	`attackatdawn`
ciphertext:	`ctmccdctwcwg`

Proceedings of the 1st Conference on Historical Cryptology, pages 39– 46,
Uppsala, Sweden, 18-20 June, 2018

Letter	a	b	c	d	e	f	g	h	i	j	k	l	m
Frequency	.082	.015	.028	.043	.127	.022	.020	.061	.070	.002	.008	.040	.024
Letter	n	o	p	q	r	s	t	u	v	w	x	y	z
Frequency	.067	.075	.019	.001	.060	.063	.091	.028	.010	.023	.001	.020	.001

Table 1: English monograph statistics

That is, each C in the keyword specifies a shift by 3, each A represents a shift by 0, and each T is a shift by 19, and the keyword is repeated as many times as needed. Of course, if the keyword is known, it is trivial to decrypt a Vigenère ciphertext.

2.2 Friedman Test

When attempting to break a Vigenère ciphertext, the first step is to determine the length of the keyword. The Friedman test (Friedman, 1987), which is based on the index of coincidence (IC), is a well-known method for determining the length of the keyword, provided that sufficient ciphertext is available. An alternative method of finding the keyword length is the Kasiski test (Kasiski, 1863); here we focus on the Friedman test. In any case, once the keyword is known, the Vigenère cipher consists of a sequence of shift ciphers, and the shifts can be determined by a variety of means.

The IC measures the "repeat rate," i.e., the probability that two randomly selected letters from a given string are identical. This test relies on the non-uniformity of letter frequencies in the underlying plaintext.

Suppose that we have a string of text of length N with $n_a > 0$ occurrences of A and $n_b > 0$ occurrences of B, and so on. If we randomly select two letters (without replacement) from this string, the probability that the letters match is given by

$$\frac{n_a(n_a-1)}{N(N-1)} + \frac{n_b(n_b-1)}{N(N-1)} + \cdots + \frac{n_z(n_z-1)}{N(N-1)}$$

In general, the repeat rate, or IC, which we denote as κ, is given by

$$\kappa = \frac{1}{N(N-1)} \sum_{i=0}^{c-1} n_i(n_i-1) \tag{1}$$

where c is the size of the alphabet, n_i is the frequency of the i^{th} symbol, and N is the length of the string. For English text (without spaces, punctuation, or case), we have $c = 26$, and the the expected frequency of each n_i is known from the language monograph statistics. The monograph statistics for standard English appear in Table 1.

Let κ_e denote the IC for English text. If we compute the IC for a large selection of English text, then based on Table 1, we would expect to find

$$\kappa_e = 0.082^2 + 0.015^2 + 0.028^2 + \cdots + 0.020^2 + 0.001^2 \approx 0.0656.$$

On the other hand, if we have random text drawn from the 26 letter English alphabet, we would expect to find that the IC is

$$\kappa_r = (1/26)^2 + (1/26)^2 + \cdots + (1/26)^2 \approx 0.0385.$$

For a simple substitution cipher, we relabel the letters, which has no effect on the IC. That is, when a monoalphabetic substitution is applied to English plaintext, the IC of the ciphertext is the same as that of the plaintext. Friedman noted that for a polyalphabetic substitution, the larger the number of alphabets, the closer the IC is to κ_r. Hence, for a polyalphabetic substitution, we can use the observed IC to estimate the number of alphabets and, in particular, the length of the keyword in a Vigenère cipher.

Let L be the length of the Vigenère keyword, and assume that the ciphertext is of length N. Then we have L Caesar's ciphers. To simplify the notation, we assume that each of these L ciphers has exactly N/L letters. Under this assumption, the probability of selecting two letters from the same Caesar's cipher is given by

$$\frac{N(N/L-1)}{N(N-1)} = \frac{N/L-1}{N-1}.$$

Similarly, the probability of selecting two letters from different alphabets is

$$\frac{N-N/L}{N-1}.$$

In the former case, the letters are derived from the same simple substitution (in fact, Caesar's cipher), so the chance that they match is κ_e, while in the

latter case, the letters are from different Caesar's ciphers, so the chance that they match is about κ_r.

Let κ_c be the computed IC for a given Vigenère ciphertext. Then κ_c is the probability of selecting two letters at random that match and, evidently, this probability is given by

$$\kappa_c = \kappa_e \frac{N/L-1}{N-1} + \kappa_r \frac{N-N/L}{N-1}. \tag{2}$$

Solving equation (2) for L, we obtain

$$L = \frac{N(\kappa_e - \kappa_r)}{N(\kappa_c - \kappa_r) - (\kappa_e - \kappa_r)}.$$

Since N is large relative to κ_e, κ_r, and κ_c, we can approximate the keyword length by

$$L = \frac{\kappa_e - \kappa_r}{\kappa_c - \kappa_r} \tag{3}$$

For the case of English text, the expected IC is $\kappa_e \approx 0.0656$, while for the random case (and under the assumption that we have 26 symbols), the IC is $\kappa_r \approx 0.0385$. Recall that κ_c is the IC for the ciphertext, which is computed as in (1). Thus, we can approximate the Vigenère keyword length using (3). In practice, when attempting to break a Vigenère ciphertext message, we would need to test various keyword lengths near the value given by (3).

In Section 3, we compare an HMM-based technique to the results obtained using the standard approach to Vigenère cryptanalysis, as discussed in this section. For our test cases, we find that the HMM outperforms the Friedman test, in the sense of giving us a more precise result for the keyword length. In addition, the HMM simultaneously recovers the shifts, so that the entire Vigenère key is determined.

2.3 Hidden Markov Models

True to its name, a hidden Markov model (HMM) includes a Markov process that is "hidden," in the sense that it is not directly observable. Along with this hidden Markov process, an HMM includes a sequence of observations that are probabilistically related to the (hidden) states. An HMM can be viewed as a machine learning technique that relies on a discrete hill climb algorithm for training.

A generic HMM is illustrated in Figure 1, where A is an $N \times N$ matrix that defines the state transitions in the underlying (hidden) Markov process, and the matrix B contains discrete probability distributions that relate each hidden state X_i to the corresponding observation O_i. That is, row i of the B matrix contains a discrete probability distribution that gives the probabilities of the various observation symbols when the hidden Markov process is in state i. As we show below, the component matrices of an HMM can reveal information about the underlying data that is not otherwise readily apparent to a human analyst. This could be considered an advantage of an HMM over other more opaque forms of machine learning, such as neural networks.

The following notation (Stamp, 2004) is commonly used for HMMs:

$$\begin{array}{rcl} T & = & \text{length of the observation sequence} \\ N & = & \text{number of states in the model} \\ M & = & \text{number of observation symbols} \\ Q & = & \{q_0, q_1, \ldots, q_{N-1}\} \\ & = & \text{distinct states of the Markov process} \\ V & = & \{0, 1, \ldots, M-1\} \\ & = & \text{set of possible observations} \\ A & = & \text{state transition probabilities} \\ B & = & \text{observation probability matrix} \\ \pi & = & \text{initial state distribution} \\ O & = & (O_0, O_1, \ldots, O_{T-1}) \\ & = & \text{observation sequence.} \end{array}$$

Note that the observations are associated with the integers $0, 1, \ldots, M-1$, since this simplifies the notation with no loss of generality. Consequently, we have $O_i \in V$ for $i = 0, 1, \ldots, T-1$.

If we are given a sequence of observations of length T, denoted $(O_1, O_2, \ldots, O_T)$, we can train an HMM, that is, we can determine matrices A and B in Figure 1 that maximize the probability of this training sequence. The HMM training process can be viewed as a discrete hill climb on the high dimensional parameter space of the matrices A and B, and an initial state distribution matrix that is denoted as π. Once we have trained an HMM, we can use the resulting model, denoted $\lambda = (A, B, \pi)$, to compute a score for a given observation sequence—the higher the score, the more closely the scored sequence matches the training sequence.

The HMM matrix A is $N \times N$, while B is $N \times M$ and π is $1 \times N$. Here, N is the number of hidden states and M is the number of distinct observation symbols. All three of these matrices are row stochastic, that is, each row satisfies the conditions of a discrete probability distribution. To train an HMM, we specify N, the number of hidden states,

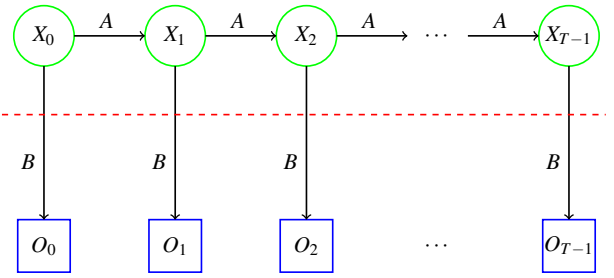


Figure 1: Hidden Markov model

while M, the number of distinct observation symbols, is determined from the data.

Typically, the matrices that define the HMM, i.e., $\lambda = (A, B, \pi)$, are initialized so that they are approximately uniform. That is, each element of A and π is initialized to approximately $1/N$, while each element of B is initialized to approximately $1/M$. In addition, each row is subject to the row stochastic condition. Also, we cannot use an exact uniform initialization as this represents a peak in the hill climb from which the model is unable to climb.

On the other hand, if we know something specific about the problem, we can sometimes use this knowledge when initializing the matrices, which can serve to speed convergence and reduce the data requirements. For example, in (Vobbilisetty et al., 2017) it is shown that an HMM can be used to recover the key in a simple substitution ciphertext, where the underlying language is English. In this case, the A matrix corresponds to English language digraph statistics, and hence we can initialize the A matrix based on such statistics, and there is no need to re-estimate A when training the model.

An HMM is a machine learning technique in the sense that very little is required of the human analyst. Specifically, we need to specify the number of hidden states N, but all other initial parameters are derived from the data, or can be generated at random. During training, we rely entirely on the "machine" (specifically, the HMM training algorithm) to generate the model. Surprisingly often, the HMM training algorithm succeeds in automatically extracting relevant and useful information from the data.

For additional information on HMMs, the standard reference is (Rabiner, 1989). The notation and description here closely follows that in the tutorial (Stamp, 2004).

In a classic illustration of the strengths of the HMM technique, (Cave and Neuwirth, 1980) show that HMMs can be successfully applied to English text analysis. In (Stamp, 2004), the specific English text example in Table 2 is given. In this case, the observations consist of the 26 letters and word space, for a total of $M = 27$ symbols, and the analyst chose to use $N = 2$ hidden states. The B matrix is initialized so that each element is approximately $1/27$, subject to the row stochastic condition—the precise initial values used in this example are given in first 2 columns in Table 2. After training the HMM using 50,000 observations, the resulting transpose of the B matrix is given in the final 2 columns of Table 2.

From the example in Table 2, we see that when the Markov process is in (hidden) state 1, the probability that the observed symbol is `a` is 0.13845, the probability that the observed symbol is `b` is 0.00000, the the probability that the observed symbol is `c` is 0.00062, the the probability that the observed symbol is `d` is 0.00000, the probability that the observed symbol is `e` is 0.21404, and so on. On the other hand, if the model is in (hidden) state 2, then the probability that the observed symbol is `a` is 0.00075, the probability that the observed symbol is `b` is 0.02311, the probability that the observed symbol is `c` is 0.05614, the probability that the observed symbol is `d` is 0.06937, the probability that the observed symbol is `e` is 0.00000, and so on. In this case, we can clearly see that the 2 hidden states correspond to consonants and vowels. Since no a priori assumption was made about the letters, this simple example nicely illustrates the "machine learning" aspect of an HMM.

	Initial		Final	
a	0.03735	0.03909	0.13845	0.00075
b	0.03408	0.03537	0.00000	0.02311
c	0.03455	0.03537	0.00062	0.05614
d	0.03828	0.03909	0.00000	0.06937
e	0.03782	0.03583	0.21404	0.00000
f	0.03922	0.03630	0.00000	0.03559
g	0.03688	0.04048	0.00081	0.02724
h	0.03408	0.03537	0.00066	0.07278
i	0.03875	0.03816	0.12275	0.00000
j	0.04062	0.03909	0.00000	0.00365
k	0.03735	0.03490	0.00182	0.00703
l	0.03968	0.03723	0.00049	0.07231
m	0.03548	0.03537	0.00000	0.03889
n	0.03735	0.03909	0.00000	0.11461
o	0.04062	0.03397	0.13156	0.00000
p	0.03595	0.03397	0.00040	0.03674
q	0.03641	0.03816	0.00000	0.00153
r	0.03408	0.03676	0.00000	0.10225
s	0.04062	0.04048	0.00000	0.11042
t	0.03548	0.03443	0.01102	0.14392
u	0.03922	0.03537	0.04508	0.00000
v	0.04062	0.03955	0.00000	0.01621
w	0.03455	0.03816	0.00000	0.02303
x	0.03595	0.03723	0.00000	0.00447
y	0.03408	0.03769	0.00019	0.02587
z	0.03408	0.03955	0.00000	0.00110
space	0.03688	0.03397	0.33211	0.01298
sum	1.00000	1.00000	1.00000	1.00000

Table 2: Initial and final B^T for English plaintext

For the example in Table 2, the converged A matrix as given in (Stamp, 2004) is

$$A = \begin{pmatrix} 0.25596 & 0.74404 \\ 0.71571 & 0.28429 \end{pmatrix}$$

This A matrix tells us that when the Markov process is in (hidden) state 1, the probability that it transitions to state 1 is 0.25596, while the probability that it transitions to state 2 is 0.74404. Similarly, if the Markov process is in state 2, it next transitions to state 1 with probability 0.71571, and it stays in state 2 with probability 0.28429. In this case, the A matrix is not particularly interesting, as this matrix simply gives the probability of transitioning from a consonant to a vowel, a vowel to a consonant, and so on.

As mentioned above, an HMM also includes an initial state distribution denoted as π, which for the example above converges (Stamp, 2004) to

$$\pi = \begin{pmatrix} 0.00000 & 1.00000 \end{pmatrix}$$

This tells us that the model started in the second hidden state which, according to the converged B matrix, corresponds to the vowel state. Again, this is not particularly enlightening. For this English text example, we see that the B matrix contains the interesting information.

Again, an HMM is defined by the 3 matrices, A, B and π, and it is standard practice to denote an HMM as $\lambda = (A, B, \pi)$. We also want to emphasize that each of these matrices is row stochastic, with each row representing a discrete probability distribution.

Now, suppose that we train an HMM with 2 hidden states on simple substitution ciphertext, where the plaintext is English. The resulting model will partition the ciphertext letters into those corresponding to consonants and vowels. On the other hand, if we set the number of hidden states N to equal the number of symbols (i.e., either $N = 26$ or $N = 27$, depending on whether we include word spaces), the simple substitution key can be easily determined from a converged B matrix of an HMM (Vobbilisetty et al., 2017). Furthermore, in this latter case, the A matrix contains digraph probabilities of the English plaintext.

An analogous HMM-based attack applies to homophonic substitution ciphers. However, in the homophonic substitution case, the key recovery from the B matrix is slightly more complex as the number of symbols mapping to each plaintext letter is typically unknown (Vobbilisetty et al., 2017).

For these HMM-based cryptanalytic models to converge, we generally require large amounts of ciphertext, making such attacks impractical for most classic cryptanalysis problems. However, since HMM training is a hill climb technique, random restarts can be used in an attempt to generate an improved solution. It is shown in (Berg-Kirkpatrick and Klein, 2013), and from a slightly different perspective in (Vobbilisetty et al., 2017), that by using large numbers of random restarts, the performance of HMM-based attacks can surpass other techniques, in the sense of requiring less ciphertext. For example, it is shown in (Vobbilisetty et al., 2017) that HMMs can outperform Jakobsen's algorithm (Jakobsen, 1995), which is a well-known general-purpose simple substitution solving technique that is based on digraph statistics.

In this paper, we consider HMM-based cryptanalysis of the classic Vigenère cipher. For the Vigenère cryptanalysis problem considered here, we will train an HMM, then we show that by examining the resulting matrices A, B, and π of a converged model, we can easily determine the Vigenère key.

2.4 Related Work

In (Berg-Kirkpatrick and Klein, 2013) an expectation maximization (EM) technique is applied to homophonic substitutions, with the goal of analyzing the unsolved Zodiac 340 cipher. The EM technique in (Berg-Kirkpatrick and Klein, 2013) is analogous to the HMM process discussed in the previous section. A novelty of this work is the use of an extremely large number of random restarts to improve on the hill climb results.

The paper (Lee, 2002) appears to be the first to explicitly apply HMMs (or similar) to substitution ciphers. However, the work in (Cave and Neuwirth, 1980), which focused on English text analysis, anticipates later cipher-based studies.

In (Vobbilisetty et al., 2017), HMMs are applied to simple and homophonic substitutions, and a careful comparison is made to other automated cryptanalysis techniques. This work shows that HMMs can achieve superior results in many cases, although the computational expense can also be quite high.

The work presented here is motivated in part by the recent paper (Gomez et al., 2018), where it is shown that a generative adversarial network (GAN), which is a type of neural network, can be used to successfully break a Vigenère cipher. However, this GAN-based Vigenère attack assumes unlimited ciphertext, which is unrealistic in any classic cryptanalysis context. In addition, in (Gomez et al., 2018) it is claimed that a strength of the GAN technique is its ability to handle a large vocabulary (up to 200 symbols), which seems to be of somewhat dubious value in the context of Vigenère cryptanalysis. Finally, as is generally true of neural networks, the resulting GAN is opaque, leaving the authors to make statements such as the following (Gomez et al., 2018):

> For both ciphers, the first mappings to be correctly determined were those of the most frequently occurring vocabulary elements, suggesting that the network does indeed perform some form of frequency analysis to distinguish outlier frequencies in the two banks of text.

The implication here is that the authors are forced to conjecture as to the relative importance of the various features in the GAN, since such basic information is not at all clear from an examination of the model itself.

In the next section, we give experimental results for an HMM-based attack on a Vigenère cipher. We also provide some discussion of our results, and we compare our technique to the GAN-based approach mentioned above.

3 Experimental Results

First, we train an HMM with $N = 3$ hidden states on a Vigenère ciphertext that was generated using the keyword CAT. Note that in this experiment we have selected the number of hidden states N to be equal to the keyword length. Also, we have used an observation sequence (i.e., English text) of length 1,000 extracted from the Brown Corpus (Francis and Kucera, 1969). In all of our experiments, we have removed all special characters and word space, and all letters have been converted to lower case, resulting in $M = 26$ distinct observation symbols.

For this experiment, the converged A matrix is give by

$$A = \begin{pmatrix} 0.00000 & 0.00000 & 1.00000 \\ 1.00000 & 0.00000 & 0.00000 \\ 0.00000 & 1.00000 & 0.00000 \end{pmatrix}$$

In contrast to the English text and simple substitution examples discussed in Section 2, here the A matrix is very informative—for one thing, this A matrix tells us that the transition between the $N = 3$ hidden states is actually deterministic. From the nature of the Vigenère cipher, it is clear that these states correspond to individual column shifts, and hence this is a result that we would expect for a keyword of length 3.

The corresponding B matrix appears in Table 3, which reveals that the first hidden state corresponds to a shift of 0 (i.e., keyword letter A), as the probabilities approximately match the expected letter frequencies of English. We also see that the second hidden state corresponds to a shift by 2 (i.e., keyword letter C) since the letter frequencies in this column are offset by 2 from those of English, while the final column corresponds to a shift by 19 (i.e., keyword letter T).

From the converged B matrix and the state transitions in the converged A matrix, we deduce that the keyword must be either ATC, TCA, or CAT. In this specific example, we also find that the initial state distribution matrix π converges to

$$\pi = \begin{pmatrix} 0.00000 & 1.00000 & 0.00000 \end{pmatrix}$$

a	0.08761	0.01290	0.04950
b	0.01560	0.00000	0.06811
c	0.03540	0.07411	0.00480
d	0.04290	0.01470	0.00450
e	0.13171	0.03030	0.04320
f	0.02100	0.04740	0.02520
g	0.02190	0.12181	0.06661
h	0.04170	0.02160	0.07291
i	0.06841	0.01470	0.02610
j	0.00180	0.04470	0.00060
k	0.00600	0.08101	0.06541
l	0.04080	0.00360	0.06541
m	0.02340	0.00300	0.09871
n	0.06001	0.04800	0.02520
o	0.08131	0.02280	0.01050
p	0.02430	0.06721	0.01680
q	0.00090	0.07711	0.00300
r	0.06601	0.02160	0.02130
s	0.06151	0.00090	0.00030
t	0.09481	0.06451	0.07951
u	0.02910	0.06541	0.01500
v	0.01020	0.09781	0.03090
w	0.01500	0.03180	0.03870
x	0.00180	0.00960	0.13171
y	0.01590	0.02040	0.02310
z	0.00090	0.00300	0.01290

Table 3: Final B^T for Vigenère ciphertext with keyword CAT

This implies that we start in the second hidden state, which corresponds to C, and hence we have determined that the keyword is CAT.

Suppose that instead of using $N = 3$ hidden states, we train an HMM with $N = 2$ hidden states using the same Vigenère encrypted data as in the previous example. In this case, we find that the A matrix converges to

$$A = \begin{pmatrix} 0.75236 & 0.24764 \\ 0.34235 & 0.65765 \end{pmatrix}$$

which tells us that we do not have deterministic transitions between the states, and hence the keyword length is greater than 2.

If, on the other hand, we attempt to train a model with $N = 4$ hidden states, we obtain

$$A = \begin{pmatrix} 0.00000 & 1.00000 & 0.00000 & 0.00000 \\ 0.00000 & 0.00000 & 0.99884 & 0.00116 \\ 1.00000 & 0.00000 & 0.00000 & 0.00000 \\ 0.00000 & 0.15595 & 0.00000 & 0.84405 \end{pmatrix}$$

Since some state transitions are deterministic, we suspect that the keyword length is less than 4 in this case. Similarly, an HMM with $N = 5$ hidden states yields

$$A = \begin{pmatrix} 0.00 & 0.00 & 0.00 & 1.00 & 0.00 \\ 0.00 & 0.00 & 1.00 & 0.00 & 0.00 \\ 0.00 & 0.00 & 0.00 & 1.00 & 0.00 \\ 0.00 & 0.47 & 0.00 & 0.00 & 0.53 \\ 1.00 & 0.00 & 0.00 & 0.00 & 0.00 \end{pmatrix}$$

which, again, implies that the keyword length is likely less than 5. Finally, we point out that multiples of the keyword length behave similarly—for this example, with $N = 6$ hidden states we obtain

$$A = \begin{pmatrix} 0.00 & 0.00 & 0.54 & 0.00 & 0.46 & 0.00 \\ 0.00 & 0.00 & 0.00 & 0.00 & 0.00 & 1.00 \\ 0.00 & 0.00 & 0.00 & 1.00 & 0.00 & 0.00 \\ 0.49 & 0.51 & 0.00 & 0.00 & 0.00 & 0.00 \\ 0.00 & 0.00 & 0.00 & 1.00 & 0.00 & 0.00 \\ 0.00 & 0.00 & 0.00 & 1.00 & 0.00 & 0.00 \end{pmatrix}$$

From these results, we conclude that the A matrix in a converged HMM will enable us to precisely determine the keyword length used to encrypt a Vigenère ciphertext. Furthermore, if sufficient ciphertext is available so that English letter distributions are (roughly) apparent, the B matrix, together with the initial state matrix π, will completely determine the keyword. That is, we simply train HMMs with different values of N until we obtain a deterministic A matrix, and then we use the corresponding B and π matrices to determine the Vigenère key. Due to the fact that an HMM is a hill climb, to obtain a converged model, we might need to train each HMM multiple times with different randomly-selected starting values.

Next, we consider the amount of ciphertext needed to determine the Vigenère key using this HMM-based attack. Of course, the amount of ciphertext will depend on the length of the keyword.

We tested a few small keyword lengths until we found an initialization that yielded a solution. Then we reduced the amount of ciphertext until the HMM was unable to solve the problem. This gives us an upper bound on the amount of ciphertext needed, at least in these selected cases. In these experiments, we define a "solution" as a trained HMM where the average of the maximum value in each row of the A matrix is at least 0.99. Our results are given in Table 4, based on 100 random restarts of the HMM for each test case.

Keyword	Keyword length	Minimum ciphertext	Friedman test
IT	2	175	1.4235
DOG	3	250	3.7209
MORE	4	450	3.8208
NEVER	5	1200	3.6467
SECURE	6	1400	4.5545
ZOMBIES	7	1300	9.9334

Table 4: HMM attack (100 random restarts)

From the results in Table 4, it seems likely that with a large number or random restarts, we can significantly reduce the required length of the ciphertext. In any case, even the ciphertext lengths in Table 4 are far from the "unlimited" ciphertext that is assumed for the GANs training discussed in (Gomez et al., 2018). It is also interesting that our HMM result is accurate, even in cases where the Friedman test gives an incorrect result.

4 Conclusion

In this paper, we showed that a hidden Markov model (HMM) is a powerful and effective tool for the cryptanalysis of Vigenère ciphertext messages. We also showed that a trained HMM is informative in this context, in particular when compared to the neural network (GAN) based Vigenère attack discussed in (Gomez et al., 2018). Undoubtedly, GANs are powerful and useful tools for many types of problems. However, it appears that the Vigenère cipher may not be an ideal test case to illustrate the strengths of this particular type of neural network.

For future work, it would be interesting to test an HMM-based Vigenère attack with large numbers (i.e., millions) of random restarts to determine the minimum amount of ciphertext needed. It would also be interesting to test similar HMM based attacks on other more complex polyalphabetic substitutions. Various combinations of classic substitution and, perhaps, elementary transposition ciphers are also possibly amenable to HMM-based analysis. Due to their general applicability to classic substitution ciphers, HMMs might be useful as a first line of analysis in cases where a (classic) encryption technique is not completely known.

References

Taylor Berg-Kirkpatrick and Dan Klein. 2013. Decipherment with a million random restarts. In *Proceedings of the Conference on Empirical Methods in Natural Language Processing*, pages 874–878.

Robert L. Cave and Lee P. Neuwirth. 1980. Hidden Markov models for English. In J. D. Ferguson, editor, *Hidden Markov Models for Speech*, IDA-CRD, Princeton, NJ, October 1980, pages 16–56. https://www.cs.sjsu.edu/~stamp/RUA/CaveNeuwirth/index.html.

W. Nelson Francis and Henry Kucera. 1969. The Brown Corpus: A standard corpus of present-day edited American English. http://www.nltk.org/nltk_data/.

William F. Friedman. 1987. *The Index of Coincidence and Its Applications in Cryptography*. Aegean Park Press.

Aidan N. Gomez, Sicong Huang, Ivan Zhang, Bryan M. Li, Muhammad Osama, and Lukasz Kaiser. 2018. Unsupervised cipher cracking using discrete GANs. https://arxiv.org/abs/1801.04883.

Thomas Jakobsen. 1995. A fast method for the cryptanalysis of substitution ciphers. *Cryptologia*, 19:265–274.

Friedrich W. Kasiski. 1863. *Die Geheimschriften und die Dechiffrirkunst (Cryptography and the Art of Decryption)*. Mittler und Sohn, Berlin. http://pages.mtu.edu/~shene/NSF-4/Tutorial/VIG/Vig-Kasiski.html.

Dar-Shyang Lee. 2002. Substitution deciphering based on HMMs with applications to compressed document processing. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24(12):1661–1666, December.

Lawrence R. Rabiner. 1989. A tutorial on hidden Markov models and selected applications in speech recognition. *Proceedings of the IEEE*, 77(2):257–286.

Mark Stamp. 2004. A revealing introduction to hidden Markov models. https://www.cs.sjsu.edu/~stamp/RUA/HMM.pdf.

Rohit Vobbilisetty, Fabio Di Troia, Richard M. Low, Corrado Aaron Visaggio, and Mark Stamp. 2017. Classic cryptanalysis using hidden Markov models. *Cryptologia*, 41(1):1–28.

Wing Wong and Mark Stamp. 2006. Hunting for metamorphic engines. *Journal in Computer Virology*, 2(3):211–229.

WORLD WAR I

The Solving of a Fleissner Grille during an Exercise by the Royal Netherlands Army in 1913

Karl de Leeuw
University of Amsterdam / Informatics Institute
Science Park 904, 1098 XH Amsterdam
karl.de.leeuw@xs4all.nl

Abstract

In 1885 the General Staff of the Royal Netherlands Army had adopted a variant of the turning grille devised by Edouard Fleissner von Wostrowitz as a means for encrypting messages, exchanged by telegraph between the General Headquarters and commanders in the field. Some staff members harbored serious doubts about the security of this device, however, and during a military exercise in 1913 it was solved with surprising ease by an army captain. The matter was investigated by a committee of staff officers, concluding that the army lacked the expertise to judge matters like this. It recommended the training of a staff officer for this purpose in particular. The outbreak of the First World War was to speed up the decision process, but – against all odds – the newly trained experts were not drawn from the ranks that had demonstrated their talent for code breaking a year earlier, because these were destined to follow different career paths altogether.

1 Introduction

Kahn (1967) describes the original grille, as conceived by Cardano as:

"a sheet of stiff material, such as cardboard, parchment or metal into which rectangular holes, the height of a line of writing and of varying lengths, are cut at irregular intervals. The encipherer lays this mask over a sheet of paper and writes the secret message through the perforations, some of which will take a whole word, others a single letter, others a syllable. He then removes the grille and fills in the remaining spaces with an innocuous sounding cover message." [1]

[1] Kahn, 144-145

Initially the grille was intended for hiding that a secret message was being sent at all, rather than as a means of encryption. This all changed during the course of the 18th century, when the grille was increasingly used for jumbling the characters in a message by rotating them, according to the holes in the mask. The first description of such use we find by the German mathematician Carl Friedrich von Hindenburg (1796) who was aware that such use could only be made at the expense of a loss in entropy and, therefore, cryptographic strength. The perforation pattern in one quadrant of the mask would automatically limit the possibilities for perforation in all others, because two punch holes could not be allowed to cover the same position after a rotation.

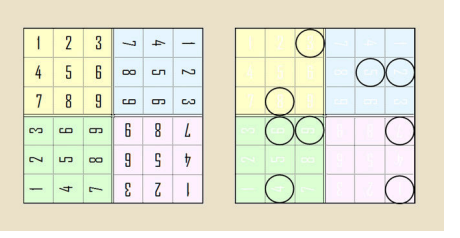


Figure 1: drawing showing how a turning grille can be punched

The appearance of the turning grille in scientific literature only at the end of the 18th century does not mean, however, that it wasn't used before. Karl de Leeuw and Hans van der Meer (1995) have demonstrated that the practice existed already 50 years earlier. The device gained wide popularity much later, after a Austrian Colonel Edouard Fleissner von Wostrowitz (1881) had drawn attention to it in a handbook about military cryptography. Essentially, he proposed the adding of two or more columns with nulls in order to hide the center of rotation of the actual cryptogram. At the eve of

Proceedings of the 1st Conference on Historical Cryptology, pages 49– 54,
Uppsala, Sweden, 18-20 June, 2018

and during the first world war his suggestion was followed widely. Kahn (1967) mentioned the use of turning grilles in different sizes by the Germans during the first months of 1917, only to be solved by French code breakers not much later.[2] The Dutch were no exception. In a circular announcement dated 23 April 1885 the General Staff proscribed the use of the turning grille for telegraph traffic in times of crisis between the General Headquarter and field commanders.[3] Some staff members, however, doubted the cryptographic strength of the device and one of them proposed the enciphering of the original message by means of a addition table, before deploying the turning grille proper.[4] This proposal did not get any follow-up, but the matter became urgent again on 20 June 1913, when another army captain, C.J.H. van der Harst (1876-1938), was able to break an encrypted message from GHQ with surprising ease. This incident caused commander in chief General C.J. Snijders (1852-1939) to appoint a committee to re-examine the use of cryptography by the army.

In this paper I will briefly discuss the military exercise and then show how the message was broken by Captain van der Harst. Subsequently I will analyse the way in which the entire incident was evaluated by the General Staff. In the conclusion, I will assess the viability of the measures taken.

2 The exercise

The Netherlands had been a neutral country since the defeat of Napoleon in 1815. Apart from colonial warfare, mainly in the East Indies and a military expedition to prevent Belgium from gaining its independence in 1830 it had not fought a major war for almost 100 years, when finally war broke out in 1914. The Netherlands managed to stay out of conflict, but were heavily affected by trade embargoes and the flooding of half a million refugees from Belgium. The army was not unprepared. It had to reckon with a military invasion by the British in the south west to liberate Antwerp and with a German attack from the east. The German building of armored flatboats with heavy guns had caused the army much distress, because these could enter the shallow waters protecting the Dutch capital and its surroundings. This clearly indicated that a German attack could not be ruled out, in case war broke out in Western Europe (Klinkert, 2017).

During this exercise, lasting two days in June 1913, a deployment of troops in the IJssel valley was simulated, entailing a movement of troops by train from the western to the eastern part of the country, including the transport of equipment for a field hospital. On the eve of the second day of the exercise – on 20 June – a cable message was sent by the field commander in the western part of country with orders for his troops already present in the eastern part. It was to be intercepted by the party supposedly defending the East, located in the stronghold Cortenoever, overlooking the valley.[5]

The encrypted message was given to Captain C.J.H. van der Harst who was to find out which orders were given for the next day. It consisted of 15 columns and thirty rows filled with letters only, no digits included. Captain van der Harst – who was detached by his regiment with the General Staff – had three advantages: (1) he knew exactly how the turning grille had to be handled according to the guidelines, issued by his colleagues at the General Staff, when it was introduced nearly twenty years before; and (2) he was familiar with the language used by army officers in cables like these; and (3) he was well aware of the limitation in entropy, offered by the turning grille, as he makes a remark about this in his notes.

To start with the first: the use of punctuation marks and digits was strictly prohibited. Numbers were to be represented by the first 10 letters of the alphabet, omitting the "j"; punctuation marks were to be spelled out. The sides of the grille were always indicated by means of the first eight letters of the alphabet. The square in the exact middle of the grille was used to indicate which side had to be placed on top to start with, from that position on every following rotation was to be made clockwise. If the message contained too many letters to fit one cipher block, this procedure was simply repeated. Remaining squares had to be filled in with nulls. The adding of at least two columns with nulls, recommend by Colonel Fleissner von Wostrowitz to hide the rotating center of the cryptogram, was not mandatory for regular use. The

[2] Kahn, 308-309

[3] The Hague, Nationaal Archief, Department van Oorlog, Generale Staf, inv. nr. 82

[4] Ibid., inv. nr. 305: Captain A. van Mens to General C.J. Snijders, Arnhem 1911, January 19. Van Mens wrote his advice on request of the chief of staff, given by mouth five days earlier.

[5] Ibid., inv. nr. 305: handwritten note without date containing instructions for the exercise.

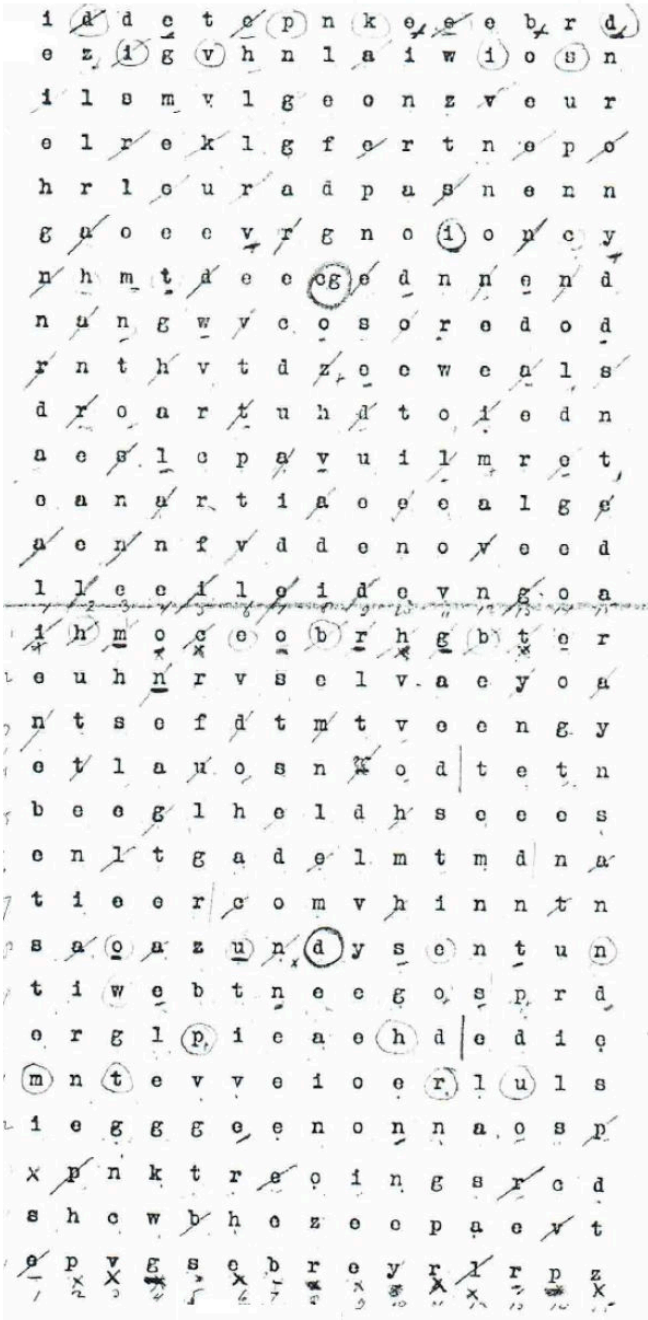


Figure 2: the supposedly intercepted message. Source: Nationaal Archief Den Haag

guidelines did mention this possibility, but only as a complicating measure, to be applied at will. A second complicating measure mentioned was the filling of the mask before rotation with nulls and starting writing the actual message after turning the backside up. This procedure could only be indicated if the center for rotation was filled with two letters: one to indicate the original position of the mask and one to indicate how it had been laid after the backside had been turned up.[6]

3 Reconstructing the grille in use

The approach taken by Captain Van der Harst to solve the cryptogram can be derived from his personal notes, handed over after the exercise to the commander in chief Lieutenant-General Snijders.[7] The captain started his analysis by stating that the size of the letter square, consisting 15 columns and 30 rows, probably indicated a plain use of the turning grille twice, without columns added. This implied that the letter square had to be divided into two halves of 15 rows each and that the punch hole in the exact middle of each letter square would have to contain a letter indicating which side of the grille had to be put on top first.

The square in the middle of the first cipher block contained two letters, however, 'cg', the square in the middle of the second cipher block only one letter: 'd'. Therefore, Van der Harst decided to proceed with the second cipher block.

The captain subsequently asked which words were likely to emerge in the message, words that could be detected easily, because of their spelling that is to say. He mentioned several: 'vyand' (enemy), because the 'y' does not occur very often in Dutch; 'bericht' (message), because the trigram 'cht' is rare; and 'opperbevelhebber' (commander in chief), because this word contained two doublings of consonants: 'pp' and 'bb' which is rare in Dutch also. Generally speaking, Van der Harst expected the message to contain information about troop movements, not yet known to the field commander, orders, or reconnaissance about the enemy.

The first row of the cryptogram contained the letters 'i', 'c'. 'h', and 't', likely constituting the last syllable of the word of 'bericht'; the last row contained 'b', 'e' and 'r', constituting the first syllable of the same word. These letters had to correspond with three punch holes of the mask. Consequently, these squares had to remain black when the grille is turned. The drawing of the mask could now begin. The last row contained one more probable word: 'g', 'r', 'y', 'p', (*attack*). This word is likely to occur in a sentence like this: 'gryp morgen vyand aan' (*attack the enemy tomorrow*). These words can be constituted from letters also to be found in the first and second row, indicating the position of the punch holes when side II is put on top. Another probable grouping of words would be: 'met uwe geheele macht' (*with your entire force*). Detecting of these words makes the unveiling of the second cipher block almost complete. The text occurring in the punch holes when side IV is put on top can now be reconstructed: 'or u vastgestelde stations zijn uitgeladen kondschapsber' (*Railway stations allocated by you reconnaissance mess...*). This implicates that the square is to be used first with side IV being put on top, before side I, II and III are moved to this position, correponding with the letter 'd' in the middle of the second cipher block. The remaining letters occurring when side III is put on top constitute rubbish. The entire text emerging in this cipher block is now clear:

'door u vastgestelde stations zijn uitgeladen volgens kondschapsbericht heeft vyand te helder minstens drie divisies ontscheept gryp morgen vyand aan met uwe geheele macht en werp hem terug opperbevelhebber slot'

(allocated railwaystations are unloaded according to reconnaissance message the enemy has disembarked at least three divisions in helder attack the enemy tomorrow with your entire force and throw him back commander in chief end).

With help of the reconstructed grille, but only after moving the mask in various positions in a process of trial and error, the following message emerged:

Derde divisie, korps RA en vliegafd zullen hedenavond en nacht worden aangevoerd en be-

[6] Ibid., inv. nr. 82: Aanwijzing voor het gebruik van geheimschrift (*Clues for the use of Secret Writing*). It is unclear to me how this recommendation was to be put into practice, if a cable gram was actually sent. After all, all of this depended on the neatly reorganizing the cryptogram in groups of four letters. Clearly, in one way or the other, it had to be indicated that the telegram contained two letters that had to be placed in one square, but how?

[7] Ibid., inv.nr. 305: | Methode van ontcijfering van het geheimschrift (*Method of Deciphering of Cryptogram*). Annex to the letter sent by Lieutenant-General C.J. Snijders to staff captains P. Huizer, E.F. Insinger and P.J. Van Munnekrede, s'Gravenhage, 7 November 1913, GS no 138, Geheim.

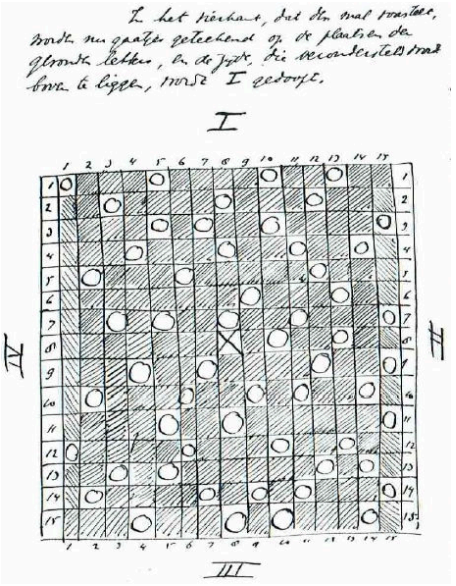


Figure 3: The grille as teconstructed by Van der Harst. Source: Nationaal Archief

halve verpleging en veldhosp afd morgenochtend om zes uur aan de door u vastgestelde stations zijn uitgeladen volgens kondschapsbericht heeft vyand te helder minstens drie divisies ontscheept gryp morgen vyand aan met uwe geheele macht en werp hem terug opperbevelhebber slot'

(third division, royal horse artillery and aircraft unit will be conveyed this evening and night and except for hospital staff and hospital equipment tomorrow morning at six o' clock unloaded at the designated railwaystations according to reconnaissance message the enemy has disembarked at least three divisions in helder attack enemy tomorrow with your entire force and throw him back commander in chief end)

4 The staff report

On 7 November 1913 General C.J. Snijders decided to put the matter before a committee of three staff officers: the captains P. Huizer, E.F. Insinger and P.J. Van Munnekrede. He asked whether the turning grille could be improved or had to be replaced altogether. If the last was to be case, he demanded to pay attention to the question whether the system in use by the Royal Netherlands Navy could be adopted by the Army as well. This would have the advantage that Army and Navy could exchange secret messages without additional effort.[8] He also wanted them to take notice of a system, described recently in a French journal.[9]

Unfortunately, this committee lacked all code breaking experience. It proved, however, to be well versed in the cryptologic literature of the day. It cited among other titles *Les chiffres secrets dévoilées* by E. Bazeries (1901); *Etude sur la cryptographie* by A. Collon (1906); *Kryptographik* by L. Kluber (1809); *Die Geheimschriften im dienste des Geschäfts- und Verkehrslebens*, by H. Schneikert (1905); not to mention of course the well-known *Handbuch der Kryptographie* by E. Fleissner von Wostrowitz (1881).[10] This sufficed, however, to discourage adoption of the cipher system used by the navy, because this consisted of a simple Caesar alphabet to encipher the existing optical signal register whenever needed, offering no genuine protection at all.[11] What is more, according to the committee, a common cipher system for army and navy was unnecessary and even dangerous: unnecessary because army and navy units were not be in direct contact, orders being always given top down; and dangerous, because the distribution of ciphers would become too widespread to offer security any longer. Encryption had to remain limited to messages exchanged between the GHQ and the field commanders.[12]

Surprisingly, a careful examination of the literature had lead the committee to believe that the turning grille was one of the strongest encryption devices available, as no convincing cases were presented of its solution. It did believe, however, that the way in which the system was used in the Netherlands, was ready for improvement.[13] In the view of his colleagues, Captain van der Harst was able to break the cipher, only because he had a some idea what the messages was about; because he was well aware what probable words to look

[8] Ibid., inv.nr. 305: Lieutenant-General C.J. Snijders to staff captains P. Huizer, E.F. Insinger and P.J. Van Munnekrede.s'Gravenhage, 7 November 1913, GS no 138, Geheim.

[9] Génie Civil,XXIII (26), 420.

[10] The Hague, Nationaal Archief, Departement van Oorlog, Generale Staf, inv. nr. 305: Beschouwingen en voorstellen in verband met het bij den Generale Staf in gebruik zijnde geheimschrift. d.d. 30 May 1914. (*Reflections and Propositions with regard to Secret Writing as practiced by the General Staff.*

[11] Ibid., 4.

[12] Ibid., 5-6.

[13] Ibid., 6-7

for; and, last but not least, because no complicating measures, such as the adding of columns to hide the real rotating center of the cipher block were ever taken.[14] Much in line with the original suggestion made by Captain Van Mens in 1911, the committee recommended the enciphering of the original message before putting it under a turning grille by way of a Vigenère, carefully explaining how a Vigenère worked.[15]

The committee did not go into the actual cryptanalysis of the message. It was well aware that it lacked the hands-on experience, needed in an actual war. Therefore, it recommended the appointment and training of an additional staff officer to gain expertise in this particular field. It doubted, however, that this job was suited for a career officer, who had to rotate jobs on a regular basis. The mindset needed was one of patience, perseverance and wisdom: with the possible exception of perseverance attributes difficult to find among people who joined the army in most cases, because they wanted to see action. The committee believed that a reserve officer would be better suited for this task, because he would lack the ambition to make a career in the army to start with. Descent was irrelevant, in this particular case.

5 Conclusion

Less than a month after the committee had completed its report, Archduke Franz Ferdinand and his spouse were murdered and less than two months later war broke out, changing the face of the continent. In this context it should not surprise us that the committee's advice was followed. Henri Koot, a young lieutenant from the colonial army who happened to be in the country to follow a training program, possessed all the required qualities and proved to be able to lay the groundwork for the institution of modern cryptology in the Netherlands, as Karl de Leeuw (2015) has shown. Koot – recognizably of mixed descent – was highly intelligent, but also modest and obedient to the extreme and he had no career expectations outside the colonial army whatsoever. Nor should it, after all that has been said, surprise us, that Van der Harst – who clearly had demonstrated his talent as a cryptologist – wasn't called upon to do the job. He was to rise high in the Royal Netherlands Army, ending his career as a Major General and governor in charge of the Royal Military Academy.

[14] Ibid., 8.

[15] Ibid., Bijlage B.

References

Edouard Fleissner von Wostrowitz. 1881. *Handbuch der Kryptographie*. Seidl & Sohn, Wien, Austria.

Carl Friedrich von Hindenburg. 1796. Fragen eines Ungenannten über die Art durch Gitter geheim zu schreiben. *Archiv der reinen und angewandten Mathematik III*: 347–351, V: 81-99.

David Kahn. 1967. *The Codebreakers. The Story of Secret Writing.* Macmillan Publishing Company, New York, USA.

Wim Klinkert. 2017. 'Espionage Is Practised Here on a Vast Scale'. The Neutral Netherlands, 1914-1940. Floribert Baudet et al., *Perspectives on Military Intelligence from the First World War to Mali. Between Learning and Law.* T.M.C. Asser Press, The Hague, The Netherlands, 23-54.

Karl de Leeuw and Hans van der Meer. 1995. A Turning Grille from the Ancestral Castle of the Dutch Stadtholders. *Cryptologia*, XIX(2), 153-164.

Karl de Leeuw. 2015. 'The Institution of Modern Cryptology in the Netherlands and the Netherlands East Indies, 1914-1935.' *Intelligence and National Security*, 30: 26-46.

Deciphering German Diplomatic and Naval Attaché Messages from 1914-1915

George Lasry
University of Kassel
Germany
george.lasry@gmail.com

Abstract

In World War One (WW1), the German diplomatic services and the Imperial Navy employed codebooks as the primary means for encoding confidential communications over telegraph and radio channels. The Entente cryptographic services were able to reconstruct most of those codebooks, to obtain copies of others, and to overcome various enhancements introduced by the Germans.

A collection of diplomatic and naval attaché cryptograms from and to the German consulate in Genoa, dating from the late 19th Century to 1915, has been preserved and is held in German archives.[1]

In this article, the author describes the process of identifying the encoding methods, of reconstructing the 18470 diplomatic codebook, and of recovering the superencipherment applied to the German Navy's Verkehrsbuch.

The vast majority of the messages can now be read in clear. Before the war, the communications are mainly about routine consular matters. From the summer of 1914, they reflect the sequence of events leading to war, including the declarations of war. The messages also describe the crucial role played by the German consulate in collecting naval intelligence, and in assisting the German warships Goeben and Breslau in their escape to the Dardanelles in August 1914.

1 Overview

Collections of original encrypted messages are hard to find. As a standard security procedure, it was not allowed to keep records in their encoded form. Diplomatic archives in most cases do not contain original cryptograms. Furthermore, signal intelligence and codebreaking agencies which intercept enemy communications also have a policy of not preserving the original cryptograms. As a result, the discovery of a collection of such documents is a rare event and can be of significant value for cryptology history research and general historians. For example, hundreds of Enigma cryptograms from 1941 and 1945 were decrypted in 2005, shedding new light on German communication procedures and on the fate of resistance leaders who died in Nazi concentration camps (Sullivan and Weierud, 2005). In 2016, a collection of ADFGVX cryptograms from the Eastern Front of WW1 was deciphered, providing new insight into events which occurred towards the end of the war (Lasry et al., 2017).

The Politisches Archiv des Auswärtigen Amtes (PA AA), the political archives of the German Foreign Office in Berlin, holds a series of documents recording communications to and from the German consulate in Genoa (Genova), a port in northwestern Italy (PAAA, c 1915). The records cover the period from 1867 to 1915, most of them from 1914 until May 1915, at the time Italy left the Triple Alliance and declared war on the Austro-Hungarian Empire. While a large part of the documents consists of non-encrypted plaintexts, hundreds of them consist of original cryptograms, encoded using several types of diplomatic and naval codebooks.

This article describes the process of recovering the original plaintexts and analyzing their contents. It is structured as follows: In Section 2, we provide an introduction to codebooks, as well as a description of the main German diplomatic and naval codebooks used in WW1. In Section 3, we describe, step-by-step, the process of identifying the various encryption methods, of recon-

[1] RAV Genua - Records from the German General Consulate in Genoa. Politisches Archiv des Auswärtigen Amtes.

Proceedings of the 1st Conference on Historical Cryptology, pages 55– 64,
Uppsala, Sweden, 18-20 June, 2018

structing one of the codebooks, and of recovering the superencipherment key for another codebook. In Section 4, we provide preliminary findings about the contents of the messages. In Section 5, we briefly assess the cryptographic weaknesses of WW1 German codebooks and procedures.

2 German WW1 Code Books

A codebook is essentially a dictionary of words and other entities that may be encoded using a code, such as a 5-digit number, or a 4-letter code. In this section, the various types of codebooks are described, focusing on diplomatic and naval codebooks used by the German Empire in WW1.

2.1 One-Part Codebooks

The *one-part codebook* is the most convenient form of a codebook. Compiling such a codebook is a relatively simple process. The codebook entries appear in alphabetical order. Numerical codes are assigned to each entry in the same order. It is easy to search for a word and its corresponding numerical code while enciphering a message, or to search for a numerical code while deciphering an encoded message. Therefore, the same physical copy of the codebook can be used for both enciphering and deciphering.

Like any other form of enciphering using substitution, codebooks may be reconstructed by adversaries using frequency analysis. The most frequent codes are most likely to represent the most frequent words of the language. To reduce the frequency of the most common codes, codebook compilers also included expressions and even full sentences as entries in the book. Furthermore, they assigned multiple codes for the most heavily used words. Those measures were not always effective, as they often depended on the operator choices for encoding sentences instead of single words, and for not always selecting the same numerical code for a common word. The main weakness of one-part codebooks is the strong relationship between the alphabetic location of words and their corresponding numerical codes. If two numerical codes are close to each other, and the meaning of the first word is known, it might be possible to guess the meaning of the second word, as it is alphabetically close to the first one.

2.2 Two-Part Codebooks

To achieve better cryptographic security, there should ideally not be any relationship between the (alphabetical) order of the words and the numerical order of the corresponding codes. While doing so increases the cryptographic security of a codebook, at the same time, it is not possible anymore to use the same codebook for both enciphering and deciphering. Two versions of the codebook are required, the first one in alphabetical order for enciphering, and the second one in numerical order for deciphering, in other words, a *two-part codebook*.

At first, the designers of German codebooks introduced two-part codebooks in which they scrambled the order of the pages, but the numerical codes for words within a page (usually 100 per page) were still ordered according to the alphabetical order of the words. As a result, numerically close codes could still be guessed. Worse, new codebooks were often no more than a copy of a previous codebook (possibly already reconstructed by the enemy) in which only the original pages had been reshuffled, but not the words inside each page. To reconstruct such a codebook, it was enough to map each page from the previous version to the corresponding page in the new version. For that purpose, the knowledge of the meaning for only a few tens of codes (in the new codebook version) was usually sufficient.

To achieve a purely random ordering, 'hat codes' (also known as 'lottery codes') were introduced during the war. Their name is derived from the manual methods used in WW1, such as mixing paper strips inside a hat, and extracting them randomly and assigning them numerical codes, so that the numerical codes have no relation to the alphabetical order of the words. Reconstructing a hat code by codebreaking agencies required a significantly larger and longer effort, including extensive trial-and-error. In general, cryptanalysts could never reconstruct such a codebook in its entirety.

2.3 Superencipherment

Physical copies of a codebook may always fall into the enemy's hands, and while harder with hat codebooks, reconstruction by analytical means is still possible. Therefore, codebooks should not be used for an extended period of time. On the other hand, compiling a new codebook and distributing its physical copies was often difficult, es-

pecially to embassies in countries without a border with Germany, such as Spain. To increase the security of existing codebooks without replacing them, German cryptographers often applied a *superencipherment* (an additional encipherment) on the numerical codes. Methods of superencipherment either consisted of transpositions (changing the order of the digits in the numerical code), substitutions (replacing a digit with another digit), or additives (some number mathematically added to the numerical codes). At first, superencipherment methods were simple or used over a long time span, allowing Room 40, the section in the British Admiralty responsible for cryptanalysis, to recover the keys on a regular basis.[2]

Toward the end of the war, the Germans introduced more sophisticated methods, but often made the severe mistake of communicating the details of a new superencipherment method in a message encoded with a previous version, already known to Room 40.[3]

2.4 German Diplomatic Code Books

Germany started the war with several families of diplomatic codebooks in place, mainly the 13040 and the 18470 families. A family of codebooks includes several codebooks derived from one another. Those first German diplomatic codebooks usually consisted of the following sections:

- **Dreinummerheft**(3-digit code): This section was common to all codebooks in the 18470 and 13040 families. The prewar 18102 codebook also used the same Dreinummerheft codes. The Dreinummerheft consists of 3-digit codes, from 000 to 999. They represent numbers (000 to 500, 00 to 99) and dates (January 1 to December 31). The mapping follows an almost predictable pattern. As a result, to fully reconstitute the Dreinummerheft, an adversarial code-breaking organization such as Room 40 needed to know the meaning of only a few of the Dreinummerheft codes.

- **Places**: A set of pages (randomly numbered) dedicated to names of cities, countries, nationalities, and foreign government institutions. Each page contains 100 entries.

- **Words and Expressions**: A set of pages (randomly numbered) dedicated to words, expressions and some full sentences. Each page contains 100 entries.

- **Persons**: A set of pages dedicated to names of persons, and entities such as banks and commercial shipping lines. Those pages, randomly numbered, were sparsely populated (usually only ten names out of the possible 100 in a page).

- **Supplement**: A set of pages with additional names and places, with numerical codes randomly assigned.

Except for the Dreinummerheft, which consists of 3 digits, the numerical codes have 4 or 5 digits. The three leftmost digits (for a 5-digit code) or the two leftmost digits (for a 4-digit code) represent the page number. The second digit to the right represents the *block* number. Each page has ten blocks (from 0 to 9), each block containing ten words. For example, code `10275` corresponds to the word *Dampfer* (steamer), and it is the sixth word (the last digit is 5, we start counting from 0) in block 7 of page 102. The order of the pages (the page numbers) does not correspond to the alphabetical order of the words they contain. Furthermore, the order of the 10-word blocks inside a page does not correspond to the alphabetical order of their contained words. However, all the 100 words inside a page are always relatively close alphabetically. Also, the ten words inside each block are in alphabetical order. While those codebooks are nominally two-part codebooks, it is still possible to deduce the meaning of one numerical code based on the meaning of another code on the same page or block.

The 18470 and its derivatives, such as the 12444, the 1777, and the 2310, were fully recovered by Room 40, aided by the capture of codebook 3512 in Persia in 1915. Interestingly, it seems that Room 40 never shared their copy of the captured codebook 3512 with their US counterparts, despite closely cooperating in various domains. Room 40 was able to analytically reconstruct most parts of the 13040 codebook (which was used to encipher the famous Zimmerman Telegram), as well as its derivatives, the 5950 and the 26040 (the 13040 superenciphered using

[2] (Gannon, 2010), p. 130.
[3] (Gannon, 2010), p. 261, footnote 20.

a constant additive).[4,5]

The German diplomatic services also developed a series of two-part hat codes, such as the 5300, 6400, 7500, 8600, and 9700 codebooks. Room 40 was able to recover large parts of those codes, and in particular, codebook 7500, used to encipher one of the versions of the Zimmerman Telegram.[6]

Interestingly, despite the capture of a copy of the 3512 codebook, and the publication of the Zimmermann Telegram, the German diplomatic cryptographers never realized that both the 18470 and 13040, and their relatives, had been compromised. In a report from April 1917, Herman Stützel, a German Navy cryptographer, describes how he was able to decipher messages encoded with the 18470 codebook, only from intercepted communications. He was also able to decipher messages encoded with the 5300 hat code with various superencipherment methods (Stützel, 1969). Ironically, Room 40 intercepted and deciphered a message containing the report. The reaction of the German diplomatic services to the report is unknown. The Imperial Navy swiftly reacted, implementing a series of new complications on top of their naval attaché codes (see Section 2.5).

2.5 Naval Code Books

At the outset of the war, the Navy had several codebooks in use for various purposes, including the *Signalbuch der Kaiserlichen Marine (SKM)*, used mainly for signaling and communications between ships, and the *Handelsverkehrsbuch (HVB)*, for communications with merchant ships. For communicating with naval attachés, the Imperial Navy also employed the *Satzbuch (SB)*, as well as the *Verkehrsbuch (VB)*. The SKM, HVB, SB, and VB were all one-part codebooks. The VB and the SB were usually superenciphered, but at the beginning of the war, the keys were not frequently changed. The German Navy was slow to realize that copies of its books had fallen into enemy's hands, early on in the war. Later on, the Navy implemented various methods for superencipherment, and also introduced new codebooks such as the *Flottenfunkspruchbuch (FFB)*, which replaced the SKM in 1917.

The main codebook for communicating with naval attachés, the Verkehrsbuch, maps words and entities into groups of 5 digits. It consists of several sections, for words and expressions, for names of places and ships, as well as for indicating positions of ships on maps. The Stützel report (see Section 2.4) caused great alarm at the German Admiralty, and the Navy introduced new, more complex superencipherment methods. Based on the voluminous numbers of transcripts in British National Archives in Kew, which also mention the types of code and superencipherment, those probably did not pose serious problems to Room 40's codebreakers. Using decrypts from the traffic between Berlin and the naval attaché in Madrid, Room 40 was able to unravel and prevent various plots and espionage activities conducted from the German embassy in Madrid.[7]

3 Deciphering the Genoa Cryptograms

In this section, we present the step-by-step process of deciphering the majority of the cryptograms in the Genoa collection. We describe the processes of classifying the various types of cryptograms, of reconstructing a diplomatic codebook, of identifying the superencipherment method for a naval attaché code, and of recovering its key. This detective work also required the retrieval and survey of a multitude of documents from archives in Germany, the UK, and the US, with the assistance of leading experts. The work continued with building a computerized database of the cryptograms, successfully deciphering most of them, and validating the decryptions with newly found documents.

3.1 Classifying the Cryptograms

At first, we obtained six files from the RAV Genua collection at the PA AA, containing both plaintexts and cryptograms.[8,9,10,11,12,13]

After analyzing the structure of the cryptograms, we were able to divide them into four categories:

[4] (Gannon, 2010), p. 130.
[5] (Gannon, 2010), p. 205.
[6] (Gannon, 2010), p. 131.
[7] (Gannon, 2010), Chapter 13 - The Spanish Interception.
[8] PA AA - RAV Genua 09, Acten betreffend Ziffern 1867-1908.
[9] PA AA - RAV Genua 10, Chiffrierwesen 1898-1913.
[10] PA AA - RAV Genua 11, Sammlung der Chiffres 1889-1908.
[11] PA AA - RAV Genua 12, Sammlung der Chiffres mit Ausschluss der Korrespondenz mit den Marinebehörden, Bd. 2, 1904-1914.
[12] PA AA - RAV Genua 13, Chiffrierte Telegramme 1914-1915
[13] PA AA - RAV Genua 14, Telegramme in Chiffre. 1914-1915.

- **Sequences of letters**: Two messages from 1897 and 1898, each composed of series of letters, from a to z. After a quick analysis, we identified the encryption method to be Vigenère, and we deciphered the two cryptograms. The German plaintexts contain references to another cipher system, as well as new keywords for that system, for which there are no corresponding cryptograms in the Genoa collection.

- **5-digit codes with indicator 1847X:** A set of messages composed of groups of 3, 4, or 5 digits, from December 1913 to mid-1915. Those cryptograms have an indicator of the form 1847X (18470 to 18479, usually 18470) as one of the first groups.

- **5-digit codes with indicator 1810X:** A set of messages composed of groups of 3, 4, or 5 digits, from 1898 to November 1913. Those cryptograms have an indicator of the form 1810X (18100 to 18109, usually 18102) as one of the first groups.

- **10-letter codes:** A set of nine messages from August 1914, composed of groups of 10 letters each, sent between the Kaiserliche Marine Admiralsstab (German Imperial Navy Admiralty), German warships Goeben and Breslau, and the German consulate in Genoa.

3.2 Deciphering Diplomatic Codebook 18470 Cryptograms

Following the successful decryption of the Vigenère messages, we first analyzed the cryptograms with the 1847X indicators. In the archive records, a few hundred of them are available. Although plaintexts also appear in the original records, we could not match any of them to a corresponding cryptogram with a 1847X indicator. We found a key document on the subject, *Studies in German Diplomatic Codes Employed during the World War*, written by Charles J. Mendelsohn, and compiled into a War Department report in 1937 (Mendelsohn, 1937). The first of its three sections is named *Code 18470 and Its Derivatives*. It describes the structure of codebook 18470, based on a 1918-19 study by Mendelsohn and a team of cryptographers at the Military Intelligence Division of the General Staff in Washington. The study also includes a few original messages encoded using 18470, as well as the German meaning for the codes in those cryptograms. With those, we were able to reconstruct about 10% of the 18470 codebook and to produce fragmentary decryptions for some of the messages in the Genoa files.

In codebook 18470, while the pages are scrambled, the words inside each page (such as the words with codes between 12100 and 12199) are alphabetically close. Based on this, we tried to guess assignments for unknown numerical codes in pages for which we had other known assignments. A team of linguists investing time on the problem would probably have been able to reconstruct large parts of the codebook and decipher most of the cryptograms, given the availability of hundreds of them. However, such resources were not available to the author. To progress, either a copy of the codebook, or some plaintexts matching the cryptograms were required. A search for matching plaintexts in archives produced only a single message, dated August 1, 1914, sent by the German consul in Genoa, von Herff, to the German Foreign Office. [14]

It reads as follows:

> Nummber 7. Im hiesigen Hafen liegende englische Dampfer der White Star Line und British India Company 'Celtic' und 'Malda' sind von ihren Gesellschaften angewiesen möglichst rasch auslaufen und westlisch.[15]

The plaintext is a report about British ships leaving Genoa westbound. Using the date, the message length, and the correspondents, we were able to locate the original ciphertext in the Genoa files.[16]

The code corresponding to the word *Dampfer* (steamer), 10275, also appears in Mendelsohn's study and has the same meaning. Other codes correspond to words or expressions located in alphabetical positions as expected from Mendelsohn's interpretation of the 18470 code. Based on this, we were able to conclude that not only the messages with the 1847X indicators were indeed encoded with the 18470 codebook, but that they

[14] PA AA, R 19875, Bl. 31. Generalkonsul von Herff an das Auswärtige Amt.

[15] 'In local port anchored steamers of the White Star Line and British India Company 'Celtic' and 'Malda' have been instructed by their companies to leave port as soon as possible and (sail) westbound.'

[16] PA AA - RAV Genua 13, Chiffrierte Telegramme 1914-1915, p. 6.

were encoded without any additional encipherment. This finding was an important step. But while the plaintext also provided the meaning for a few additional codes, this was not enough to progress with the decryption of other 18470 messages in the collection.

We started to look for copies of original codebooks. Copies of various WW1 German codebooks are available at the British National Archives at Kew, including naval codes such as the SKM, captured in 1914 from the German warship Magdeburg. The archives also include a version of code 13040, reconstructed via cryptanalysis by Room 40, and used to encode the (in)famous Zimmermann Telegram in 1917. The successful decipherment of the Zimmermann Telegram, along with German pursuance of unrestricted submarine warfare, contributed to the entry of the United States into the war. However, neither the 18470 codebook, nor the 18102 appear in British, German, or US archives.

In his study, Mendelsohn described how the 18470 codebook was part of a larger family of codes, including the 12444, the 1777, and the 2310 codebooks, all derived from the same division of words and expressions to pages, the pages being reshuffled differently. We could not find any of the 18470 derivatives listed by Mendelsohn in US, British, or German archives. Further research in the British National Archives at Kew produced another document, *The Political Branch of Room 40*, which mentions two other codebooks, 89374 and 3512, captured by the British in Persia in 1915. According to this report, an analysis by the Political Branch led to the conclusion that those two codes stem from the same source, albeit reordered differently.[17]

Several recent papers also link those two codebooks to the 18470 family, and this assumption was strengthened by the fact that Mendelsohn mentions there existed at least one member of that family, unknown to him (Freeman, 2006; Kelly, 2013). Fortunately, a copy of the 3512 codebook is available at Kew.[18]

After obtaining a photocopy of the 3512 codebook, we needed to establish the precise relationship between the 3512 and the 18470, using the known numerical codes from Mendelsohn. Eventually, and after an extensive trial-and-error process, we were able to reconstruct almost the entire mapping between the codebooks. While some random elements of the mapping created some challenges, the compilers of the 18470 derivatives (including the 3512) had applied several regular patterns in the process, which helped us significantly (and also weaken the security of the codebook). After the mapping was established, we wrote a special software and used it to decrypt all the messages encoded with 18470, except for a few names which appear in a special supplement of the codebooks (and for which there is no conversion formula or pattern).

3.3 Diplomatic Codebook 18102 Cryptograms

After successfully reconstructing codebook 18470, we turned to the 1810X cryptograms. Several plaintexts from October and November 1913 announce the transition from the 18102 codebook to the 18470 codebook, and an order to destroy all physical copies of the 18102. Unfortunately, we were unable to find copies of the 18102 codebook in any of the relevant British, German or US archives. An analysis of the ranges of pages showed that the 18102 code could not have been a derivative of the 18470. Codebook 18102 might still be a derivative of the 13040 codebook, as the 13040 was also in use before the war, but there is no evidence in that direction, and further work is needed to check this hypothesis. Lacking a corresponding plaintext for any of the 18102 messages, or a derivative of this code, we were neither able to reconstruct the codebook, nor to decipher any of the cryptograms. Since the 18102 and the 18470 share the encoding of numbers and dates (Dreinummerheft), it might be possible to look for matching plaintext-ciphertexts in the files based on the message serial numbers.

3.4 Deciphering Naval Codebook Cryptograms

The last category is comprised of only nine cryptograms, sent in August 1914, and involving Navy recipients or senders. They consist of 10-letter codes, such as `DUMOSEPIRE` or `CLYHMUIMUS`, with the prefix (the first five letters) of one of the 10-letter codes often used as the prefix in another 10-letter code, or the suffix (the last 5 letters) of one code often used as the suffix of another code. A likely codebook candidate appeared to be the

[17](ADM, 223) ADM 223/773, George Young, Political Branch of Room 40, Section '89374 and 3512'.

[18](HW, 7) HW 7/26 German Codebook Number 3512.

HVB, used for communicating with German merchant ships. While the HVB is primarily a 4-letter code, each code also has a 10-letter equivalent, composed of a combination of a 5-letter prefix and a 5-letter suffix. However, none of the HVB prefixes or suffixes seemed to match any of those found in the Genoa cryptograms. The HVB also had an optional substitution superencipherment.[19]

This substitution preserves the vowel-consonant structure of the original ten letters, and since this characteristic can be used to validate possible outputs, we were able to rule out the possibility that the cryptograms were encoded with HVB with substitution.

The next obvious candidate was the VB, intended for naval and military attaché communications. The VB consists of 5-digit codes. With the assistance of other scholars, the author was able to obtain a photocopy of the VB, as well as a copy of a VB supplement.[20,21]

The supplement describes a mapping of 5-digit VB codes to 5-letter prefixes (representing the first three digits) and 5-digit suffixes (representing the last two digits). Those prefixes matched those found in the Genoa files. Therefore, we were able to map all the 10-letter codes in the collection, into their 5-digit equivalents. However, none of these 5-digit codes would map to words or expressions in VB which have a logical or relevant meaning, indicating that some form of superencipherment had been employed. After all, naval communications were deemed to be more sensitive than regular diplomatic communications. There was no clue, however, about the specific type of superencipherment employed here. At this stage, the research had reached a dead end regarding the 10-letter cryptograms.

After several months of extensive research, we found in the British National Archives at Kew a message sent on August 3, 1914, to the Goeben warship by the Admiralty in enciphered VB. The file consists of a log of English transcripts (translations) of VB messages from 1914, intercepted and deciphered by Room 40. The message from August 3, 1914, is the only one in the file for which the cryptogram is also available. The German plaintext was also available from other sources (Lorey, 1928). Unfortunately, we could not (yet) draw any conclusions from this sample alone.[22]

A breakthrough came from a review of the messages sent in the 18470 codebook, which by then we were already able to decipher. A message from Berlin was sent in 18470 code to Genoa on August 1, 1914, with the following instructions:

```
Nummer 9 unter Bezugnahme auf Telegr.
Nummer 10.  Schlüsselzahlen zu Marine
Chiffres lauten:  Schlüssel B: 469,
reserve B: 718.  Auswärtig.  Amt.[23]
```

In a serious breach of security, this message specifies the primary key (469) as well as the reserve key (718) for the Navy's cipher. We hypothesized that those could be the key for some superencipherment. The next step was to look for references to any of the two keys, hoping this might help to identify the type of superencipherment. We were unable to find any reference to key 469. However, the author vaguely remembered a mention of key 718, in the multitude of archive files already reviewed. Luckily, an extensive survey of all the material gathered so far resulted in the (re)discovery of a reference to key 718, in Mendelsohn's study (Mendelsohn, 1937). The third chapter lists several methods for the superencipherment of codes. One of them is based on *sliders* (*Schieber* in German), which consist of a set of three substitution slides. Those slides map some of the digits of the 5-digit codes to other digits according to some random pattern. A 3-digit key specifies the starting position of each one of the three sliders. Mendelsohn provides the ordering for a set of 3 sliders used before the war and until 1917, described in Table 1 (Mendelsohn, 1937). In this example, the sliders are set to key 718, and are to be applied on the second, third, and fourth digits (the first and last digits are kept unchanged).

Interestingly, the example given by Mendelsohn uses key 718 which happens to be the reserve naval key mentioned in the 18470 message. This was a clear indication that the 10-letter cryptograms might have been superenciphered using

[19](ADM, 137) ADM 137/4320, Chiffresschlüssel H.V.B. 1913.

[20](ADM, 137) ADM 137/4374, Verkehrsbuch (VB) 1908.

[21](ADM, 137) ADM 137/4314, Verkehrsbuch Supplement.

[22](ADM, 137) ADM 137/4065, Log of intercepted German signals in Verkehrsbuch code from various sources 1914-1915, entry 113.

[23]'Number 9 with reference to telegram number 10. The keys for Marine cipher are: Key B: 469, reserve B: 718. Foreign Office.'

Original Digit	Second Digit Becomes	Third Digit Becomes	Fourth Digit Becomes
0	7	1	8
1	0	9	3
2	9	4	4
3	2	6	6
4	6	2	5
5	3	7	2
6	5	3	7
7	8	5	1
8	1	0	9
9	4	8	0

Table 1: Slider for VB

sliders. Next, we tried to decode some of the 10-letter cryptograms using the sliders with key 718, but this failed to produce any plausible plaintext. Another option was key 469. We tested that slider key on one of the cryptograms and obtained a few German words related to *Kohle* (coal), a topic very much relevant to the escape of the Goeben. When applying the sliders with key 469 to other cryptograms, we could finally recover plausible plaintexts. To further validate those findings, we tried to apply the same slider method to the message from August 3, 1914, sent from the Admiralty to the Goeben. While this message could not be deciphered using key 469, further analysis showed that another key was applied, namely 5288, with the 3rd slider (at key position 8) also being applied to the fifth digit (in addition to being applied to the fourth digit). This message reads as follows:

```
August 3 Bündnis geschlossen mit
Türkei Goeben Breslau sofort gehen
nach Konstantinopel bescheinigen.
```
[24]

We had thus achieved a complete solution for the elusive 10-letter naval cryptograms in the Genoa collection. We were now certain that those consisted of VB codes superenciphered with sliders, using key 469.

3.5 New Genoa Files

Our project did not end here. One year after successfully deciphering the cryptograms in the first six files, we were able to obtain three new files from the Genoa collection in the PA AA. Two of them included plaintexts, many of which could be matched to original 18470 cryptograms based on their serial numbers. The matching could not be done before as the serial numbers appear encoded in the cryptograms. Further analysis showed that those new files include plaintexts for about 40% of the 18470 cryptograms, and it was possible to validate that they had been (mostly) corrected deciphered.[25,26]

A third file contained messages from 1910 encoded using VB with sliders. Surprisingly, those could be decrypted using slider key 469, which indicates that this key was in effect for several years and until the war broke, highlighting a severe breach of security.[27]

Those decryptions further confirmed the correctness of our solutions for the 1914 naval messages in the collection.

4 The Contents of the Cryptograms

The "RAV Genua - Generalkonsulat Genua" collection at the PA AA covers the period from 1867 to May 24, 1915, when the German consulate was closed after Italy entered the war on the side of the Entente powers. It also covers the period from 1921, after the consulate reopened, until the end of World War 2. Our research focuses on the first period, and especially on the years 1913, 1914, and 1915. The records cover a wide area of topics, including administrative and legal matters (such as passports and visas), protocol, local politics, naval intelligence, economy, trade, and shipping.

Of particular interest are the decryptions related to three subjects, namely the declarations of war in summer 1914, the role played by the consulate in gathering naval intelligence, and its role in assisting the Goeben and Breslau warships to escape to the Dardanelles. The latter event had a significant impact on the war in the Mediterranean Sea and the Middle East.

4.1 No War Without Declaration

World War I was one of the last modern, major military conflicts in Europe which started with formal declarations of war, by all parties involved. Countries felt obliged to formally declare war, as part of an official international protocol defined

[24] 'August 3: Alliance with Turkey concluded. Goeben and Breslau should at once sail to Constantinople.'

[25] PA AA - RAV Genua 74, Kriegsgefahr 1914-1915.

[26] PA AA - RAV Genua 77, Krieg, Militärsachen 1914-1915.

[27] PA AA - RAV Genua 68, Chiffres nach d. Marine 1907-1914.

at The Hague Peace Conference of 1907, and for internal legal and political reasons. With a formal declaration, a country could start mobilizing its army. Also, military and merchant navy ships had to be informed that they should leave hostile ports, to avoid being seized. As this was usually done before issuing the formal declaration of war, any signs of movement of ships in times of crisis might indicate an upcoming declaration of war. The Genoa collection includes a series of messages informing the consulate of the various declarations of war, and of their impact such as the freedom of movement of German nationals. From the first declaration of war between Russia and the Austro-Hungarian Empire, and throughout August 1914, the tensions escalate, and this is reflected in the communications. For example, on August 2, 1914, the following message is sent from the German Foreign Office to Genoa:

```
Nummer 8.  Durch allerhöchst
kabinettsorder ist Mobilmachung
angeordnet.  Bitte deutsche Schiffe
im dortig Amtsbezirk ohne rücksicht
auf Geheimhaltung weiter warnen
und Dienstpflicht zur Rückkehr
auffordern.  Jagow.
```
[28]

4.2 Naval Intelligence

A large number of cryptograms relate to naval intelligence collected mainly from public sources, such as newspapers, or German nationals returning from British and French colonies. Movements of ships, including warships as well as merchant ships transporting troops, are routinely reported. An example of such a report is given in Section 3.2.

4.3 Assistance to the Goeben and Breslau Warships

The most interesting findings in the decrypted records are about the extensive assistance given by the German consulate in Genoa (as well as other German representations in the region), to the German warships Goeben and Breslau in their escape to the Dardanelles, in August 1914. To extend its presence and influence in the Mediterranean Sea, the German Empire had before the war sent to the region one of her most modern warships, the battle cruiser Goeben, together with the light cruiser Breslau, under the command of Rear Admiral Souchon. Given the vast superiority of the British and French fleets in the Mediterranean Sea, those two lone ships were threatened to be isolated, captured or destroyed, as the war broke out. Souchon was first ordered to escape via the Gibraltar straights but instead decided to attack French facilities in North Africa. After the attack, with the westbound route being blocked, he was ordered to reach the Dardanelles, following the signing of an alliance between the Ottoman Empire and the German Empire in the beginning of August 1914. To successfully escape vastly superior enemy forces, the Goeben needed large quantities of coal, required to reach higher speeds. Supply of coal in sufficient quantities could only be found in Italy or obtained from German merchant ships. For that purpose, the German Foreign Office instructed its local representations to assist the Goeben and Breslau to secure large quantities of coal. This effort is reflected in several messages, encrypted with the 18470 codebook, as well as with the VB with superencipherment. For example, the following message was sent on August 1, 1914, from von Herff, the consul in Genoa, to Rear Admiral Souchon:

```
Goeben - Messina.  Auf Ersuchen von
Breslau:  Kohlendampfer ist nicht
vorhanden.  Deutsches Kohlendepot
ist bemüht, möglichst viele Kohle
kaufen, hoffen Montag 2000 Tonnen
gemischte gut Kohle zu sammeln und
Bescheid zu geben.  Welche Menge von
Kohle gebraucht und wohin zu liefern?
Herff
```
[29]

Other records describe the requisition of German merchant ships and their coal, the securing of funds for transactions, and negotiations with Italian authorities. Eventually, the Goeben and Breslau were able to obtain significant quantities of coal, allowing them to escape the British and French fleets, and to reach the Dardanelles. They joined the Ottoman fleet under the Ottoman flag. Their attack on Russian facilities, carried indepen-

[28] 'Number 8. By highest cabinet decision mobilization has been ordered. Please continue warning German ships in the local district, regardless of confidentiality, and request those liable for [military] service to return. Jagow.'

[29] 'Goeben - Messina. At the request of Breslau: Coal steamer is not available. German coal depot working hard to buy as much coal as possible and expects to collect 2000 tons of mixed, good quality coal on Monday, and will report on it. How much coal is needed and where to deliver? Herff'

dently of their Turkish counterparts, later precipitated the entry of the Ottoman Empire into the war (Van der Vat, 2000). As a result, the Entente powers had to divert significant resources to the Mediterranean Sea and the Middle East, including for the catastrophic Dardanelles offensive in 1915. The critical role played by the consulate in Genoa is for the first time exposed in the decrypted messages from the Genoa collection.

5 Conclusion

This research highlights inherent weaknesses in German cryptographic methods and procedures for diplomatic and naval communications at the beginning of WW1, as follows:

- Most of the confidential diplomatic communications relied on codebooks, which were in use for long periods of time. Also, the compilers of codebooks often used regular patterns, rather than fully random patterns, to map certain elements of the codebook to their equivalent numerical codes, thus facilitating the work of adversarial codebreakers.

- Instead of issuing entirely new codebooks, the German cryptographic services created new variants of existing codebooks by only modifying the order of their pages. As a result, the capture of one codebook was often enough in order to reconstruct other related codebooks.

- The key for the superencipherment of one codebook was often transmitted using another, possibly compromised codebook. Moreover, the superencipherment methods, as well as the keys, were infrequently modified.

As a result of those weaknesses, the author was able to decipher the vast majority of the Genoa encoded traffic, using methods which are very similar to those employed by Room 40 and other WW1 codebreaking agencies. The decipherment of the cryptograms in the Genoa collection also exposes new historical material related to key developments and events in 1914-1915. Further research is underway to analyze the contents of the messages, and their historical context and significance.

References

ADM. 137. *Admiralty: Historical Section: Records used for Official History, First World War*. The National Archives.

ADM. 223. *Admiralty: Naval Intelligence Division and Operational Intelligence Centre: Intelligence Reports and Papers*. The National Archives.

Peter Freeman. 2006. The Zimmermann Telegram Revisited: A Reconciliation of the Primary Sources. *Cryptologia*, 30(2):98–150.

Paul Gannon. 2010. *Inside Room 40: The Codebreakers of World War 1*. Ian Allan Publishing Ltd.

HW. 7. *Room 40 and successors: World War I Official Histories*. The National Archives.

Saul Kelly. 2013. Room 47: The Persian Prelude to the Zimmermann Telegram. *Cryptologia*, 37(1):11–50.

George Lasry, Ingo Niebel, Nils Kopal, and Arno Wacker. 2017. Deciphering ADFGVX messages from the Eastern Front of World War I. *Cryptologia*, 41(2):101–136.

Hermann Lorey. 1928. *Der Krieg in den türkischen Gewässern: Bd. Die Mittelmeer-Division*, volume 1. ES Mittler.

Charles J. Mendelsohn. 1937. *Studies in German Diplomatic Codes Employed during the World War*. War Department, Office of the Chief Signal Officer, Government Printing Office, Washington, DC. Register 191.

PAAA. c. 1915. *RAV Genua - Records from the German General Consulate in Genoa*. Politisches Archiv des Auswärtigen Amtes.

Hermann Stützel. 1969. Geheimschrift und Entzifferung im Ersten Weltkrieg. *Truppenpraxis*, 7:541–545.

Geoff Sullivan and Frode Weierud. 2005. Breaking German Army Ciphers. *Cryptologia*, 29(3):193–232.

Dan Van der Vat. 2000. *The Ship that Changed the World. The Escape of the Goeben to the Dardanelles in 1914*. Edinburgh.

Learning Cryptanalysis the Hard Way: A Study on German Culture of Cryptology in World War I

Dr. Ingo Niebel
Historian and journalist
Kasparstr. 10
50670 Köln, FR Germany
ingo.niebel@berriak-news.de

Abstract

The history of World War I is well documented, but a comprehensive study of German cryptology during that epoch is yet to be undertaken. Owing to the silence of German cryptologists and intelligence officers, this topic remains almost untouched to date. Hence, a perspective on the role of German cryptology in World War I comes mainly from British and US authors, but generally not from German sources. This paper provides an overview of an ongoing research, focused on the German culture of cryptology between 1871 and 1918. It is based on the assumption that a fixation on cryptography is the essential part of that cryptology culture of those times. From 1914 on, Germans had to learn cryptanalysis the hard way. Questions regarding who started this learning process, how it developed, the failures and successes it produced, and the structures that were involved in the process, are yet to be answered. This investigation links the current state of the art with data obtained from the archives. Connecting cryptology with intelligence and technology, it also evaluates its impact on decision-making. Finally, understanding the antecedent German culture of cryptology enables us to investigate that of its descendants – spanning the decades from World War II to the Cold War, as well as today's "information security culture".

1 Introduction

This article resumes the research to a still unwritten monograph on the German culture of cryptology (1870/71-1918/19), whose investigation intended to reconstruct the historical context of the intercepted and encrypted German telegrams collected after World War I by the US cryptanalyst, James R. Child. This collection was successfully decrypted by George Lasry, Nils Kopal, and Arno Wacker (Lasry et al. 2017). An outcome of that investigation was a realization that we lack a comprehensive study of German cryptology during the second German Empire (1871-1918).

Our investigation starts from David Kahn's statement on this subject: "German cryptology goose-stepped toward war with a top-heavy cryptography and no cryptanalysis." (Kahn 1996:pos. 5347). His conclusion underscores a specific aspect, namely: talking about German cryptology between 1870 and 1914 is clearly an oxymoron.

Today, we understand cryptology as a science with well-defined theories, methods, and results, consisting of cryptography and cryptanalysis as its two main pillars. As a third, we can add steganography. This, however, is a very modern (20th century) Anglo-Saxon definition, which does not match the German understanding of secret writing and deciphering prior to and at the beginning of World War I. In fact, the German term "Kryptologie" was neither introduced in German encyclopedias nor in the Duden dictionary until the end of the 20th century. The German "Geheimwissenschaft" (secret science) is the literal translation of the cryptology, which in general referred to occultism, and is therefore unsuitable for use in the modern context.

The research becomes even more complicated because prominent German cryptanalysts during both World Wars remained silent and their line of work was never publicly discussed. All what we know about the German cryptanalytic efforts, successes, and failures originate mainly from

Proceedings of the 1st Conference on Historical Cryptology, pages 65– 75,
Uppsala, Sweden, 18-20 June, 2018

Anglo-Saxon publications and sources. Kahn's books and articles are only a tip of that iceberg, and the German perspective awaits exploration. Uncovering this perspective will provide a better description of the German culture of cryptology.

Focusing on the cultural aspect is of importance because – though the science of cryptology itself can be applied irrespective of the language in use or the nationality of those using it – the national circumstances define the characteristics of its development and use; for instance, whether or not civilians are permitted to use this science.

"Culture is the art ('ars', 'téchne'), through which societies secure their survival and their evolution in an overwhelming nature", states Hartmut Böhme. (1996:53). In our case, the culture of cryptology can be understood as the art of utilizing this science in a hostile environment comprising of alien interests to convey information and intentions in secret. This definition can be applied to all countries involved in a given war during this time period and used cryptology to gather intelligence and plan their military and diplomatic operations.

However, we have to "nationalize" every culture of cryptology because it is defined by the cultural, social, political, and military characteristics of each country. All these factors may explain why the German culture of cryptology in 1914 was defined exclusively by a presence of cryptography and a near absolute absence of cryptanalysis. German decision-makers therefore came to learn of this imbalance the hard way.

During the Russian offensive against Prussia in August 1914, German reserve army officers – at great personal risk after ignoring several orders – discovered the advantages of signal intelligence (SIGINT) in combination with cryptanalysis. This new kind of intelligence enabled their commander to win the battle of Tannenberg. Therefore, this victoryalso shows that the culture of cryptology entails a learning process. In the aftermath of this military success, German commanders initiated a large, complicated, and inconsistent learning process to improve their interception and cryptanalytical skills.

German military and diplomats learned the benefits of cryptanalysis the hard way, because – around the same time – they had already lost their first battle at the Marne river in France, as a consequence of French cryptanalysts breaking their codes. Despite all the efforts towards improvement, Germany would ultimately lose the war because her vulnerable codes would provide critical information to her enemies at crucial junctures. So, the history of the German culture of cryptology during that epoch is about how Germany's leadership learnt from a defeat it unknowingly suffered even before the imperial troops crossed the borders to Belgium, Luxembourg, and France.

Although British, French, and US went through their own learning processes, whose outcomes are known, it is worth describing how the Germans managed to transform their cryptography into cryptology by incorporating cryptanalysis. Therefore, we have to look for the various structures and personnel that intervened in this process.

On the one hand, we have the governmental structures and agents concerned above all with cryptographic matters. On the other hand, it is surprising how freely civilian "amateurs" wrote about cryptology and even criticized the government. That raises further questions, namely: Who were they, how could they acquire knowledge of cryptology, and how did the governmental institutions react to this kind of non-governmental cryptology? Looking for these answers, we have also to take into consideration the impact of their work on intelligence, as well as military and political decision-making.

Nearly a 100 years after the end of World War I, an investigation focused on the German culture of cryptology matches actual studies on what we call now the "information security culture". Maria Bada und Angela Sasse (2014) used this term when they analyzed how to improve Cyber Security Awareness Campaigns. The information security culture requires, according to the authors, on the one side, knowledge and awareness, on the other, positive information security behaviors. Though since 1914 our technology has improved a lot, the user remains to be the weakest link, not so much his hard- and software.

All these aspects should be taken into consideration if the goal is not to write a purely technical history of German cryptology concentrated only on its theories, methods, and

results, but also to link it with other fields and disciplines. That approach will be explained in the following three parts.

In the following section, I will present the assumptions on which I have based this investigation. In two subsections, my aim is to define my understanding of intelligence and why it is still a "missing dimension" in historiography. This in turn leads to the second subsection, which encroaches upon the German "culture of cryptology". The third section focuses on telecommunication and its impact on cryptology as in the earlier 20th century, the field of telecommunication was a relatively new with unknown advantages and disadvantages. Finally, I shall refer to the sources, with a focus on the the problems that historians encounter when using records obtained from the intelligence services.

Following which, I shall present some of my first results in chronological order. The four subsections describe different aspects of the German cryptology culture. It begins with specific terms Germans referred to in cryptology encyclopedias. The second subsection resumes the case when a German citizen publicly accused the Foreign Office of having plagiarized his code-system. The quarrel reveals that the Foreign Office showed no concern for security. The Crypto-Crisis of 1917 served two purposes, on the one hand, it discussed the problems a historian deals with when he or she has to rely on intelligence records; on the other, it indicated also how such a source can push the investigation forward. The last subsection provides a firsthand explanation as to why there is still no comprehensive study on German cryptology.

The fourth and last section brings us back from the past to the presence. It provides some hints as to why the German cryptology culture of 1914/1918 is linked in some way to the today's "information security culture". This would also provide some proposals for further investigations.

Due to time and space restrictions, and to the fact that this article resumes the status of a current investigation, it raises no claim to completeness.

2 Methods

Since the first decade of the 21st century, we count with declassified records and information recovered from encrypted radiograms. The US foreign secret service, the Central Intelligence Agency (CIA), and its technological partner, the National Security Agency (NSA), published historical documents related to cryptology including the names of persons, on their webpages. In parallel, the community of non-governmental researchers, who dedicate themselves to historical cryptology, were seeking unsolved messages from both World Wars. So, on the one hand, historians and cryptologists have access to new sources, on the other, cryptanalysts provide "new" records and insights by recovering and solving forgotten cryptograms. (Lasry et al. 2017, Sullivan and Weierud 2005) All these new sources need to be put in a greater academic context.

The ongoing investigation is based on two suppositions: Firstly, every state creates the intelligence community it considers necessary. Therefore, the organizational charts of its ministries and armed forces can reveal the importance given to the secret and cryptologic services. Investigating these structures, also sheds light on how the government allowed privateers to handle cryptology.

Secondly, the saying “once an agent, always an agent” defines the other mainline of research. It focusses on the persons who worked for one or various secret and/or cryptologic institutions. Both research fields are connected by seeking the interactions between institutions and their personnel. That implies that one must follow the organizational change in the departments. It would be interesting to know the social, professional, and cryptologic background of the personnel.

Today it is common to talk about the intelligence community by referring to all governmental, military, and police institutions dealing with intelligence. In parallel, we have the cryptology community, composed also of officials, privateers, and their departments or firms. In contrast to their British and US counterparts, the German cryptologists remain relatively unknown. This fact makes both cryptology and intelligence a part of a "missing dimension" in historiography.

2.1 Intelligence, a "Missing Dimension"

Spies were additional pawns on the great chessboard where the European powers played the tragedy of World War I. As previously mentioned, some crucial moves performed by the decision-makers of one or the other sides, were based on the intelligence gathered by their radio stations and cryptanalysts. The question lies in understanding to what extent this kind of intelligence influenced military and political decision-making.

In the 1980s some German and British authors had already mentioned intelligence as being the "missing dimension" in political and military historiography. (Höhne 1993:7) After analyzing several dozen international publications on the topic, Larsen (2014:282) concludes that this military conflict "remains in many ways underexplored by intelligence scholars." In fact, he found less than a handful of German works on that subject.

This problem is caused partly by the intelligence agencies themselves, because it is part of their nature to act secretly, without always acting in a legal or morally correct manner. So, for the sake of security, the intelligence services have good reason not to share their records with historians who, on the other, without these documents could not evaluate how large the "missing dimension" really is.

Although intelligence services release their records from time to time, historians cannot expect to receive complete files. Due to the fact that deception and cover-ups belong to the working tools of secret services and their assets, scholars are forced to crosscheck every disclosed information. Moreover, this makes their investigations more complicated. On the other hand, just Paul Gannon (2010) proved, referring to the British interception log books, that His Majesty's codebreakers could read enciphered German Naval messages already months before the war broke out and the Room 40 was installed. In consequence, his finding contradicts the official version and requires reviewing of the prewar history of British cryptological efforts.

Another complication derives from the necessity to define what intelligence really means. "I define intelligence in the broadest sense as information" concluded Kahn (2001).In my mind, information becomes intelligence according to the importance that is given to e.g., things, individuals, organizations, data, messages at a concrete time and for a specific aim.[1]

For delimiting intelligence as a "missing dimension", I consider its three principles very helfpful, which according to Kahn (2001), describe its function. First, it helps to optimize one's resources. Second, intelligence "is an auxiliary, not a primary, element in war". Thirdly, it is "essential to the defense but not the offense". The yet mentioned battles of the Marne and Tannenberg seem to confirm Kahn's theory. At this point we have the intersection between intelligence and cryptology, but it is not necessarily the only one.

In 2016 the German Historical Institute London (GHIL) held a conference on "Cultures of Intelligence". In that context, the GHIL stated that "Culture was understood to include the role of intelligence services in society and/or the state, the representation of intelligence in the public sphere and among the members of the military/intelligence community itself, as well as the interests, assumptions, and operating procedures of intelligence." (Sassmann, Schmidt 2016:135) This definition can be used to define the German culture of cryptology.

2.2 About a German Culture of Cryptology

It is difficult to answer whether it is "a" or "the" German culture of cryptology because it depends on the epoch. When we refer to a time before 1870/71, we should preferably use "a", because the culture in question may be linked to a specific kingdom on German soil. For example, Rous (2011) analyzed the Saxon culture of cryptology in the 17th and 18th century. But we unfortunately lack a similar investigation on the Prussian culture prior to 1870.

When the Germans created their second empire, the Prussian king got also their emperor. As a result all key areas such as the military, foreign, economic and home policy, for instance, became centralized to the Prussian capital,

[1] This is another very Anglo-Saxon definition of "intelligence", it differs to how German secret service officers used to interpret "Information" which, according to them, becomes "Nachricht" (intelligence) when it is confirmed by other sources.

Berlin. In the light of lacking documents, we have to assume that the overwhelming presence of cryptography and the absence of cryptology reflects the Prussian culture of cryptology.

A characteristic of the new Reich was that the ruling aristocracy managed to integrate the bourgeoisie in the new project. Instead of democratizing the state, by getting rid of the aristocrats, the bourgeois supported the monarchy. So entrepreneurs and bankers pushed Germany's industrialization and implementation of new technologies. Their crème de la crème were further ennobled. "Nonetheless the Wilhelminian Germany was still an authoritarian society with a static social order of considerable stickiness", states the historian Wolfgang Mommsen (1995:71).

This and further investigations on the social order should be taken into consideration, as they might explain the absence of an intelligence and cryptologic community, and also the incompetence of the armed services and the Foreign Office to develop intercepting and codebreaking capabilities, as it had occurred in the United Kingdom. The known facts indicate that listening to foreign conversations and reading confidential messages could have put the above mentioned rigid order and separation of powers at risk.

From this point of view, the use of cryptography seemed have come into place as a measure to guarantee the established order. In fact, only officers and high ranking civil servants were allowed to cipher and decipher encoded messages. Following that logic, another measure was to avoid the promotion of cryptanalytic skills.

Germany's oldest cryptographic institution was Chiffrierbureau of the Foreign Office. It was built in 1814 and belonged to the ministry's Zentraldepartement. (PAAA 1936), thereby putting the Chiffrierbureau and its personnel in the focus of the current investigation. During that time, the head of the government, the chancellor, was responsible for foreign policy. But his role was limited, as he was only a counselor to the monarch.

The Kaiser acted also as the commander-in-chief of the armed services. It is known that he used cryptography, but the extent to which it was used remains unknown. He supposedly got the codes and keys from the cipher-bureau. The Foreign Office provided the naval attachés with codes, too.

One research line focuses on the indivuuals within the the Army and the Navy structures who dealt with cryptography. The other research line concentrates on the "Abteilung für Nachrichtenmittel" (department of communication means)[2] of the Royal Prussian War Ministry, another on the "Reichsmarineamt" (Empire's Navy Office). Both produced codes and ciphers, and delivered them to the troops and the civil authorities. They primarily had administrative functions, not operative. Therefore, another research line looks for the importance the armed services gave to cryptography in the education of their officers.

The common denominator of these three governmental institutions was that they favored cryptography, reducing cryptanalysis to a "guessing" or buying codes and keys on the black market. This German credo of cryptography expressed itself by the main code books such as the Handelsschiffsverkehrsbuch (HVB), the Signalbuch der Kaiserlichen Marine (SKM) and the Verkehrsbuch (VB). These became one of the essential parts of the very specific German culture of cryptology

Opposite to the governmental cryptographic structures we find a considerable number of non-governmental cryptologists, who along the 19th and at the beginning of the 20th century, published a certain number of articles and books on secret scripts and their decipherment. This allowed people interested in the specific field access information without major problems.

2.3 Telecommunication and cryptology

Telecommunication is in many ways essential for understanding the development of the German culture of cryptology. On the one hand, the new technology changed how people handled communication. Telegraph, radio and telephone replaced the traditional royal messenger services, as the depeches were delivered faster by wire,

[2] The German "Nachrichten" can mean "news", "intelligence", "signals" or "communications". That makes is complicate to decide whether a "Nachrichtenoffizier" is an "intelligence" or a "signals/communications officer".

wave and cable. This mode of communication seemed to secure to everyone who believed that his or her codes were unbreakable.

At the very beginning of World War I, the British destroyed the German transatlantic telegraph cables. So they forced the Germans to communicate via radio with their colonies and embassies or by telegraph connections. These connections could be monitored by British telecommunication companies. In both cases, London could intercept the communication and try to read the encoded messages.

For this project it is necessary to take into account this fact because there are several German thesis in which lawyers addressed the legal and strategic issues of such a violation of the postal secrecy long before the Royal Navy made their worries real in 1914.

Another important aspect is that the importance of SIGINT can only be understood if we know the technical equipment of the signals troops and its limitation. Because of the technology, climate and geography, messages had to very often be repeated. This increased the possibility of a radiogram being intercepted. In this way, experienced cryptologists and analysts could complete crippled messages.

In this context it is also necessary to refer to the technical efforts to mechanize the encoding and decoding process. Although the German Army would purchase the Enigma only in the 1920s, some documents indicate that, at least, its theoretical development might have already started before World War I.

2.4 "Ad fontes" - To the Sources

As I mentioned above, Kahn's publications on cryptology are essential because they frame the investigation. Articles such as those written by Stützel (1969), Brückner (2005), and Samuels (2016) give further information on facts and sources regarding the German cryptology. In contrast, selected monographies on the French, British, US cryptology and SIGINT describe the "hostile environment" in which the German culture of cryptology started to grow in the summer of 1914.

The investigation takes into account, how the military commanders integrated cryptology SIGINT and this kind of intelligence gathering into their decision-making. This in itself constituted another learning process because in 1914 they had still not changed their plan of attack that had been drawn up in 1905 under very different circumstances. Nine years later, they still believed they could win the war in the west by the same manner as in 1870/71. They thought that once again infantry, artillery, and cavalry plus modern weapons would bring victory, but not the less regarded signals troops.

The information that is not included in the publications has to be found in the archives. This makes the project difficult because the principal Prussian-German military archives vanished during World War II. The records of the different cryptologic departments were either destroyed or captured by the victors who delivered them to their cryptologic or intelligence services. As mentioned before, the CIA and NSA declassified such documents, as also did the British services. In consequence, the respective holdings could aid in recovering such information that is lacking in the German archives.

A first look into the Political Archive of the German Foreign Ministry (PAAA) showed that the entire holdings of the Chiffrierbüro have disappeared. The existence of the cipher-bureau is only confirmed because its name appears in the organizational charts of the ministry, and on several documents which can be found in other holdings. If there has once been a correspondence, for example, between the cipher-bureau, the Army and the Navy on codes, it not longer exists, at least not in this archive. The unpublished memories of cryptologists such as those of Adolf Paschke somewhat enlightened the gloomy situation.

The situation in the German Federal Archive, the Bundesarchiv, is slightly different. On the one hand, there are only a few sources related to the cryptography in the Army, on the other hand there is much more information on the cryptological work done by the Navy before and during World War I. The first impression after a stay in the Military Archive of the Bundesarchiv at Freiburg is that there is more information than I expected.

Due to the fact, that the archives of the Prussian Army and the War Ministry were destroyed, there is some hope that the correspondent holdings of the Bavarian State Archive could close this gap in some way. The

research in the regional archive of North Rhine-Westfalia provided some information on how the Prussian Interior Ministry introduced cryptography in its communication with the regional military institutions.[3]

In this context, the "William F. Friedman Collection of Official Papers", as called by the NSA, is of particular interest. It contains more than 7,600 documents spanning over 52,000 pages. The collection can be searched and downloaded as a PDF via Internet.[4] Due to the close relationship between the cryptologic and intelligences communities of the US and the UK, the NSA collection must be seen in connection to the respective holdings in the British National Archives at Kew, as some German related documents of supposed US origin were gathered in fact by their English "cousins".

In this context, and from a purely academic point of view, the decrypts of intercepted German radiograms published by Lasry et al. (2017) present a special kind of document. To some extent, they are "retranslations" from an original text which was encoded and sent by radio. Albeit the cryptanalysts broke the code and got a plaintext again, the latter should be compared with the original message, if possible.

In any case, researchers need an organizational chart of the institution in question. This is essential for two reasons. First, an organizational chart helps to identify the departments concerned with cryptology inside a ministry, which can be helpful if the search using keywords was not successful. Second, an organizational chart uncovers the position of a cryptologic section in the respective structure. It makes a difference if it is attached directly to the minister's bureau or if it is a department or if it positioned on a lower level being only a section or a subsection. So, the archives and their holdings themselves generate valuable "intelligence" on the German culture of cryptology.

3 How Germans learnt cryptology

3.1 Ignoring cryptanalysis and SIGINT

In search of reasons to explain the German fixation on cryptography, I consulted several editions of the popular encyclopedias such as Meyer's Konversations-Lexikon and the Brockhaus. Between the 19th and 20th centuries, both publications not only ignored the existence of the word "Kryptologie", but also indicated that the term should be replaced by "Geheimschrift" or "Chiffre". Since the beginning of the 19th century, the cryptologic horizon seemed to be limited to cryptography.

This limitation is curious because just a retired officer published a classic on cryptology in 1863. Major Friedrich Wilhelm Kasiski titled his book "Die Geheimschriften und die Dechiffrir-Kunst" (Secret scripts and the art of decipherment). As the title indicates, it reflects upon our modern understanding of cryptology and is based on cryptography and cryptanalysis.

The facts collected on Kasiski indicate that he had nothing to do with the cryptology while in the military. Though he dedicated his book to the acting war minister Albrecht von Roon, the author addresses him only as his former commander. It seems that the military hierarchy decided to ignore both Kasiski's cryptological efforts and SIGINT as well.

"In Germany to be sure, the General Staff thought of such possibilities, but down to the outbreak of World War I had undertaken practically nothing. Even in the Foreign Office nothing had been done in this direction which was worthy of mention" states the signals officer Wilhelm Flicke.[5] Only during the battle of Tannenberg in 1914, the high command would discover the advantages of SIGINT and cryptanalysis. It took several months until the new possibilities were included into its military organization.

3.2 The Chiffrierbureau Accused of Plagiarism

Due to the lack of documentation, it is assumed that the Foreign Office and its

[3] LAV NRW, Abteilung Rheinland, BR 0021 Nr. 107, 108

[4] https://www.nsa.gov/news-features/declassified-documents/friedman-documents/, last seen 15.01.2018

[5] https://www.nsa.gov/news-features/declassified-documents/cryptologic-spectrum/assets/files/beginnings_radio_intercept.pdf, p.21.

Chiffrierbureau underestimated cryptanalysis and the interception of foreign messages by technical means. Security did not seem to feature high on their list of priorities.

It seems strange, at first, that until the end of World War I the Auswärtiges Amt published in the "Handbook for the German Reich" the identities of all the officials who worked for its Chiffrierbureau. This extent of governmental transparency included the names of individuals who were civil servants and all the medals they had been awarded. Any foreign intelligence serviceman would have been grateful to get his hands on the list of potential targets, who had access to classified material.

Secondly, neither the Ministry nor the cipher-bureau seemed to be concerned when in 1872 the printer M. Niethe accused both to have stolen his code-system. The fact that several editions of his book can be found in various German public libraries proves his enthusiasm but also that neither the Reich government nor the Auswärtiges Amt tried to silence him using censorship, albeit at one point during the conflict Niethe was summoned by the police.

The background information on the cipher-bureau personnel mentioned in the Handbook, and the Niethe case are the basis for further investigation on the culture of cryptology followed by the Auswärtiges Amt.

3.3 The Crypto-Crisis of 1917

The publication of the Zimmermann-telegram in spring of 1917 not only brought the US into the war but also exposed the opinion of the Auswärtiges Amt about the security of its codes. The incident caused a major discussion reagarding cryptography between the Foreign Office, High Army Command, the Army and the Navy. The “crypto-crisis” can be considered also as the endstart of the German cryptology because from that point on, cryptanalysis was used as a means to test the strength or weakness of German codes.

On 23 March 1917, the secretary of State, Alfred Zimmermann, wrote to the representative of his Foreign Office at the General Headquarters, the baron Kurt von Lersner:

"Decipherment of these telegrams is simply impossible even for the most clever specialists. It can only result if the entire cipher is betrayed or essential parts and keys come to the knowledge of a foreign government. Of course, there is no absolute security against betrayal and the only aid is the frequent change of cipher and of keys, which is abundantly provided for here."[6]

This information on the Foreign Office's culture of cryptology is provided by a document kept in the above-mentioned Friedman Collection. The NSA labeled it "CRYPTOGRAPHIC SYSTEMS USED BY GERMAN FOREIGN OFFICE; THE ZIMMERMAN [sic] TELEGRAM.” A handwritten remark on the first page of the PDF indicates that it belonged to a folder where Friedman stored various information on the Zimmermann-telegram. This thereby leads to the beginning of the problem.

The NSA, as the CIA, does not scan entire folders but only documents. At this point, we see again the primacy of intelligence and information over the archival context of a document, as described in chapter 2.4. From the historical point of view we are not dealing with an original but with a copy, meaning, an English translation.

Though the translator seemed to be a professional -he or she even reproduces the layout of the German original- but we are unaware of how Friedman got possession of the document. Nor do we have further information on the remaining original German texts. Despite all these questions, Zimmermann's statement and other correspondences scanned into the PDF seem to be genuine because they are supported by the article Stützel (1969) mentionededited in a West German military publication.

In 1917, Stützel was a "lieutenant of the reserve", as we can read in one of the translated letters. He proved that in terms of the strength and security of its codes, the quoted assumption of the Foreign Office was inaccurate. Stützel intercepted and solved the encrypted messages sent between the Auswärtiges Amt and the German Embassy at Madrid. His discovery generated the mentioned discussion on insecure codes.

This incident is important because it uncovers different aspects of the German cryptology culture. First, it stresses the role of the

[6] The PDF’s filename is 41716799075610.pdf

Chiffrierbureau as the unique provider of diplomatic codes. Second, to believe that its codes are unbreakable can be considered as ignorance but it also expresses the inflexibility that was characteristic of imperial Germany. Third, itthis above mentioned stickiness made it impossible that the governmental structures reacted quickly regarding changes in its structures and codes. Finally, Stützel's cryptanalysis on the diplomatic codes questioned not only the expertise of the Chiffrierbureau but also theput at risk the trust competence of the entire division of the the armed services in the Foreign Office.

3.4 The imposed silence

In the 1920s, the former Austrian captain, Andreas Figl, planned to publish his memoires and experiences as the head of the cryptologic section of the Austro-Hungarian army intelligence service, Evidenzbüro. This publication reveals reasons as to why German cryptology of World War I never was treated by its protagonists as the British did.

After the first of three volumes werewas published, Figl was pressurized to step back from his project. "The action against me came from the [Austrian] Federal Army and -as I ascertained later- from the German General Staff", Figl recognized in his unpublished memories.[7] He states that the intelligence and cryptologic communities held opposite opinions on weather he and his colleagues were still bound by the duty of secrecy or not. Figl thought he was no longer bound as the state he swore to - the Austro-Hungarian Monarchy- was no longer in existence since 1918, when it broke into several independent republics. The Austrian Emperor had to abdicate and go into exile, similar to his German incumbent.

Obviously, on the other side of the Alps, the German military saw that quite differently. From the legal perspective, one has to question whether the duty of secrecy sworn before 1918 persisted or not. The oath was considered legitimate if it was to the German Reich but not to the Kaiser and king. The latter, although converted from monarchy into republic, persisted as the official denomination of the new state.

[7] Bundesarchiv, MSG 2_18031

Though the political system changed, and the military had to downsize its structures according to the Treaty of Versailles, the Army and the Navy maintained their principal SIGINT and cryptology organizations, which also included part of the personnel.

Lasry et al. (2017) provide solved radiograms sent by the signals captain Walther Seifert. After the collapse and defeat of 1918, he switched over to the Chiffrierstelle (cipher-section) of the Reichswehrministerium (Ministry of the Armed Forces). In 1933, he was a part of the founders of the Forschungsamt (Research Office). The latter became the technical intelligence agency of the National-Socialist Germany, which was a part of Hermann Göring's Reich Air Ministry, and Seifert its head of cryptanalysis.

Albert Praun started his military career in the signals troops of the Bavarian Army. He later took over several military commands until 1944 and then became the Army's Chief Signals Officer. From 1956 to 1965 he headed the SIGINT department of the West German foreign intelligence service, the Bundesnachrichtendienst (BND). Although Praun published some articles on that subject, he kept his imposed silence.

4 The Presence of the Past

In spite of the mentioned publications and sources, the imposed silence on the German culture of cryptology persists. The research on this area has recently begun and some questions might never be answered. Investigating the German culture of cryptology prior to and during World War I is linked to our modern security culture because both are parts of the same chain.

There are at least two further links, those of cryptology and intelligence during World War II and the Cold War. For the latter it would be interesting to know whether the cultures of cryptology in the two German states were different because of their opposite politicalideological views due to their particular intelligence cultures. The next step would be to compare it at least with the French, English, US, and Russian cultures of cryptology, if possible.

But before we follow the chain up to the present time, we should look back from the German Reich of 1871 to the earlier epoch of the 18th-century-Black Chambers. Perhaps, on the one hand, this investigation can provide

information for closing the gap between the cryptologic and intelligence system of the late 19th century and that of Prussian king Frederick the Great in the 18th century. If, on the other, due to the lack of reliable sources, it could be helpful to compare at least the code-systems used in both periods. Maybe similarities could be found and shed some light on Prussian cryptology and its continuity.

Describing the learning process the German culture of cryptology, it underwent, between 1870 and 1918, several changes. The truereal activity of the Chiffrierbureau will never be discovered but at least the files on its personnel could provide information on how they entered the section and what kind of preparation they undertook for their work. In this context it would be interesting to analyze the path and networks of those cryptologists who started their career in the Army or in the Navy.

A part of a learning process is also how people handle their successes and above all their failures. As Figl mentioned, the German military and political elites avoided being held liable for their failures in matters of cryptology and intelligence. They covered up their first major defeat in France by calling the correspondent battle the "wonder of the Marne". In this and other cases, the history of German cryptology can correct the greater picture of World War I by demythologizing some of its narratives.

In this context, the fact that humans tend to copy behaviors, becomes a problem. To change certain cultures renders itself even more difficult if people are not used to questioning ideals. The official silence imposed on cryptology and its history was absolutely not helpful. This might explain the reason, amongst others, why in World War II German officials kept using the Enigma cipher machine even though they knew of its weaknesses. Referring to Zimmermann's statement on code security, one has to question human ignorance because till date some things were not meant to be. In this context matches the warning, the US-philosopher George Santayana gave us: "Those who cannot remember the past are condemned to repeat it."

Acknowledgements

I would like to express my appreciation to Prof. Christof Paar (Bochum) who brought me from history into the world of cryptology, to Prof. Arno Wacker, Dr. Nils Kopal, and Dr. George Lasry who invited me to reconstruct the historical context of the German messages they had solved. I also thank the three anonymous reviewers whose commentaries made me rethink some aspects of this article. Last but not least, I am deeply indebted to Dr. Roopika Menon who helped me to improve my English text.

References

Maria Bada and Angela Sasse. 2014. Cyber Security Awareness Campaigns: Why do they fail to change behaviour? http://discovery.ucl.ac.uk/1468954/1/Awareness%20CampaignsDraftWorkingPaper.pdf, last seen 15.01.2018.

Böhme, Hartmut: Vom Cultus zur Kultur(wissenschaft). Zur historischen Semantik des Kulturbegriffs. In: Renate Glaser/Matthias Luserke (Ed.). 1996. *Literaturwissenschaft – Kulturwissenschaft. Positionen, Themen, Perspektiven.* Westdeutscher Verlag, Opladen: 48-68.

Hilmar-Detlef Brückner. 2005. Germany's first Cryptanalysis on the Western Front: Decrypting British and French Naval Ciphers in World War I. *Cryptologia,* 29(1):1-22.

Paul Gannon. 2010. *Inside Room 40: The Codebreakers of World War 1.* Ian Allan Publishing, Hersham.

Heinz Höhne. 1993. *Der Krieg im Dunkeln. Macht und Einfluss der deutschen und russischen Geheimdienste.* [The war in the dark. Power and influence of the German and Russian secret services.] (Special printing). Gondrom Verlag, Bindlach.

David Kahn. 1996. *The Codebreakers. The Story of Secret Writing,* [Kindle, ipad mini version]. Downloaded from Amazon.com.

David Kahn. 2001. An Historical Theory of Intelligence. *Intelligence and National Security*, 16:79-92. http://david-kahn.com/articles-historical-theory-intelligence.htm, last seen 14.01.2012.

Friedrich Wilhelm Kasiski. 1863. *Die Geheimschriften und die Dechiffrir-Kunst.* [The Secret Scripts and the Art of Decipherment] E.S. Mittler, Berlin.

Daniel Larsen. 2014. Intelligence in the First World War: The State of the Field. *Intelligence and National Security*, 29(2):282-302.

George Lasry, Ingo Niebel, Nils Kopal, and Arno Wacker. 2017. Deciphering ADFGVX messages from the Eastern Front of World War I. *Cryptologia* 41(2): 101-136.

Wolfgang J. Mommsen. 1995. *Bürgerstolz und Weltmachtstreben. Deutschland unter Wilhelm II. 1890 bis 1918.* Propyläen Verlag, Berlin.

David Paull Nickles. 2003. *Under the Wire: How the Telegraph Changed Diplomacy.* Harvard Univ. Press, Cambridge, Mass.

M. Niethe. 1875. *Das "Suum cuique" in neuer Interpretation seitens des Auswärtigen Amts: nothwendig gewordener Anhang zu des Verfassers Werk: Das bei der Chiffrir-Abtheilung des Deutschen Reichskanzleramts eingeführte telegraphische Chiffrirsystem etc.* [The "Suum cuique" (to each his own) in a new Interpretation from the Foreign Office: An Annex, which had become necessary, to the Author"s Work: The Telegraphic Cipher-System introduced into the Cipher-Department of the German Reich Chancellory etc.] M. Niethe, Berlin.

Markus Pöhlmann. 2005. German Intelligence at War, 1914-1918. *Journal of Intelligence History,* 5(2):25-54.

Politisches Archiv des Auswärtigen Amtes (PAAA). 1936. Organisation des Auswärtigen Amtes bis 1936. [handwritten chart] Berlin.

Anne-Simone Rous. 2011. Geheimschriften in sächsischen Akten der Neuzeit [Secret Writing in Saxon Files of the Modern Age]. *Neues Archiv für sächsische Geschichte*, 82:243-254.

Anne-Simone Rous and Martin Mulsow (Ed.). 2015. *Geheime Post: Kryptologie und Steganographie der diplomatischen Korrespondenz europäischer Höfe während der Frühen Neuzeit* [Secret Mail: Cryptology and Steganography in the Correspondance of the European Courts during the Early Modern Age]. Duncker & Humblot, Berlin.

Martin Samuels. 2016. Ludwig Föppl: A Bavarian Cryptanalyst on the Western front. *Cryptologia,* 40(4):355-373.

Bernhard Sassmann and Tobias Schmitt. 2016. Cultures of Intelligence Conference Report. *German Historical Institute London Bulletin*, 38(2):135-140.

Hermann Stützel. 1969. Geheimschrift und Entzifferung im Ersten Weltkrieg [Code and Decipherment in World War I]. *Truppenpraxis* 7:541-545.

Geoff Sullivan and Frode Weierud. 2005. Breaking German Army Ciphers. *Cryptologia*, 29(3):193-232.

New Findings in a WWI Notebook of Luigi Sacco

Paolo Bonavoglia
former teacher of Mathematics
Convitto Nazionale Marco Foscarini,
Cannaregio 4942, I 30121 Venezia, Italy
paolo.bonavoglia@liceofoscarini.it

Abstract

A small size booklet was found by the author among the papers of Luigi Sacco, his grandfather, founder and chief of the Italian Army cryptographic office (a.k.a. *Reparto crittografico*) during WW1. This paper presents a new research, still work in progress, about new cryptograms found in the booklet containing historical links to events of WW1.

1 The booklet

The booklet has 160 pages, mostly handwritten, some left blank. The cover has the date 18 July 1916, the last pages are dated November 1916. Therefore, the book covers the very beginning of the Italian cryptographic office in WW1.

The first part looks like an exercise book with examples and explanations. The following pages have a mix of German language cryptograms, mainly transposition ciphers.

A paper about this booklet has been already published on-line by the author (Bonavoglia 2018). Recent research has produced more interesting results.

2 Are these real WW1 cryptograms?

This is the first question arising from this booklet. Are all these cryptograms real war messages? Or are only examples, exercises?

Examining the pages, the most likely hypothesis is there both are true. A first good criterion is language; several cryptograms at the beginning are in French; since France was an ally of Italy, it looks very likely these are mere exercises. And the text states clearly these are examples taken from Valerio (the French treatise of cryptography which Sacco used extensively).

And most other messages are in German and this is a first clue in favor of the hypothesis that these cryptograms are real WW1 messages. Most cryptograms have names of persons or places of the war on the eastern front, mainly on the Rumanian theatre, which is consistent, both in space and time, with the conjecture that these German messages were intercepted by Sacco's radio stations in the Italian Friuli region, not so far from the Danube region. They could also come from other Italian intercepting stations, a good candidate is for instance the one in Lecce, not far from the Danube region.

3 A transposition cryptogram

A particularly interesting transposition cipher appears in the following couple of pages[1] :

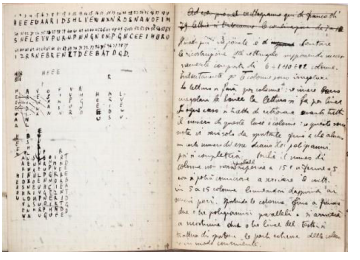


Figure 1 : The couple of pages.

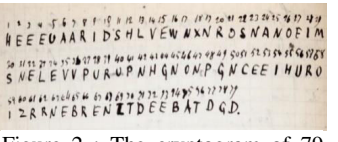


Figure 2 : The cryptogram of 79 letters on top of the left page.

1 Only a few pages have a date; these are between a page dated 24-09-1916 and one dated 11-10-1916; this should be a good clue about the date.

In the right page Sacco writes down a possible strategy to decrypt it: he tries to arrange the text in 6 8 10 12 columns rectangles in the hypothesis of an irregular rectangle. No solution is given.

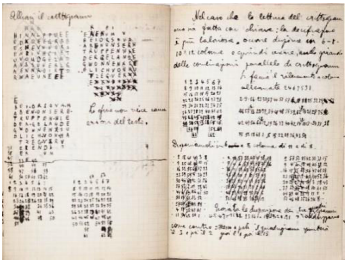


Figure 3 : The second couple of pages.

Two pages forward we find another couple of pages with a slightly different cryptogram, a few letters changed with similar letters, e.g. *L → V, H → E, N →W*. It's likely Sacco found some transcription errors from the original.

Finally, Sacco finds a solution which has strange errors in the last lines.

The decrypted text is:

```
BEI ORSOVA HABEN UNSERE TRUPPEN
WIEDER GELANDE GWONNEN X
SUDLICH VON HATZEG VERVEREN DIE
RUME
```

Taking the X as a separator, and GWONNEN for GEWONNEN we have a text sounding good in German, except for the last line:

Bei Orsova haben unsere Truppen wieder Gelande gewonnen. Sudlich von Hatzeg ververen die Rume.

But *Ververen die Rume* has no meaning in German, and Sacco writes near this solution: "The end does not work for errors in the text". Quite puzzled by these strange final errors I supposed there was some mistake in the cryptogram, maybe a handwriting problem, and made a few attempts; I restored the D present in the first cryptogram and for some reason removed from the second and changed it in O. So we have this 80 letters cryptogram:

```
HEEEU AARID SHLVE WNXNR OSNAN
OEIMS NELEV VDURU PENHG NONPG
NCEEI EUROI ZRRNE BREWL TOEEB
ATDGD
```

The decrypted text is:

Bei Orsova haben unsere Truppen wieder Gelände gewonnen. Sudlich von Hatzeg verloren die Rumen.[2]

and at last the final words make sense!

This text is interesting because of the geographic names: Orsova and Hatzeg are Rumanian cities by the Danube; and in September 1916 the German Army under General Falkenhayn launched a counter offensive between Orsova and Hatzeg against the Rumanian Army to regain the ground lost in August and early September when Romania declared war to Austria-Hungary and occupied regions near Transylvania.

This gives a good accordance of times between these cryptograms of Sacco's notebook, and historical events of WW1. Another clue in favor of the idea that these cryptograms are real WW1 encrypted messages which Sacco decrypted and used to find a method for decrypting transposition ciphers.

4 Solved transposition cryptograms

These two pages[3] of the booklet have a lot of decrypted transposition cryptograms of various kinds.

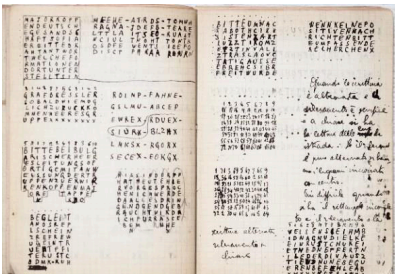


Figure 4 : A few have the original cryptogram, many only the final solved rectangle.

Here is the first, top left, a simple transposition cipher with alternate up and down writing; the original cryptogram is also shown on the right.

The decrypted text is:

2 English: At Orsova our troops have gained ground again. South of Hatzeg lost the Rumanians

3 These pages are between a page dated 11-10-1916 and one dated 17-10-1916.

Major Koppen deutsche Gesandtschaft Sofia erbitte Draht Antwort welche Formationen dort unterstellts in[4]

Another cryptogram is an irregular rectangle key transposition, much more difficult to break.

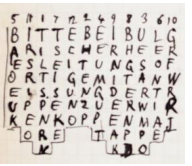


Figure 5 : The original cryptogram is missing, but of course it can easily be reconstructed.

The decrypted text is:

Bitte bei Bulgarischer Heeresleitung sofortige mit Anweisung der Truppen su erwirken Koppen Major Etappen Kdo[5]

Who was this Major Koppen, named twice here? I could find an answer only in the German Wikipedia[6]; he was a chief of staff at the High Command of the German Army.

A third cryptogram is shown hereafter.

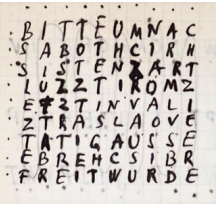


Figure 6 : A simple transposition, with alternate direction of writing, left-right, right-left.

Not very hard to break, in spite of some typos like *Artz* instead of *Arzt*.

The decrypted text finally is:

Bitte um Nachricht ob Assistenzarzt Moritz zuletzt in Valievo[7] *als Arzttatig aus Serbischer befreit wurde*[8]

5 October '16: three grille cryptograms

Near the end of the booklet, October 19169, a few grilles appear; Sacco only presents them together with some conjecture about a possible solution, but no solution is given.

In the following couple of page, Sacco displays two 8x8 grilles, both unsolved, the second incomplete.

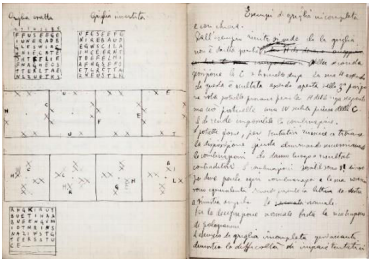


Figure 7 : A couple of pages with grilles.

Here is the first grille; Sacco, searching for the digraph 'CH' very common in German, thought it was a double transposition grille and tried a permutation of the columns shown on the right, under the label "*Griglia invertita*":[10]

5.1 Decrypted texts

In 2017 a challenge was launched on the *Cryptograms & Classical Ciphers* Facebook group and both grilles were decrypted with the aid of dedicated software**.**

The Fleissner 7x7 grille[11], with a black case in the middle is shown in the following figure.

At first look the X and Y on the bottom left could be nulls to fill the grille; and this was a first aid for the cryptanalyst. At last the raw decrypted text is[12]:

[4] English: Major Koppen asks the German Embassy in¨ Sofia a wired answer, which formations are placed there.

[5] English: You are asked to get by the Bulgarian Army Command the disposition of the troops. Major Koppen, Stage (rear) command.

[6] Wikipedia is not the best source for serious research and its reliability is variable; but in this case it was the only source I could find about this Major Koppen; and, after all, I just needed a confirmation he was a real German military officer.

[7] Valjevo is a city of Serbia.

[8] English: Please let us know if the assistant physician Moritz recently in Valjevo as aid physician has been released.

[9] these pages have a beginning date, 17-10-1916; the next is dated 20-10-1916.

[10] under these two grilles he showed some unfinished and unsuccessful trials.

[11] See (Bauer 1997) p. 96,97.

[12] The cryptogram was decrypted by Barth Wenmeckers with a hill cipher algorithm and independently by the author with a computer aided software implemented *ad hoc*.

ESWURDENDREIPUNKTEGESEHEN
OTLLICHWEITESRSSUCHENXY

There are a few typos and some extra S; the spaced and cleaned text is:

Es wurden drei Punkte gesehen östlich weiter suchen XY[13]

Figure 8 : The 7x7 grille

The 8x8 grilles were also decrypted; here is the first:

Feuer eingestellt feindliche Fahrzeuge abgewandte ausser Sicht Flotten K[ommando?][14]

And here is the decrypted text of the second 8x8 grille, which happened to be encrypted with the same grille:

Krieg Ministerium ist ersucht beantragtes Guthaben von Zw[15]

6 Open questions

A few questions remain unanswered:

Bauer in his book[16], writes that the German Army "early in 1917 suddenly introduced turning grilles with denotations like ANNA (5x5), BERTA(6x6), CLARA(7x7), DORA(8x8), EMIL(9x9), FRANZ(10x0)." Are these grilles the first of this kind? A few months earlier that reported by Bauer? Why this small difference?

Did Sacco manage to solve these grilles in the following months? At the end of October 1916, he moved to Rome, and his booklet ends in the same days. We simply do not know. The answer could be in the notebooks and papers of Sacco in his Rome office, but all these papers were likely destroyed or lost.

Could these cryptograms be Austrian rather than German? The first two cryptograms look like Navy messages and could come from the Austrian fleet in the Adriatic Sea; not very likely from German ships in the Black Sea.

7 Conclusion

As already stated, the booklet has 160 pages, there are still a lot of pages to be studied; these are the more interesting found so far, but there is always the possibility of something more important to be found.

Other pages are about the Austrian diplomatic code, Austrian and German Navy codes, and others, but no complete cryptograms with decrypted texts are given.

I'm publishing the whole booklet on the web, so any researcher will be able to examine it.

Acknowledgements

I wish to thank Cosmo Colavito, engineer and telecommunications historian, for help about Italian Army history in WW 1, and Diana Schindler, for help in translating German cryptograms.

References

Friedrich L. Bauer. 1997. *Decrypted Secrets*. Springer, Berlin, D. ISBN: 3-540-24502-2

Paolo Bonavoglia. 2017. *A 1916 World War I notebook of Luigi Sacco*. Cryptologia, 42:3, 205-221 DOI:10.1080/01611194.2017.1362064

Yves Gylden. 1933. *The contribution of the cryptographic bureaus in the world war*. Signal Corps Bulletin 75 and 81, Washington, DC.

David Kahn. 1967. *Codebreakers*. Scribner, New York, NY. ISBN: 978-0-684-83130-5

Luigi Sacco. 1947.*Manuale di Crittografia*. Ist. Poligrafico dello Stato, Roma, Italy.

Luigi Sacco. 1977. *Manual of Cryptography* Laguna Hills, Aegean Park Press, (English translation).

[13] English: Three points were seen eastwards, seek further XY.

[14] English: Ceased fire, enemy vehicles got out of sight. Fleet Command.

[15] English: The War Ministry is requested of the required balance by Zw

[16] (Bauer, 1997) pag. 96; see also (Kahn, 1967) pag. 308.

World War II

The First Classical Enigmas
Swedish Views on Enigma Development 1924-1930

Anders Wik
S Catalinagr 9
S-18368 Täby, Sweden
anders.h.wik@gmail.com

Abstract

This paper concerns the very first "classical" Enigma from 1924, with rotors, reflector and lamp display. A description is given of the Enigma machines bought by the Swedish General Staff in early 1925, of the competition regarding the first standard crypto machine for the Swedish armed forces, and of some later developments.

1 Introduction

The Enigma cipher machine which had such importance in the Second World War has its roots in a machine that was first shown publicly at the Universal Postal Union Congress in Stockholm 1924. In Sweden it generated a strong interest which lasted for about five years during a time when the Enigma machine was developed through a number of models. This paper is mainly based on some 80 pages of correspondence between the Swedish General Staff (SGS) and Chiffriermaschinen AG (ChiMaAG) in Berlin and documents in connection with that. That material is used in a multitude of places throughout this paper and is not specifically referenced. It comes from the archive of FRA, the National Defence Radio Establishment, Stockholm, Sweden (FRA 1924-1930). Communication and cooperation was handled through the Swedish military attaché in Berlin. Much of the correspondence is in Swedish, whereas letters and documentation from ChiMaAG are in German.

2 Crypto use in Sweden 1924

The main players regarding ciphers were the General Staff and the Ministry for Foreign Affairs. Codes and simple lookup-tables were used, sometimes with a superencipherment, e.g. by the Köhl cipher ruler which was the Ministry for Foreign Affairs "System 1920" (Faurholt, 2006). Systems of the Wheatstone clock type were in use in the Military since 1907. Captain de Champs had developed a revolving cylinder cipher for the Navy in 1920 but it was just a prototype until 1926. A.G. Damm at AB Cryptograph had developed an impressive number of different crypto devices since the mid 1910s but at the time the only system Cryptograph could offer to the General Staff was the handheld model A22.

Looking at the available options it is easy to understand that the Enigmas on show at the exhibition in 1924 seemed very attractive.

3 The Stockholm machine

At the exhibition during the Congress of the Universal Postal Union in Stockholm in the summer of 1924 ChiMaAG demonstrated two crypto machines, an Enigma "Handelsmaschine" and a small "Militärmaschine". The Handelsmaschine was big machine (about 65 x 45 x 38 cm) and was quite heavy (about 50 kg). It had earlier been shown at exhibitions in Leipzig and Bern in 1923. It could print the output using a type wheel. The "Glühlampenmaschine" was a new model, probably made in just a few copies. It was the first model in a development, which was to last for more than 20 years. No such original machine or parts of it have been found. Since SGS had a strong interest in both machines the company left them in Stockholm for trials by the prospective customer. Also supplied was a one page typewritten description entitled "Glühlampenmaschine Enigma A" as well as a 16 page printed booklet describing the Handelsmaschine (ENIGMA Chiffriermaschinen, 1924).

Proceedings of the 1st Conference on Historical Cryptology, pages 83– 88,
Uppsala, Sweden, 18-20 June, 2018

It should be noted that ChiMaAG uses the name Enigma A and later Enigma B for the early "Glühlampenmaschine". The Enigma A is also called "die kleine Militärmaschine" and in this paper, for clarity, "the Stockholm machine". This is contrary to what has earlier been assumed, i.e. that A and B were the printing Enigma models. This paper will use the notations A and B as ChiMaAG used them in the correspondence.

Some details about the Stockholm machine can be gathered from the letters and the short description:

1. It measured 23 x 27 x 13 cm with a weight of about 5 kilograms.
2. It had 26 keys and 26 lamps arranged in two rows each, alternating lamp rows and key rows.
3. The keys and the lamp covers were unmarked and left for the user to mark (with characters or symbols).
4. There was an "Antriebstaste", a key that advances the rotors and that must be pressed each time before ciphering a character.
5. There were three rotors, one marked with letters and two with numbers. It had a period length of 676 and "more than 17000" (presumably 26^3) different settings.
6. Ciphering and deciphering were the same.
7. A reasonable conclusion is that it had two rotors and in addition an important novelty, a settable reflector (Umkehrwalze).

There does not seem to be any other remaining documents elsewhere about the Stockholm machine (Enigma A). It may have been a further development of a German patent application, DE407804, filed on January 18, 1924 by the inventor Paul Bernstein for ChiMaAG (Bernstein 1924). That construction was the first with a lamp field but it had straight ciphering from the keyboard through two rotors to the lamps field without a reflector, i.e. similar but simpler than the Handelsmaschine. It is not known whether any machines were produced on basis of Bernstein´s patent.

The Handelsmaschine and the Enigma A were returned by courier to ChiMaAG in September 1924. Captain Gyllencreutz who handled the matter for SGS asked for changes in the Enigma A they would like to see and test. In October 1924 he wrote that they considered buying 15 such machines. The desired modifications of the machine were:

1. A possibility to turn on all lamps at the same time to check that no lamps are broken.
2. The lamp field should have dark background and the letters lit. *(Apparently this was not the case with the Stockholm machine.)*
3. The lamp field ought to be behind the keyboard and the keys should not be blank but instead marked with letters.
4. The lever to move the wheels (presumably the Antriebstaste) should be on the left side of the machine.

Gyllencreutz added further tentative improvements

5. The machine should have a larger character set, preferably around 40, with digits, comma and period.
6. It would be desirable to have four wheels like in the big machine.

As to the bigger machine, the Handelsmaschine, Gyllencreutz was less certain, but possibly SGS might be interested in buying two or three.

4 Further negotiations

During the rest of 1924 discussions continued between SGS in Stockholm and the company in Berlin through the Swedish military attaché Major Henry Peyron in Berlin. In October the price with the requested modifications and some other improvements was given as 100 dollars each at an order of 15 machines. The technical officer at SGS suggested that the offer should be accepted. The total cost for 15 Enigma A machines with modifications 1-4 above would be 6250 Swedish crowns. The problem was funding. An attempt to influence the Swedish government was made through General von Bender who knew the Grand Duke of Baden, father of the Swedish queen Victoria. This seems to have been unsuccessful.

In November 1924 ChiMaAG offered a new possibility, a model they call "Enigma B". In this machine the third rotor, which in the first model was a settable reflector, would be a true rotor and

step in the encipherment process giving it a period length of "about 17500" ($26^3=17576$). The new machine could also be delivered with a 28-character alphabet whereas the Enigma A only could have a 26-character set. The Enigma A was apparently in stock since they stated that up to 10 machines could be sold with immediate delivery. Improvements for the Enigma B compared to the machine shown in Stockholm should be:

1. Different layout: From back to front first two rows of lamps, then the rotors, then two rows of keys.
2. The rotors move automatically when a key is pressed making the Antriebstaste unnecessary.
3. The letters are white on a black background
4. The possibility to check that no lamp is faulty.

Photo 1: A133 without cover. Source: FRA

5 Swedish Enigmas

On January 13, 1925 SGS places an order for two "Enigma B" with a Swedish 28-character alphabet A…Z ÅÄÖ without W. The price was 650 RM each. The machines were delivered on April 6, 1925. They have serial numbers A133 and A134 and are today part of the FRA Crypto collections. The machines do not seem to be much used, possibly only for evaluation purposes. The weight is 5 kilo (without the wooden box) and the measures WxDxH = 26 x 27,5 x 11 cm, somewhat wider and lower than the Stockholm machine.

ChiMaAG had changed the layout compared to what they had offered, probably after consent from SGS. From the back are now rotors, three rows of lamps and then the keyboard set up in alphabetical order. The rotors have an adjustable ring setting.

The wiring of the rotors is as follows in cyclical notation:

I: (ÖAPRE) (CBSZYLÄKOFXN) (DGQTVI) (JH) (MUÅ)

II: (7, 1, 3, 14, 23, 21, 11, 20, 5, 24, 16, 27, 22, 17, 9, 13, 25, 6, 28, 10, 15, 2, 8, 4, 19, 26, 12, 18)

III: (5, 1, 26, 11, 28, 12, 25) (10, 2, 22, 4, 9) (15, 3, 17, 24, 13, 19, 14, 16, 6, 27, 7, 23) (8, 18, 21) (20)

The reflector is fixed in one position and has the following connections:

(1,12) (2,4) (3,7) (5, 27) (6, 14) (8,16) (9,19) (10,11) (13, 22) (15,25) (17,23) (18,21) (20,26) (24,28)

In theory it would be possible to change the wiring. The following picture shows that this would be a tricky procedure with clear risks to damage the function.

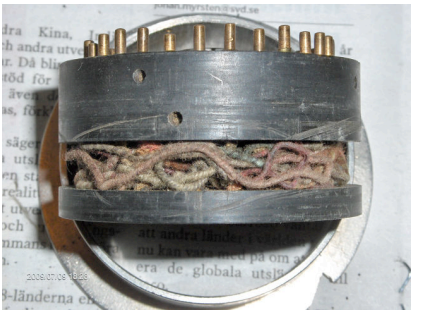


Photo 2: Opened rotor A133. Source: FRA

6 Funkschlüssel C

ChiMaAG was also negotiating with the Reichsmarine which in December 1924 ordered 10 prototype machines. That model was called "Funkschlüssel C" and had rotors with 28 contacts. This fits very well with what was offered to Sweden and the two machines that were ordered in January 1925. The

"Funkschlüssel C" had 29 keys and 29 lamps where the letter X went straight to the lamps without being enciphered. The wiring of the rotors was most likely different. The Swedish machine had a reflector which was fixed in one position whereas the Funkschlüssel C had a possibility to fix the reflector in four different positions. Apart from that the two machine types would very likely have been the same.

A delivery of 50 machines to the Reichsmarine took place in January 1926 (Weierud 2014). These machines were supplied with two extra rotors. This was mentioned in a report from the Swedish military attaché in October 1925, which said that a customer had ordered two extra rotors which gives 60 different rotor combinations instead of 6. ChiMaAG suggested that SGS should do the same.

7 Swedish competition

Boris Hagelin, who was now in charge of AB Cryptograph, heard about the strong interest from SGS for the new Enigma machines. Cryptograph had good contacts with the Swedish military, but their only viable product was the A22, which was far less attractive than the Enigma.

Nevertheless, the two machines were tested against each other in May 1925. Captain Backlund limited his comparison to practical matters such as encryption speed where he stated that encrypting a 100 character message would take 6 1/2, 4 and 3 minutes respectively for 1, 2 or 3 persons whereas for the A22 it would take around 4 minutes independently of the number of people involved. Backlund noted that the Enigma machines had a stepping error. This is the double stepping effect described by Hamer (1997).

Lt Samsioe gave a preliminary assessment of the security in November 1925. He wrote that the A22 seems to give a fairly low security, which possibly could be improved. His study of Enigma B was not concluded. He notes that the period is 28^3 but that there are subperiods of 28 which it might be possible to isolate. (*Actually the period is 28 x 27 x 28 because of the double stepping.)* A22 and Enigma B share the problem that a change of message keys does not change the character of the cipher enough. A new key is just a new starting position in the same crypto period. Since the order of the three rotors could be changed there could be six different key series.

It seemed clear that SGS thought highly of the Enigma and were going to buy it. In his memoirs Boris Hagelin wrote that he visited the person in charge at SGS, major Warberg, and asked him to wait six months with their decision. This would allow Cryptograph to make a prototype of a machine of Enigma type – but better. He was granted the time.

A G Damm had in 1919, independently of Scherbius and Koch, patented a form of wired rotors (Damm 1919). This was essential for Hagelin. By using parts of Damm´s B1 and B13 machines he was able to produce a prototype of what was to become the B21 machine. His machine had lamps and rotors, an irregular stepping mechanism for the rotors and a wider variety of operator key settings. Hagelin´s prototype was enough to stall immediate decisions and eventually secure the order from SGS and the Ministry for Foreign Affairs.

Cryptograph had acquired an Enigma (A344), which was sent to Damm in Paris. He sent back a preliminary report in August 1927 (Damm 1927). There he noted that he made a study already in September 1924 based on patent descriptions and other available information. That earlier report has not been found. In the 1927 report he wrote that the security is low if the wirings are known. He claims that he is developing a method to solve Enigma but writes that it would be improper to give details in a letter. Instead he goes into a detailed discussion of the machine.

He concluded his seven-page report with his verdict. *Enigma is a reasonably handy method to encipher…* but *… the security is directly dependent on keeping absolutely secret not only machine details but also texts - even if they are meaningless – that have been enciphered.*

His report might have helped Cryptograph by casting doubt on the Enigma even if his report does not contain arguments to show that the Enigma system is weak.

8 The next generation Enigmas

Contacts between SGS (through the embassy in Berlin) and ChiMaAG continued during 1925 while the two delivered machines were being evaluated in Stockholm. A request from SGS concerned a machine with printer and compatible with the lamp machines. At first the company seemed to be developing such a compatible pair.

However, in April 1926 the company stated that such a solution would not be developed since the printing machine would lose functionality and the lamp machine would be heavier, costlier and less reliable.

In the summer of 1926 LtColonel Carl Herslow succeeded Henry Peyron as military attaché. Herslow had a good knowledge of crypto matters and had worked in the group of officers at SGS which solved Russian diplomatic code traffic during WW1. This work was in cooperation with Germany, which may have benefitted Herslow´s insights into German security matters (Grahn 2017). In August 1926 Herslow visited the company and reported that the new machine was in its final shape. It had been introduced at the Auswärtiges Amt and would soon also be presented to the Reichswehrministerium. The new machine had four rotors (presumably three plus a reflector) and also spare rotors in a separate box. The price was quoted as 600 RM. Warberg at SGS was interested. He would like to test the new machine, preferably with a 28-character alphabet.

In November 1926 Herslow wrote to Warberg to tell him that the Reichswehrministerium had got delivery of a small series of the new machine. With Swedish specifications (28 characters) the new machine would be slightly bigger and could be offered at a price of 600 RM a piece at an order of 30-40 machines. A counter (Zählwerk) was optional and would add 40 RM to the price. A new machine with printer (a development of the Handelsmaschine) was expected to be developed by March 1927. It was aimed for use by higher staffs and had a price of about 2000 RM.

Test machines meeting Swedish requirements would be quite costly. Therefore, in February 1927, Warberg asked Herslow to buy two 26-character Enigmas with Zählwerk (at 700 RM a piece). In March 1927 Warberg reminds him that he should check the machines on delivery so that they do not have the stepping error of the earlier machines (cf section 7 above). The new machines were Zählwerk machines and had a different stepping mechanism. That check should therefore have worked without problem.

Herslow was going to take up a position as military attaché in Moscow. He was instructed to take one machine with him to Moscow. The other one should be delivered to Stockholm so that the pair of machines could be tested in operational use. Herslow was quite familiar with the Enigmas after many discussions at ChiMaAG.

When Herslow left for Moscow in the beginning of April 1927 the new machines were not ready so the company supplied two machines on loan (A361, A362), one for Herslow, one for Stockholm. Warberg provided a 12-page document with detailed instructions for key settings etc. (FRA 1927). The two Zählwerk machines (A350 and A351) were delivered in May 1927 and the machines on loan were sent back.

9 Enigma or B21

Presumably the Zählwerk Enigma was studied and tested. There is no communication in the file for the coming six months. In December 1927 SGS asked for a quotation for the delivery of 40-60 machines with a 28-character alphabet – with or without Zählwerk. The reply from the company was prompt. They quoted a basic price of 600 RM for a 26-character machine and gave two options. A Zählwerk would add 100RM and 28-character alphabet 30 RM.

Parallel negotiations were going on between SGS and Cryptograph and the decision was made. B21 was chosen as m/29, SGS standard machine model of 1929. No final evaluation has been found in the archives. Therefore one can only speculate about which arguments were the decisive ones. A longer key period? Rotors wired in Sweden? Wider user key space? Support to Swedish industry?

The Navy had some independence from SGS. Their order for three Enigmas was the last sign of interest from the Swedish armed forces. After delivery of A853, A854 and A855 in April 1929 there seems to be no interest in Enigmas from Swedish authorities.

10 Not quite the end

Carl Herslow, mentioned above, was in 1928 recruited by Ivar Kreuger, a Swedish industrialist and entrepreneur known as the “Match King”. By aggressive investments and innovative financial instruments he built a financial empire which in the end controlled between two thirds and three quarters of worldwide match production. His activities needed secure communications and the Swedish match

company Svenska Tändsticks AB (S.T.A.B) became one of just a few non-government buyers of Enigma machines.

There is a note that Herslow bought two machines "for Kreuger" in the spring of 1928. Also there is a note from 1935 that two machines (A343 and A344) were presumed to be at S.T.A.B. All in all it seems that Kreuger´s company bought six Enigmas (numbered A327, A328, A343, A344, A801, A802) (Weierud 2014)

Apart from these regular machines S.T.A.B also bought three small Enigmas, model Z30, aimed at enciphering digital codes. No documentation concerning this has been found. The acquisition of these three machines, bought around 1930, concludes all dealings between Sweden and Chiffriermaschinen AG. The three Z30 machines are part of FRA Crypto collections (Wik 2016).

A broader picture of Swedish cryptography and early Swedish Sigint between the world wars is given by McKay and Beckman (2003).

Acknowledgements

The author is most grateful to Frode Weierud for sharing his Enigma expertise and for his valuable advise.

References

Bernstein, Carl. 1924. German patent DE 407 804. http://www.cryptomuseum.com/crypto/enigma/patents/files/DE407804.pdf

Damm, Arvid Gerhard. 1919. Swedish patent SE52 279. Filed Oct 10, 1919. US patent 1 502 376, July 22, 1924.

Damm, Arvid Gerhard. 1927. Preliminärt utlåtande angående "Glühlampen-Chiffriermaschine Enigma". Krigsarkivet, Stockholm. Boris Hagelins privatarkiv, vol F II:3.

ENIGMA Chiffriermaschinen. 1924. Handelsmaschine. FRA Crypto collections. Booklet.

Faurholt, Niels O. 2006. Alexis Køhl: A Danish Inventor of Cryptosystems. Cryptologia vol 30.

FRA archive. 1924-1930. Bearbetningsbyrån F V:1. "Chifferapparaten Enigma".

FRA archive. 1927. Bearbetningsbyrån F V:1. Instruktion för användning av Chifferapparat Enigma B /Chiffer EZ/.

Grahn, Jan-Olof. 2017. Om svensk signalspaning - Pionjärerna ("On Swedish SIGINT – The pioneers"). Medströms bokförlag, Stockholm.

Hamer, David. 1997. Enigma: Actions involved in the 'double stepping' of the middle rotor. Cryptologia vol 21.

McKay and Beckman. 2003. Swedish signal intelligence 1900-1945. Frank Cass, London.

Weierud, Frode. 2014. Personal communication.

Wik, Anders. 2016. Enigma Z30 retrieved. Cryptologia vol 40.

An Inventory of Early Inter-Allied Enigma Cooperation

Marek Grajek
Freelance cryptography consultant and historian
Poland
mjg@interia.eu

Abstract

Shortcomings in the earliest reports coming from the wartime work at Bletchley Park resulted in a slightly distorted picture of the early inter-Allied cooperation in cryptology. The ultimate evidence of the Polish contribution to the success over Enigma, a report passed on to the British and French participants of the meeting in Pyry in July 1939, remains unavailable to historians.
Some files declassified in 2015 by the French intelligence service contain a document representing most probably an abridged and rewritten version of the Pyry report. This paper offers a preliminary analysis of this document.

1 Introduction

Although some attempts to coordinate the British, French and Polish efforts aimed at breaking the Enigma ciphers had been undertaken earlier, the conference at Pyry on 24-27 July 1939 marked the effective start of the inter-Allied cooperation in that field. The general nature of the reports from the Pyry meeting, as known so far, does not allow the precise assessment of the contribution of the countries participating in the conference in unravelling the secret of Enigma at that early stage of work.

Both cryptographers and historians have been aware for a long time of the existence of a definitive source of information regarding the Pyry conference and early work on Enigma. Before the chiefs of Polish intelligence service authorised the invitation of the British and French codebreaking services to Warsaw, they instructed the Cipher Bureau to prepare a detailed report presenting the complete Polish knowledge about, and experience with, the Enigma machine and its ciphers. Copies of that report were passed on to the British and French guests during the Pyry meeting. British post-WWII reports (Alexander, 1945; Mahon, 1945; Millner-Barry et al., 1945) contain references to the report indicating that it was available at Bletchley Park in 1945. Unfortunately this document is lost or at least has not been declassified so far and remains unavailable to historians.

This author believes that he has identified a document representing an edited, albeit a slightly later and abridged version, of the original Pyry report. The document found is potentially even more valuable than the original report, covering events up till the fall of France in June 1940. It may be regarded as an inventory of the early inter-Allied cooperation in the struggle against the Enigma ciphers. This paper presents early findings regarding this document.

2 Historical context

Since their first meeting in Paris, in January 1939, chiefs of the codebreaking services of the three countries, France, Great Britain, and Poland, knew that finding a common language was not going to be easy. In the literal sense of the word they could hardly find a way to communicate, before they agreed to use the language of their common cryptologic adversary – German. They did not know at that stage that they were coming to the table bearing different levels of knowledge regarding Enigma, experience and probably – different instructions and goals. The tension around the table was almost palpable, in spite of Bertrand's efforts to integrate the group using the services of the best restaurants in Paris. In those circumstances, it is not surprising that the meeting's only measurable result was a decision to convey further meetings, once any of the parties had news to communicate.

That moment arrived sooner than expected; in July invitation from Warsaw arrived, declaring that 'il y a du nouveau'. But when the codebreakers arrived in Warsaw on July 24th they had to switch back to German again, as the document they were discussing was in that language. Mahon (1945, p. 13) stated in his post-war report that "(n)early all the early work on German Naval Enigma was done by Polish

Proceedings of the 1st Conference on Historical Cryptology, pages 89– 94,
Uppsala, Sweden, 18-20 June, 2018

cryptographers who handed over the details of their very considerable achievements just before the outbreak of war", and added that "the Poles devised a new method which is of considerable interest. Their account of this system, written in stilted German, still exists and makes amusing reading for anyone who has dealt with machines" (Mahon, 1945, p. 13).

British post-war reports were compiled by G.C.&C.S. section heads, who had no first-hand knowledge of events of 1939. In fact in 1945 no participant of the Pyry conference remained at Bletchley Park. Dilly Knox had passed away in February 1943; Alastair Denniston had been sacked from his position in February 1942 and exiled to the diplomatic section. Mahon admits having gained most of his knowledge about the early attacks at Enigma from Alan Turing; but Turing had neither participated in the Pyry conference, nor was he known to be an effective communicator. Under the circumstances as described, it is natural that post-war reports are full of unanswered questions and presumptions of disputable value.

The view of early work on Enigma became even more confused after the British secret services felt obliged in mid-1970s to react to the publication of Bertrand's book. They obviously considered Bertrand's revelation as premature and decided to wrap them up with a shroud of disinformation. Frederick Winterbotham was commissioned to provide a cover version of history: "In 1938 a Polish mechanic had been employed in a factory in Eastern Germany which was making (…) some sort of secret signalling machine. (…) In due course the young Pole was (…) secretly smuggled out under a false passport (…), installed in Paris where (…) he was given a workshop. With the help of a carpenter to look after him, he began to make a wooden mock-up of the machine he had been working on in Germany" (Winterbotham, 1974). Similar versions of this story were later on presented by Cave Brown (1975), Stevenson (1976) and, in more recent times, by Aldrich (2010) and Davies (2008). Their stories have a crucial element in common in attempting to provide a cover for the compromise of Enigma ciphers in the breach of machine's physical security. That reaction is understandable; in 1973, when Bertrand (1973) revealed the Allied success with Enigma ciphers, the Cold War was at full swing and the armies of Warsaw Pact were making extensive use of rotor cipher machines derived from the results of the evolution of Enigma. While we could understand the versions of events presented by Winterbotham, Cave Brown and Stevenson as obvious disinformation, the same information produced in the 21st century represents nothing more than anachronism. On the other hand, however, it illustrates the need for an ultimate proof of the real scope of contributions delivered by the Allied nations to the victory over Enigma. For the author of this paper, this was the main reason to spend several years searching for the document which could provide indisputable evidence.

Until recently this search did not bring encouraging results. Archivists representing major institutions were sceptical. According to their opinions, if the document in question had been written in the German language, the chances are that it had been transferred to the German files immediately after the war, where it has stayed unrecognised up till now or has been entirely lost. However, on 2 December 2015, the French Direction Générale de la Sécurité Extérieure announced the declassification of the set of documents relating to the French role in Enigma breaking and the transfer of those documents to the archives of the Service Historique de la Défence. Preliminary investigation of these documents at Château de Vincennes confirmed that they represented part of the private archive accumulated by the late Gen. Gustave Bertrand over the years of his active service at various units of French intelligence service and seized by his former employer immediately after the General's death at his home at Théoule-sur-Mer.

3 Preliminary analysis of the document

Bertrand's collection represents an extremely interesting object of research for Enigma historians. In this paper we shall focus on just one of its elements; an unsigned and undated typescript described in the inventory as "Technical note in German"[1] (unsigned, 1940a). The document is 61 pages long, contains a title page, a table of contents, and 38 sections. Its title page leaves no doubt as to its contents: "ENIGMA. Abridged presentation of solution

[1] In original: Notice technique en allemande.

methods"[2], and its preface partially reveals the identity of its, otherwise unsigned, authors; "Below we sketch how the Cipher Bureau of the Polish General Staff managed to reconstruct the Enigma model described above, and methods invented to assure prompt deciphering of its messages, in spite of the changes and improvements introduced by the German cipher service to protect their security". A brief mention in one of Lt. Col. Langer's (former head of Polish Cipher Bureau) reports allowed this author not only to place the document in its time-line, but also to understand the circumstances of its creation. After his liberation from the German internment camp, Langer (1945) was commissioned to write a report presenting the circumstances of his team's evacuation from southern France in 1942 and the events that followed. It is in that report that we find a following statement: "At Château des Fouzes, Bertrand requested that a report be prepared presenting the contribution brought by each of three partners to Enigma solution. The report was prepared by Lt. Rejewski and Zygalski. After Bertrand had studied the result he declared that the work must be rewritten from scratch, as reading it in its present form one gets the impression that the contribution of the French was negligible". The declared purpose of the report is consistent with its otherwise somewhat mysterious fragment; Section 38 presents an inventory of contributions of the three countries towards the success over Enigma ciphers (see Figure 1 below).

The analysed document is unsigned; the same report by Langer sheds some light and a bit of doubt on the question of its authorship. According to that report, the document was prepared by Marian Rejewski and Henryk Zygalski. That would point to its creation either in 1941 (during Jerzy Różycki's detachment to Algiers) or in 1942 (after Różycki's death). This author believes that more probable time of its creation was late 1940 or early 1941, when Bertrand was still unable to provide the codebreakers with enough intercepts to keep them engaged. Moreover, should the document have been written in 1942, it would most probably include some references to codebreakers' work at P.C. Cadix. It is also possible that Langer, when writing his report in 1945, had confused the question of the document's attribution. The German reports based on his interrogation in 1944 mention only two mathematicians; it seems probable that Langer's mind adjusted (consciously or unconsciously) to the situation after Różycki's death.

While the scope of the document covers events having taken place between the Pyry conference and the fall of France in June 1940, its basic structure and form, as well as comparison with other documents edited by Marian Rejewski and his colleagues, suggest existence of their common source – presumed to be the Pyry report. The term "abridged" used in the title might suggest existence of a full version of the same document. Working in France, in 1940 or later, at Bertrand's request, it would be natural for the codebreakers to prepare the text in French (at least two members of the team were fluent in that language). However, existence of the German language reference, and economy of labour dictated the preparation of an abridged version of the existing German language document, complementing it with coverage of the recent events and adding elements specifically requested by Bertrand.

While working on the original Pyry report, the codebreakers having full access to their own archive, could, and certainly would have wanted to, demonstrate their mastery of the subject by including as much detail as possible. However, the archive of the Cipher Bureau was lost during its evacuation towards the Romanian border. When the team attempted to continue its work in France, the Poles had to recreate their documentation using their memory as the only reference available. Process was slow and gradual, as can be seen from the effects of its first stage – the so called "Dokument L" (unsigned, 1940b), representing an appendix to Langer's report from the pre-war activity of the Cipher Bureau. "Dokument L" was written during the first half of 1940 and supposedly covers the period 1930-1940 (although its scope ends with the Pyry conference). In spite of its scope similar to the discussed document it counts only 31 pages – about half of the latter.

British reports prepared in 1945 include some details of the Polish pre-war activities, which are otherwise unknown from the available Polish sources. Alexander (1945, p. 18) describes the Polish attack on naval Enigma using the term "Forty Weepy". That term was coined by the

[2] In original: ENIGMA. Kurzgefasste Darstellung der Auflösungsmethoden.

Poles from the representation of numbers used by Kriegsmarine cipher clerks in 1937. The British codebreakers could not have known about that from their own experience, as the system was changed before they focused attention on the naval Enigma. The same report by Alexander names the call sign, AFA, of the German torpedo boat whose signals permitted Polish codebreakers to break the new Enigma procedure adopted by Kriegsmarine in May 1937. None of those details ("Forty Weepy" or AFA) are mentioned in the analysed document (or any other Polish sources) and must have been known to the British codebreakers from the original Pyry report.

The scope of information regarding pre-war efforts of the Polish Cipher Bureau available in the analysed document goes far beyond the limits of the original, Polish sources available so far. On the other hand it does not include some details quoted in the existing British reports. The structure of the document is very similar, even in translation, to the structures of other documents edited by the members of Cipher Bureau team ("Dokument L" or Rejewski's "Memories"), hinting at their common source. All those details considered together permit the positioning of the document as an intermediate link between the fragmentary sources known so far and their common reference – the original Pyry report.

4 Preliminary findings and conclusions

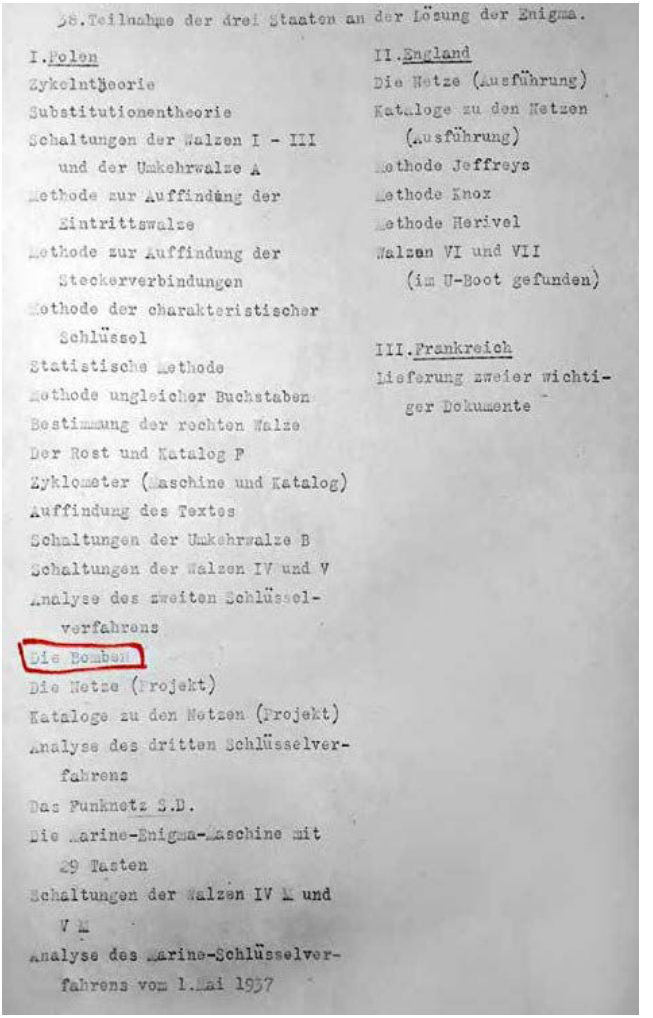
Systematic analysis of this recently found document is far beyond the scope of this paper, although the preface to the edited version (Grajek, 2017) of the report provides its early stage. The document, although obviously not identical to the original Pyry report, represents the best approximation currently available. It has been created by the same team, for the similar purpose and using the same language. It is the first material proof of otherwise obvious fact – the transfer of Enigma secrets by Polish Cipher Bureau to the Allies, which was found in the Allied archives. This author hopes that this information might spark a wider search for its presumed predecessor – the original Pyry report.

Most facts presented in the report are known from other sources, in particular from "Dokument L" and Rejewski's "Memories"; however, in the discussed document they are presented in a more systematic way than in other versions. At least some novel elements deserve special attention. The first one concerns the radio network of the German Sicherheitsdienst (S.D.). Section 34 presents the history of Polish struggle with the S.D. network between its first appearance in October 1937 and a major change on 1 August 1939. Messages in the S.D. network were masked with a 3-letter code before enciphering with Enigma. That did not prevent Polish codebreakers from breaking both the code and the Enigma key and reading the messages up to 31 July 1939.

This statement contradicts the opinion formulated in Dilly Knox's (1939a) report from the Pyry meeting, and repeated since then by numerous sources, that Poles were unable to read Enigma after the change of the indicator structure on 15 September 1938. The statement in Section 27 reinforces this argument indicating that the military key from 25 August 1939, the day of general German mobilization, was the last broken day before the evacuation of the Cipher Bureau from Warsaw.

Section 29 refers to the preparation by Bletchley Park staff of a special catalogue already proposed by the Poles before the outbreak of war. Lack of resources prevented the Polish team from implementing its own idea, but the more resourceful British were able to manufacture the proposed catalogue, which went into history as Jeffreys' sheets. Jeffreys' sheets represented an extension of Zygalski sheets; while the latter identified only the location of a female, the former permitted also to identify the character corresponding to the female ("(…) we had the idea to create catalogues with characters that would correspond to all female cases, (…) now the British (…) put our plans into practice").

Section 30 offers an update to the history of the Herivel method, which was brilliantly conceived but useless as long as the positions of the turnover notches in rotors IV and V were unknown. Herivel's discovery was complemented by the Polish team, who identified the notch positions in both rotors and communicating them to BP thereby enabling the practical application of the Herivel Tip.



38.Teilnahme der drei Staaten an der Lösung der Enigma.

I.Polen
Zykelntheorie
Substitutionentheorie
Schaltungen der Walzen I - III
und der Umkehrwalze A
Methode zur Auffindung der
Eintrittswalze
Methode zur Auffindung der
Steckerverbindungen
Methode der charakteristischer
Schlüssel
Statistische Methode
Methode ungleicher Buchstaben
Bestimmung der rechten Walze
Der Rest und Katalog P
Zyklometer (Maschine und Katalog)
Auffindung des Textes
Schaltungen der Umkehrwalze B
Schaltungen der Walzen IV und V
Analyse des zweiten Schlüssel-
verfahrens
Die Bomben
Die Netze (Projekt)
Kataloge zu den Netzen (Projekt)
Analyse des dritten Schlüsselver-
fahrens
Das Funknetz S.D.
Die Marine-Enigma-Maschine mit
29 Tasten
Schaltungen der Walzen IV M und
V M
Analyse des Marine-Schlüsselver-
fahrens vom 1.Mai 1937

II.England
Die Netze (Ausführung)
Kataloge zu den Netzen
(Ausführung)
Methode Jeffreys
Methode Knox
Methode Herivel
Walzen VI und VII
(im U-Boot gefunden)

III.Frankreich
Lieferung zweier wichti-
ger Dokumente

Figure 1: Final section of the analysed document - contributions of the three states to the breaking of Enigma

Section 31 refers to the new Enigma ciphering procedure used from 1 May 1940. We learn that some German cipher clerks started to use it prematurely, on 30 April. The Poles, who managed to break the military key for that day, were able to work out the procedure and communicate its details to Bletchley.

While sections 1–32 have a more or less chronological structure, section 33 is dedicated to the S.D. network, Sections 34–37 break the chronological narration and represent an appendix dedicated to the area only incidentally covered in the reports known so far – the ciphers of the German Kriegsmarine. The story long established among Enigma historians states that while Poles provided the foundations for breaking the Wehrmacht and Luftwaffe ciphers, breaking the Kriegsmarine Enigma represented a purely British adventure. The analysed document presents this question in a new light. The Poles were obviously watching the evolution and breaking the Kriegsmarine ciphers from their non-machine beginnings to the establishment in May 1937 of the system used during the war. The report confirms that they were able to work out the details of the new procedure and, thanks to the German blunder in the transition period, to

break enough messages to provide the British codebreakers with the reference material for their own efforts. Alan Turing and his team designed a number of methods (EINS-ing, banburismus) which could assure regular decryption operation once the system is first broken, however they could not advance their practical mastery of the cipher beyond the point reached by the Poles in 1937. Their final success in 1941 was based both on the information provided by the Poles and the documents captured on board the seized German ships.

Section 38 represents an element of the document most appealing to the reader's mind; it offers an enumerative list of elements contributed by the three participants of the cryptologic cooperation until June 1940 (cf. Figure 1 below). While this picture has changed significantly in the later stages of war, there is no doubt that during the first year of this conflict, the Enigma adventure was still heavily dominated by the achievements of the Polish Cipher Bureau team.

Acknowledgements

I would like to express my gratitude to Sir Dermot Turing for providing an important clue, and to Philippe Guillot for assisting my research. I would like to thank also the Internal Security Agency of Republic of Poland for its help in publishing the source version of the document.

References

Aldrich, Richard J. 2010. *GCHQ. The Uncensored Story of Britain's most secret intelligence agency*, Harper Press.

Alexander, C.H.O'D. 1945. *Cryptographic History of Work on the German Naval Enigma*, NA HW 25/1.

Bertrand Gustave. 1973. *ENIGMA ou la plus grande énigme de la guerre 1939-1945*, Librarie Plon, Paris

Cave Brown, Anthony. 1975. *Bodyguard of Lies*, Harper and Row.

Davies, Norman 2008. *Europe at War 1939-1945. No Simple Victory*, Pan Macmillan.

Denniston, A. G., *How News was Brought from Warsaw at the end of July 1939*, NA 25/12

Grajek Marek. 2017. Sztafeta Enigmy. Odnaleziony raport polskich kryptologów, ABW, Centralny Ośrodek Szkolenia ABW, Emów.

Knox, A. D. 1939a. *Letter to A. G. Denniston*, 1939, NA HW 25/12

Knox, A. D. 1939b. *Memorandum*, NA HW 25/12.

Langer, Gwido Karol. 1945. *Sprawozdanie dotyczące ewakuacji Ekspozytury Nr 300*, Instytut Józefa Piłsudskiego w Londynie, 709/133/5.

Mahon, A.P. 1945. *The History of Hut Eight*, NA HW 25/2.

Milner-Barry, Philip Stuart (ed.). 1945. *The History of Hut Six*, NA HW 4/70.

Rejewski, Marian, Zygalski, Henryk. 1940. *ENIGMA 1930-1940. Metoda i historia rozwiązania niemieckiego szyfru maszynowego (w zarysie)*.

Rejewski Marian. 1967. *Memories of my work at the Cipher Bureau of the General Staff Second Department 1930-1945*, Adam Mickiewicz University Press, Poznań 2013

Stevenson, William. 1976. *A Man Called Intrepid*, Skyhorse Publishing, New York.

Unsigned. 1940a. *Notice technique en allemande [sans date]*, SHD DE2016 ZB25 6, Dossier 281.

Unsigned. 1940b. *Dokument L, appendix to Lt. Col. Langer's report on Polish Cipher Bureau's pre-war activities*, Instytut Józefa Piłsudskiego w Londynie, 709/133/5.

Winterbotham, Frederic. 1974. *The Ultra Secret*, Weidenfeld and Nicolson, London

The Poles and Enigma after 1940: le voile se lève-t-il?

Dermot Turing
68 Marshalswick Lane, St Albans, UK
dermotturing@btinternet.com

Abstract

Recently declassified papers, together with other archival material, begin to reveal more details of the activities of the Polish code-breakers after the outbreak of war in France in 1940. Despite challenging operating conditions, they continued to work on Enigma problems, though without the benefits of the new technology developed at Bletchley Park. Their role in the war effort, with particular focus on Enigma, can thus be re-examined. Although various questions remain unanswered, it is fair to conclude that the Polish contribution continued to be valued by the Allies, and that the role played by the Polish code-breakers in the final year of the war needs to be re-evaluated in light of the prevailing political climate.

1 Introduction

It is a persistent myth that the Polish code-breakers who had successfully attacked the Enigma cipher before World War 2 were rejected by the UK's Government Code and Cypher School (GCCS). It is, however, just that, a myth: GCCS made concerted efforts in 1940 after both the fall of Poland and the fall of France to have the Poles join Bletchley Park.[1] Instead, the Poles were integrated into the operation of Gustave Bertrand, initially as part of the official French Service de Renseignements and, after the Armistice agreed between France and Germany, as part of the Vichy regime's Bureau des Menées Antinationales (BMA) at a secret location called 'PC Cadix'. This state of affairs continued until the takeover of the Zone Libre of France in November 1942, when after some adventures, the survivors of the Polish team were brought to the UK and integrated into the cryptanalytical team of the Polish General Staff located at Felden, just outside London (Rejewski, 2011).

A more genuine mystery concerns the actual work of the Poles after they left Poland, and the extent to which they were able to work on Enigma ciphers. It is well understood that, during the first period at 'PC Bruno', before the invasion of France, they were attacking Enigma using the Zygalski sheets method (Kapera, 2015). But their later work at PC Cadix and Felden has, until recently, remained more obscure. In 1944, Marian Rejewski wrote a semi-official memorandum,[2] objecting to being excluded from current work on Enigma, which has been interpreted as further evidence of side-lining of the Polish code-breakers by the official British authorities. Borrowing a title from the work of Paul Paillole on Enigma (Paillole, 1985), this paper looks at the archival material concerning the Polish team's work, considers the extent to which the veil has been lifted from it, and re-examines the nature of Rejewski's discontent.

2 The Source Materials

There are three principal contemporary accounts of the Polish codebreakers' activities in the period 1940-1945: by Gwido Langer,[3] by Gustave Bertrand,[4] and by Marian Rejewski (2011). Comments may be made about each of them. Langer's account was prepared as part of his campaign for rehabilitation with the Polish General Staff, which had been induced to question Langer's leadership of the Polish team at the

[1] UK National Archives (TNA) HW 14/3 (Jan 1940), HW 14/5 (Jun 1940).

[2] Polish Institute and Sikorski Museum (PISM), London, Kol 242/92 (Jul 1944).

[3] PISM Kol 79/50 (1946).

[4] Service Historique de la Défense (SHD), Vincennes, DE 2016 ZB 25/1 (1949).

Proceedings of the 1st Conference on Historical Cryptology, pages 95– 102,
Uppsala, Sweden, 18-20 June, 2018

time of its forced withdrawal from France in late 1942. The circumstances in which Bertrand's account - only declassified in December 2015 - was prepared in 1949 are less certain. However, his motivation can be imagined. At that time it was important to Bertrand, who had acquired a senior position in the intelligence service re-established by President de Gaulle after the war, to bring to the fore his patriotic Resistance credentials notwithstanding his arguably-dubious association with the Vichy regime during the period of the BMA. Rejewski's account, prepared in the late 1960s, was careful to avoid any mention of activities which might expose him further to the attentions of the Soviet-inspired Polish security services (Polak, 2005). The ambiguity of the position of Bertrand in relation to the Vichy régime after the Armistice of June 1940 led to a degree of concealment, even from Bertrand himself, of the true nature of the Polish operation (Medrala, 2005)[5]. The British were also concerned as to where Bertrand's loyalties lay.[6] Each of these reports, then, may be open to an accusation of partiality or selective reportage.

Notwithstanding these criticisms, the three accounts may be relied on for what they say about the nature of the cryptological activities of the Polish team, except in that Rejewski's account we are unlikely to find evidence of attacks on Russian ciphers. In relation to the assault on German Enigma, all three accounts might be expected to be straightforward and reliable, if not complete.[7]

In addition to the three main accounts, there is a wealth of correspondence and supporting evidence in the UK National Archives, the remaining Polish Intelligence Bureau archives at the Polish Institute and Sikorski Museum in London, and the dossiers of original papers accompanying Bertrand's 1949 account. These last-mentioned dossiers, only recently declassified, provide a new and informative perspective on the cryptanalysis conducted under Bertrand, including for the period when the Polish team was included within his organisation. Taken together, the materials build a good picture of the activities of the Polish code-breakers during the years 1940 to1945, and facilitate a re-assessment of their contribution and of their ongoing involvement in the Enigma story.

2.1 Literature

The work of the Poles on Enigma has been covered by many authors (Grajek, 2010; Garliński, 1979; Kozaczuk, 1998) to name just a few. Their achievement in uncovering the workings of the Wehrmacht Enigma machine and finding methods to expose the daily key-settings in use has, naturally, been the focus of these works. A smaller body of scholarship focuses specifically on the Poles' activities after June 1940, when their operating conditions had become much more difficult. Medrala (2005) gives a comprehensive and objective account of this period, but his sources revealed little about the nature of the code-breaking activities or the methods used. Ciechanowski and Tebinka (2005) specifically discuss Enigma, but in relation to the period after June 1940 they have little to add on what ciphers were broken or how.

Paillole (1975) and Navarre (1978) provide much insight on the Vichy period, but they cover all aspects of intelligence, rather than focusing on cryptanalysis. Given the background, with Poland overrun by Germany and the USSR, one might expect the efforts of the Polish code-breakers to have been directed against those powers, and not, for example, following the more complex agenda of Vichy, which included the Allies as objects of its intelligence-gathering.[8] Bloch (1986) focuses on the code-breakers, raising a number of pertinent questions concerning the Polish team, and their relationship with Bertrand; but like the other authors does not go into detail on the ciphers or techniques. In any case,the French writers all draw heavily on Betrand as their source. Bertrand's own book (1972) is entitled 'Enigma' and gives the impression that Enigma must have been the main, if not the only, target of the Polish team. However, the hypothesis that the Poles were devoting themselves at this time to Enigma, without code-breaking machinery and possibly

[5] Langer's account also shows how thousands of encrypted messages were relayed by his team from Polish Intelligence in North Africa to London.

[6] See, for example, TNA HW 14/8, telegrams of November 1940.

[7] It may, however, be observed that the typewritten account of Enigma code-breaking entitled 'Kurzgefasste Darstellung der Auflösungsmethoden', also revealed as part of the Bertrand Archive (SHD DE 2016 ZB 25/6, Dossiers Nos. 281 and 282), is not comprehensive, and conceals important facts now known about co-operation between the Allies on Enigma cryptanalysis. The three accounts mentioned may also suffer from the same issue of selective reportage.

[8] Cf. Paillole (1975).

without even an Enigma machine, presents some difficulty; existing literature does not face up to that challenge.

3 The Cadix Period

After the fall of France, the Polish code-breakers were rapidly evacuated to French North Africa, despite the plea of Alastair Denniston, the head of GCCS, to assimilate them into his team at Bletchley Park. There, there was a near-mutiny when some of the team, including notably Marian Rejewski and Jerzy Różycki, did not want to return to France but to go to Britain instead. Gwido Langer put down the rebellion and the team moved to a new location near Uzès in the so-called Zone Libre, the Château des Fouzes, in October 1940. The conditions were sub-optimal: the code-breakers complained of having to peel potatoes, chop wood, and do other manual labour, and the nearest bath was 27 km away; but on the other hand Bertrand had arranged for the team's work, accommodation and wages to be funded by the Vichy Government (Bertrand, 1972).

Initially, the team had to struggle to obtain intercept material to work on, though Bertrand arranged a system by which the organs of the Vichy state would feed intercepted encrypted material to him to be worked on. Insofar as this was manually-enciphered material, the talented Polish team were able to tackle it without special equipment or machinery. So it appears that a substantial amount of the work carried out consisted of an attack on German transposition ciphers, notably a difficult double-Playfair method, though there were also successful attacks on Swiss machine ciphers and, in a moment causing some embarrassment to the Poles themselves, on the Poles' own cipher machine Lacida (Rejewski, 2011). The targets included the Wehrmacht, operating all across Europe from France to well beyond the Soviet frontier, the SS and other 'police' units, the Abwehr and the Sicherheitsdienst in France and North Africa, and the German Armistice Commission (Kozaczuk, 1998).

3.1 Enigma

The paucity of resources at PC Cadix was not limited to firewood and intercepted signals. In the flight from Poland, the Polish team had been able to bring with them only one of their synthetically reconstructed Enigma machines. With the one they had sent to Bertrand through the diplomatic bag in 1939, that made a total of two to work with. Bertrand had just made arrangements for the production of duplicates of the synthetic Enigma machines by a factory in Paris when the invasion of France took place.[9] For the purposes of the reproduction, one of the precious machines had been dismantled, leaving the team with only one. Before the invasion, a teleprinter link between Bertrand at PC Bruno and Britain had enabled some degree of sharing of key-finding results derived from Zygalski's sheets, and some decipherment of intercepts, but these had little impact on military operations[10] and in any case the work had come to an end with the evacuation of PC Bruno. Evidently, at PC Cadix, there was at best the one surviving Polish reconstruction to work with, and none of the sophisticated key-finding machinery which the British Enigma team at Bletchley Park were beginning to exploit from mid-1940 onwards.

Thus it is legitimate to enquire to what extent the Poles at PC Cadix were able to work on Enigma, if at all, and if so how. In the first place it must be mentioned that the attack on Swiss machine ciphers was an attack on Enigma. 'The Swiss machine turned out to be an ordinary commercial model of Enigma, naturally with different internal rotor connections' (Rejewski, 2011). Tackling this machine would have been straightforward for Rejewski and his colleagues, who had honed their skills on the much harder Wehrmacht version of Enigma without the modern machinery now in use at Bletchley Park. Reverse-engineering the Swiss machine, without the fearsome plugboard, would have been a challenging but ultimately routine task, and Rejewski gives a brief description of it in his account.

However, a substantial contribution to intelligence derived from Wehrmacht Enigma messages was not likely to be feasible without the assistance of modern technology. Zygalski's sheets had been rendered obsolete by the change in key-transmission procedure adopted in May 1940, after which the Germans ceased to encipher the 'indicator' (the required orientation of the

[9] Bertrand 1949 report, and dossier No.272.

[10] As both the Langer account of 1946 and the Bertrand account of 1949 graphically describe.

three Enigma rotors for the transmitted message) twice over. From that point onwards, there were basically two methods for key-finding. The first was to use what the British called 'Cillying' and 'Herivelismus', and the Franco-Polish team called the 'Method Kx' (after the British cryptanalyst Dilly Knox, who had presumably described the technique to them at one of the trilateral conferences in 1939). Cillying assumes that the German operator has chosen a predictable six-letter word like HITLER, or another predictable sequence like QWERTZ, for the indicator; the first three letters (transmitted in clear) give a clue to the second three (which are enciphered). Herivelismus is named for John Herivel, a Bletchley Park code-breaker who imagined an operator would be lazy enough to use the last position of the rotors (or a position very close to it) showing at the end of the previous transmission - which helped when a long message was broken into several parts (Herivel, 2008). These methods could have been exploited at PC Cadix without the need for special technology - apart from the much-needed replica Engima machine itself.

The other method of tackling Enigma in the period after October 1940 was machine-based. Developing ideas suggested by the pre-war Polish bomba, Bletchley Park cryptanalysts, including Alan Turing, had invented a new means of key-finding based on guessed-at message content and running a logic-check through all 17,576 possible combinations of rotor start-positions. Their machine, the famous Bombe, was used to find thousands of keys each month for the remainder of the war. This option was denied to Bertrand and the team at PC Cadix: indeed, it seems that Bertrand was kept largely, if not wholly, in the dark about the degree of success achieved by the British with their Bombes.[11]

However, Bertrand had not lost contact with his engineering firm in Paris, and eventually the reproductions of the Polish reconstructed Enigmas began to arrive in pieces for reassembly at PC Cadix. By 10 September 1942, Bertrand was able to contact his British liaison and report that he had reassembled three of these Enigma machines,[12] suggesting that one of them be used for secure communication between London and PC Cadix.[13] Bertrand's cryptologist colleague Henri Braquenié noted with amusement that the arrival of the machines enabled PC Cadix to communicate with MI6 using Enigma technology: to rub in the irony he would sign off his messages (in cipher) with the words 'Heil Hitler' (Braquenié, 1975). However, the use of Enigma machines at PC Cadix, for any purposes, was short-lived. Within weeks of the approval by London of the use of the new Enigma-type machinery for communications, the possibility of the Zone Libre being overrun had become a live threat; the team at PC Cadix knew they were being tracked by the 'Funkabwehr', German counter-intelligence's radio direction-finding unit; and on 7 November 1942, continued operations at the château became imprudent. The premises were evacuated and code-breaking by the Poles in France came to an end.

3.2 Results

By all accounts the Polish team at PC Cadix were kept extremely busy for the two years they were there. Much of the work involved relaying (and re-enciphering) messages for London from the outpost of Polish Intelligence in North Africa, an activity which seems to have taken place under Bertrand's nose but without his knowledge. As for the actual code-breaking, PC Cadix was able to obtain copies of signals which were unavailable to Bletchley Park, which meant that the Polish team's reports on the activities of the SS as German forces moved east, following the outbreak of hostiliies with the USSR in 1941, were highly prized in London.[14] Those reports do not make comfortable reading, as they itemize round-ups and ethnic cleansing carried out in the newly-occupied areas of Belarus and the Ukraine.

Towards the end of the Cadix period, the code-breakers achieved a breakthrough against the hand ciphers of the Funkabwehr. In another irony, the trackers from the Funkabwehr who were hunting down illicit radio transmissions in the (increasingly Nazified) Zone Libre were themselves being tracked by their own prey. Gustave Bertrand built up a detailed profile of the Funkabwehr, its activities and personnel, its vehicles and locations, and above all its secret

[11] TNA HW 65/7 (Mar-May 1942).

[12] Medrala (2005), page 183, says there were seven machines of which four were reassembled models; unfortunately in this instance his source is not specified.

[13] TNA HW 65/7.

[14] TNA HW 65/7.

signals. The Cadix team thus knew exactly when the net was closing in; and Bertrand himself was able to equip de Gaulle with a detailed profile of German direction-finding and radio-suppression in occupied France, once he joined the Free French in 1944.[15]

These examples show that the Polish team continued to make a valuable contribution to intelligence based on decrypted signals throughout their time at PC Cadix. In conclusion, however, it seems unlikely that any significant results were obtained at PC Cadix by the Polish code-breakers as a result of decrypting Enigma. However, a different story emerges when the remnants of the team reached Britain in August 1943.

4 The Felden Period

The story of what happened to the Poles of PC Cadix after their forced departure is highly dramatic and in some instances tragic. Suffice it to say that only a handful, including Marian Rejewski and Henryk Zygalski, eventually made it over the Pyrenees, only to be arrested and spend several months in Spanish prisons. On 3 August 1943 the escaped Polish code-breakers - only five in number - were relocated to Britain, and assigned to the Polish signals intelligence unit at Felden, a rural hamlet situated on the outskirst of Hemel Hempstead, north-west of London. Felden was the heart of an operation, approved and directed by MI6, which was clandestinely monitoring the signals output of the USSR, notwithstanding that the USSR was notionally the ally of both Britain and Poland in the struggle against Germany (Maresch, 2005).

On arrival at Felden, Rejewski, Zygalski and their colleague Sylwester Palluth were assigned to 'Team N', which was directed against German rather than Russian traffic.[16] During this period, they enjoyed particular and noteworthy success against 'German Police' signals, and received commendation from Bletchley Park, relayed via MI6, for their work. To understand this better, it is necessary to know that the phrase 'German Police' covered a wide range of uniformed services carrying out a wide range of activities ordinarily associated with armed forces rather than law enforcement agencies. Nazi Germany had many such organizations, some substituting for mainstream Wehrmacht units in combat roles, and others engaged in 'special' activities now known to be part of the program for extermination of Jews and other classes of society. 'German Police' signals were thus regarded as being of significant value in building up an overall picture of German military and political activities and plans. In October 1943, the British told Polish Intelligence, 'We are very glad to receive the T.G.D. German traffic taken at Felden,' and 'Police Traffic is steadily gaining in operational importance'.[17]

4.1 TGD

The specific version of German Police signals on which the Poles were working was known by its old call-sign 'TGD'. TGD was described in the GCCS History of Hut 6 as 'the famous T.G.D.', with the comment 'this key was never broken during the war and to this day is one of the classic mysteries of Hut 6. It never cillied so far as we know and no convincing re-encodement from any other key was ever produced.'[18] Reports filed by Gordon Welchman of Bletchley Park's Bombe team in 1942 reinforce the idea that Bletchley Park had got nowhere with TGD, unlike other German Police ciphers based on Enigma.[19] However, from the GCCS reports it is quite plain that TGD was indeed an Enigma cipher, and one of particular significance, since it was immune to ordinary means of attack. The careful security measures in place to protect TGD traffic imply that the content of the signals was more sensitive than other SS material.

In terms of TGD's structure, the recently-declassified Bertrand archive includes an intriguing dossier (Dossier 278) prepared by the Poles in approximately 1940. This dossier has not been discussed in the previous literature, and it gives the missing technical detail on the cipher. The dossier was part of a series of intelligence exchanges between PC Bruno and Bletchley Park on technical matters, and it summarises the key procedure being used, and thus explains why TGD resisted the attacks which worked for ordinary SS messages. In summary, TGD used a rigorous key system which precluded cillies. All three letters of the indicator had to be different, and the message-setting was first enciphered using a substitution alphabet before

[15] SHD DE 2016 ZB 25/1, file 01H002.
[16] PISM Kol 242/64 (Oct 1943).
[17] PISM Kol 242/92, TNA HW 14/90.
[18] TNA HW 43/71 (undated, c.1946).
[19] TNA HW 25/27 (Mar, Jun, Dec 1942).

re-encipherment on the Enigma machine. (In practice this is unlikely to have made a major difference to security, and the dossier reports that the preliminary encipherment of indicators was discontinued before the war.) More significant was the jumbling-up of material normally located in a standardized way in a message's preamble: in TGD messages message-data like the sender, addressee, message-key and so forth could be positioned differently on different days, albeit following a pattern. The 'biggest surprise', according to the Polish authors of the dossier, related to the content of messages. A coding-system was used to mask the content (before the entire message was enciphered on the Enigma machine), but with a twist: only part of the text would be in code, and the rest was in plain-text. The toggle between code and plain-text would have made a crib-based attack to find the Enigma key extremely hard. The code was in three-letter groups which used no vowels and omitted Q, X and Y; Q denoted a shift from alpha to numeric, X was punctuation, and Y denoted a shift from code to plain-text. Instead of spelling out numbers in full, as in standard Enigma procedure, the alphabet was used (A, B, C, ... standing for 1, 2, 3, ..., with redundancy, so that K, L, M, ..., and V, W, Z would also stand for 1, 2, 3, ...). Unfortunately, the dossier does not divulge the extent to which the code-book had been reconstituted by the Poles.

The significance of the messages is mentioned briefly in the dossier. The Poles had, at the time the dossier was written, been monitoring exchanges between the Sicherheitsdienst headquarters in Berlin and various border outposts responsible for gathering political and other intelligence from Germany's annexed territories and peripheral states. At the time, before the outbreak of hostilities, this included reports on subversive action being taken on behalf of the Nazis. Evidently TGD traffic was at that time more high-level political material than short-term operational information. The extent to which the nature of the traffic had evolved by 1943 is difficult to ascertain.

4.2 A veil half-raised

The declassified dossier thus unveils part of the 'classic mystery' of TGD. But in doing so, it merely intrigues us with further unsolved puzzles. First, how was it that Bletchley Park was unable to exploit TGD, given that it had been armed with the dossier? The answer may be a lack of resources, or that Bletchley Park decided to focus on the Enigma keys that were susceptible to the Bombe technique. Breaking Enigma keys on a Bombe requires a crib, i.e. guessed-at plaintext, and without a history of prior decrypts it is a tough assignment to come up with a viable crib. Furthermore, the structure of TGD will have precluded the use of cribs. The Poles at Felden were not relying on Bombes, and it seems reasonable to infer that they dusted off their previous know-how and reapplied it in their new working environment.

A second intriguing feature of the success against TGD at Felden relates to Enigma machines. Not only is it absurd to imagine that the PC Cadix Poles managed to smuggle a counterfeit Enigma with them when they escaped, but there is sound evidence that the Enigma duplicates made in France remained there, with Rejewski and Zygalski making a special trip to France after the war's end to retrieve them from where they had been concealed.[20] Without an Enigma machine the effort against TGD at Felden would surely have been doomed. It would therefore appear that the British, who had been supplying Felden with equipment of various descriptions, may also have provided an Enigma (or more likely, a modified Typex machine reconfigured to emulate an Enigma, as used by deciphering clerks at Bletchley Park). Unfortunately there is no archival evidence to clarify how exactly the Poles did their work.

5 Rejewski's 1944 request

By the summer of 1944, as the Allied forces began their recapture of continental Europe from the Wehrmacht, the importance of German Police traffic to the overall intelligence picture waned. The Polish General Staff were told by MI6 that the British no longer required the 'German Police Intercepts' on 8 July.[21] If it is right that TGD signals were being relied on for the insights they provided into high-level thinking at the top of the Nazi hierarchy, the timing of the shut-down of work on TGD is no coincidence. By this stage in the war, Bletchley Park had begun to tap into a

[20] PISM Kol 242/69, Kol 242/93 (May 1945).
[21] PISM Kol 242/92.

far more powerful and informative source, namely the teleprinter traffic enciphered on the Lorenz Schlüsselzusatz device and broken at Bletchley Park with the help of novel electronic machinery. The change in British priorities for Felden also signalled a redisposition of Rejewski, Zygalski and Palluth, who were assigned in November 1944 to 'Team R', which was responsible for monitoring and decrypting Soviet traffic.[22] Their reassignment followed an unwelcome period of idleness and was, for Rejewski at least, an unwanted development. Rejewski was moved to write a long note, dated 20 October 1944, in which he eloquently sets out the Enigma-related debt owed by the British to the Poles and requests closer involvement in the British work against Enigma.[23] Rejewski's request was viewed sympathetically by Polish Intelligence, and passed on to the British, but nothing came of it.

By this date, though, Bletchley Park had become a thoroughly industrial operation, churning out intelligence based on its Bombes, in a volume which would have astonished Rejewski if he had been aware of the scale of the operation. While there remained brilliant code-breakers at Bletchley whose skills were put to use right up to the end of the war, the focus of intellectual attention was no longer the Enigma. The old hands who had met and learned to respect Rejewski and Zygalski were out of the picture: Denniston in a new role relating to diplomatic ciphers, Knox dead, and Alan Turing redeployed onto speech encipherment. Rejewski had no advocates at Bletchley, and, in truth, no Enigma-related role there. Moreover, it would have been wholly counter to the culture of secrecy at Bletchley Park to allow a Polish code-breaker to see the nature of the new operation there. The British brush-off must also be seen against the prevailing political climate, where Poland was, in 1944, thought to be an 'unreliable' ally owing to tension growing between the Poles, aggrieved at the murders at Katyn, and the acquisitive USSR.

Viewed in the light of the politics of 1944, Rejewski's plea takes on a different colour. Like all exiles whose family were left behind, Marian Rejewski was in no doubt that he intended to return home after the war. As future events would show, this was a courageous thing to do; but already in late 1944 it would have been plainly obvious that the Soviet influence in Poland was pervasive and pernicious. To be involved in the assault on Russian ciphers was an extremely unwelcome change for Rejewski, as it ratcheted up the danger-level for him personally. Yet precisely the same reasoning would have led Bletchley Park, assuming they were aware of his request,[24] to feel uncomfortable with Rejewski obtaining knowledge of the achievements and methods in use there, if Rejewski were going to go back to Poland after the war. Regardless of all the rhetoric about the USSR as an ally, the British were only too well aware that the Soviets needed to be watched, and what the dangers were. After all, it was the British who were sponsoring the Polish efforts at Felden which were directed against the USSR's secret messages.

6 Conclusion

The Polish attacks on the plugboard version of the Enigma machine in the 1930s stand as one of the most impressive achievements of mathematical cryptanalysis of all time. The fact that, after May 1940, the individuals who had created those earlier successes did not become part of the Bletchley Park team which took over, built from, and multiplied, their achievements, has been a source of dismay to many observers. It has been considered shameful that no place was found in Britain for Marian Rejewski and his colleagues after the fall of Poland or after the German takeover of the Zone Libre in France. No doubt, until late 1942, a valuable role could have been found for them at Bletchley Park alongside code-breakers of other allied nations who were already there. But the political weather had changed by 1943 when the Poles eventually arrived in Britain, and in any event the Polish code-breakers were still under Polish, not British, military command.

The fact is that the Poles did manage to carry on valuable cryptanalytical work in France until the end of 1942 and in Britain from 1943 until the end of the war. Only to a limited extent was their effort directed against Enigma, but that should not be regarded as official lack of interest in the Poles, rather as a decision about deployment of cryptanalytic talent in a changing world. What

[22] PISM Kol A.XII.24/63, Kol 242/54.

[23] PISM Kol A.XII.24/63.

[24] Rejewski's paper, or a summary of it, was almost certainly provided to MI6, but it may have gone no further. There is no indication in the GCCS files that it was received or acted upon at Bletchley Park.

the Poles actually did, both at PC Cadix and at Felden, was of high quality and highly regarded, and it should not be seen as a slight on them that they were asked to carry out this work.

Acknowledgments

The author acknowledges the invaluable assistance of Dr Janka Skrzypek in interpreting and translating Polish-language material and Dr Marek Grajek for useful discussions. He also wishes to thank the staff of the SHD, and of the Sikorski and Piłsudski Institutes in London for help with archival material, and to acknowledge the contribution of the reviewers of the draft manuscript for their helpful comments. No external funding was provided and no conflict of interest is believed to exist in the creation of this paper.

References

Bertrand, Gustave. 1972. *Enigma, ou la plus grande énigme de la guerre 1939-1945* PLON, Condé-sur-Escaut, France.

Bloch, Gilbert. 1986. *Quelques Eléments Relatifs au PC 'Cadix', à sa fin et au Sort de l'Équipe Polonaise* (unpublished manuscript) SHD GR 1K 953/2.

Braquenié, Henri. 1975. *Interview avec le capitaine Henri Braquenié,* in *'Geheimoperation Wicher', p318-328,* 1989, Karl Müller, Bonn, Germany.

Ciechanowski, Jan Stanisław, and Jacek Tebinka. 2005. *Cryptographic Cooperation - Enigma,* in *The Report of the Anglo-Polish Historical Committee,* vol 1, chapter 46 (Tessa Stirling, Daria Nałęcz and Tadeusz Dubicki, eds) Vallentine Mitchell, Edgware, UK.

Garliński, Józef. 1979. *Intercept* J.M. Dent & Sons Ltd, London, UK.

Grajek, Marek. 2010. *Enigma - Bliżej Prawdy* Rebis, Poznań, Poland.

Herivel, John. 2008. *Herivelismus and the German Military Enigma* M and M Baldwin, Cleobury Mortimer, UK.

Kozaczuk, Władysław. 1998. *Enigma* Greenwood Press, Westport, CT.

Kapera, Zdzisław J. 2015. *The Triumph of Zygalski's Sheets* The Enigma Press, Kraków-Mogilany, Poland.

Maresch, Eugenia. 2005. *The Radio-intelligence Company in Britain,* in *'Living with the Enigma Secret', p 185-200,* Bydgoszcz City Council, Bydgoszcz, Poland.

Medrala, Jean. 2005. *Les Reseaux de Renseignements Franco-Polonais 1940-1944* L'Harmattan, Paris, France.

Navarre, Henri. 1978. *Le Service de Renseignements 1871-1944* Plon, Évreux, France.

Paillole, Paul. 1975. *Services Spéciaux (1939-1945)* Robert Laffont, Paris, France.

Paillole, Paul. 1985. *Notre Espion chez Hitler* Robert Laffont, Paris, France.

Polak, Wojciech. 2005. *Marian Rejewski in the sights of the Security Services,* in *'Living with the Enigma Secret', p 75-88,* Bydgoszcz City Council, Bydgoszcz, Poland.

Rejewski, Marian. 2011. *Memories of my work at the Cipher Bureau of the General Staff Second Department* Adam Mickiewicz University Press, Poznań, Poland.

US Navy Cryptanalytic Bombe - A Theory of Operation and Computer Simulation

Magnus Ekhall
magnus.ekhall@gmail.com

Fredrik Hallenberg
fredrik.hallenberg@gmail.com

Abstract

This paper presents a computer simulation of the US Navy Turing bombe. The US Navy bombe, an improved version of the British Turing-Welchman bombe, was predominantly used to break German naval Enigma messages during World War II. By using simulations of a machine to break an example message it is shown how the US Navy Turing bombe could have been operated and how it would have looked when running.

1 Introduction

In 1942, with the help of Bletchley Park, the US Navy signals intelligence and cryptanalysis group *OP-20-G* started working on a new Turing bombe design. The result was a machine with both similarities and differences compared to its British counterpart.

There is an original US Navy bombe still in existence at the National Cryptologic Museum in Fort Meade, MD, USA. The bombe on display is not in working order and the exact way it was operated is not fully known.

The US Navy bombe was based on the same principles as its British version but had a different appearance and thus a different way of operation. The bombes were used to search through a part of the Enigma key space, looking for a possible Enigma rotor core starting position which would not contradict a given enciphered message and its plaintext (Carter, 2008).

A theory, based on previous research (Wilcox, 2006) and knowledge of how the British bombe works, is presented of how the US Navy bombe was operated and it is shown with a computer simulation that the theory is sound.

The computer simulation presents a graphical user interface and runs at approximately historically accurate speed. The simulator will be made available to the public.

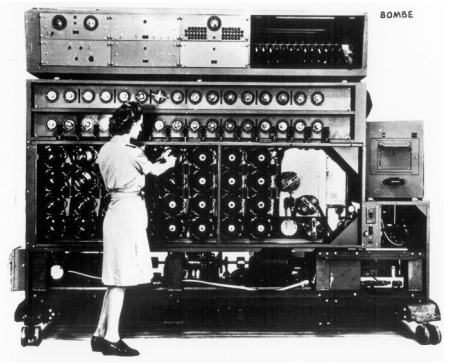


Figure 1: An operator setting up the wheels on a US Navy bombe. Source: NSA

It is assumed that the reader is familiar with the Enigma machine. This knowledge is widely available, for example in (Welchman, 2014).

To find an Enigma message key with the bombe it is necessary to have a piece of plaintext, a crib, corresponding to a part of the encrypted message. A crib could be a common word or a stereotyped phrase which is likely to be present in a message, for example *Wettervorhersage* which is the German word for *weather forecast*. The crib is used to derive a configuration of the bombe and an assumption of the Enigma rotor starting position is made. Once started the bombe will scan through all possible Enigma rotor core positions and stop when a position has been found that does not lead to a logical contradiction for the given crib (Carter, 2008). If a logical contradiction occurs then the state of the bombe represents a setting of an Enigma where it would not be possible to encipher the assumed plaintext to the ciphertext of the crib. Each stop is subject to further tests after

Proceedings of the 1st Conference on Historical Cryptology, pages 103– 108,
Uppsala, Sweden, 18-20 June, 2018

Position:	A	B	C	D	E	F	G	H	I	J	K	L	M
Plaintext:	K	R	K	R	A	L	L	E	X	X	F	O	L
Ciphertext:	L	A	N	O	T	C	T	O	U	A	R	B	B

Table 1: Crib and corresponding ciphertext used throughout this paper

which the bombe is automatically restarted.

If a test is passed, relevant information on the stop in question is automatically printed onto paper (Desch, 1942).

2 Example Message

The bombe simulation will be tested using a real message sent May 1st 1945 (CryptoMuseum, 2017). The crib is the thirteen first letters of the plaintext. The wheels used for this message was β, V, VI and VIII, with the thin C-reflector being used. The original Enigma rotor start position was {CDSZ} (this notation will henceforth be used to show positions of the corresponding wheels). This means that the leftmost rotor on the Enigma, in this case the β rotor, is set to position C, the second rotor is set to D and so on. The ring setting of the rotors for this message was {EPEL}. Note that the difference between the ring setting and the rotor start position is 24, 14, 14, 14 positions respectively. This is called the rotor core starting position.

The row labeled "Position" in table 1 shows what setting the rightmost Enigma wheel would have when encrypting a given plaintext letter into ciphertext. The assumption is that the Enigma machine would have been set to {ZZZZ} before the message was coded. This leads to the first letter being encrypted at position {ZZZ**A**}, the next at {ZZZ**B**} and so on.

The plug board connectors, *Stecker* in German, used on the Enigma for this message was:

A	B	C	D	H	J	L	P	S	V
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
E	F	M	Q	U	N	X	R	Z	W

The letters of the alphabet not listed in the plugboard connector pairs above did not have a wire connected on the plugboard which results in them being electrically connected to themselves. There were normally ten plugboard cables used in the daily Enigma key, leaving six letters self-connected (Copeland et al., 2017).

3 Setting Up the Bombe

Preparing the bombe to work on a message consists of a number of steps. Firstly, the wheels need to be selected and set to the appropriate starting positions. Secondly, the bank switches need to be set according to the letters in the crib. Thirdly, one or two input switches need to be activated. Finally, some of the printer cables are connected to the diagonal board.

3.1 Enigma Rotor Equivalent Wheels

The bombe has sixteen wheel banks of four wheels with each wheel bank representing the rotors of an Enigma machine. Eight wheel banks are on the front of the bombe and eight are on the back.

The bombe was primarily designed to break messages encrypted with the M4 Enigma which had four rotors. However, it could also work on messages encrypted with a three-rotor Enigma such as the one used by the German Army. For this purpose there is a switch which selects between three- or four-wheel mode. In three wheel mode, the slowest wheel in each of the 16 wheel banks would be stationary (Desch, 1942). By observing how the wheels in a wheel bank are interconnected it can be assumed that the bottom wheels of each wheel bank would not move in this configuration.

To configure the bombe for the message, a wheel order which is to be tested is installed. As mentioned in section 2 the correct wheel order is already known in this case. The corresponding wheels are loaded onto all wheel banks of the bombe. Also, the "thin C"-type reflector cables are connected to all the reflector plugs on the bombe.

In reality the wheel order was not known but many different wheel orders could be tested in parallel, one wheel order per bombe. A total of 121 US Navy bombes were built (Wilcox, 2006).

Normally it is assumed that the second wheel of the Enigma does not advance during the crib. Since the second wheel of the Enigma will advance one step once or twice per revolution of the first wheel there is a high probability that this is not the case, and if so, the bombe will fail to find a possible solution. There are techniques that could have been used if a second wheel turnover was suspected, but those are not in the scope of this paper.

With the example message there was in fact a second wheel turnover before the first letter was encrypted. This knowledge will be taken into ac-

count in the following discussion. In practice this could not have been known, but the bombe would still have found a solution since there is no further second wheel movement during the crib; the entire crib has one and only one wheel position for the second wheel. The difference is that the second wheel now has to be set to A instead of Z which it otherwise would have been assumed to be. Therefore the bombe is adjusted so that the wheels on wheel bank 1 are set to 25, 25, 0, 0. This corresponds to {ZZAA}.

The wheels of wheel bank 2 are set to 25, 25, 0, 1 = {ZZAB}, wheel bank 3 to 25, 25, 0, 2 = {ZZAC} and so on all the way up to wheel bank 13 which is set to 25, 25, 0, 12 = {ZZAM}.

The wheel order, reflector plugs and the start position of the bombe wheels are now set up. The next step is to connect the wheel banks according to the letters of the message.

3.2 Bank Switches

There are two 26-step rotary switches for each wheel bank. One for the input letter to the bank and one for the output letter. The rotary switch connects the rotor bank to the diagonal board which utilises the symmetrical properties of the Enigma plugboard to interconnect the bombe wheel banks. All of the 32 switches are located on the front of the bombe. These switches eliminate the need of a plug board as found on the back of the British bombe and thus makes setting up a crib on the bombe much faster (Turing, 1942).

The British bombe, on the other hand, could have up to three cribs or wheel orders connected at the same time on one bombe. The British bombes usually had 36 wheel banks of three wheels each, corresponding to 36 Enigma machines.

The plaintext letters of the message are considered to be the input to the corresponding rotor bank and the ciphertext letters to be the output.

For example, for wheel bank 1 which corresponds to the first letter of the message, the input is K and the output L. Therefore the left switch of the two bank switches corresponding to rotor bank 1 is set to 10 for the letter K. The right switch is set to 11 for L.

For wheel bank switch 2 the input switch is set to 17=R and the output switch to 0=A.

The rest of the wheel bank switches are set up in the same way with the last, number 13, set to 11=L, 1=B according to the last letter of the crib (see table 1).

3.3 Wheel Positioning

Apart from the four wheels in a wheel bank, one for each Enigma rotor, there is also a reflector plug which has the same function as the reflector on the Enigma. Since the top wheel of the bombe is connected to the reflector plug it can be assumed that this represent the leftmost Enigma-rotor which is connected to the reflector of the Enigma. The bottom wheel of the bombe corresponds to the rightmost Enigma-rotor.

3.4 Input Switch

The bombe works by injecting a test current into a position corresponding to a certain letter of the diagonal board. This current then propagates through the system and stops the bombe if it fails to reach all other letters of the alphabet.

To select the letters where test currents are injected the bombe has two 26-step rotary switches marked PRI and SEC for primary and secondary. Normally only the primary input is set. When using a crib where the letters of the crib and the corresponding ciphertext are forming two separate graphs the secondary input is also needed.

The input should be connected to a frequently occurring letter in the crib. L is selected as it occurs at three places in the example message. The primary input switch is switched to 11 which corresponds to L. The secondary input switch is not needed in this case and is set to OFF.

3.5 Printer

On the back of the bombe the cables of the printer are connected to the diagonal board sockets representing the letters in the message. The following letters are present: A, B, C, E, F, K, L, N, O, R, T, U, X. The printer cables for these letters should be connected to their respective socket on the diagonal board with A=0, B=1 and so on.

4 US Navy Bombe Model

A theoretical model is presented of how it is assumed the different parts of the US Navy bombe interacted.

4.1 Diagonal Board

The central component in the US Navy bombe is the diagonal board. The diagonal board has 26 input nodes, one for each letter of the alphabet. Each

input node consists of 26 conductors, one for each letter of the alphabet. The diagonal board utilises the fact that if a letter A on the plugboard of the Enigma is connected to letter B, then it follows by the symmetrical design of the plugboard that letter B must be connected to A. Let conductor y of diagonal board node x be denoted $DB(x,y)$, then the connections on the diagonal board can be described: $DB(x,y)$ is connected to $DB(y,x)$.

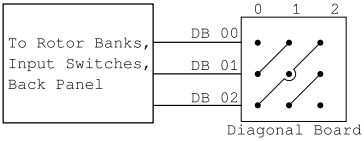


Figure 2: The principle of the diagonal board, here in a simplified form as if the alphabet would only have three letters. The actual diagonal board is of size 26 x 26.

The use of the diagonal board greatly reduces the number of false stops the bombe otherwise would have had. All the rotor banks of the bombe can be connected to any of the letters on the diagonal board.

There are also two input switches which can inject a test current to any node on the diagonal board.

On the back of the US Navy bombe there is a panel which exposes the diagonal board. The checking logic and printer is connected to to the diagonal board through cables plugged into sockets on this panel.

Each input node on the diagonal board thus has quite a large number of potential inputs connected in parallel.

4.2 Rotor Banks

The 16 rotor banks are connected to the diagonal board via the two rotor bank switches A and B (see section 3.2) of each bank as illustrated in figure 3.

5 Operation

Once the message has been set up on the bombe the machine is started. It will iterate through every possible rotor core position, searching for a condition which will satisfy the crib.

The bombe will stop if the test current fails to reach all 26 conductors of the input letter node on the diagonal board. This is called a "cold point test" and was implemented with a *Rossi circuit*

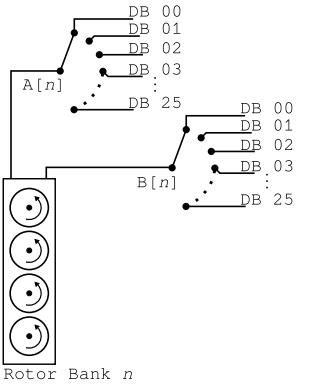


Figure 3: Rotor bank n, where n = 1, ..., 16. All wires in this figure are 26-way. The 26-way input switches A and B of rotor bank n controls where on the diagonal board the two rotor bank nodes are connected. DB 00 is diagonal board position 0, corresponding to the letter A, and so on.

which can be seen as a 26-input AND-gate. Following this, a second test called the "hot point test", is automatically performed. This test applies a voltage in sequence to the 26 conductors of the input letter node on the diagonal board. This test will determine the possible plugboard connections for the stop and if contradicting connections are found the stop is ignored (Desch, 1942).

When a stop which passes the tests mentioned above has occurred, the ring setting for that rotor core position will be printed along with the plugboard connections that could be concluded from the given bombe connections.

The operating speed of the US Navy bombe was much higher than the British Turing Welchman bombe. The fastest wheel on the US Navy bombe rotated at about 1725 revolutions per minute, almost twenty times the speed of the British bombe. A complete four wheel run on the US Navy bombe took approximately 20 minutes (Wilcox, 2006).

The simulation of this example message yields 188 stops out of the $26^4 = 456,976$ possible rotor core positions tested. Of these, only one stop will pass the hot point test resulting in the following information being printed:

- Ring setting: 24 14 14 14
- Plugboard: B/F E/A K/K O/O T/T X/L

The exact format of the original printouts is unclear. The information in the example above would most likely have been represented by numbers only (Wilcox, 2006) as this is the norm on the rest of the bombe. This matches the rotor core starting position of the Enigma used to encrypt the message (see section 2).

The setting found will be subject to further, manual, tests using a simplified Enigma machine: the *M-9 Checking Machine*. The output from this process would be either more of the plugboard connection pairs, or the conclusion that the stop was in fact false.

After this there would be a brief set of trial and error tests to find a suitable ring setting that would decrypt the whole message.

6 Computer Simulation

A computer simulation was setup based on the model described in section 4. The main difficulty of simulating the bombe lies in the parallel nature of the electrical circuit implemented by the bombe. For each rotor position the simulator has to calculate what happens if an input current is injected into a certain position in the circuit. This input current is propagated until it does not reach any new nodes. At that time the stop condition is checked. The US Navy bombe tested about 750 rotor positions per second. Since the simulator aims to run at a historically accurate speed, for every frame drawn on the screen several rotor positions will have to be simulated and tested.

To implement this the simulator uses a switchboard model, which basically is a bi-directional list of nodes that can be connected to each other. Each switchboard node has a state which is a list of 26 booleans, one for each letter of the alphabet. This switchboard does not exist in the bombe but is a way to handle the parallelism described above.

Most components in the modeled bombe will add connections to the switchboard, this includes the rotor banks, the printer, the diagonal board and the bank switch selectors. Each of the components owns one or more switchboard sockets which allows the components to react to voltage state changes from the switchboard and to send an updated state.

At every iteration the simulator clears the states of all the nodes in the switchboard. It is then given the input voltage in one of its nodes. The switchboard propagates this change of state to the node

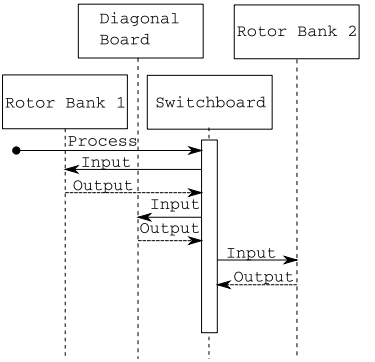


Figure 4: Sequence diagram showing how the central switchboard component of the simulator distribute information between two rotor banks and the diagonal board.

that is connected, according to the list of nodes, to the input. This triggers the owner of the connected node to calculate the effect of this state, which usually will propagate the voltage state to another node in the circuit, and so on. This process is repeated until no node has registered any change. The simulation of that rotor position is then complete. In the real bombe this process would be carried out almost instantaneous. Figure 4 illustrates how the switchboard works.

The simulator, which runs at approximately the same speed as a real US Navy bombe, lets the user setup and run the machine by a graphical user interface as shown in figure 5.

7 Conclusion

It has been shown, using an authentic M4 Enigma message, that the simulated US Navy bombe is able to find the correct rotor core starting position as well as six correct plugboard connector pairs.

The simulated bombe stopped 188 times but only one stop, matching the correct Enigma key, passed the automatic tests. This shows that the theory presented in this paper is plausible but further research is needed to verify if this was exactly how the bombe was operated.

Some effort has been made to make the simulation as graphically accurate as possible. The photographs that exist of the US navy bombes shows that there were several different models in operation. The simulator is mostly based on photographs of the US Navy bombe located in the Na-

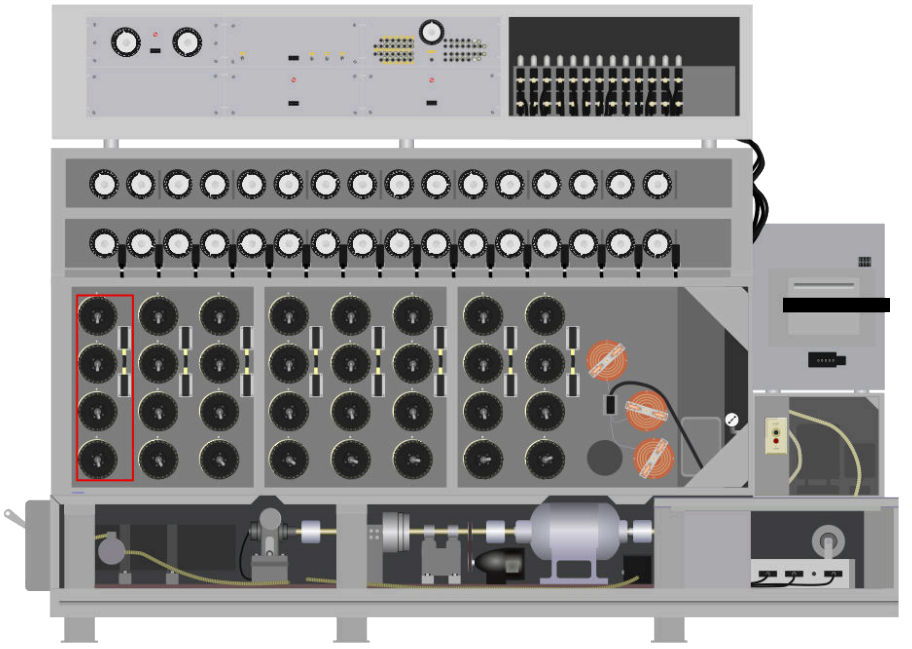


Figure 5: US Navy Bombe computer simulation screenshot showing the front of the bombe. By interacting with the various parts of the bombe in the simulation, a crib can be set up and run. The simulator is written in the *Haxe* programming language and uses the *NME* framework.

tional Cryptologic Museum. This bombe is supposedly the last one manufactured.

8 Acknowledgments

We would like to thank the National Cryptologic Museum for providing us with useful information on the US Navy bombe, and we thank the three anonymous reviewers for their valuable comments. We would also like to thank Dr. J Jacob Wikner, Associate Professor at the Department of Electrical Engineering, Linköping University, Sweden, for hints and tips on how to shape the manuscript.

References

Frank Carter. 2008. *The Turing Bombe*. Report No. 4. Bletchley Park Trust, new edition. ISBN: 978-1-906723-03-3.

B. Jack Copeland, Jonathan P. Bowen, Mark Sprevak, and Robin Wilson. 2017. *The Turing Guide*. Oxford University Press. ISBN: 978-0-19-874782-6.

CryptoMuseum. 2017. Enigma M4 message. `http://www.cryptomuseum.com/crypto/enigma/msg/p1030681.htm`. [Online; accessed 24-October-2017].

Joseph R. Desch. 1942. Memo of Present Plans for an Electro-Mechanical Analytical Machine. `http://cryptocellar.org/USBombe/desch.pdf`. [Published online by Frode Weierud in 2000, accessed 16-September-2016].

Alan M. Turing. 1942. Visit to NCR. `http://cryptocellar.org/USBombe/turncr.pdf`. [Published online by Frode Weierud in 2000, accessed 16-September-2016].

Gordon Welchman. 2014. *The Hut Six Story*. M & M Baldwin, 6 edition. ISBN: 978-0-947712-34-1.

Jennifer Wilcox. 2006. *Solving the Enigma: History of the Cryptoanalytic Bombe*. Center for Cryptologic History, NSA.

What We Know About Cipher Device "Schlüsselgerät SG-41" so Far

Carola Dahlke
Deutsches Museum, Germany
c.dahlke@deutsches-museum.de

Abstract

Almost everyone knows the Enigma. But the cipher device "Schlüsselgerät 41"? Never heard of it. This German cipher machine is much rarer than its famous predecessor. Only around 1500 units were manufactured towards the end of the Second World War. And information is even scarcer. Up to now, the Deutsches Museum has only been able to collect broken devices. Recent contacts to collectors reveal that functional Schlüsselgeräte 41 still exist. They could help to solve the secret of the encryption algorithm. This contribution aims to present our current state of research.

1 Menzer's Machines at OKW/ Chi

In 1941, the cryptologist Fritz Menzer (1908-2005) from the OKW/Chi (Signal Intelligence Agency of the Supreme Command of the Wehrmacht) designed a mechanical cipher device that for certain would have complicated all decipherment efforts of Bletchley Park (Mowry, 1983-1984).

Menzer was chief of the communications security for the Wehrmacht, and his staff had criticized for a long time that the German coding devices (including ENIGMA and LORENZ SZ-42) had not been mathematically checked for security. In fact, this was only carried out from 1942 onwards (Hüttenhain, 1970). Consequently, Menzer insisted - against the ignorance of the troops and their command – upon the construction of an enhanced cipher device. First, he started to develop "Schlüsselgerät 39" – an enhanced version of ENIGMA, but as we know so far, only three models existed (Mowry, 2014). In 1941, Menzer invented a second cipher machine called "Schlüsselgerät SG-41".

But despite the highly sophisticated encryption of SG 41, in fact far above the security level of ENIGMA, its development was neglected and even blocked by the army (WDGAS-14).

When it finally came to a decision to build and spread the machine, wartime shortages of aluminium and magnesium caused the machine weight up to 15 kilograms – too heavy for field use. Although already about 11.000 machines were ordered (see Sächsisches Staatsarchiv Chemnitz), only few – an unknown quantity - were really fabricated at the Wanderer Werke AG, Siegmar-Schönau (today a part of Chemnitz) and used. TICOM documents speak about 1000 pieces (Mowry, 2014).

2 About Schlüsselgerät SG-41

Menzer wanted to design a pure mechanical, lightweight, durable and practical machine. So he invented several interesting features to make the device robust and practical for military use, e.g. he developed an improved, reversible insert for the ink pad and a mechanism to quickly remove the daily key settings (Kopacz, in prep).

And Menzer was a cryptoanalyst as well who had already developed two decipherment methods to break C-36. Subsequently, his knowledge about Hagelin devices was strong. He designed SG-41 with a printer and a keyboard, and with a crank handle like Hagelin's BC-38. Cipher text and plain text would be printed on two stripes of paper.

The algorithm was based on the Hagelin C devices with a characteristic Hagelin pin-and-lug-principle, but showed an enhanced encryption because of two characteristics (WDGAS-14; Kopacz, in prep):

Proceedings of the 1st Conference on Historical Cryptology, pages 109– 111,
Uppsala, Sweden, 18-20 June, 2018

1) The wheel stepping was not only interacting but irregular – controlled by the pin positions of the wheels.

2) Five of the six wheels formed the pseudo-random key for each letter encryption. The sixth wheel, however, could accept or negate the settings of the other five wheels.

Although there are basic explanations of the working principle of the machine (e.g. WDGAS-14), it was hitherto not possible to understand the exact mode of operation of the machine and to be able to simulate it. No construction drawings were found, and interrogation papers from Menzer himself and from colleagues have not been released so far (e.g. TICOM I-71, I-72, I-73 & DF-174). In addition, only few devices are known. Mostly, they were destroyed, dumped or burnt at the end of WW2. So after all, if a device is found nowadays, it is in most cases not in working order anymore.

2.1 Standard Model

Menzer's standard Schlüsselgerät 41 had a QWERTZ keyboard and was used from 1944 until the end of the war by the Abwehr (Secret Service) (Mowry, 1983-84). The letter J replaces the space-key (Kopacz, in prep) and is marked in red on the keyboard. According to Batey (2009), Bletchley managed to decipher few messages due to handling mistakes of the user, but they could not reconstruct the principle of the machine until they captured it after the end of WW2.

The Deutsches Museum owns a SG-41 that has lately been found in the forest grounds near Munich. It seems that someone had deposited it there at the end of WW2. Of course, after approximately 70 years in the ground, it is completely corroded – so it is not possible to gain helpful information from it regarding its encryption algorithm.

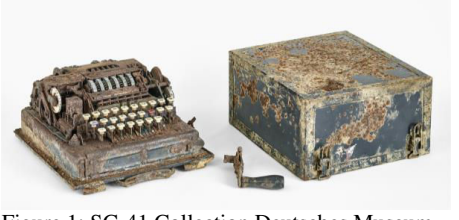


Figure 1: SG-41 Collection Deutsches Museum No. 2017-803, Photo: Konrad Rainer

Material analyses showed that the keys of the keyboard are made of nitrocellulose which is a problematic substance because it emits nitrous gases. As well, it decomposes when exposed to light and heat – facts that have to be considered when planning to store or to exhibit the object.

2.2 Special Model Z

A special model Z with ten figure traffic was constructed to be used for encrypting weather reports. Originally, 2.000 – 7.000 pieces were ordered at Wanderer Werke AG at Siegmar-Schönau/ Chemnitz (see Sächsisches Staatsarchiv Chemnitz). But TICOM documents speak of very few (TICOM I-194) or about 1.000 (TICOM I-57) pieces that were truly fabricated and used by the Luftwaffe (Air Force) from 1944 until the end of the war.

Figure 2: SG-41Z Collection Deutsches Museum No. 2013-1092, Photo: Inga Ziegler

In 2013, the Deutsches Museum was able to purchase a SG-41Z that had been dumped in a lake near Berlin at the end of WW2. As it was restored before it was put up for sale, it looks as new, at least from the outside. Internally it is - like our other model - completely corroded.

3 Sources and Outlook

The Schlüsselgerät 41 and its inventor, Fritz Menzer, are largely unknown up to date. Some interesting details have already been provided by documents from the Target Intelligence Committee, USA and UK (TICOM). Immediately after the end of the war, TICOM conducted surveys and investigations with prisoners of war and recorded these in the TICOM documents; since 2009 released by the NSA as so-called declassified documents).

But as long as the respective TICOM documents are not available it will only be possible to reconstruct the encryption algorithm by the help of a functional Schlüsselgerät. Fortunately, the engineer and specialist for cipher machines Klaus Kopacz from Stuttgart, Germany, was recently able to purchase and repair an original SG 41. A publication about the working principle and the complete technical details is planned by him in the near future.

As soon as the encryption details are published, it will be possible to simulate the algorithm and to evaluate the real impact of this device for the development of cipher machines after WW2. For example, the wheel-stepping mechanism, as well as the negation function of the sixth wheel, were implemented again in other pin-and-lug cipher devices after WW2, although mechanically solved in a different way (see H54 from Hell, and Version M of the CX52 from Crypto AG; Kopacz, in prep).

Other sources, especially German, British and U.S. American sources from archives, museums, and collectors, could provide more aspects and information. As well, we intend to perform a CT-scan to retrieve information about the internal parts of our machines. This is the focus for the next year.

Acknowledgments

First of all we would like to thank Dr. Marisa Pamplona and Christina Elsässer from the restoration research department of the Deutsches Museum for the material analysis and the helpful tips for designing the showcase, and Konrad Rainer and Inga Ziegler for the beautiful photos. We also thank Robert Jahn from Libellulafilm for his research in the Chemnitz Archive. Finally and most of all we thank Klaus Kopacz for his time and energy to explain the Schlüsselgerät 41 and to share his exciting insights with us.

References

David Mowry. 1983-1984. *Regierungs-Oberinspektor Fritz Menzer: Cryptographic Inventor Extraordinaire.* Cryptologic Quarterly Articles, 2 (3-4).

David Mowry. 2014. *German Cypher Machines of World War II*. NSA history program.

Erich Hüttenhain. 1970. *Einzeldarstellungen aus dem Gebiet der Kryptologie.* Bavarian State Library, Reading Room for Manuscripts and Rare Books. Munich.

Klaus Kopacz. In prep. *Schlüsselgerät 41*.

Mavis Batey. 2009. *Dilly, The Man Who Broke Enigmas*. ISBN 978-1-906447-01-4.

Sächsisches Staatsarchiv Chemnitz, 31030 Wanderer-Werke AG, Sigmar-Schönau, Signatures: 1975, 3156 and 1212.

TICOM I-194: *Report on German meteorological cipher systems and the German met. Intelligence service*. Released by NSA 2009. No DOCID.

TICOM I-57: *Enciphering devices worked on by Dr. Liebknecht at Wa Pruef 7*. Released by NSA 2009. DOCID: 3541302.

The cryptology of German Intelligence Services. Released by NSA 2009. DOCID: 2525898

TICOM I-194: *Report on German meteorological cipher systems and the German met. Intelligence service*. Released by NSA 2009. No DOCID.

WDGAS-14: *Volume 2 – Notes on German high level cryptography and cryptoanalysis*. Released by NSA 2009. DOCID: 3560816.

POSTER AND DEMO

An Automatic Cryptanalysis of Playfair Ciphers Using Compression

Noor R. Al-Kazaz[1]
School of Computer Science
Bangor University
Bangor, UK
n.al-kazaz@bangor.ac.uk
noor82.nra@gmail.com

Sean A. Irvine
Real Time Genomics
Hamilton, New Zealand
sairvin@gmail.com

William J. Teahan
School of Computer Science
Bangor University
Bangor, UK
w.j.teahan@bangor.ac.uk

Abstract

This paper introduces a new compression-based approach to the automatic cryptanalysis of Playfair ciphers. More specifically, it shows how the Prediction by Partial Matching ('PPM') data compression model, a method that shows a high level of performance when applied to different natural language processing tasks, can also be used for the automatic decryption of very short Playfair ciphers with no probable word. Our new method is the result of an efficient combination between data compression and simulated annealing. The method has been tried on a variety of cryptograms with different lengths (starting from 60 letters) and a substantial majority of these ciphers are solved rapidly without any errors with 100% of ciphers of length over 120 being solved. In addition, as the spaces are omitted from the ciphertext traditionally, we have also tried a compression-based approach in order to achieve readability by adding spaces automatically to the decrypted texts. The PPM compression model is used again to rank the solutions and almost all the decrypted examples were effectively segmented with a low average number of errors. Furthermore, we have also been able to break a Playfair cipher for a 6×6 grid using our method.

1 Introduction

Compression can be used in several ways to enhance cryptography and cryptanalysis. For example, many cryptosystems can be broken by exploiting statistical regularities or redundancy in the source. Since compression removes redundancy from a source, it is immediately apparent why compression is advocated prior to encryption (Irvine, 1997). However, this paper considers another application of compression to tackle the plaintext identification problem for cryptanalysis. This is an approach that has resulted in relatively few publications compared to the many other methods that have been proposed for breaking ciphers. The purpose of this paper is to explore the use of a compression model for the automatic cryptanalysis of Playfair ciphers.

The primary motivation for data compression has always been making messages smaller so they can be transmitted more quickly or stored in less space. Compression is achieved by removing redundancy from the message, resulting in a more 'random' output. There are two main classes of text compression adaptive techniques: dictionary based and statistical (Bell et al., 1990). Prediction by Partial Matching ('PPM'), first described in 1984 (Cleary and Witten, 1984), is an adaptive statistical coding approach, which dynamically constructs and updates fixed order Markov-based models that help predict the upcoming character relying on the previous symbols or characters being processed. PPM models are one of the best computer models of English and rival the predictive ability of human experts (Teahan and Cleary, 1996).

Our new approach to the automatic cryptanalysis of Playfair ciphers uses PPM compression to tackle the plaintext recognition problem. We rank the quality of the different plaintexts using the size of the compressed output in bits as the metric. We also use another PPM-based algorithm to automatically insert spaces into the decrypted texts in order to achieve readability.

This paper is organised as follows. Section 2 covers the basics of Playfair ciphers and

[1] Computer Science Department, College of Science for Women, Baghdad University, Baghdad, Iraq.

Proceedings of the 1st Conference on Historical Cryptology, pages 115– 124,
Uppsala, Sweden, 18-20 June, 2018

also includes a general overview of previous research on the cryptanalysis of Playfair ciphers as well as a discussion of its weaknesses. Our PPM based method and the simulated annealing search we use are explained in section 3. Section 4 covers the experimentation and results obtained with the conclusions to our findings presented in the final section.

2 Playfair Ciphers

The Playfair cipher is a symmetric encryption method which is based on bigram substitution. It was first invented by Charles Wheatstone in 1854. The cipher was named after Lord Lyon Playfair who published it and strongly promoted its use. It was considered as a significant improvement on existing encryption methods. A key is written into a 5×5 grid and this may involve using a keyword (as in the example below). For English, the 25 letters are arranged into the grid with one letter omitted from the alphabet. Usually, the letter 'I' takes the place of letter 'J' in the text to be encrypted.

To generate the key that is used, spaces in the grid are filled with the letters of the keyword and then the remaining spaces are filled with the rest of the letters from the alphabet in order. The key is usually written into the top rows of the grid, from left to right, although some other patterns can be used instead. For example, if the keyword 'CRYPTOLOGY' is used, the key grid would be as below:

C	R	Y	P	T
O	L	G	A	B
D	E	F	H	I
K	M	N	Q	S
U	V	W	X	Z

To encrypt any plaintext message, all spaces and non-alphabetic characters must be removed from the message at the beginning, then the message is split into groups of two letters (i.e. bigrams). If any bigrams contain repeated letters, an 'X' letter is used to separate between them. (It is inserted between the first pair of repeated letters, and then bigram splitting continues from that point). This process is repeated (as necessary) until no bigrams with repeated letters. If the plaintext has an odd number of letters, an 'X' is inserted at the end so that the last letter is in a bigram (Klima and Sigmon, 2012). For example, the message "*To be or not to be that is the question*" would end up as:
"TO BE OR NO TX TO BE TH AT IS TH EQ UE ST IO NX".

There are three basic encryption rules to be applied (Klima and Sigmon, 2012):

- If both letters of the bigram occupy the same row, replace them with letters to the immediate right respectively, wrapping from the end of the row to the start if the plaintext letter is at the end of the row.

- If both letters occupy the same column, then replace them with the letters immediately below them. So 'IS' enciphers to 'SZ'. Wrapping in this case occurs from the bottom to the top if the plaintext letter is at the bottom of the column.

- If both letters occupy different rows and columns, replace them with the letters at the free end points of the rectangle defined by both letters. Thus 'TO' enciphers to 'CB'. The order is important—the letters must correspond between the encrypted and plaintext pairs (the one on the row of the first letter of the plaintext should be selected first).

Following these rules, the encrypted message would be:

"CB LI LC KG PZ CB LI PI BP SZ PI HM VD ZB DB QW"

The Playfair cipher is one of the most well known multiple letter enciphering systems. However, despite the high efficiency demonstrated by this cipher, it suffers from a number of drawbacks. The existing Playfair method is based on 25 English alphabetic letters with no support for any numeric or special characters. Several algorithms have been proposed aiming to enhance this method (Srivastava and Gupta, 2011; Murali and Senthilkumar, 2009; Hans et al., 2014). One particular extended Playfair cipher method (Ravindra Babu et al., 2011) is based on 36 characters (26 alphabetical letters and 10 numeric characters). Here, a 6×6 key matrix was constructed with no need to replace the letter 'J' with 'I'. By using the same previous keyword 'CRYPTOLOGY', the key matrix in this case would be:

C	R	Y	P	T	O
L	G	A	B	D	E
F	H	I	J	K	M
N	Q	S	U	V	W
X	Z	0	1	2	3
4	5	6	7	8	9

Plaintexts containing any numerical values such as, contact number, house number, date of birth, can be easily enciphered using this extended method (Ravindra Babu et al., 2011).

2.1 Cryptanalysis of Playfair Ciphers

Different cryptanalysis methods have been invented to break Playfair ciphers using computer methods. An evolutionary method for Playfair cipher cryptanalysis was presented by Rhew (2003). The fitness function was based on a simple version of dictionary look-up with the fitness calculated based on the number of words found. However, results obtained from this method were poor with run-time requiring several hours. A genetic algorithm was proposed by Negara (2012) where character unigram and bigram statistics were both used as a basis of calculating the fitness function. The efficiency of the algorithm is affected by different parameters such as the genetic operators, ciphertext length and fitness function. Five initial keys out of twenty were successfully recognized in less than 1000 generations and ten out of twenty were fully recovered in less than 2000 generations. Two ciphertexts were examined in this paper: one with 520 characters and the other with 870 characters. Hammood (2013) presented an automatic attack against the Playfair cipher using a memetic algorithm. The fitness function calculation was based on character bigram, trigram and four-gram statistics. A ciphertext of 1802 letters was examined in this paper and 22 letters out of 25 were successfully recovered using this method.

Simulated annealing was successful at solving lengthy ciphers as reported by Stumpel (2017). However, he found that short Playfair ciphers of 100 letters or so were unable to be solved. Simulated annealing was also used with a tetragraph scoring function for the automatic cryptanalysis of short Playfair ciphers by Cowan (2008). Cowan managed to solve seven short ciphertexts (80-130 letters) that were published by the American Cryptogram Association.

In summary, several different cryptanalysis methods have been proposed aiming to break Playfair ciphers with varying degrees of success. However, most of these methods were focused on long ciphertexts of 500 letters or more, except Cowan's method (2008). A large amount of information that is provided by long ciphertexts makes breaking them easier while short Playfair ciphers are extremely difficult to break without some known words. In our paper, even Playfair ciphertexts as short as 60 letters (without a probable crib) have been successfully decrypted using our new universal compression-based approach. We use simulated annealing in combination with compression for the automatic decryption. Moreover, we have also effectively managed to break extended Playfair ciphers that use a 6×6 key matrix.

2.2 Playfair's Weaknesses

The Playfair cipher suffers from some major weaknesses. An interesting weakness is that repeated bigrams in the plaintext will create repeated bigrams in the ciphertext. Furthermore, a ciphertext bigram and its reverse will decipher to the same pattern in the plaintext. For example, if the ciphertext bigram "CD" deciphers to "IS", then the ciphertext "DC" will decrypt to "SI". This can help in recognising words easily, especially most likely words. Another weakness is that English bigrams that are most frequently occurring can be recognised from bigram frequency counts. This can help again in guessing probable plain words (Smith, 1955; Cowan, 2008).

Breaking short Playfair ciphertexts (less than 100 letters) without good depth of knowledge of previous messages or with no probable words has proven to be a challenge. Past research has often used much longer ciphertexts—for example, Mauborgne (1914) developed his methods by deciphering a Playfair ciphertext of 800 letters. Also, the Playfair messages that were circulating between the Germans and the British during war had enough depth with many probable words to make them easily readable between these two sides, with no predictor of decrypting success for short messages on anonymous topics (Cowan, 2008). However, the two conditions that the message is short with little depth (no probable words) apply to cryptograms published by the American Cryptogram Association.

3 Our Method

This section describes our new method for the automated cryptanalysis of the Playfair cipher. The problem of quickly recognising a valid decrypt in a ciphertext only attack has been acknowledged as a difficult problem (Irvine, 1997). What we require is a com-

puter model that is able to accurately predict natural language so that we can use it as a metric for ranking the quality of each possible permutation (Al-Kazaz et al., 2016). The PPM text compression algorithm provides one possibility since it is known that PPM compression models can predict language about as well as expert human subjects (Teahan and Cleary, 1996).

Hence, the main idea of our approach depends on using the PPM method to compute the compression 'codelength' for each putative decryption of the ciphertext with the given key. The codelength of a permutation for a cryptogram in this case is the length of the compressed cryptogram, in bits, when it has been compressed using the PPM language model. The smaller the codelength, the more closely the cryptogram resembles the model. Experiments have shown that this metric is very effective at finding valid solutions automatically in other types of cryptanalysis (Al-Kazaz et al., 2016). In this paper, we show how to use this approach to quickly and automatically recognise the valid decrypt in a ciphertext only attack specifically against Playfair ciphers.

In the PPM compression algorithm, the probability of the next symbol is conditioned using the 'context' of the previously transmitted symbols. These probabilities are based on simple frequency counts of the symbols that have already been transmitted. The primary decision to be made is the maximum context length to use to make the predictions of the upcoming symbol. The 'order' of the model is the maximum context length used to make the prediction. Many variants of the original Cleary and Witten approach have been devised such as PPMA, PPMB, PPMC and PPMD. These differ mainly by the maximum context length used, and the mechanism used to cope with previously unseen or novel symbols (called the zero frequency problem). When a novel symbol is seen in a particular context, an 'escape' is encoded, which results in the encoder backing off to the next shorter context. Several escapes may be needed before a context is reached which predicts the symbol. It may be necessary to escape down to the order 0 (null) context which predicts each symbol based on the number of times it has occurred previously, or for symbols not previously encountered in the transmission stream, a default model is used where an order '-1' context predicts each symbol with equal probability.

Most experiments show that the PPMD variant developed by Howard (1993) produces the best compression compared to the other variants. The probabilities for a particular context using PPMD are estimated as follows:

$$p(s) = \frac{2c(s) - 1}{2n} \quad \text{and} \quad e = \frac{t}{2n}$$

where $p(s)$ is the probability for symbol s, $c(s)$ is the number of times symbol s followed the context in the past, n is the number of times the context has occurred, t denotes the number of symbol types and e is the probability assigned to perform an escape. For example, if a specific context has occurred three times previously, with three symbols a, b and c following it one time, then, the probability of each one of them is equal to $\frac{1}{6}$ and escape symbol probability is $\frac{3}{6}$.

As PPM is normally an adaptive method, at the beginning there is insufficient data to effectively compress the texts which results in the different permutations producing similar codelength values. This can be overcome by priming the models using training texts that are representative of the text being compressed. In our experiments described below, we use nineteen novels and the Brown corpus converted to 25 letter English by case-folding to upper case with I and J coinciding for the 5×5 grid and 36 alphanumeric characters for the 6×6 grid to train our models. Also, unlike standard PPM which uses purely adaptive models, we use static models which are not updated once they have been primed from the training texts.

Our new method is divided into two main phases. The first phase (Phase I) is based on trying to automatically crack a Playfair ciphertext using a combination of two approaches, which is the compression method for the plaintext recognition and simulated annealing for the search. The second phase (Phase II) is based on achieving readability by automatically adding spaces to the decrypted message produced from phase I, as the spaces are omitted from the ciphertext traditionally.

A variation of an order 5 PPMD model without update exclusions has been used in our experiments for both Phase I and Phase II. This variation is where symbol counts are updated for all contexts unlike standard PPM where only the highest order contexts are updated

until the symbol has been seen in the context. In our experiments, this variation has proven to be the most effective method that can be applied to the problem of automatically recognising the valid decryption for Playfair ciphers, but also in other experiments with transposition ciphers (Al-Kazaz et al., 2016).

Simulated annealing is a probabilistic method for approximating the global optimisation of a given function in a large search space. It is a descendant of the hill-climbing technique. This latter technique is based on starting with a random key, followed by a random change over this key such as swapping two letters, to generate a new key. If this key produces a better solution than the current key, it replaces the current one. Different n-graph statistics were used as the scoring function to judge the quality of solutions. After millions of distinct random changes, this technique attempts to discover the correct key.

The weakness of this approach lies in the possibility of being stuck in local optima, where the search has to be abandoned and it is necessary to restart all over again. Simulated annealing (inspired by a process similar to metal annealing) is similar to hill-climbing with a small modification that often leads to an improvement in performance. In addition to accepting better solutions, simulated annealing also accepts worse solutions in order to avoid the local optima. This approach permits it to jump from local optima to different locations in order to find new optima. The probability of the acceptance of the specific solution is dependent on how much the score value is worse. The formula for calculating the acceptance probability is $P_A = \frac{1}{e^{(d/T)}}$ where e is the exponential constant 2.718, d denotes the difference between the score of the new solution and the score of the current solution, and T is a value called temperature (further details concerning this parameter are described below). Whenever the difference is small, the probability of accepting the new solution is high, while if this solution is much worse than the current one (the difference is large in magnitude), the probability becomes small. The probability value is also influenced by the temperature T. Initially, the algorithm starts with a high temperature value, then it is reduced ('cooled') at each step according to some annealing schedule, until it reaches zero or some low limit. As the temperature drops, the probability of acceptance also decreases and when T is set to zero, the simulated annealing becomes identical to the hill climbing technique.

The main idea of using simulated annealing for the breaking of Playfair ciphers is to modify the current key in the hope of producing a better key. This is based on an approach proposed by Cowan (2008). This can be done by randomly swapping two characters. However, this random change is not enough to effectively break the Playfair cipher by itself. It will usually result in a long search process that often gets stuck within reach of the final solution. So other modifications are needed such as randomly swapping two rows, swapping two columns, reversing the key, and reflecting the key vertically and horizontally (flipping the key top to bottom and left to right). Using a mix of these modifications can lead to the valid solution. For example, swapping two rows will help rearrange rows if they are out of order, as it is very important that rows be in the correct order according to the encipherment rules (Lyons, 2012).

During the whole search process, the hope is that the best plaintext solution that appears is also the correct plaintext. Alternatively, the whole process must be restarted all over again and the value of the temperature should be reset to its original high value (Cowan, 2008). An important aspect of this whole process is the metric that is used to rank the different plaintexts (such as our PPM method). A good metric needs to be able to distinguish effectively between good and poor plaintexts.

Algorithms 1 and 2 present the pseudo code for the first phase of our method. In a preprocessing step prior to the applications of these algorithms, all non-letters including spaces, numbers and punctuation were removed from the ciphertext if a grid of 5×5 is chosen. If a 6×6 grid-width is selected, all non alphabetic letters and numbers were removed from the ciphertext instead. According to selected grid-width, a random key is generated (line 1) and the deciphering operation is initiated using this key. In order to rank the quality of the solutions, the PPM compression method is used by calculating the codelength value for each possible solution (lines 3 and 4). For each iteration, a sequence of changes is performed over the generated key in order to find a solution with a smaller codelength value which represents the valid decryption (lines 5 to 33). The greater the number of iterations, the more likely a solution will be found, but longer ex-

ecution time will be needed. It is important to note here that we have used negative scores based on the PPM codelengths values in order to maximize rather than minimize scores for the simulated annealing process as per the standard approach adopted in various solutions (Cowan, 2008; Lyons, 2012).

The temperature for the simulated annealing based algorithm is initially set to 20 and reduced by 0.2 in subsequent iterations. (The smaller this amount is, the more likely a solution will be found but this will also result in longer execution time). The initial temperature value is essentially dependent on the cryptogram's length. The shorter the ciphertext, the lower the temperature will be needed and vice versa. We have found in experiments with different length ciperhetexts that for cryptograms of a length of around 70, an initial temperature will need to start at around 10, but for the cryptogram of 700 characters, a temperature at 20 or so is effective.

For each temperature, 10,000 keys are tested then a reduction in the temperature is performed (see lines 9 to 32 in the algorithm). A loop is executed 10,000 times (lines 10 to 31) that modifies the key in the hope of finding a better key with a smaller codelength value. A sequence of different modifications over the key is performed in lines 11 to 17. The encrypted text is then deciphered using the modified key and the codelength value is calculated using the PPM compression method (lines 19 and 20). Then, the difference is calculated between the new codelength value and the previous one. If the new value (line 21) is better (that is, the codelength value is smaller), then the maximum score is set to the new score (line 22), otherwise a probability of acceptance is calculated (line 24) if the temperature is greater than 0 (line 23). In this case, a random number between 0 and 1 is generated, and if the calculated probability is greater than this number, the modified key is accepted (see lines 26 to 27). If we have a new best score, then the old one is replaced (line 29) and systematic rearrangements are performed by calling Algorithm 2. These include mutations (lines 4 to 10 in the new algorithm), row swapping and column swapping (lines 11 to 17) and an exhaustive search over all 4! possible permutations of each group of four symbols (lines 18 to 24). Swapping single pairs of letters results in the search getting stuck in local maxima too often, so we added the swapping of all possible combinations of 4 symbols to try to avoid that. Trying 3, 5, or even more combinations of symbols is possible, but of course the higher the number, the search starts getting very expensive, so 4 provides a reasonable compromise. Finally, the deciphered text is returned with the smaller codelength value which represents the best solution found (line 34). This has proved adequate for the solution of most ciphers, but if necessary, it is still possible to iterate the attack several more times.

Algorithm 1: Pseudo code of the main decryption phase 'Phase I'.

```
   Input  : ciphertext, Playfair grid-width to be either 5×5
            or 6×6
   Output: deciphered-text
 1 generate a random key according the Playfair grid-width
   selected
 2 currentBestKey ← randomKey
 3 decipher the ciphertext using the currentBestKey and
   calculate the codelength value using the PPM
   compression method
 4 currentBestScore ← − PPM-codelength score (decipher-text)
 5 for Iteration ← 0 to 99 by 1 do
 6     maxKey ← currentBestKey
 7     decipher and calculate the codelength value using
       the PPM compression method
 8     maxScore ← − PPM-codelength score (decipher-text)
 9     for Temp ← 20 downto 0 by 0.2 do
10         for Count ← 0 to 9999 by 1 do
11             modify maxKey by choose a random
               number between (1,50):
12                 if the number is 0 then swap two
                   rows, chosen at random
13                 if the number is 1 then swap two
                   columns, chosen at random
14                 if the number is 2 then reverse the
                   key
15                 if the number is 3 then reflect the
                   key vertically, flip top to bottom
16                 if the number is 4 then reflect the
                   key horizontally, flip left to right
17                 if any other number then swap two
                   characters at random
18             newKey ← modified-maxKey
19             decipher and calculate the codelength
               value using the PPM compression method
20             newScore ←
               − PPM-codelength score (decipher-text)
21             calculate diff ← newScore − maxScore
22             if diff >= 0 then {maxScore ← newScore;
               maxKey ← newKey}
23             else if Temp > 0 then
24                 calculate probability ← exp(diff/Temp)
25                 generate a random number between
                   (0,1)
26                 if probability > randomNumber then
27                     {maxScore ← newScore;
                       maxKey ← newKey}
28             if maxScore > currentBestScore then
29                 currentBestScore ← maxScore;
                   currentBestKey ← maxKey
30                 Make systematic
                   rearrangements(ciphertext,
                   currentBestKey, currentBestScore)
31         end
32     end
33 end
34 return the deciphered text with the best key
```

Concerning the second phase of our approach, Algorithm 3 illustrates the pseudo code for this phase. The main idea of this phase, as stated before, is to try to insert spaces into the deciphered text outputted from

Algorithm 2: Make systematic rearrangements

```
   Input  : ciphertext, currentBestKey, currentBestScore
   Output: currentBestKey, decipher-text
1  flag ← true
2  while flag do
3      flag ← false
4      perform systematic mutations over the
       currentBestKey:
5          decipher and calculate the codelength value
           using the PPM compression method
6          newscore ←
           – PPM-codelength score (decipher-text)
7          if newscore > currentBestScore then
8              flag ← true
9              currentBestScore ← newScore;
               currentBestKey ← newKey
10             continue outer While loop
11     perform systematic row-swaps and column-swaps
       over the currentBestKey:
12         decipher and calculate the codelength value
           using the PPM compression method
13         newscore ←
           – PPM-codelength score (decipher-text)
14         if newscore > currentBestScore then
15             flag ← true
16             currentBestScore ← newScore;
               currentBestKey ← newKey
17             continue outer While loop
18     perform swapping of four characters:
19         decipher and calculate the codelength value
           using the PPM compression method
20         newscore ←
           – PPM-codelength score (decipher-text)
21         if newScore > currentBestScore then
22             flag ← true
23             currentBestScore ← newScore;
               currentBestKey ← newKey
24             continue outer While loop
25 end
26 return currentBestKey, decipher-text
```

Phase I in order to achieve readability. PPM is again applied to rank the solutions. The Viterbi algorithm is used in this phase to find the best possible segmentation. In this algorithm, looping over the deciphered text (that was produced as output from Algorithm 1) is performed in line 2. A word segmentation algorithm based on the Viterbi algorithm (Teahan, 1998) is then used to search for the best performing segmentations to keep in a priority queue, and those which showed poor codelength values are pruned (see lines 3 to 5). The best segmented deciphered text is returned in the last line (line 6).

Algorithm 3: Pseudo code for Phase II

```
   Input  : the deciphered text from Phase I
   Output: segmented deciphered text
1  maximum size of Q1 (priority queue) ← 1;
2  do
3      use the Viterbi algorithm to search for the best
       segmentation sequences;
4      store the text that have the best segmentation
       which present in Q1;
5  while the end of the deciphered text;
6  return the best segmented deciphered text from Q1;
```

4 Experimental Results

In this section, we discuss the experimental results of our approach. As stated, in our method the order-5 PPMD model has been trained on a corpus of nineteen novels and the Brown corpus using 25 English letters (when a 5×5 grid is used) and 36 alphanumeric characters (when a 6×6 grid is used). After this training operation and during cryptanalysis, these models remain static. Regarding the cryptograms test corpus, 70 different cryptograms were chosen at random from different resources including cryptograms published by the American Cryptogram Association, cryptograms published by geocache enthusiasts, and two cryptograms that were also experimented with by Negara (2012). Cryptogram lengths ranged from 60 to 750 letters.

A sample trace of a decryption is shown in Figure 1 for the cryptogram: '`dohrxnwpscqusfrwchrnpctsehagvpstsfaprdtuipwolacgqupfwptslaqsizbedxqusfwscosfraevstngqu`'. This shows the best score as it changes during the execution of Algorithm 2 for the main decryption phase. The scores are increasing (i.e the codelengths are decreasing). The solution of this ciphertext is a proverbial wisdom that has been attributed to Damon Runyon: "*It may be that the race is not always to the swift nor the battle to the strong but that is the way to bet*". This ciphertext is one of the short cryptograms (82 character long) that have been published by the American Cryptogram Association, which usually publishes 100 ciphertexts every two months including one or more Playfair ciphers, as a challenge to its members (Cowan, 2008). Cowan has stated that it is extremely difficult to break short messages of 100 letters or so, especially when there are no suspected probable words or cribs and very little depth of knowledge of previous messages. However, our method is able to solve the following examples in addition to the other cryptograms that were listed by Cowan as well as even shorter ciphertexts of 60 letters or so.

A second example in Figure 2 illustrates the robustness of our compression approach by showing how it is able to solve a very short cryptogram. The ciphertext is a 60 letter sentence (a quote by Garrison Keillor): *Cats are intended to teach us that not everything in nature has a purpose.* The best solution for this example is '`catsareintendedtoteachusthatnotexerythinginxnaturehaoapurposew`' with the best codelength value `-137.68` resulting in only two errors: `x`→`v` in '`exerything`' and `o`→`d` in '`hao`'.

```
Iteration:35
Mutation  -221.66 ridaybetoktxtherkdeconotalwaystothescru-
gain:     fyorthebrtxtletothestucngmitxthatoithewaytobetx
          Key:zkbncwagerfhmlduvxyitsqpo
Mutation  -220.15 ridaybetvstxthersaeksnotalwaystotheskru-
gain:     fyorthebatxtletothestukngmitxthatksthewaytobetx
          Key:  zcbnkwagerfhmlduvxyitsqpo
Mutation  -215.91 ridaybetvstxthersaemsnotalwaystothesmru-
gain:     fyorthebatxtletothestumngkitxthatmsthewaytobetx
          Key:  zcbnmwagerfhkldu vxyitsqpo
Mutation  -207.60 rmdaybetvstxthersaeisnotalwaystothesiru-
gain:     fnorthebatxtletothestningkmtxthatisthewaytobetx
          Key:  zcbniwagerfhkldu vxymtsqpo
Mutation  -204.66 itzaybetvstxthersaeisnotalwaystotheswiu-
gain:     fnorthebatxtletothestorngbutxthatisthewaytobetx
          Key:  dcbniwagerfhklzuvxymtsqpo
Mutation  -195.04 itmaybetvstxthersaeisnotalwaystotheswiu-
gain:     fnorthebatxtletothestomngbutxthatisthewaytobetx
          Key:  dcbniwagerfhklmuvxyztsqpo
Row-swap  -184.98 itmaybethvtxthervaeisnotalwaystotheswif-
gain:     tnorthebatxtletothestzongbutxthatisthewaytobetx
          Key:  dcbniwagerfhklmtsqpouvxyz
Row-swap  -162.46 itmaybethatxtheraceisnotalwaystotheswif-
gain:     tnorthebatxtletothestrongbutxthatisthewaytobetx
          key:  dcbnifhklmtsqpouvxyzwager
```

Figure 1: Example cryptogram of 82 letters from the American Cryptogram Association.

```
Iteration:89
          -164.32 catsareintencectoteakiusthhonotexerythi-
          nginxnaturehatapurposid
Mutation  -161.21 catsareintencectoteakiusthaonotexerythi-
gain:     nginxnaturehatapurposid
Mutation  -160.36 pltsapeintencectoteadbusthahnotexerythi-
gain:     nginxnatureoatapurposid
Mutation  -159.28 pltsapeintendedtoteacbusthahnotexerbthi-
gain:     nginxnatureoatapurposic
Mutation  -156.08 datsareintendedtoteakiusthaonotexerfthi-
gain:     nginxnaturehatapurposic
Mutation  -155.29 katsareintendedtoteakiusthatnotexerythi-
gain:     nginxnaturehaoapurposic
Mutation  -154.12 ratsakeintendedtoteakiusthatnotexeocthi-
gain:     nginxnaturehasapukposic
Mutation  -150.31 ratsileintendedtotealausthatnotexeokthi-
gain:     nginxnaturehasapudiospc
2-Mutation-149.97 ratsileintendedtoealhusthatnotexevcthi-
gain:     nginxnaturehasapudiosev
Mutation  -143.16 ratsaceintendedtoteachusthatnotexelvthi-
gain:     nginxnaturehasapucposev
Mutation  -138.52 catsareintendedtoteachusthatnotexerythi-
gain:     nginxnaturehaoapurposev
Mutation  -137.68 catsareintendedtoteachusthatnotexerythi-
gain:     nginxnaturehaoapurposew
```

Figure 2: Example short 60 letter cryptogram.

A third example is a puzzle cryptogram of 96 letters from the geocache world (`https://bcaching.wordpress.com/2008/08/08/puzzles-part-3/`): '`sa cb av hm ka do st th ps mn qs fr hm sx bt su tw tg wg mh mc ok sd oz ts fy tw ts vc ec gs gt wl dl sr oz tb tl ps tg ex cm co dl kh wl wg mh ex av`'. Figure 3 presents the intermediate results and the final solutions produced by each iteration for this cryptogram. According to this example, iteration 89 produced the best solution with the best score with a compression codelength value of 215.81 and is the valid decrypt.

Our method was also able to solve a 6×6 Playfair cipher with a few minor errors. The next sample is a cryptogram that was posted on a puzzles forum originating from geocache enthusiasts (`http://members2.boardhost.com/barryispuzzled/msg/1500564217.html`):

```
Iteration:0
Mutation  -311.85 tuemuirecolstaurytrtforxreafmstoopanile-
gain:     rcekqbsulatydopatiekedanalondtfulsmonytancheck-
          andeqloilerchui
...
Iteration:2
          -311.01 adpcdhowwhsvalarcaucedofowleyldmailiumw-
          oseheatrelarbailaonmemlilgatstorelylscalikeese-
          ctswpgaumwokedh
...
Iteration:24
          -309.15 hkxepmmaskbitesratokhdtvmabasedaeferela-
          mlamntbinetnrefetlpgwhereeceithinesevaterbcalx-
          leismecelambcpm
...
Iteration:30
Row       -304.26 amsegplaysonasarealmcarblaterstcrustita-
swap      lsniymeinsahirusaezkstatsorodtbinsrmreastpensn-
gain:     kodyboritalpegp
...
Iteration:89
Row       -215.81 thecoxordinatesarenorthfortydegrexeszer-
swap      opointfivethrexetwowestseventyfivedegreestwopoi-
gain:     ntfivezerotwox
...
Iteration:100
```

Figure 3: Solutions produced during selected iterations for a puzzle cryptogram of 96 letters.

```
lpqtj zfpvf ndsvb joamd j4mva nrfeu nbhis nhcru
chhfs otb1e kbueg qejtv kgscn kq3ez kgwix eavej
nstda usbfj cvkgs cbtqz 5nmqa nc0jc xeiue nhtnb
rbwhg krabz 1j0mn dierf rabfq vjvkf dnrbk nkd0u
cbwhn dsdlv vpvha gvucb bnyjc vtzpf brrab gtmqa
j4fmt ryjbu vldtq fsnts awfhl pvthc 0hpvv obvmd
jvra7 zhfew irgh3 8qpck r5z7r gaw1k biyjg h3w8w
qfau3 v7dra bfnbe jgkke kvhfc 0dsjy raghx bjbqm
bhhgc hnwyj bxgkk ekvhf dcvjo uebxr rsch1 jwmvu
bxlbi nmraw ckbnh g1jrn dtchl vfpur raihj 4fmoq
jbrbj zfmtr yjbur acjck vughh tchjv rauxc hrzkc
hchff elnob mvvjh cgerf rgawu xchrz uxvfb fcqbt
mdfjh chgrf sujep qbrej yjrgy jchmv eseue ckgau
ejrbr uvlej mq1jv mh0mv txhz
```

Part of the execution trace is shown in Fig. 4.

```
Iteration: 1
-1604.59 jolxlygoodandwelldoneyouhavecrackedanextendedpl-
ayfaircipherusingasixbysixgridtheadvantageofusingall30sl-
phanumericxcharactersisthatyoucangivethecoxordinatesasnu-
mbersandnotwordsbutbecarefultogetthefullkeycorxrecttoavo-
idawastedjourneynowofftonorthztdegrexesx3poinwytzwest3de-
greess5x9xoint1x2athecacheishidxdenunderthestilepleaseens-
ureitishidxdenfromviewxwhenyouputitbackjustincaseyouhave-
notgotxthekeycompletelycorxrecttheminutesarenorthtwentyn-
inedecimalfouronefivewesttwentytwodecimaloneonesevenweho-
petherewereenoughcribsinthetexttohelpyouonyourway
-1594.57 jolxlygoodandwelldoneyouhavecrackedanextendedpl-
ayfaircipherusingasp5bysixgridtheadvantageofusingall50kl-
phanumericxcharactersisthatyoucangivethecoxordinatesasnu-
mbersandnotwordsbutbecarefultogetthefullkeycorxrecttoavo-
idawastedjourneynowofftonorthztdegrexesw3poinxytzwest5de-
greeswp3point1w2athecacheishidxdenunderthestilepleaseens-
ureitishidxdenfromviewxwhenyouputitbackjustincaseyouhave-
notgotxthekeycompletelycorxrecttheminutesarenorthtwentyn-
inedecimalfouronefivewesttwentytwodecimaloneonesevenweho-
petherewereenoughcribsinthetexttohelpyouonyourway
```

Figure 4: Example solutions produced for a 6×6 Playfair cryptogram.

The experimental results of Phase I, when the order 5 PPM method without update exclusions is used, showed that most of the cryptograms are successfully decrypted with no er-

rors. Table 1 presents the results from testing ciphertexts for various lengths. The results overall showed that we are able to attain very high success rates and 60 ciphertexts out of 70 were efficiently solved. Also, 100% of ciphers of length greater than 120 were decrypted.

Cipher Length	**60-79**	**80-99**	**100-119**	**120-149**	**150-199**	**200-750**
No. of Ciphers	9	21	15	11	8	6
Success Rate (%)	67	81	80	100	100	100

Table 1: Results when testing ciphertexts with different lengths.

Referring to the second phase of our method, as the spaces are omitted from the ciphertext traditionally, this phase focuses on segmenting the decrypted messages that are outputted from the first phase. The edit distance (or Levenshtein distance) metric is used to qualify how the decrypted message is differentiated from the original message by counting the minimum number of the removal, insertion, or substitution operations required to transform one message into the other (Levenshtein, 1966). In almost all cases, the correct readable decryptions were efficiently found as the illustrated in Figure 5.

Ciphertext	byntlbneonnuimmzqnhpbkxnqmfqoqnmugclqmeuersuqpnzigqbqyipilqtku
Decrypted text	cats are intended to teach us that not exerything in nature ha o a purpose
Ciphertext	kuinbrnuikcnqmhuvgtnnmybkgbromruknqmnknqdmpvgniignkoneumokgpgxytqsu
Decrypted text	experience is the worst teacher it gives the test before presenting the lesson
Ciphertext	pqghqncnndqyhfqugqqmeusxqmfqdpkgqbitqdkunurqioinnlpgvqvpbmlvhuqoimigbzka
Decrypted text	a n egotist is a man who thinks that if he hadnt been born people would have wondered why
Ciphertext	qmghblxytkyfihogkunugiqoqmgnqmgincimtlqmmpnuikiwszqmgiknliqrbhafgtigtldnnqgtxz
Decrypted text	the grass may be greener on the other side of the fence but there s probably more of it to mow
Ciphertext	hmfnuwfntufdbgushmtuqmckqnutfpmatuzfmbfntylxqpthrkucnrkrmcqdamibarurntumucoffdummbrnki
Decrypted text	the likeliness of a thing happening is inversely proportional to its desirability fin agles first law
Ciphertext	dohrxnwpscqusfrwchrnpctsehagvpstsfaprdtuipwolacgqupfwptslaqsizbedxqusfwscosfraevstngqu
Decrypted text	it may be that the race is not always to the swift nor the battle to the strong but that is the way to bet

Figure 5: Example of solved ciphertexts with spaces inserted after Phase II.

The number of space insertion errors for each testing cryptogram is plotted in Figure 6. We can see that the number of errors for most cryptograms are very low and the correct segmentations are obtained in most cases. The average space insertion errors for the ciphertexts that were experimented with in Phase II is less than one error.

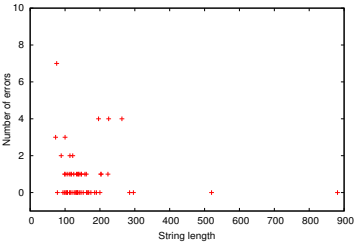


Figure 6: Segmenting errors produced as a result of the Phase II algorithm.

Table 2 lists the high recall and precision rates and the low error rate produced by our segmentation algorithm. The recall rate is calculated by dividing the number of successfully segmented words over the number of words in the original testing texts, the precision rate by dividing the number of successfully segmented words by the number of words which are correctly and incorrectly segmented and the error rate by dividing the number of unsuccessfully segmented words by the number of words in the original testing texts (Al-Kazaz et al., 2016).

Recall (%)	**Precision (%)**	**Errors (%)**
96.72	96.12	3.28

Table 2: Recall, precision and errors rates for our method for word segmenting the decrypted output produced from Phase I.

The execution times required to decrypt a number of Playfair ciphertexts by our method are presented in Table 3. This table shows the decryption time in seconds for Phase I of our method. The results indicate that our method produces reasonable decryption times, and in most cases the successful decrypts of longer ciphertexts were obtained after only one or two iterations.

Ciphertext Length *(Letter)*	**60**	**71**	**86**	**100**	**124**	**185**	**235**	**526**	**730**
Time *(Sec)*	457	539	507	93	36	17	135	107	101

Table 3: Decryption times for Phase I for different ciphertexts.

5 Conclusion

An automatic cryptanalysis of Playfair ciphers using compression has been introduced in this paper. In particular, a combination of simulated annealing and PPM compression was used in the automatic decryption method. The compression scheme was found to be an effective method for ranking the quality of each possible permutation as the search was performed. In 60 of the 70 ciphertexts that were experimented with (without using a probable word) for different lengths (from as short as 60 letters up to 750), almost all the correct solutions were found. The exception was just two very short ciphers which resulted in two minor errors in the decrypted output. Moreover, we have also managed to decrypt an extended Playfair cipher for a 6×6 key matrix.

In addition, a compression-based method was used to segment the decrypted output by insertion of spaces in order to improve readability. Experimental results show that the segmentation method was very effective producing on average less than one space insertion error with a recall and precision of over 96% for the ciphertexts that were tested.

As PPM provides a different type of scoring function compared to the standard n-gram analysis (such as update exclusions, the escaping back-off mechanism for smoothing the models), it is not clear whether using longer context for n-grams might lead to better results. It is also not clear how PPM compares to the standard n-grams approach and further experimentation (for example with hexagrams) needs to be done.

References

Noor R Al-Kazaz, Sean A Irvine, and William J Teahan. 2016. An automatic cryptanalysis of transposition ciphers using compression. In *Int. Conference on Cryptology and Network Security*, pages 36–52. Springer, Springer Int. Publishing.

Timothy C Bell, John G Cleary, and Ian H Witten. 1990. *Text compression*. Prentice-Hall, Inc.

John Cleary and Ian Witten. 1984. Data compression using adaptive coding and partial string matching. *IEEE Transactions on Communications*, 32(4):396–402.

Michael J Cowan. 2008. Breaking short playfair ciphers with the simulated annealing algorithm. *Cryptologia*, 32(1):71–83.

Dalal Abdulmohsin Hammood. 2013. Breaking a playfair cipher using memetic algorithm. *Journal of Engineering and Development*, 17(5).

Swati Hans, Rahul Johari, and Vishakha Gautam. 2014. An extended playfair cipher using rotation and random swap patterns. In *Computer and Communication Technology (ICCCT), 2014 International Conference on*, pages 157–160. IEEE.

Paul Glor Howard. 1993. The design and analysis of efficient lossless data compression systems. Ph.D. thesis, Brown University, Providence, Rhode Island.

Sean A Irvine. 1997. Compression and cryptology. Ph.D. thesis, University of Waikato, New Zealand.

Richard E Klima and Neil P Sigmon. 2012. *Cryptology: classical and modern with maplets*. CRC Press.

Vladimir I Levenshtein. 1966. Binary codes capable of correcting deletions, insertions, and reversals. In *Soviet physics doklady*, volume 10, pages 707–710.

James Lyons. 2012. Cryptanalysis of the playfair cipher. `http://practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-playfair/`.

Joseph Oswald Mauborgne. 1914. *An advanced problem in cryptography and its solution*. Fort Leavenworth, Kansas: Leavenworth Press.

Packirisamy Murali and Gandhidoss Senthilkumar. 2009. Modified version of playfair cipher using linear feedback shift register. In *Information Management and Engineering, 2009. ICIME'09. International Conference on*, pages 488–490. IEEE.

G Negara. 2012. An evolutionary approach for the playfair cipher cryptanalysis. In *Proc. of the Int. Conference on Security and Management (SAM)*, page 1. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

K Ravindra Babu, S Uday Kumar, A Vinay Babu, IVN S Aditya, and P Komuraiah. 2011. An extension to traditional playfair cryptographic method. *International Journal of Computer Applications*, 17(5):34–36.

Benjamin Rhew. 2003. Cryptanalyzing the playfair cipher using evolutionary algorithms. Available: `http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.129.4325&rep=rep1&type=pdf`.

Laurence Dwight Smith. 1955. *Cryptography: The science of secret writing*. Courier Corporation.

Shiv Shakti Srivastava and Nitin Gupta. 2011. Security aspects of the extended playfair cipher. In *Communication Systems and Network Technologies (CSNT), 2011 International Conference on*, pages 144–147. IEEE.

Jan Stumpel. 2017. Fast playfair programs. `www.jw-stumpel.nl/playfair.html`. last accessed December 13, 2017.

William J Teahan and John G Cleary. 1996. The entropy of English using PPM-based models. In *Data Compression Conference, 1996. DCC'96. Proceedings*, pages 53–62. IEEE.

William J Teahan. 1998. Modelling English text. Ph.D. thesis, University of Waikato, New Zealand.

ManuLab System Demonstration

Eugen Antal
Slovak University of Technology
Bratislava, Slovakia
eugen.antal@stuba.sk

Pavol Zajac
Slovak University of Technology
Bratislava, Slovakia
pavol.zajac@stuba.sk

Abstract

ManuLab is a software product for statistical analysis of encrypted historical manuscripts. The document analysis is performed via a chain of *filters* (main building elements). A filter represents any operation realizable on a document transcription divided into a set of pages. The implemented filters allow to change the reading direction, select sub-pages, or a subsection from the document, and calculate several statistics like the index of coincidence, Shannon's entropy, *n*-gram frequency, etc. The software design also includes document visualization, displaying pairs of manuscript pages with corresponding transcriptions.

1 Introduction

A lot of historical ciphers[1] (both solved and unsolved) are well studied, and can be analysed by well known tools (CrypTool, 2018), (dCode, 2018). The main problem with the existing tools is that they are not adapted to perform the analysis on manuscripts with multiple pages and sections. In most of these tools, there are missing features like the document visualization, the reading direction management, etc.

ManuLab (**Manu**script **Lab**oratory) is an open source project. The goal of this project was to create a framework (application) for document analysis adapted to historical manuscripts. ManuLab is fully compatible to analyse manuscripts like the Voynich manuscript or the Rohoncz Codex.

2 ManuLab software design

ManuLab is an open source and multi-platform software, written in *C++*, *Qt*.

[1] A lot of historical ciphers and manuscripts can be found at (Cipher Mysteries, 2018), (The Cipher Foundation, 2018) or (Klausis Krypto Kolumne, 2018).

2.1 Project background

While preparing the software to study the Voynich manuscript, we have identified a lack of support software that helps an analyst with his work on an electronic version of a historical manuscript. We have originally prepared a software enabling parallel side-by-side display of the original Voynich manuscript, its transcription, and possibly some different substitutions of symbols and basic statistics. Later on, we have decided to create a more general framework allowing any researcher to work with different manuscripts in an efficient way, and to apply multiple transformations on the document transcription.

2.2 Goals and requirements

During the analysis of the proposed software we have identified the following design requirements:

- Operating system independence.
- Manuscript visualization, including visual data (scanned document), and its transcription.
- Chain of filters. Each filter can do atomic operations on document transcription (see section 2.3).
- Adjustable reading direction (both horizontal and vertical).

The most important requirement was to enable a side-by-side manuscript visualization. This feature allows to display image-transcription pairs. This can be very helpful during a document analysis, especially if it is integrated with a display of analytic results (via filters).

To adopt the system to any manuscript or historical cipher, we have analysed several documents to identify their main properties and include them in the software design. We analysed the Voynich manuscript, the Rohoncz codex, the Codex

Proceedings of the 1st Conference on Historical Cryptology, pages 125– 128,
Uppsala, Sweden, 18-20 June, 2018

Seraphinainus, the Blitz cipher and other documents. Many manuscripts consist of several pages, where the reading direction of the used cryptosystem is not necessarily clear. Another possible problem is that documents may contains hundreds of symbols/glyphs.

2.3 Filters

Filter is the main building element used to perform any analysis/action on the loaded document. Every filter is derived from a common interface and works with a set of strings, where each string represents a page transcription. A filter can perform it's action per page or on the whole document transcription (merged pages) depending on the implementation.

The application is using two types of filters, that

a) modify the transcription,

b) do not modify the transcription, and are only used in analysis.

In both cases, the filter contains a set of strings as an input, and also produces a set of strings as an output. In case b), the output corresponds with the input. This feature allows to join several filters as a chain of operations. This chain can be also saved and loaded.

We have already implemented the following filters:

- *n*-gram frequency,
- *n*-gram distances,
- index of coincidence,
- Shannon's entropy,
- substitution,
- sub-pages selection,
- changing the read direction,
- pattern search.

The result of the analysis is visualised through pop-up menu for each filter. In most cases, the data can also be exported into a *csv* file for further processing.

2.4 Source code

The source code is available online at the following GIT repository: `https://bitbucket.org/jugin/manulab.git`.

2.5 License

The project is open source, licensed under Apache License, Version 2.0.

3 Software description

The ManuLab software provides two main functions: manuscript visualisation, and analysis. In the following subsections, we shortly introduce the main components, with example screenshots of the software.

3.1 Main components

The user interface (Figure 1) of the ManuLab software consists of 5 main components:

- Menu (not visible in the figure)
- 1a - selected page (image) of the manuscript,
- 2 - the transcription of the selected page,
- 3 - available filters palette,
- 4 - selected filters palette.

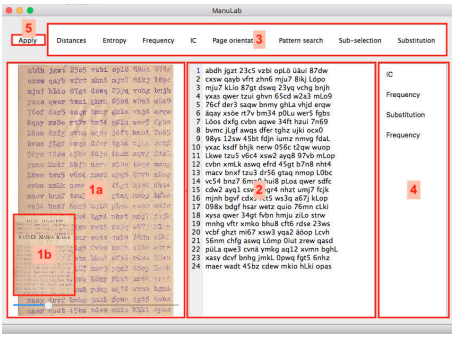


Figure 1: Main components of the UI, displaying a page of the Rilke Cryptogram (Klausis Krypto Kolumne, 2018).

ManuLab was designed to provide a manuscript visualisation with a good user experience. This visualisation is visible in the major part of the application window (parts *1a* and *2*). A side-by-side image/transcription pair is displayed on the screen. In case of multiple images, the scrollbar (visible under part *1a*) or the *left arrow* and *right arrow* keys of the keyboard can be used to switch to other page. The orientation/alignment of components *1a* and *2* can be changed to display the parts vertically (see Figure 2).

The document transcription may contain any valid characters. It is recommended to use a line separator for each line and to use a custom delimiter between the symbols. This is very helpful in case of documents containing special symbols, like the Rohoncz codex, where each symbol can be transcribed into a unique number. The transcription can be also displayed using any custom font[2] (In Figure 2, the upper part is the original image and the lower part is the transcription using a custom font).

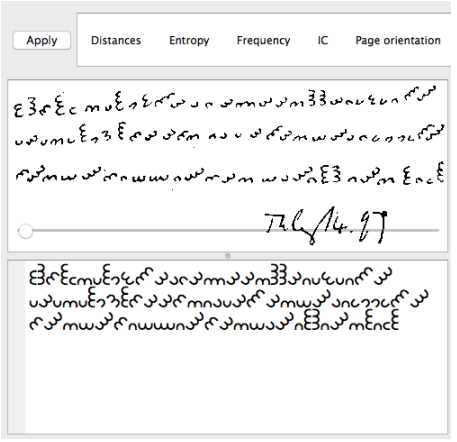


Figure 2: The Dorabella cipher (Klausis Krypto Kolumne, 2018).

To enable a quick per-page analysis, a classical *Find and Replace* functionality (Figure 3) can be enabled through the *Edit* menu item. It is displayed at the bottom of component *2*, when enabled. This widget is only for preliminary analysis. The searched pattern is highlighted on the page. Replaced symbols are never saved to the original transcription on exit.

The document analysis (all actions) is performed using filters. The filters from palette *3* are displayed in palette *4* in the selected order. Some filters change the document transcription directly, so each filter can be selected multiple times. Applying the chain of filters to the whole document (all pages) is done by the *Apply* button (Figure 1, part *5*). Each filter can be set up through a pop-up menu. After the setup, the *Apply* button should be pressed.

[2]Installed on the operating system.

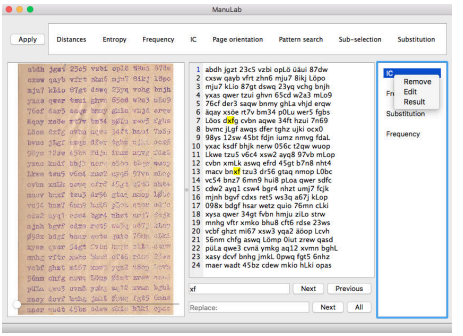


Figure 3: Find and Replace; filter settings; displaying a page of the Rilke Cryptogram (Klausis Krypto Kolumne, 2018).

For example, in case of available transcription of the Rilke cryptogram (see Figure 3), we can calculate the frequency of quads (four letters separated with space) with setting the space character as the delimiter. If a researcher decides to calculate the frequency of unigrams excluding the space character, it is enough to add two filters. One filter to remove the space characters (the filter *Substitution*) and the *Frequency* filter second time. The frequency calculation then works with a modified dataset. The results can be displayed separately for each filter.

A selected chain of filters with specific settings can be saved to files, thus there is no need to set it up every time. The same manuscript analysis is therefore replicable. Some predefined chains of filters can also be shared between researchers.

An example of the pop-up menu for the *Frequency* filter is visible in Figure 4. Pressing the *Edit* button shows a new pop-up with the available filter settings (visible in Figure 5).

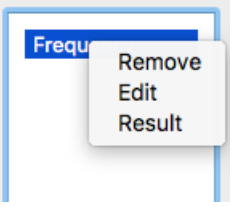


Figure 4: Pop-up menu for the *Frequency* filter.

The pop-up menu also serves to display the analysis results. Figure 6 shows the frequency

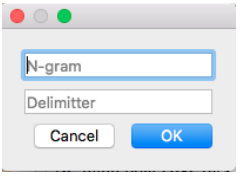


Figure 5: Pop-up menu for the *Frequency* filter, with available filter settings.

analysis result of the Rilke Cryptogram (Klausis Krypto Kolumne, 2018). Figure 7 shows the results displayed as a histogram.

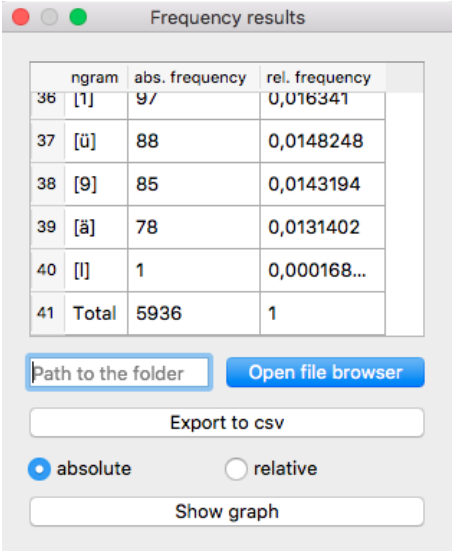


Figure 6: Frequency analysis result of the Rilke Cryptogram (Klausis Krypto Kolumne, 2018).

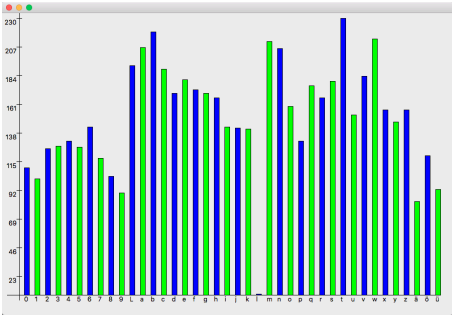


Figure 7: Frequency analysis result - histogram of the Rilke Cryptogram (Klausis Krypto Kolumne, 2018).

Acknowledgments

This work was partially supported by grant VEGA 1/0159/17.

References

CrypTool Contributors. *Cryptool Portal*, `https://www.cryptool.org/en/`

Team dCode. *dCode The ultimate 'toolkit' to solve every games / riddles / geocaches. dCode*. `https://www.dcode.fr/`

Klaus Schmeh. *Klausis Krypto Kolumne* `http://scienceblogs.de/klausis-krypto-kolumne`

Nick Pelling. *Cipher Mysteries* `http://ciphermysteries.com/`

Nick Pelling. *The Cipher Foundation* `http://cipherfoundation.org/`

Willard's System

Niels O. Faurholt
MJ, DAA, retired
DDIS Technical-Historical Collection
faurholt@fasttvnet.dk

Abstract

Willard's cryptosystem is an unusual system, designed by an otherwise unknown American around 1870. It was used for a short period of time by the Danish Ministry of Foreign Affairs. The article describes the system. Furthermore the article mentions an interesting and lively period of Danish crypto activities 1873 - 1918.

1 Background

For a few years before 1873 the Danish Ministry of Foreign Affairs (MFA) used for its enciphered communication a crypto system invented by a person named Willard, presumably an American. It has not been possible to find more information about Willard. According to papers in the MFA he was an acquaintance of the Danish diplomatic representative in Washington D.C., and the MFA must have bought the system around 1870. In 1873 a Danish school teacher, Gravers Pedersen, who later took the name Orloff, showed to the MFA that messages enciphered in Willard's system could fairly easily be broken by simple cryptanalysis. The result was that the MFA stopped using Willard's system, and on 18th October 1873 introduced a new system, invented by Mr. Orloff, for its enciphered communication. However, Willard's system is a curious invention, even if it had a short life in the Danish MFA.

2 Danish Crypto Activities 1873 - 1918

Before going into the details of Willard's system I would like to mention the remarkable crypto activity in Denmark from 1873 to about 1918. The inspirator was professor Julius Petersen (1839-1910). He was teaching mathematics at the Polytechnical University and later became professor of mathematics at Copenhagen University. He was for a few years from 1875 very active in cryptography, before he went on to other fields of mathematics and geometry. He is mostly known for his contribution to graph theory. In 1875 he, anonymously[1], wrote a remarkable series of articles in the Danish weekly journal "Nær og Fjern" (Near and Far) about seven international and Danish cryptographic systems, describing the systems and showing how they could be broken. At least three of the systems had been in use in the Danish MFA. Each article ended with some ciphertexts in that system, and amateur cryptanalysts had two weeks to solve them and report them to the journal, before the solutions were given in the next issue. The systems described were:

Carré Indéchiffrable (Vigenère type)
Willard's System
Léopold Auvray's System
Wheatstone's Cryptograph
Clausen's Apparatus (Danish Military)
Orloff's System
Orloff's Modified System.

Julius Petersen followed up with a paper&pencil system of his own later in 1875. It is assumed that it originally should have been included in the series in the journal. It was a rather complicated system, and Julius Petersen consid-

[1]The articles were written under a pseudonym: 46,9,4 – 57,3,5. The meaning of this is not known, but might indicate page, line and place in a book, as seen in book ciphers. However, the authorship of Julius Petersen is strongly indicated by three facts:

a. Immediately after the articles in "Nær og Fjern", where he demonstrated the lack of secure cryptosystems, Julius Petersen published his own (unbreakable) Système Cryptographique.

b. Alexis Køhl in an unpublished article in 1916 refers to the articles in "Nær og Fjern", that "long ago were written by the late Julius Petersen", as his inspiration for going into cryptography. Køhl publishes his first system in 1876.

c. The plaintext used in one of the examples in the Willard article in "Nær og Fjern" is a quote from one of Julius Petersen's own mathematical textbooks (observation by Knud Nissen, Aarhus Academy).

Proceedings of the 1st Conference on Historical Cryptology, pages 129– 132,
Uppsala, Sweden, 18-20 June, 2018

ered it unbreakable which in principle probably was correct at the time. It seems likely that Julius Petersen's intention with the series in "Nær og Fjern" was the creation of a Danish "Black Chamber". The successful problem solvers might be recruited for such an organisation. However, there was no political will to support such a project, and nothing came out of it. In his footsteps followed the Danish engineer, Alexis Køhl (1846-1920) who openly admitted that Julius Petersen was his inspirator. Køhl started with two paper&pencil systems in 1876, not unlike Petersen's from 1875, and in 1883 Køhl presented his Automatic Cryptograph, based om Rasmus Malling-Hansen's Writing Ball (now in Musée des Arts et Métiers in Paris). Køhl continued constructing crypto systems, a paper&pencil system in 1888, a cryptograph in the late 1880es (now in Deutsches Museum im München), other cryptographs around 1890 and around 1913 (both now in the Danish Technical Museum). His last devices are from 1917-18. Army captain (later colonel) E.J.Sommerfeldt was another inventor of cryptosystems, and his cryptograph was adopted by the Danish army in 1883 and used for a number of years.

3 Willard's System

The description of the system is mainly based on professor Julius Petersen's article from 13th June 1875. The heart of the system is a table consisting of 28 columns with a Danish alphabet that in addition to the standard 26 characters has the letters Æ and Ø. (Figure 1)

The table is constructed as follows: In the top **row** are the letters **A** to **Ø**. In the second **row** is the alphabet starting with **B**. The **A-column** is filled in alphabetic order, but every second place is left open. When the bottom of the A-column is reached, the alphabet is continued upwards in the empty spaces. The rows are then filled alphabetically, starting with the letters in the A-column. When **Ø** is reached the row continues with **A**. The system "hardware" is simply 28 cardboard sticks, each corresponding to one of the columns in the table. The top letter on each stick is called the key letter. The set is enclosed in a red cardboard box (Figure 3).

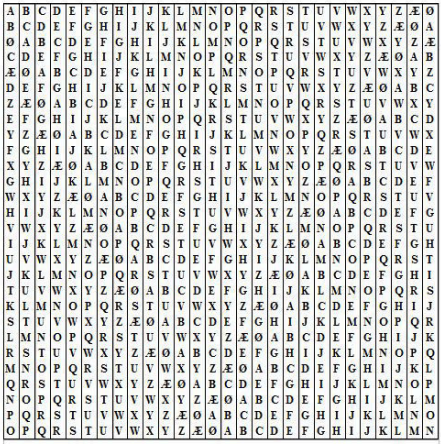


Figure 1: Willard's Table

4 Encipherment/Decipherment

A keyword must be ordered, here e.g. DANMARK. From the keyword we choose the columns (sticks) to be used for the encipherment, here the columns with the key letters D,A,N,M,R,K (repeated letters are skipped). The sticks are laid up, so that they form a rectangle. (Figure 2 and 3)

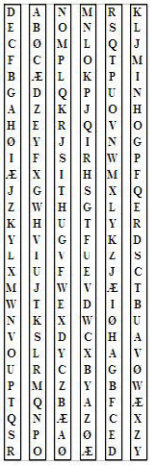


Figure 2: Sticks, selected according to ordered keyword

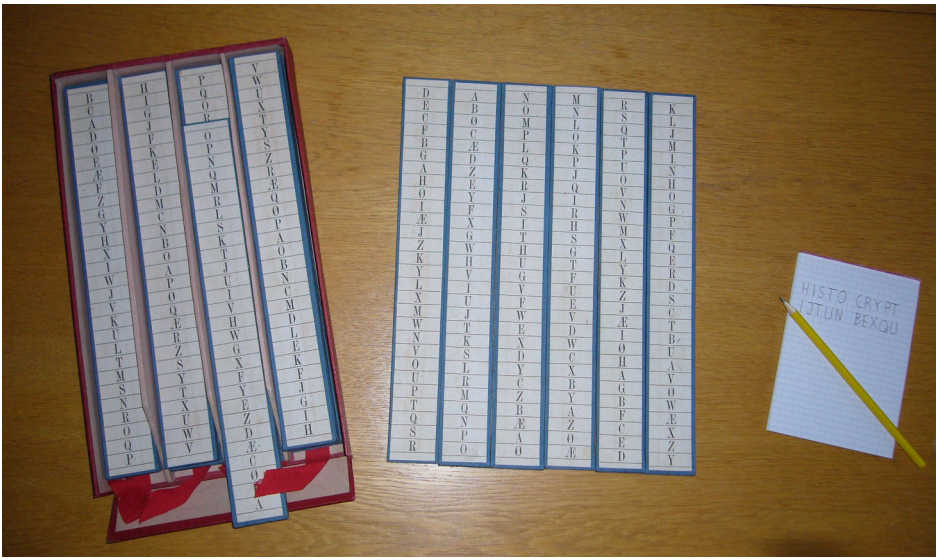


Figure 3: Willard ”hardware” and the encipherment process

You want to encipher the word ”HISTOCRYPT”. You find the first plaintext letter ”H” in the first column. The corresponding cipher letter stands x places above or below ”H”. This must be agreed beforehand. If the agreed rule is ”x=go down 2”, you go two places down from ”H” in the first column and find the cipher letter *”I”*. The second plaintext letter ”I” is found in the second column. Down 2 gives cipher letter *”J”*. The third plaintext letter ”S” is found in the third column. Down 2 gives cipher letter *”T”*. And so on. If a plaintext letter is at the bottom of a column, you go to the top of that column to find the cipher letter.

Plaintext HISTOCRYPT thus becomes ciphertext

IJTUN BEXQU

Decipherment is performed in exactly the same manner, except that you go ”up 2” from the cipher letter.

5 Security

How secure is this system? As the Danish school teacher showed in 1873, it is not particularly secure.If you have a cipher message long enough (15 - 20 times the length of the keyword) it can be broken. The periodicity is the weak point. Another weak point is that if you have to count many places up or down in the columns, it will be difficult and give frequent errors. So normally you could assume that 5 places up or down will be the maximum. The length of the keyword will also for practical reasons seldom exceed 6 -10 letters. In theory all the sticks could be used, 28 in all, but that would give a very cumbersome operation.

6 Cryptanalysis

Due to the construction of the Willard table, breaking the cipher depends largely upon the number of steps you go up or down in the operation. Even numbers are much easier to break than uneven numbers.

Even number of steps (2 or 4): As the columns are in alphabetic order with every second place skipped, only a few letters can come 2 or 4 places above or below a given cipher letter. We start with 2 places up and down: E.g. cipher *"I"* above will become plaintext "J" or "H" (there are exceptions in columns A and Ø). Cipher *"J"* will become plaintext "K" or "I". It is possible quickly to form tables with 2 up or down, and 4 up or down, and it will be obvious which of these is the correct one. The plaintext can then be read in the table. Finding the keyword requires a longer message. If the test for even number of steps does not succeed, uneven steps are probably used.

Uneven number of steps (1, 3 or 5): Here the construction of the table cannot help in the same way. In principle any cipher letter can become any plaintext letter. So we will have to use the Kasiski[2] method to find the length of the keyword, e.g. 5, and then solve the resulting monoalphabetic cipher texts the hard way. However, there is a possibility to find the keyword: You have a good chance to locate "E" in each of the 5 monoalphabetic cipher texts. You can construct a table that for each (cipher) letter shows in which column that letter stands 1, 3 and 5 steps above or below "E". If you combine the "E"-equivalents with that table, you may find which 5 columns (sticks) were used in the encipherment. This gives the keyword and an easy way to read the whole message.

[2]The Kasiski method looks after repeated trigrams or longer in the ciphertext, and determines the distances between these. These distances will in most cases be a multiple of the length of the keyword. Once the length of the keyword is found, the cipher message is split into that number of monoalphabetically enciphered texts, that must be solved by frequency analysis.

Acknowledgements

I am most grateful to professor emeritus Ole Immanuel Franksen from the Danish Technical University. Mr. Franksen brought the old periodical, "Nær og Fjern", to my attention and kindly allowed me to use his extensive research in the Danish crypto history in this article.

Without the great help of my good colleague, Hans-Erik Hansen, this article would never have been converted to the required format.

The Danish Defence Intelligence Service (DDIS) Technical-Historical Collection owns the Willard hardware, presented to the collection by a former MFA employee. I am the curator (volunteer, unpaid) of the collection.

References

Buonafalce, Augusto, Niels Faurholt and Bjarne Toft. 2006. *Julius Petersen - Danish Mathematician and Cryptologist.* Cryptologia, Vol. 30: 353-360.

Faurholt, Niels. 2006. *Alexis Køhl: A Danish Inventor of Cryptosystems.* Cryptologia, Vol. 30: 23-29.

Johnsen, Erik, Morten Christensen, Ole Immanuel Franksen and Knud Nissen. 1994. *Willard's System*. Matematiklærerforeningen DTU, Lyngby, DK

Kasiski, Friedrich W. 1863. *Die Geheimschriften und die Dechiffrier-Kunst.* E.S.Mittler und Sohn, Berlin

Kjølsen, Klaus and Viggo Sjöqvist. 1970. *Den danske Udenrigstjeneste 1770-1970, Vol. I.* J.H.Schultz, Copenhagen, DK

Petersen, Julius. 1875. *Nær og Fjern*, 154:4-7. Periodical, Copenhagen, DK

The Application of Hierarchical Clustering to Homophonic Ciphers

Anna Lehofer
Department of Philosophy and History of Science
Budapest University of Technology and Economics
Budapest H-1111, Egry József u. 1. E 610, Hungary
lehofer.anna@gmail.com

Abstract

In this work in progress study I examined whether the method of hierarchical clustering could be used efficiently on Hungarian homophonic ciphers from the early modern age. First I have tested the methodology on artificial homophonic ciphers. The original corpora of these artificial codes were appropriate to ascertain the effectiveness of the method: knowing the plaintext I could control the outcome. In connection with text length I have identified the limits of the applicability of hierarchical clustering. In a second part, the investigation of eight original letters from the early modern age followed. The testing of original manuscripts shows whether the results based on the artificial ciphers are applicable to original historical documents as well.

1 Homophonic Ciphers of the Early Modern Age

In a homophonic substitution cipher single plaintext letters can be replaced with several code characters. In simpler cases only the vowels and the most frequent letters are replaced with more code characters, but in an advanced, complex cipher key, each of the plaintext letters receive several code characters, so-called homophones. I call these ciphers pure homophonic ciphers. But in many cases, early modern homophonic ciphers used separate tokens for syllables, logograms (characters representing frequent words or names) and nulls (meaningless tokens to confuse the cryptanalysis) beyond the homophones. I call these types of ciphers advanced homophonic systems.

Both pure homophonic ciphers and advanced homophonic systems were part of the early modern practice, even the simple monoalphabetic substitution was in use in some cases. Breaking these monoalphabetic codes can even be an easy task. The frequency analysis of the code characters, recurring character lines, vowel-consonant analysis can bring us closer to find the plaintext letters of the ciphers.

The same cannot be said about homophonic ciphers. Speaking of advanced homophonic systems of the 16th century, the few pages long character tables consisted of two or three homophones for each plaintext letter, about 10 symbols for nulls, 10 for bigraphs, 100-150 characters for syllables and even 300 characters for logograms (Láng, 2015, 37). For such codes, a properly composed and correctly used cipher-key can result in an almost even distribution in the frequency of the code characters, making the task of the codebreakers much harder. So the tools that can lead us to the decryption of monoalphabetic codes give us no help for decrypting homophonic systems.

In the practice, using homophonic substitution meant a higher security compared to simple monoalphabetic ciphering, but it also had its drawbacks. The complexity of the cipher-keys made the usage of this encrypting method slower and more complicated.

2 Hierarchical Clustering

"Cluster analysis groups data objects based only on information found in the data that describes the objects and their relationships. The goal is that the objects within a group be similar (or related) to one another and different from (or unrelated to) the objects in other groups. The greater the similarity (or homogeneity) within a group and the greater the

Proceedings of the 1st Conference on Historical Cryptology, pages 133– 136,
Uppsala, Sweden, 18-20 June, 2018

difference between groups, the better or more distinct the clustering (Kumar et al., 2005, 490)."

Speaking of homophonic ciphers, the base set of these data objects is the multitude of the code characters. The aim of the clustering process is to ascertain with which right and left neighbors the particular code characters appear in the text.

To illustrate the operation of hierarchical clustering to homophonic codes let's suppose that we have a homophonic cipher using 100 different code characters. The aim of the method is to investigate which code characters are likely to appear together. Based on the 100 code characters of the text, we prepare two 100x100 matrices. Both the rows and columns of the matrix represent the code characters of the cipher. If we point at a number in this matrix, it indicates the occurrence-frequency, how often the concerning two code characters (indicated by the row and the column) appear together. One matrix shows the occurrence frequency with the left neighbors, the other shows the occurrence frequency with the right neighbors. To create one attribution from the left and right neighborhood, we combine these two matrices and use the new 100x200 matrix in the following step. In this matrix, each line is a 200-dimensional vector, representing one code character. Depending on the neighbors of these code characters, each vector points to different directions. Similar vectors point almost to the same direction, vectors that differ from each other point into different directions.

From the upper vectors, on the basis of cosine distance function we generate a 100x100 distance matrix with values from 0 to 1. In the diagonal of this matrix (where the distance of the vectors from themselves appears, namely the distance of two equal vectors) the function gets a value of 1. The other values – depending on the angle locked together – will get values between 0 and 1. The more similar these vector pairs, the more they point to the same direction (the closer this value is to 1).

To display hierarchical clustering graphically I have used the open source Cran R software. It uses a tree-like diagram called a dendrogram to visualize these relationships. It draws these dendrograms on the basis of the distance-matrix.

Exactly the same method was efficiently used by the decryption process of the famous Copiale code (Kevin et al., 2011).

3 Artificial Ciphers

Hereupon I have created artificial homophonic codes from a Hungarian corpus (Géza Gárdonyi, Eclipse of the Crescent Moon) to be able to tell a bit more about the criteria for the optimal application. These artificial codes are pure homophonic codes which were created by Cran R that randomly assigned the desired number of homophones to the plaintext letters.

In the testing process I have investigated two things. First I have gradually increased the number of homophones assigned to a plaintext letter (starting with a monoalphabetic set of code characters) to see how long hierarchical clustering is able to detect the homophone groups. Secondly I have gradually reduced the length of the examined part of the text to find the point where hierarchical clustering loses its efficiency in finding the vowel and consonant groups and the groups of homophones.

3.1 Full Text Codes

Based on the artificial codes created from the full text of the novel I have faced with the followings. The first, monoalphabetic code has immediately brought in an interesting result. The software separated two bigger clusters on the dendrogram: one big cluster showed only vowels, the other bigger group contained only consonants. So the method can be used on monoalphabetic ciphers as well: it can almost perfectly separate vowels and consonants in a monoalphabetic ciphertext.

By tripling the number of the homophones clustering can also find the vowel and consonant groups, furthermore it can correctly recognize the three-element homophone groups belonging to the particular plaintext letters.

I was surprised when the program could even identify the vowel and consonant groups and the homophone groups when 20 homophones were assigned to a plaintext letter. It seems that in case of a 400-page corpus hierarchical clustering can identify the homophone groups belonging to the particular plaintext letters, even if we have far more homophones than the early modern practice shows (early modern cipher keys usually have 2-3 or 5-6 code characters for one plaintext letter at most).

Of course, in reality, codebreakers do not have book-lengthy texts. Most often they have a paragraph or at most a few pages written with encrypted characters. In the following, I have examined how the method worked when I started to reduce the length of the examined text.

3.2 Unicity Point

According to the writings of Elliot Fischer and James Reeds the limits of using hierarchical clustering efficiently will be discussed here with the concepts of text redundancy and unicity point. The unicity point of a cipher is U=H(k)/D where H(k) is

the logarithm of the number of possible keys of the ciphers and D is the redundancy of the language. The unicity point is the message length beyond which decipherment using a known system becomes a unique process. From the given formula it is clear that the lower the redundancy of a language, the greater the unicity point for a given cipher (Fischer, 1979 and Reeds, 1977).

I examined the original corpus in two ways. The first table shows how entropy – thus redundancy – and the unicity point changes when increasing the number of homophones gradually from 1 to 5 on the 700000-character-long corpus. Despite of the indicated infinite limit of the 5th case, all of the related five dendrograms have identified the vowel and consonant groups correctly and clustering could even find the 1-2-3-4-5 element homophone groups of the ciphers.

Number of homophones	Number of used code characters	H_{max}	H_{real}	Redundancy	Unicity point
1	35	5.129	4.58	0.107	1240
2	70	6.129	5.579	0.09	3706
3	105	6.714	6.164	0.082	6816
4	138	7.109	6.579	0.074	10569
5	174	7.443	6.901	0.073	∞

Table **1**: Increasing the number of homophones in the full text

The second table shows how unicity point changes when decreasing text length assuming 2 homophones for each plaintext letters. The first value (around 700000 characters) shows the full length of the text, 100%. Than follows 10%, 1%, 0.5% and finally 0.1%.

Text length (number of characters)	Number of used code characters	Unicity point
700934	70	3706
70093	66	3986
7009	66	4059
3504	65	4203
700	62	3515

Table **2**: How unicity point changes when reducing text length using 2 homophones per letter

We can see that in the given artificial code, speaking of pure homophonic substitution, using two homophones for each plaintext letter, the efficiency of hierarchical clustering falls down around the text length of 3500 characters. Here the unicity point is around 4200 characters, so a longer text is needed for a safe codebreaking than the examined one. The dendrograms of these cases also corroborate this statement: while the dendrogram of the 3500-character-long text can still separate a big cluster for vowels and another one for consonants almost perfectly, the dendrogram of the 700-character-long text (of which unicity point value is already much lower than the real text length) falls into smaller clusters. These small clusters may still support the individual codebreaking process but neither separate vowels and consonants, nor identify the homophone pairs of the ciphertext in a proper way.

4 Early Modern Letters

In this section, I will investigate encrypted letters[1] from the early modern age. The cipher keys of these letters were also available (in an archive or reconstructed form), thus the keys offered help and control when examining the efficiency of clustering.

The first letter I have examined – C.Bay.01 – was a 419-character-long almost fully encrypted letter that uses a very complex cipher key: beyond the homophonic set of code characters it also indicates syllables, logograms and nulls with separate signs. The dendrogram outlined as a result of clustering proved that this letter was too short, the cipher key was too complex to give any help in the decoding process.

After the Bay letter I looked for a letter with a less complex cipher key than the first one, and examined C.Wes.03.a. It was a 2359-character-long letter using an all-in-all 43-element cipher key, assigning more (5-6) code characters only to the vowels.

The cluster map of this cipher looked more promising. The software separated two bigger clusters: one showed only consonants, the other bigger cluster contained almost exclusively vowels. The program identified homophone pairs in five cases. The remaining smaller groups and the characters that were not grouped to other ones were mostly logograms, so they were "outranked" correctly from the homophones.

So far I have examined 6 more early modern ciphers to find out where the limits of applicability are. All of the scrutinized letters come from the period 1664-1706 and have their cipher keys in an available form as well.

To describe applicability, two outcomes were tested: 1) whether the clustering process could identify the vowels and consonants in different

1 Up to now I have investigated 8 early modern Hungarian letters. Since this is a work in progress, this outcome will be better grounded, after I will have transcribed and analyzed several other manuscripts in the near future.

clusters, and 2) whether the clustering process could identify the homophone groups belonging to the particular plaintext letters. In cases where clustering can show up any of these two identifications, hierarchical clustering can be stated effective. In these cases hierarchical clustering can support the codebreaking process.

The outcomes of the examined letters are summarized in the following table. The first column shows the name of the letters following the notation of Benedek Láng (Láng, 2015, 233). The column of *text length* shows how many code characters the concrete letters are made of; *number of used code characters* shows how many characters were actually used in the concrete letters. H_{max} shows the maximum value of entropy, H_{real} stands for the actual values of entropy. *Redundancy* shows the text redundancy of the letters, the column of *unicity point* indicates the required text length. *Vowel-consonant groups* shows whether the method of hierarchical clustering could separate the vowels and the consonants in different clusters; and homophone groups shows if the clustering process could identify the *homophone groups* belonging to the particular plaintext letters.

Letters[2]	Text length	Number of used code characters	H_{max}	H_{real}	Redundancy	Unicity point	Vowel-consonant groups	Homophone groups
C.Bay.01	419	113	6.82	6.113	0.104	5905	no	no
C.Bay.02	494	130	7.022	6.338	0.097	7490	no	no
C.Kov.02	1537	189	7.562	6.689	0.115	∞	no	no
C.Wess.03.a	2359	64	6	4.92	0.18	1643	vowels	in 6 cases
C.Wess.03.b	828	61	5.931	4.939	0.167	1662	vowels	in 5 cases
C.Wes.04	1525	77	6.267	4.994	0.203	1850	vowels	in 5 cases
C.Wes.05	749	26,	4.7	4.029	0.143	618	partly	-
C.Wes.06	417	37	5.209	4.231	0.188	763	no	no

Table **3**: Features of the examined early modern letters

5 Summary

In this paper I have first tested hierarchical clustering on artificial codes by modifying two parameters: increasing the number of homophones assigned to a plaintext letter and decreasing the text length. It can be stated that in case of a 400-page corpus hierarchical clustering could identify the homophone groups successfully, even if we had far more homophones (20) than the early modern practice showed (2-6). Investigating the unicity points of ciphertexts it can be stated that hierarchical clustering was still efficient when text length was under the unicity point, but near to it. In cases when text length was much lower than the unicity point, the dendrograms could not give any help for the codebreaking process.

In a second part I have processed original early modern ciphers with the upper methodology. I have stated that hierarchical clustering was efficient if it could clearly identify the vowels and consonants in separate clusters on the dendrogram and/or if it could find the homophone groups belonging to the particular plaintext letters. The features and outcomes of the eight early modern letters showed that when the unicity point was under or near the text length the dendrograms could help the codebreaking process. Hierarchical clustering could not bring any results in case of letters that were much shorter than the unicity point.

Consequently, speaking of homophonic substitution ciphers we can state that the longer an encrypted letter, or the less symbols its cipher key uses, the more probable the cipher can be solved with the help of hierarchical clustering. Since the historical manuscripts of the early modern age do involve such encrypted letters – we can find ciphers with thousands of code characters, or cipher keys that have only 30-40 symbols – hierarchical clustering offers significant contribution to the codebreaking process of historical homophonic substitution ciphers.

2 These letters can be found in the Hungarian National Arcives, G 15 Caps. D. Fasc 81. and G 15 Caps. C. Fasc 36. fol. 3-4. and in the ÖStA HHStA Ungarische Akten Specialia Verschwörerakten VII. Varia (Pressburger Kommission etc.) Fasc. 327. Konv. D. Chiffres 1664-1668, fol 35-37, 40-41, 62, 63.

References

Benedek Láng. 2015. *Titkosírás a Kora Újkori Magyarországon.* Balassi Kiadó, Budapest.

Elliot Fischer. 1979. Language Redundancy and Cryptanalysis. In *Cryptologia*, volume 3, pages 233-235.

James Reeds. 1977. Entropy Calculations and Particular Methods of Cryptanalysis. In *Cryptologia*, volume 1, pages 235-254.

Kevin Knight, Beáta Megyesi, Christiane Schaefer. 2011. The Copiale Cipher. Presented at the *ACL Workshop on Building and Using Comparable Corpora*.

Vipin Kumar, Michael Steinbach, Pang-Ning Tan. 2005. *Introduction to Data Mining*. Pearson (Education Inc.), Boston.

Teaching and Promoting Cryptology at Faculty of Science University of Hradec Králové

Michal Musílek
Faculty of Science
University of Hradec Kralove
Rokitanskeho 62, Hradec Kralove
michal.musilek@uhk.cz

Štěpán Hubálovský
Faculty of Science
University of Hradec Kralove
Rokitanskeho 62, Hradec Kralove
stepan.hubalovsky@uhk.cz

Abstract

University of Hradec Králové is one of the smaller public higher education institutions in the Czech Republic. At present, there are about 7,000 students studying here. Even though at any of their faculties it is not possible to study a study program closely focused on cryptology, we pay attention to the historical and modern cryptology at the Faculty of Science in several subjects. Basic concepts, principles and methods of modern computer cryptology form an important part of the subject Computer and Data Protection. Principles of encrypting, decrypting and deciphering of basic substitution and transposition ciphers and the history of cryptology have become part of the subjects of Computer Science and Structured Programming in various degrees and with different approaches.

1 Introduction

Overview of the history of cryptology is included in the subject History of Computer Science as an expanding and enlightening of the curriculum. Special attention is paid to rotate encryption machines such as Enigma, the Lorenz SZ42 cryptographic telegraph and to machines used to break them as well - Turing's bomb, the first British computers, Colossus Mark 1 and 2 (Boone, 2005; Singh, 2000). Part of the exercises in the subject History of Computer Science is devoted to the encryption, decryption and deciphering of some basic types of hand ciphers, because this course also has practical lessons in which students learn, for example, to multiply numerical numbers using a counter or to perform calculations on a logarithmic ruler.

Different way to learning of cipher is used in the subject of Programming subject. The cipher system is used to enter interesting and motivating programming tasks during Structured Programming course. In addition to cryptology, attention is also paid to the problems associated with wireless transmission and plain coding of information (Musílek, 2012; Musílek, Hubálovský, & Hubálovská, 2017).

2 Theoretical Background

A deeper insight into the issue of cryptology is then made possible for students who are interested in this topic within realization of the bachelor as well as diploma thesis. The Department of Cybernetics of the Faculty of Science of the University of Hradec Králové, with the two authors of this article, prepares future lower and upper secondary schools teachers of Informatics in the Czech Republic. Teacher preparation is always carried out for two teaching subjects and significant space is devoted not only to these two areas, but also to basic pedagogical-psychological, general and subject didactics preparation. Interestingly, although our students are studying many different combinations of subjects, interest in historical ciphers has so far been shown only by students of two different combinations, namely Informatics - Mathematics and Informatics - History.

The individual bachelor theses of the students of the program Mathematics and Informatics with a focus on education had following topics:

Proceedings of the 1st Conference on Historical Cryptology, pages 137– 143,
Uppsala, Sweden, 18-20 June, 2018

"Deciphering of substitution ciphers with computer support" (Procházka, 2012), "Deciphering of ciphers with computer support" (Hanzalová, 2014; Hájková, 2015). The diploma theses in the follow-up master's program Teaching of Mathematics and Informatics for Secondary Schools was oriented more didactically with following topics: "Ciphers as motivation in the teaching of algorithms and programming" (Bukáček, 2013); "Board games, puzzles, anagrams and ciphers as motivation in the teaching of algorithms and programming" (Procházka, 2014); "Fundamentals of cryptology as a teaching topic in subject "Informatics" at lower secondary school" (Hájková, 2017). The topics of bachelor's thesis in the study program Informatics and History were "Computer Analysis of Encrypted Correspondence of House of Piccolomini" (Vlnas, 2017) and "History of ciphering of transposition ciphers with computer support" (Musílek, 2017).

Thesis focused on specific historical clues used by Marshal Ottavio Piccolomini during the Thirty Years War links the work of the historian - investigator in the archive - with the approach of informatics. The routine decryption algorithms were realized in macros in Visual Basic for Applications in a MS Excel spreadsheet. This thesis was evaluated by the Dean of the Faculty of Science of the University of Hradec Králové for the best bachelor thesis in the study program Informatics.

3 Samples of advancement of students

In the following text, we will discuss in detail two bachelor's theses: work for the automatic analysis of text encoded by monoalphabetic substitution based on the trigram frequency analysis (Hanzalová, 2014) and work analyzing real historical ciphers of the early 17th century (Vlnas, 2017).

3.1 Using spreadsheet in cryptanalysis of short cipher text

The authors of the paper suggest new method and algorithm for deciphering and automation analysis of the ciphered monoalphabetic text. The method generalized frequency analysis of the bigram saved in a two-dimensional array to frequency analysis of the trigrams saved in a three-dimensional array with 26 x 26 x 26 = 14576 elements.

The algorithm for automatic deciphering of short simple substitution cipher text is similar to algorithm for deciphering of long ciphered text.

The algorithm for deciphering of long ciphered text is based on method of evaluation of frequency of pairs of consecutive letters and compares it with the frequency of bigrams of reference text using the evaluation function:

$$f = \sum_{i=1}^{26} \sum_{j=1}^{26} \mid D_{ij} - E_{ij} \mid \qquad (1)$$

where E_{ij} is matrix of bigrams of reference text and D_{ij} is matrix of bigrams of ciphered text.

Similarly, the algorithm for deciphering of short ciphered text is based on automatic analysis of evaluation function *f* of trigrams:

$$f = \sum_{i=1}^{26} \sum_{j=1}^{26} \sum_{k=1}^{26} \mid D_{ijk} - E_{ijk} \mid \qquad (2)$$

where E_{ijk} is matrix of trigrams of reference text and D_{ijk} is matrix of trigrams of ciphered text.

The algorithm consists o three relatively independent sub-procedures (Hanzalová, Hubálovský, & Musílek, 2012).

The first sub-procedure *Frequency* creates three-dimensional reference matrix ***E*** that corresponds to the frequencies of letters in the reference text.

The second sub-procedure *Trigrams* creates three-dimensional matrix ***D*** of relative frequencies of the trigrams of the cipher text. The part of the matrix ***D*** is shown on the Figure 2. In next step (Hanzalová, Hubálovský, & Musílek, 2012) the procedure evaluates the compliance with the reference text by using an evaluation function:

$$f = \sum_{i=1}^{26} \sum_{j=1}^{26} \sum_{k=1}^{26} \mid D_{ijk} - E_{ijk} \mid \qquad (2)$$

The third sub-procedure *Exchange* provides exchange of two *x*-vectors, two *y*-vectors and two *z*-vectors of three dimensional matrix ***D*** and creates new matrix ***D'***. The vectors are exchanged in the order of the frequencies of the letters in the cipher text from the most frequent to the least frequent based on following rules - see Hanzalová, Hubálovský, & Musílek (2012):

- the *x*-vector corresponding to the order of the first exchanged character is replaced by the x-vector corresponding to the second exchanged character;
- then *y*-vector corresponding to the order of the first exchanged character is replaced by the y-vector corresponding to the second exchanged character;
- then *z*-vector corresponding to the order of the first exchanged character is replaced by the y-vector corresponding to the second exchanged character;

After each substitution a new matrix ***D'*** is obtained, and the evaluation of the compliance of the relative frequency of the trigrams in the cipher text and the reference text is obtained using the evaluation function:

$$f' = \sum_{i=1}^{26} \sum_{j=1}^{26} \sum_{k=1}^{26} \mid D'_{ijk} - E_{ijk} \mid \quad (3)$$

After each substitution the values f and f' are compared and if $f' < f$, the procedure immediately stops the process of the letter substitution and the exchange in the conversion table is proposed, which will improve the compliance (lowering the value of evaluation function *f*). Finally, the sub-procedure will creates a new matrix ***D*** of relative frequencies of the trigrams of the cipher text, and it will provide a new assessment of compliance with the reference text using the evaluation function (3).

The sub-procedure *Frequency* is run only once at the beginning of the program to set the appropriate initial conditions. The sub-procedures *Trigrams* and *Exchange* are run alternately.

Above mentioned sub-procedures were realized in Visual Basic for Application in MS Excel Spreadsheet. Deciphering based on trigrams' analysis has been studied in cipher text with the length in the range from 200 to 500 characters. It was proved that algorithm for deciphering of short simple substitution cipher text based on automatic analysis of the trigrams enables decryption almost without manually performed exchanges

3.2 Computer Analysis of Encrypted Correspondence of House of Piccolomini

Bachelor thesis titled Computer Analysis of Encrypted Correspondence of House of Piccolomini interconnects the two author's study areas (Vlnas, 2017). The author is a student of Informatics and History in education. Archives, especially archives of aristocratic families whose members held important state, military or diplomatic positions, contain, in addition to open documents, very often-encrypted documents.

The analysis of archive ciphertexts is a complex task. Standardly, the task is necessary to do in large part by hand, such as recognizing different forms of written fonts (different types of ancient shape handwritings or special cipher characters), counting frequencies of individual characters, etc. Some monotonous tasks can be performed a computer. The author of the bachelor thesis had appropriately used custom-made macros in Visual Basic for Applications to decrypt encrypted texts transcribed into Excel spreadsheets. After identifying a given cipher system and determining the transmission table, it is a purely mechanical matter. Macro combined both basic principles used to make mono-alphabetic substitution, i.e. simple swapping and supposed words, and was created in such a way that allow the gradual uncovering of the spreadsheets that effectively supports cipher shredders in the phase of stepwise reconstruction of the encryption table.

The first phase of the work was to obtain appropriate cipher texts. The State Regional Archive of Zámrsk offers to researchers a family archive of the genus Piccolomini on microfilms. It has advantages and disadvantages. The advantage is the possibility of fast document browsing, where the scrolling of the microfilm in the reader can be significantly faster than working with original archives. The disadvantage is the lower contrast and the overall loss of quality and the worse possibility of photographic documentation. The student focused on documents related to the person of Ottavio Piccolomini and his activities during the Thirty Years' War. He found two microfilms with a number of cryptic texts, partially decrypted, apparently immediately after receiving the addressee, but partly un-decrypted. The student took photographs of the corresponding microfilm images. He thought he had captured only a small

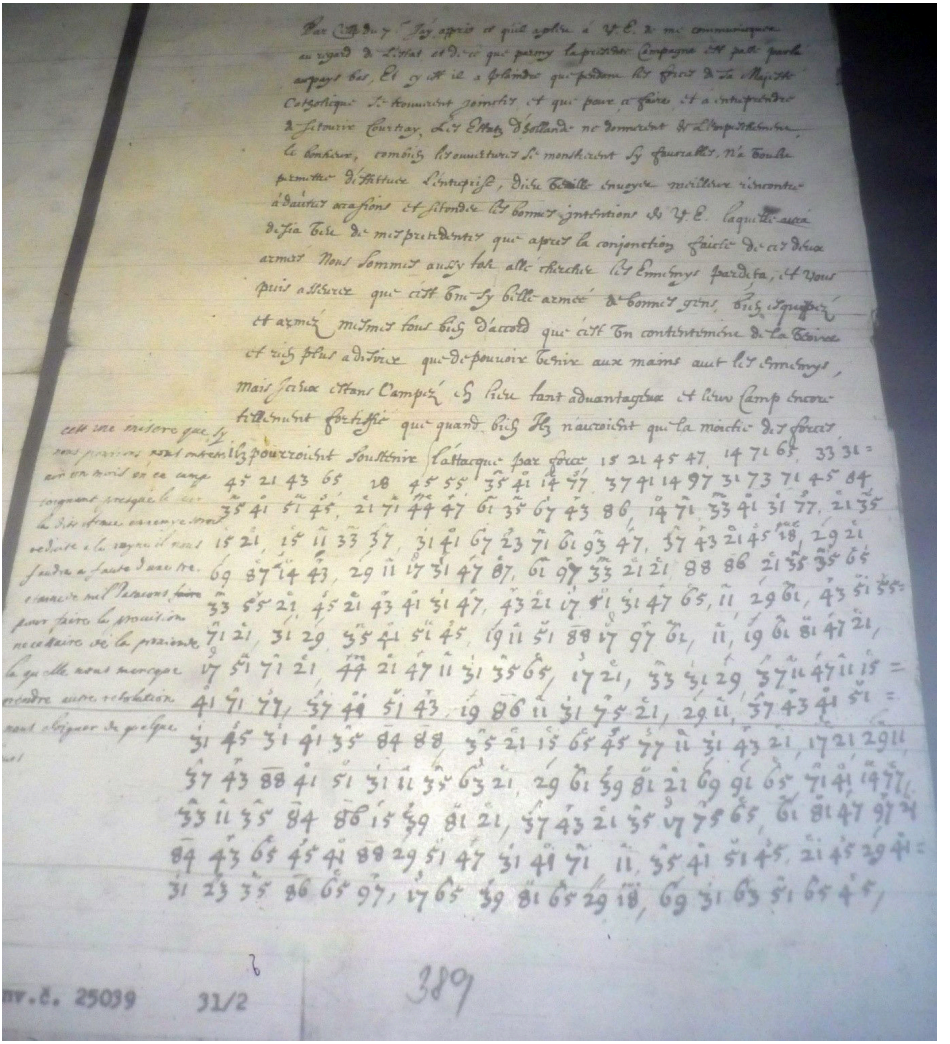


Figure 1: A homophone substitution cipher - pair of digits represents a letter or null character

part of Ottavio Piccolomini's cipher correspondence. The archive contains large number of the ciphertext than cannot be found within one business day.

Firstly, the document number 25039 was analyzed, see Figure 1. Part of this letter was written in plain text and part was written in numerical code. Some letters of the alphabet have been written above the two-digit codes. It allows reconstructed the decryption conversion table - see Table 1. The entire cipher text, composed only of digits, was read quite well. It was certainly easier to read digits then to read handwritten characters in shapes which had been written in individual manuscripts of many different scribes. This text was copied in the cell of Excel spreadsheet. Also deciphering table was placed in the same sheet. The deciphering table was step by step filled in and simultaneously was used for decrypting of prepared ciphertext. It was found that the open text in French was encrypted by simply replacing the alphabet letters with two-digit numbers, but with the use of vowel homophones and special codes for some selected short words, supplemented by several null

characters. It is a simple nomenclator. Partially decrypted text was a significant help, however, the use of macros in Visual Basic for Application significantly simplified the complete decryption of the encrypted part of the letter.

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1	a		b	u	C		d	que	f
2	e		g	et	L		a	e	l
3	i		m	sko	n		p		q
4	o		r	tre	s		t	m	o
5	u				y		s		
6	a	a	g		e		i		l
7	n		o		r		s	rc	t
8	u			*		*	e	*	
9	e		n				r		

Table 1: Encryption table of the document 25039
(* = null characters)

„C'est une misère que si nous puissions nous entretenir un mois dans ce camp Xabucd que fais-je là et lim skonpqor très tmouysaageilnorsrctu et en joignant presque le leur, ladite armée, ennemie seroit réduite à la ruine, il nous faudra, à faute d'une trentaine de mil patacons pour faire la provision nécessaire de la prouiange laquelle nous manque, que prendre autre résolution à nous? sloigcer de quelques ligues d'ici où nous puissions muuerles dit su iures et fourrage à fin de ne voir ce que dit une plais est réduit et cette belle armée en teees état misérable comme elle samuue du passé au camp skoprocle Bérenburg. En quoi consiste néanmoins la conservation ou perte du reste de l'empire gedlusrc?“

The similar system, based on a square table, with otherwise delimited letters, was used in several other cipher letters. From the cryptanalysis point of view, the letter with non-encrypted cipher sections consisting of letters and numbers was more interesting. This letter was included in document number 24873, see Figure 2. The cipher was taken by standard methods, i.e. by frequency analysis and predicted words. The plain cipher text was in Italian. Even this cipher contained the null characters represented by all even digits (2, 4, 6, 8). The cipher does not contain any homophones. If these null characters were omitted, the very simple monoalphabetic substitution cipher was reached - the consonants did not replace and the vowels, were successively replaced by the numbers 1, 3, 5, 7, 9. As soon as the eyes of the solver became used to the Italian handwriting of the first half of the 17th century, reading the text was relatively simple. Fig. 3.

b	c	d	f	g	h	j	k	l	m	n	p	q
b	c	d	f	g	h	j	k	l	m	n	p	q

r	s	t	v	1	2	3	4	5	6	7	8	9
r	s	t	v	a	*	e	*	i	*	o	*	u

Table 2: Encryption table of the document 24873
(* = null characters)

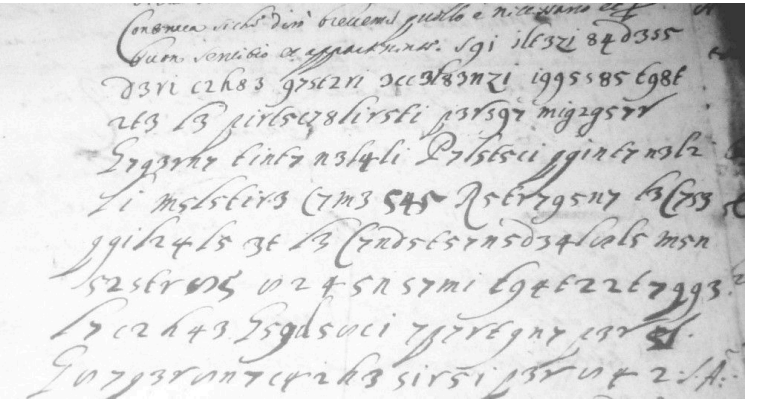


Figure 2: An example of a cipher text (cut-off from document 24873) that was not decrypted by the recipient

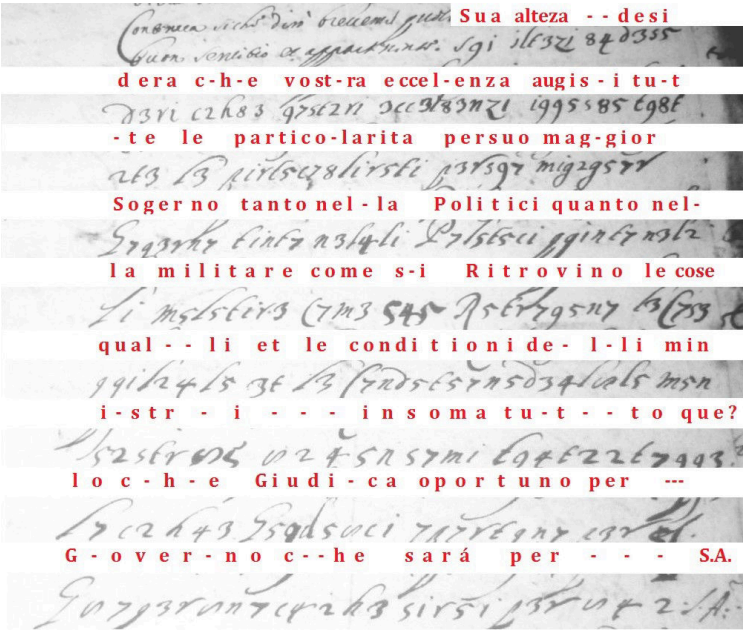


Figure 3: Sample of decryption of the text from the Figure 2 (cut-off from document 24873)

4 Conclusion

It is pleasing that some of the students of the Faculty of Science of the University of Hradec Králové, supervised by the authors of this paper, contributed to solution of tasks of historical cryptology. The important is the fact that not only students mentioned above, but also many other graduates of study program the teaching of informatics or also teaching mathematics or history will to motivate the secondary school students by examples of cipher systems, or by historical events that were affected by revealing of secret correspondence or by breaking of cipher systems.

Acknowledgments

The research was supported by Specific research project at Faculty of Science, University of Hradec Kralove, 2018.

References

Boone, J. V. 2005. *Brief History of Cryptology.* Annapolis: Naval Institute Press. 192 p. ISBN 1-59114-084-6.

Bukáček, D. 2013. *Ciphers as motivation in the teaching of algorithms and programming.* Diploma Thesis at Faculty of Science University of Hradec Králové. Supervisor . 118 p.

Hájková, S. 2015. *Deciphering of transposition ciphers with computer support.* Bachelor Thesis at Faculty of Science University of Hradec Králové. Supervisor . 41 p.

Hájková, S. 2017. *Fundaments of cryptology as teaching topic in subject "Informatics" at lower secondary school.* Diploma Thesis at Faculty of Science University of Hradec Králové. Supervisor . 74 p.

Hanzalová, P., Hubálovský, Š., & Musílek, M. 2012. Automatic cryptanalysis of the short monoalphabetic substituted cipher text. In *Proceedings of the 5th WSEAS International Conference on Visualization, Imaging and Simulation*. Sliema, Malta: Wseas Press. p. 199-204. ISBN: 978-1-61804-119-7.

Hanzalová, P. 2014. *Using of spreadsheet in cryptanalysis of short cipher text.* Bachelor Thesis at Faculty of Science University of Hradec Králové. Supervisor . 48 p.

Hubálovský, Š., & Musílek, M. 2010. Automatic cryptanalysis of the monoalphabetic substitution

as a method of the system approach in the algorithm development thinking. *International journal of applied mathematics and informatics*. 4 (4), 92-102. ISSN 2074-1278.

Hubálovský, S., & Musílek, M. 2014. Algorithm for Automatic Deciphering of Mono-Alphabetic Substituted Cipher Realized in MS Excel Spreadsheet. *Applied Mechanics and Materials*. p. 624-627

Musílek, M., Hubálovský, Š., & Hubálovská, M. 2017. Mathematical Modeling and Computer Simulation of Codes with Variable Bit-Length. *International Journal of Applied Mathematics and Statistics.* 56 (1), 1-12. ISSN 0973-7545.

Musílek, M. 2012. Morse telegraph alphabet and cryptology as a method of system approach in computer science education. In *Proceedings of 9th International Scientific Conference on Distance Learning in Applied Informatics (DIVAI)*. Štúrovo, Slovakia: Wolters Kluwer. p. 223-231. ISBN 978-80-558-0092-9.

Musílek, P. 2017. *History of ciphering of transposition ciphers with computer support.* Bachelor Thesis at Faculty of Science University of Hradec Králové. Supervisor . 58 p.

Procházka, L. 2014. *Board games, puzzles, anagrams and ciphers as motivation in the teaching of algorithms and programming.* Diploma Thesis at Faculty of Science University of Hradec Králové. Supervisor . 75 p.

Procházka, L. 2012. *Deciphering of substitution ciphers with computer support.* Bachelor Thesis at Faculty of Science University of Hradec Králové. Supervisor M. Musílek. 37 p.

Singh, S. 2000. *The code book: the science of secrecy from Ancient Egypt to quantum cryptography.* New York: Anchor Books. 411 p. ISBN 0-385-49532-3.

Vlnas, V. 2017. *Computer Analysis of Encrypted Correspondence of House of Piccolomini.* Bachelor Thesis at Faculty of Science, University of Hradec Králové. Supervisor M. Musílek. 58 p.

Examining The Dorabella Cipher with Three Lesser-Known Cryptanalysis Methods

Klaus Schmeh
Freelanced Journalist
klaus@schmeh.org

Abstract

Most mono-alphabetic substitution ciphers (MASCs) can be solved with well-known techniques, like frequency analysis, or hill climbing. However, there are exceptions. It therefore makes sense to look around for additional MASC solving techniques—like the ones described in the book *Cryptanalysis* by Helen Fouché Gaines. These techniques—vowel detection, digram analysis, and consonant lining—have been almost forgotten since the advent of computer technology. In this paper, two of these methods (the third one is not suitable) will be applied on a famous unsolved cryptogram, the Dorabella Cryptogram, and on an unencrypted comparison text. Although this paper will not present a solution of the Dorabella Cryptogram, a number of interesting insights will be introduced. Especially, it will be shown that one of the methods applied works surpsingly well on the comparison text and that there are still ways to improve this technique. In addition, some interesting properties of the Dorabella Cryptogram will be presented, which might be helpful for further cryptanalysis.

1 Introduction

With the advent of computer technology and suitable software (especially, the open source tool CrypTool), breaking a mono-alphabetic substitution cipher (MASC) has become quite easy. Frequency analysis, which once was the most important way to break a MASC, is often not even necessary any more, as a word pattern search conducted by a software is usually more effective. In addition, hill climbing—another technique that requires computer support—has proven a powerful technique to break MASCs.

In spite of all this progress, breaking a MASC encryption still may be difficult, especially if some of the following pre-conditions are given:

- The ciphertext is especially short.
- The cleartext language is not known.
- The word boundaries are not indicated.
- The cleartext contains unusual expressions or abbreviations.
- The cryptogram is hard to read because of bad penmanship or bad reproduction.

I am aware of over 20 cryptograms that have the appearance of a MASC (of course, one does not know before the cipher is broken) and that are still unsolved, potentially for one or several of the named reasons. The following are the most important of these cryptograms:

- The Dorabella Cryptogram (Wikipedia, 2018)
- The MLH cryptogram (Schmeh1, 2017)
- The Voynich Manuscript (Wikipedia, 2018)
- The Rayburn cryptogram (Schneier, 2006)
- Cigaret Case Cryptogram (Schmeh2, 2017)

For these cryptograms, frequency analysis, word pattern analysis, word guessing, and hill climbing have failed so far. An interesting question is whether there are other MASC breaking methods that can be applied in such a case. In fact, there are. The book *Cryptanalysis* by Helen Fouché Gaines mentions three MASC breaking methods that are worth considering (Fouché Gaines, 1939): vowel detection, digram analysis, and consonant lining. All three methods are as good as not mentioned in the literature that has

Proceedings of the 1st Conference on Historical Cryptology, pages 145– 152,
Uppsala, Sweden, 18-20 June, 2018

been published since computer technology came up.

The goal of this paper is to apply the three methods mentioned by Fouché Gaines on the aforementioned Dorabella Cryptogram. The Dorabella Cryptogram was created by British composer Edward Elgar (1857-1934). In 1897, Elgar, who had a strong interest in cryptology, sent an encrypted message to a female friend named Dora Penny. This cryptogram is written in symbols consisting of one, two or three bows (see figure 1)—probably an alphabet of Elgar's own creation.

The Dorabella Cryptogram has never been solved, although many experts have tried. It is covered in virtually every famous unsolved cipher list, e.g., on Elonka Dunin's website (http://elonka.com/UnsolvedCodes.html), in Craig Bauer's book *Unsolved!* (Bauer, 2017), in Klaus Schmeh's *Nicht zu knacken* (Schmeh, 2012), and in Richard Belfield's *Can You Crack the Enigma Code?* (Belfield, 2006).

To check whether the three cryptanalysis methods work, I will apply them not only on the Dorabella Cryptogram but also on a non-encrypted comparison text. When looking for a suitable text, I came across the novel *The Gadfly* by Ethel Boole (Boole 1897), the wife of Wilfrid Voynich, who is known to crypto history scholars as the person the Voynich Manuscript is named for. *The Gadfly* was published in 1897, the same year as the Dorabella cryptogram was created. I chose the following 87 letter excerpt (same length as the Dorabella Cryptogram) from the *The Gadfly* as the comparison text (I will ignore the spaces because the Dorabella Cryptogram doesn't contain any):

```
THEYW ENTOU TINTO THEST ILLSH ADOWY
CLOIS TERGA RDENT HESEM INARY OCCUP
IEDTH EBUIL DINGS OFANO LDDOM IN
```

Here's a transcription of the Dorabella Cryptogram:

```
ABCDE FGDHA IJKLJ MJJFB BJNGO GNIP
GJGFQ DHRSC JJCFN KGJIJ FTPKL QHHQI P
CPFUP CLUUN PCJFU KPNDB NPFDL ED
```

2 Basic Examinations

As both Elgar and Penny spoke English, I will assume that the Dorabella Cryptogram is written in English. As proposed by Fouché Gaines in her book, I started my examinations with a frequency count. I examined the comparison text first:

A	B	C	D	E	F	G	H	I
4	1	3	6	9	1	2	5	8

J	K	L	M	N	O	P	Q	R
-	-	5	2	7	8	1	-	3

S	T	U	V	W	X	Y	Z
5	9	3	-	2	-	3	-

According to Fouché Gaines, the nine most frequent letters of the English languange (E, T, A, O, N, I, R, S, H) make up about 70 percent of an English text. In the comparison text the nine most frequent letters are E, T, D, O, N, I, L, S, and H. These are not exactly the letters we have expected. However, they appear 62 times (71.3%), which is a pretty good fit.

Here's the frequency analysis of the Dorabella Cryptogram:

A	B	C	D	E	F	G	H	I
2	4	6	6	2	8	6	4	4

J	K	L	M	N	O	P	Q	R
11	4	4	1	6	1	8	3	1

S	T	U
1	1	4

The seven most frequent letters (J, F, P, C, D, and N) together appear 45 times (51.7%). In addition, there are four letters with a frequency of 6 (6.9%) each. If we take two of the latter we get 57 appearances (65.5%) for the nine most frequent letters. This is reasonably close to the 70% postulated by Fouché Gaines. We can take this as an indication that the Dorabella Cryptogram is a MASC encryption of an English, not a hoax.

To follow Fouché Gaines' approach, we now need to identifiy three groups of letters: the frequent, the less frequent, and the rare ones. Fouché Gaines' book does not define exactly the borders between these groups. I will work with the following definitions:

- *High frequency group (6 or more appearances)*: In the comparison text the following letters belong to this group: D, E, I, N, O, T. In the Dorabella Cryptogram the high-frequency letters are F, J, P, C, D, G, and N.
- *Medium frequency group (3-5 appearances)*: The medium-frequent letters of the com-

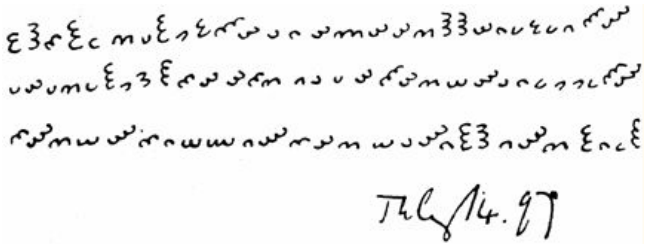


Figure 1: The Dorabella Cryptogram is an unsolved ciphertext that has the appearance of a monoalphabetic substitution cipher (MASC).

parison text are H, L, S, C, R, and Y. The medium-frequent letters of the Dorabella Cryptogram are B, H, I, K, L, U, and Q.

- *Low frequency group (1-2 appearances)*: Letters with a low frequency are B, F, G, M, P, and W (comparison text) and A, E, M, O, R, S, and T (Dorabella Cryptogram).

As the next step, we determine the contacts of each letter. A contact is defined as a letter that stands directly before or behind a certain character. As the Dorabella Cryptogram doesn't indicate spaces (and as we ignore the spaces in the comparison text), each of the 87 letters, except the first and the last one, has two contacts. The examples described by Fouché Gaines contain spaces, which means that her contact analysis is a little different from the one performed here.

Here's the contact analysis for the comparison text (below each letter the left and the right contacts are isted, one contact pair per line):

A	B	C	D	E	F	G	H
HD	EU	YL	AO	HY	OA	RA	TE
GR		OC	RE	WN		NS	TE
NR		CU	ET	HS			SA
FN			LI	TR			TE
			LD	DN			TE
			DO	HS			
				SM			
				ID			
				HB			

I	J	K	L	M	N	O	P
TN	-	-	IL	EI	ET	TU	UI
TL	-	-	LS	OI	IT	TT	
OS	-	-	CO		ET	DW	
HN	-	-	ID		IA	LO	
PE	-	-	OD		IG	YC	
UL	-	-			AO	SF	
DN	-	-			I-	NL	
MN	-	-				DM	

Q	R	S	T	U	V	W	X
-	EG	ET	-H	OT	-	YE	-
-	AD	LH	NO	CP	-	OY	-
-	AY	IT	UI	BI	-		-
-		EE	NO		-		-
-		NS	OH		-		-
-			SI		-		-
-			SE		-		-
-			NH		-		-
-			DH		-		-

Y
EW
WC
RO

Here's the contact analysis for the Dorabella Cryptogram:

A	B	C	D	E	F	G
-B	AC	BD	CE	DF	EG	FD
HI	FB	SJ	GH	LD	JB	NO
	BJ	JF	QH		GQ	ON
	DN	PP	NB		CN	PJ
		PL	FL		JT	JF
		PJ	E-		PU	KJ
					JU	
					PD	

H	I	J	K	L	M	N
DA	AJ	IK	JL	KJ	JJ	JG
DR	NP	LM	NG	NG		GI
QH	JJ	MJ	PL	PL		FK
HQ	QP	JF	UP	UP		UP
		BN				PD
		NC				
		KN				
		NF				

O	P	Q	R	S	T	U
GG	IG	FD	HS	RC	FB	FP
	TK	LH				LU
	IC	HI				UN
	CF					FK
	UC					
	NC					
	KN					
	NF					

3 Vowel Detection Method

The vowel detection method is the first one described by Fouché Gaines. It is based on eight criteria (Fouché Gaines calls them pointers) that can be used to identifiy vowels in a ciphertext. The idea of this method is to use the vowels identified for further investigations with other cryptanalysis methods (i.e., the vowel detection method alone will usually not break a cipher, but it can help to do so). Fouché Gaines' vowel detection method should not be confused with the Shukotin algorithm (Guy, 1991), which has the same purpose.

3.1 Pointer 1: High frequency of vowels A, E, I, and O

What Fouché Gaines writes: The vowels A, E, I, and O are normally found in the high-frequency section of a cryptogram.

Does this hold for the comparison text? It is true for the vowels E, I, and O. The letter A, however, has a lower frequency than expected.

What does this mean for the Dorabella Cryptogram? If Fouché Gaines is correct the ciphertext letters F, J, P, C, D, G, and N contain the cleartext vowels A, E, I, and O.

Vowel candidates in the comparison text: D, E, I, N, O, T

Vowel candidates in the Dorabella Cryptogram: F, J, P, C, D, G, N

3.2 Pointer 2: Letters contacting low-frequency letters

What Fouché Gaines writes: Letters contacting low-frequency letters are usually vowels.

Does this hold for the comparison text? Yes. The letters with frequency 1 are contacted by A, E, I, O, and U. The letters with frequency 2 are contacted by A, N, R, S, E, O, Y, and Y. This means that 10 of 13 letters contacting low-frequency letters are vowels. If we count only the contacts that appear more than once or that contact a letter that appears only once we get exactly A, E, I, O, U, and Y.

What does this mean for the Dorabella Cryptogram? The letters contacting low-frequency letters are B, B, D, D, F, H, I, J, J, L, G, G, H, S, R, C, and F. If we count only the contacts that appear more than once or that contact a letter that appears only once we get B, D, J, G, H, S, R, C, F, and B. As can be seen, the vowel detection doesn't work here as good as for the comparison text.

Vowel candidates in the comparison text: A, E, I , N, O R, S, and Y

Vowel candidates in the Dorabella Cryptogram: B, D, F, H, I, J, L, G, H, S, R, C, F

3.3 Pointer 3: Wide variety in contact letters

What Fouché Gaines writes: Letters showing wide variety in their contact letters are vowels.

Does this hold for the comparison text? Yes. Fouché Gaines does not define exactly what wide variety means. However, if we look at the three letters with the widest variety we see that these are the vowels E, I and O.

What does this mean for the Dorabella Cryptogram? The three letters with the widest variety are J, F, and P.

Vowel candidates in the comparison text: E, I, O.

Vowel candidates in the Dorabella Cryptogram: J, F, P.

3.4 Pointer 4: Repeated digrams

What Fouché Gaines writes: In repeated digrams (in immediate succession), one letter is usually a vowel.

Does this hold for the comparison text? There is no repeated digram in the comparison text.

What does this mean for the Dorabella Cryptogram? There is no repeated digram in the Dorabella Cryptogram.

Vowel candidates in the comparison text: -

Vowel candidates in the Dorabella Cryptogram: -

3.5 Pointer 5: Reveresed digrams

What Fouché Gaines writes: In reversed digrams, one letter is usually a vowel.

Does this hold for the comparison text? Yes. The reversed digrams of the comparison text are TO/OT, DE/ED, LO/OL, NA/AN, YW/WY, and SE/ES. Each of these six pairs consists of a vowel and a consonant.

What does this mean for the Dorabella Cryptogram? The reversed digrams are GJ/JG, JI/IJ, DE/ED, GF/FG, MJ/JM, GN/NG, FG/GF, JC/CJ, KP/PK, QH/HQ, PC/CP, and PN/NP. 9 of these 12 digrams contain one of the vowel candidates identified above (J, F, P). It is important to note that the Dorabella Cryptogram has double as many reversed digrams as the comparison text. It is beyond the scope of this paper to examine whether this high number of reversed diagrams is still consistent with an English text or whether it is evidence for the Dorabella Cryptogram being something else as English text.

Vowel candidates in the comparison text: -

Vowel candidates in the Dorabella Cryptogram: -

3.6 Pointer 6: Doubled consonants

What Fouché Gaines writes: Doubled consonants are usually flanked by vowels, and vice-versa.

Does this hold for the comparison text? The comparison text contains three doubled letters: LL, CC, and DD. Only CC appears inside a word (OCCUPY), while the other two stand at the end of a word (STILL) or are spread to two words (OLD DOMIN). While CC is flanked by two vowels, LL and DD aren't. It seems that this pointer is not applicable, if the word boundaries are not known.

What does this mean for the Dorabella Cryptogram: The digram JJ appears twice. HH and UU are two more doubled letters. No conclusions can be drawn from these facts at this stage.

Vowel candidates in the comparison text: -

Vowel candidates in the Dorabella Cryptogram: -

3.7 Pointer 7: Five consonants in succession

What Fouché Gaines writes: It is unusual to find more than five consonants in succession.

Does this hold for the comparison text? Yes.

What does this mean for the Dorabella Cryptogram? No conclusions can be drawn at this stage.

Vowel candidates in the comparison text: -

Vowel candidates in the Dorabella Cryptogram: -

3.8 Pointer 8: Vowels contacting each other

What Fouché Gaines writes: Vowels do not often contact one another.

Does this hold for the comparison text? Yes.

What does this mean for the Dorabella Cryptogram: There are five contacts between two of the supposed vowels J, F, and P. Further work might examine whether this information is of any use for breaking the Dorabella Cryptogram.

Vowel candidates in the comparison text: -

Vowel candidates in the Dorabella Cryptogram: -

3.9 Result of vowel detection

Only three of the eight criteria can be used to search for vowel candidates in the two texts examined in this paper. In the comparison text there are three letters that fulfill all three criteria: E, I, and O. This means that this method works to a certain degree for the comparison text, although the vowels A, U, and Y remained undetected.

Only two letters of the Dorabella Cryptogram, J and F, fulfill all three criteria. The letter P fulfills two of them. Although this is an interesting result, it is not enough to solve the Dorabella Cryptogram.

4 Digram Method

The digram solution method is the second one proposed by Fouché Gaines. However, Fouché Gaines writes that 80 letters are not enough for this technique. For this reason she demonstrates it on a 235 letter message. The 87 letters in the Dorabella Cryptogram and the comparison text are clearly not enough for this method to work. I therefore skip it in this paper.

5 Consonant Line Method

The third method Fouché Gaines introduces is the consonant line method. To apply this technique we need to assemble a table that lists the letters of the text along with their frequencies and number of different letters contacting them. Here's the table for the comparison text:

O	E	I	T	D	N	S	A	U	C
8	9	8	9	6	7	5	4	3	3
12	11	11	8	8	6	6	6	6	5

R	Y	G	H	M	W	B	F	P
3	3	2	5	2	2	1	1	1
5	5	4	4	3	3	2	2	2

According to Fouché Gaines, the lowest 20 percent of the total number of contacts are consonants. The letters G, M, W, B, F, P, and H together have 20 appearances. As we have a total of 106 contacts, we can determine these (correctly) as consonants. Here's the same table for the Dorabella Cryptogram:

J	P	B	C	D	F	G	H	I	K	U
11	8	4	6	6	8	6	4	4	4	4
10	8	7	7	9	11	7	5	5	6	6

L	N	Q	E	A	R	S	T	M	O
4	6	3	2	2	1	1	1	1	1
7	9	5	4	3	2	2	2	1	1

Here we have 117 accumulated contacts. 20 percent of 117 are 23. The letters M, O, R, S, T, A, and E together have 15 appearances, so they should be consonants. The next candidates are H, I and Q (five appearances each). If we include all of them we are above 20 percent. It seems best to omit all three.

It is important to note that Fouché Gaines' statements about contacts at this place refer to a text of roughly 100 letters. They make no sense for a much longer or shorter text. It is therefore an interesting question how the frequency of consonants can be measured in a way that is independent from the message length. This question, which is out of scope in this paper, is addressed in (Schmeh3, 2017).

In the next step, I write all the consonants I have identified in a line (see figure 2, ignore the underlined letters for now). Below, I write the left contacts of each letter left of the line, and the right contacts right of the line (see figure 2, again ignore the underlined letters).

Now, according to Fouché Gaines, all letters that don't show up as contacts left or right of the line can be identified as consonants, as well. These are C, D, L, and T (comparison text) and C, K, N, P, Q, and U (Dorabella Cryptogram). Note that this method has now correctly identified 11 consonants in the comparison text. The newly detected values are included in the upper line of consonant line diagram (underlined), and the contacts of these letters are added left and right of the vertical line (underlined).

According to Fouché Gaines, the N can now be identified, as it is a frequent letter that stands almost always left of the consonant line. The H can be identified, as it almost always stands right of it. Both identifications works pretty well for the comparison text, though the N could be confused with the T.

Following Fouché Gaines' instructions, we can now also indentify a few vowels. The vowels A, E, I, and O (i.e., the frequent ones) are expected

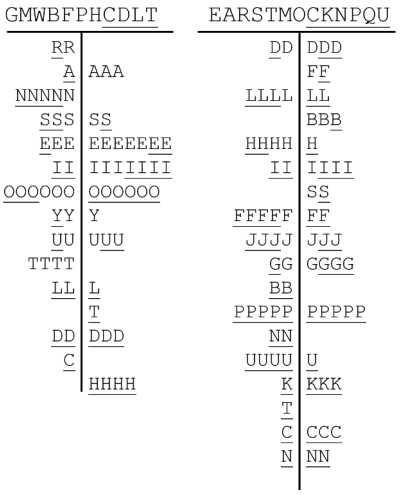


Figure 2: Consonant lines for the comparison text (left) and the Dorabella Cipher (right).

to appear in a high frequency and on both sides of the line. Looking at the comparison text, this is absolutely correct for the O and partially holds for E, I, and U, while the A behaves a little different than expected. This attempted vowel identification is far from perfect, but it would certainly provide helpful evidence when combined with other cryptanalysis methods.

The information we have gathered by now would be sufficient to break the comparison text, if it were a cryptogram. It is very likely that the consonant that precedes the H four times is T (TH is the most frequent consonant pair in the English language). In addition, it is clear that the vowel that follows TH four times in the text is E (THE is the most frequent trigram in English texts). Knowing the four letters T, H, E, and N, the rest would be routine cryptanalysis work.

In the case of the Dorabella Cryptogram, things are less clear. There are several candidates for the N (L, H, and U) and several for the H (D, I, and K). The most promising vowel candidates are J, F, and P (the same candidates as determined using the vowel detection method). Note that the letter P was identified as a consonant in the second step of the consonant line method (because it doesn't touch any of the vowels determined in the first step), though its appearance on the consonant line (five left and five right contacts) makes it look like a vowel. Figure 3 shows the Dorabella Cryptogram with marked vowels and consonants (this is the next step recommended by Fouché Gaines).

In my view, there is no obvious way to proceed from here. So, I will leave further steps (for instance, checking if one of the different candidates for N and H makes sense) to future research.

All in all, it can be said that the consonant line method, which works surpisingly well on an ordinary English text of the same length and written in the same year, doesn't render a clear result for the Dorabella Cryptogram.

6 Conclusion

To my regret, none of the three methods described in this paper has led to a solution of the Dorabella Cryptogram. Nevertheless, there are a number of interesting conclusions that can be drawn from the examinations described in the previous paragraphs. Here are some general ones:

- The consonant line method has worked surprisingly well on the comparison text. It not only correctly identified G, M, W, B, F, P, H, C, D, L, and T as vowels but also found the letters N and H. This information would be enough to break a MASC-encrypted text. The consonant line method therefore appears to be an interesting alternative, whenever other methods (including frequency analysis and word pattern guessing) don't work.

- Digram analysis doesn't work on a cryptogram consisting of 87 letters. As virtually all unsolved MASC encryptions known to me are of about this size or smaller, this method will not be of much value.

- Vowel detection has worked on the comparison text. It correctly identified E, I, and O as vowels. While this is, of course, not enough to break a cipher, it might be an interesting aid.

- Generally, the concept of letter contacts seems to be an interesting tool in cryptanalysis, which has been underestimated so far. As far as I know, this concept is not mentioned at all in the crypto history literature of the last decades.

The following conclusions can be drawn about the Dorabella Cryptogram:

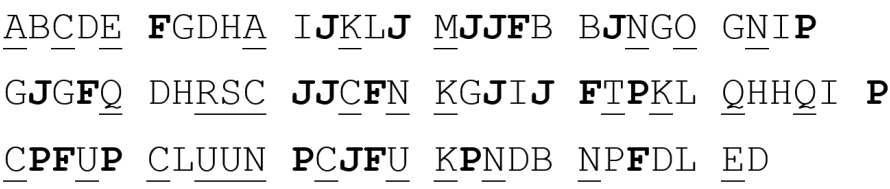


Figure 3: The Dorabella Cipher transcription with marked vowels (bold) and consonants (underlined). Further research may show whether there are conclusions that can be drawn from this.

- The frequency count and the contact counts of the Dorabella Cryptogram are consistent with the English language.
- The following letters in the transcribed Dorabella Cryptogram could be vowels: F, J, and P.
- The number of reversed digrams in the comparison text is double as high as in the Dorabella Cryptogram.
- Candidates for the letters H and N have been found in the Dorabella Cryptogram.
- The vowel detection method and the consonant line method work less good on the Dorabella Cryptogram than on the comparison text.

Here are some some ideas for future work:

- Some of the instructions given by Fouché Gaines are a little fuzzy. Especially, the definition of letter frequency classes and the quantification of contact variety is not very precise. This leaves room for further research.
- Fouché Gaines' methods assume that the ciphertext examined contains spaces. As this is not the case in many cases, the methods should be adapted to cryptograms without known word boundaries.
- The concept of letter contacts should be made more popular in cryptananalysis.
- The consonant line method should be applied on other cryptograms, as well.
- Further tests whether the Dorabella Cryptogram is a real text should be made.
- The consonant line method should be adapted to other languages.
- The concept of reversed digrams might be helpful for cryptanalysis. It should be explored.

I am optimistic that some of the unsolved cryptograms mentioned in the introduction can be solved with the methods covered here. I hope that additional research in this direction will be conducted.

References

Bauer, Craig. 2017. *Unsolved!*. Princeton University Press, Princeton, NJ.

Belfield, Richard. 2006. *Can You Crack The Enigma Code*. Orion Publishing, London, UK.

Fouché Gaines, Helen. 1939. *Cryptanalysis*. Dover Publications, New York, USA.

Guy, Jacques B. M. 1991. *Vowel Identification: An Old (but Good) Algorithm*. Cryptologia (4), 258-262 (1991)

Schmeh, Klaus. 2012. *Nicht zu Knacken*. Hanser, Munich, Germany.

Schmeh, Klaus 2017. *The Top 50 unsolved encrypted messages: 31. The MLH cryptogram* Klausis Krypto Kolumne, 2017-05-23

Schmeh, Klaus 2017. *Who can decipher this encrypted inscription on a cigaret case?* Klausis Krypto Kolumne, 2017-11-26

Schmeh, Klaus 2017. *Mathematical formula needed* Klausis Krypto Kolumne, 2017-12-22

Schneier, Bruce 2006. *Handwritten Real-World Cryptogram* Schneier on Security, 2006-01-30

Wikipedia. *Dorabella Cipher*. Retreived 2018-01-08.

Wikipedia. *Voynich manuscript*. Retreived 2018-01-08.

Design and Strength of a Feasible Electronic Ciphermachine from the 1970s

Jaap van Tuyll
Retired cryptanalyst
The Netherlands
jaapvantuyll@gmail.com

Abstract

This paper explores the design and strength of a feasible electronic ciphermachine that might have been invented in the 1970's. The design uses linear feedback shift registers, to get a key generator that satisfies some necessary requirements for a secure cryptographic algorithm. The analysis of the strength however, shows that the algorithm can be attacked successfully.

1 Introduction

Around 1970 a number of new off-line commercial cryptographic machines for the encryption of messages in telexcode, appeared on the market. Some examples are the H460 produced by Crypto AG, the TC803 produced by Gretag, the DC105 and DC26 produced by Datotek, the T1000CA produced by Siemens and the TST9669 produced by Telesecurity Timmann. These machines have in common, that they make use of electronic components, such as logical gates and shift registers. Thereby they mark a new generation of cryptographic machines, when compared with the older electromechanical machines such as the CX52. Not much is known in the open literature about the design of these machines. Therefore it might be interesting to explore and evaluate one of the possible ideas to design such a cryptographic machine, using electronic components.

2 General design criteria

Around 1970 there were several properties of a key generator known, to which a designer should pay attention. All of these have to be addressed by the designer of a cryptographic machine to make sure that the design will not a priori be a weak one.

One aspect is the need of a large key space for the initialisation keys. If the number of different initialisation keys is relatively small, it is possible for a cryptanalyst to test all the different keys (an exhaustive search) in a relatively short time.

A key generator without input is by its nature periodic. If it contains n memory elements of one bit, then the number of different states of the key generator is at most 2^n. Therefore the period can also not be larger than this number. The key generator should be designed in such a way, that the periods that are attained, are in the order of magnitude of this number. A very short period produces the possibility of reading in depth of a message shifted against itself. A somewhat longer period gives a cryptanalyst the possibility of testing all the positions of the period.

Different messages should use different parts of the period of the key generator to prevent reading in depth of the messages. This could be achieved by changing the complete initialisation key for the machine, but for many reasons this is not a practical solution. Mostly this is achieved, by changing a small part of the initialisation key (the message key) from message to message.

Then the key numbers that are used should have a flat distribution. If this distribution is skewed, it might be possible for a cryptanalyst to guess (part of) the plaintext.

Lastly there is the special off-line problem:

For an off-line machine using the telex alphabet the following problem has to be solved. If the keystream is randomly generated, it contains all 32 five bit combinations, so the result of the encryption of a plain character can be any of the 32 combinations. However, only the 26 printable combinations are acceptable as a cipher character. This problem can be solved in several ways. One of them is the following one: Generate key numbers between 0 and 31, use as encryption a modulo 32 addition of plain and key numbers, and in case

Proceedings of the 1st Conference on Historical Cryptology, pages 153– 158,
Uppsala, Sweden, 18-20 June, 2018

the result is a non-letter, repeat the encryption with the same key, until an acceptable result has been achieved.

2.1 Properties of shift registers

A linear feedback shift register (LFSR) is an important building block for electronic cryptographic machines. The reason is that an LFSR can produce a pseudo-random sequence of bits. This is a sequence with properties, resembling those of a real random sequence. Such a sequence is also called a maximum-length sequence, because the length of the period is maximal for a linear shift register (i.e. $2^n - 1$ for a shift register of length n). If this number is a prime, then each irreducible polynomial of degree n is associated with a shift register producing a maximum-length sequence. Moreover it is the polynomial with the lowest degree associated to that shift register, the so-called minimal polynomial.

The length of the period is a property that makes maximum-length sequences important for cryptographic purposes. Another property which is important is that the distribution of bit-combinations upto length n is flat.

For practical purposes it is convenient to use feedbacks that only have two connections. The polynomial then becomes a trinomial. In that case one XOR gate is sufficient to determine the feedback.

An important property of a binary LFSR is the following: Every bit in the output sequence of a binary LFSR is a linear combination of the bits of the initial content. A consequence is that as soon as n independent bits of the output sequence are known, it is possible to solve the initial content of a shift register of length n by solving a set of n linear equations.

More information on shift registers can be found in (Golomb, 1967).

3 Design

The goal is an off-line cryptographic machine that encrypts plaintexts, containing letters and the space character. The ciphertext should consist of letters only, so that a ciphertext could be printed before transmisson.

3.1 The plaintext alphabet

Because the space character is wanted in the plain alphabet, one letter (called the word separator) must be left out of the plaintext alphabet. (If not, the plain alphabet would have more elements than the cipher alphabet which is unacceptable, because that prevents unique decipherment). The space will then be replaced by the word separator during the encipherment. The consequence is, that the word separator itself cannot be used in the text of a plain message. If the resulting letter after decryption is the word separator, a space will be printed. That implies that it becomes invisible which is undesirable. A reasonable choice for a word separator could be the X and if the X itself is needed in a plaintext, then a trick must be used, e.g. representing an X by KS.

3.2 The key generator

To encrypt five-bit telex characters it is necessary to produce five-bit key characters. Therefore it seems plausible to use five binary LFSRs. Each register can then produce one of the required keybits. For convenience they can all have the same length n and the same feedback trinomial polynomial

$$X^n + X^f + 1$$

This must be an irreducible polynomial producing a maximum-length sequence of period $2^n - 1$. The required keybits can then be read off from the sections k of the registers. Because the shift registers all produce pseudo-random sequences, the produced key characters also are pseudo-random. See figure 1 for a picture.

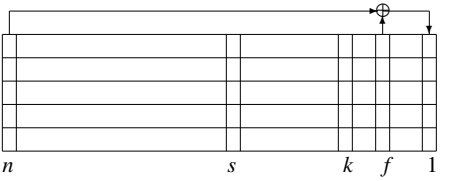


Figure 1: Shift registers

3.3 Initialising the machine

The registers could be initialised by $n-1$ key characters. One of the sections of each register (e.g. the first) should be set to 1 to ensure that no register starts in the all-zero state. The five bits of a key letter could then be read into the registers 1 through 5. As the initialisation of the machine needs to be different for every message, two keys should be used: a long-term key of $n-m-1$ letters

and a message key, unique for one message, of m letters. In practice it might be necessary to send the message key in the clear with the message, so the message key should not be used unmodified. This could be achieved by using (part of) the long-term key to change the bits of the message key, before they are entered into the machine.

The key space of this machine has the size $2^{5(n-1)}$.

3.4 Character encipherment

To encipher a plain letter, a key number K could be determined by reading off the contents of sections k of all the registers.

$$K = \sum_{i=1}^{5} R_{i,k} * 2^{i-1}$$

(where $R_{i,j}$ is the content of section j of register i).

The plain letter could be converted to a number P using its ITA2 bit value. For the word separator representing the space, the value $P = 4$ could be used.

The formula for the encipherment could be:

$$C = P - K \ mod \ 32$$

where the number C is converted through the ITA2 table into a cipher letter. If C is equal to $0, 2, 8, 27, 31$ or the number corresponding to the letter used as the word separator, it cannot be used in a ciphertext, because the corresponding character cannot be printed. (Such a character is considered illegal for this machine). In such a case the encipherment could be repeated with the same keynumber, until an acceptable result has been reached. It is easy to verify that this procedure always stops.

3.5 Character decipherment

Character decipherment is the inverse operation of the character encipherment. To decipher a cipher letter, a key number K is determined as described above, by reading off the contents of sections k of all the registers.

$$K = \sum_{i=1}^{5} R_{i,k} * 2^{i-1}$$

The cipher letter is converted to a number C using its ITA2 bit value.

The formula for the decipherment is:

$$P = C + K \ mod \ 32$$

where the number P is converted through the ITA2 table into a plain letter. If P is equal to $0, 2, 8, 27, 31$ or the number corresponding to the letter used as the word separator, it cannot be used in a plaintext, because the corresponding character cannot be printed. In such a case the decipherment is repeated with the same keynumber, until an acceptable result has been reached. If the plain number equals 4, the plain character is a space.

3.6 Stepping of the registers

After the encryption of a letter has ended successfully, the registers should step a number of times. To ensure a high period for the keystream generated by the machine, at most one register can have a constant step, so e.g. register 1 steps a constant number of steps. Then the higher numbered registers should make a variable number of steps, e.g. the number of steps could be determined by the XOR of the content of the sections s of the lower numbered registers.

$$S_i = \sum_{j=1}^{i-1} R_{j,s} \ mod \ 2$$

where S_i determines the number of steps of register i for $i > 1$.

In this way it is guaranteed, that whenever one register completes its period, all the other registers do not. This ensures that the period of the keystream of the machine is in the order of magnitude of $(2^n)^5$.

3.7 Summary of the design

The design of the machine meets the necessary criteria for a secure algorithm that were mentioned earlier:

The keyspace has a large size.

The keystream has a large period.

The keycharacters generated have a flat distribution.

Different messages use different parts of the keystream.

4 Strength

When attacking the feasible cryptographic machine described above, it is reasonable to assume that the details of the design are known to an attacker. This approach is fully in line with the second Kerckhoffs' principle that was stated by Auguste Kerckhoffs in 1883 in (Kerckhoffs, 1883).

It is clear that the variable stepping of the higher numbered registers implies that the start of an attempt to break this feasible machine, can only be an attack on the first register, the only one that has a constant step. After solving the first register the stepping pattern of the second one is known and

then the second register could be attacked and so on.

4.1 Fast correlation attack

The fast correlation attack is a procedure to determine the initial content of a shift register if only a part of the output sequence containing some errors is known.

This attack has been presented for the first time at Eurocrypt 1988 in Davos by Willi Meier and Othmar Staffelbach and has been published in (Meier and Staffelbach, 1989), although the attack was already known many years before.

The method works as follows:

The enciphering method modifies the bits of the register that will be attacked. This modification is not random, but biased to either 0 or 1. The part of the shift register sequence for which this biased information is available is initialised with values coming from the bias.

The feedback polynomial gives a relation that is satisfied by all the bits in the output sequence of the shift register. Moreover all the multiples and in particular all the 2^n powers of this polynomial (which are all also trinomials) give relations that are satisfied.

As an example if $X^n + X^f + 1$ is the feedback polynomial, then if b_i is the i-th bit of the output sequence, $b_{i+n} + b_{i+n-f} + b_i = 0 \ mod\ 2$ is satisfied for all $i > 0$. But also $b_{i+2n} + b_{i+2(n-f)} + b_i = 0 \ mod\ 2$ and so on. Moreover one can add $b_{i+n+f} + b_{i+n} + b_{i+f} = 0 \ mod\ 2$ to $b_{i+n} + b_{i+n-f} + b_i = 0 \ mod\ 2$ and in this way get the new relation $b_{i+n+f} + b_{i+n-f} + b_{i+f} + b_i = 0 \ mod\ 2$. In this way many trinomial and tetranomial relations can be found which are satisfied by the bits of the produced output sequence.

Step 1 is: Count for every position the number of relations involving that position that are satisfied and the number of relations that are not satisfied. If the number of satisfied relations is much higher, then the bit at that position is probably reliable and nothing is changed. In the other case the bit is probably unreliable and it is declared unknown.

Step 2 is: Compute for all the unknown bits a new value on the basis of the reliable bits only. For many unreliable bits this will succeed and then a new sequence has been determined.

The counting and correcting steps are repeated until enough highly reliable bits have been found. Then the initial content is solved by solving the set of equations, generated by those reliable bits. Under certain conditions on the values of the bias and the length of the used part of the shift register sequence this method converges.

4.2 Correlation attack on register 1

For every letter of the ciphertext the 32 possible decryptions can be divided into two groups, one corresponding with an even key number and the other one corresponding with an odd key number. Depending on the letter frequencies in the language of the plaintext, the two groups have a different probability of occurrence. The consequence is that the probability of the last bit of the key number being 0, is different from the probability of the last bit of the key number being 1. In other words for every cipher letter there is a bias to either 0 or 1 for the last bit (K_1) of the key number K.

Compare

$$P(K_1 = 0 \mid cipherletter = C)$$
with
$$P(K_1 = 1 \mid cipherletter = C)$$

An example: For cipher letter H the set of decryptions with an even keynumber is:

{B,G,H,L,M,O,P,Q,T,V,W,Y,Z}

The letters L, W and Z occur twice as a decryption with different keynumbers.

For odd keynumbers the set is:

{A,C,D,E,F,G,I,J,K,N,R,S,U,X}

Here F and U occur twice as a decryption with different keynumbers.

In most languages the second set is much more frequent than the first one, especially because the X in the second set is the word separator and thus represents the space character. So for cipher letter H the bias is for a 1 as the last keybit.

This bias makes it possible to determine the initial shift register sequence. First the bias is used to make an approximation of the shift register sequence produced by the first register of the machine.

If the language statistics are favourable enough and the message length is sufficiently large, the fast correlation attack reconstructs the initial content of the first register of the machine.

4.3 Correlation attack on register 2

A similar approach can be used for the higher numbered registers. Once register one is known

the stepping of register two is also known. Moreover for every cipher letter one keybit is known. In this case the decryptions of a given cipher letter are divided into four groups. In each group the key numbers have a fixed value modulo 4.

An example: For cipher letter H the four groups are:

key = 0 mod 4 {H,L,P,Q,T,W,Y,Z}
key = 2 mod 4 {B,G,L,M,O,V,W,Z}
key = 1 mod 4 {C,D,F,J,K,N,R,U}
key = 3 mod 4 {A,E,F,G,I,S,U,X}

Then depending on the value of the keybit produced by register one, either the groups with key numbers equal to 0 and 2 modulo 4 are compared or the groups with key numbers equal to 1 and 3 modulo 4 are compared.

Compare

$$P(K_2 = 0 \mid cipherletter = C \wedge K_1 = b)$$
with
$$P(K_2 = 1 \mid cipherletter = C \wedge K_1 = b)$$

where b is the known keybit from the first register.

For every ciphertext letter the bias between the groups that are compared is used to initialise an approximation for the second register. Once again if the conditions are favourable the fast correlation attack finds the initial content of register two.

4.4 Registers 3, 4 and 5

In principle the same method can be used for the registers 3, 4 and 5. However, in many languages the statistics are unfavourable for a successful attack on register 3.

One way to improve the statistics is by using bigrams of the ciphertext instead of single ciphertext letters. That improves the bias because in that case the frequencies of plain letter bigrams are used to calculate the bias.

Compare

$$P(K_3 = 0 \mid cipherpair = CC' \wedge K_1 = b_1 \wedge K_2 = b_2 \wedge K_1' = b_1' \wedge K_2' = b_2')$$
with
$$P(K_3 = 1 \mid cipherpair = CC' \wedge K_1 = b_1 \wedge K_2 = b_2 \wedge K_1' = b_1' \wedge K_2' = b_2')$$

where b and b' are the keys for the consecutive cipherletters C and C'.

4.5 Probable word method

There is however another method: the probable word method. If for every cipher letter the key bits of the registers 1 and 2 are known only 8 possible decryptions remain possible.

If the cipher letter is H and the keybits from the first and second register both are 1 then the plainletter must be one of the set {A,E,F,G,I,S,U,X}.

Now it is possible to test for every position in the ciphertext, whether a word that probably will be present in the plaintext, fits the ciphertext.

So you might get the following situation: (CT is the ciphertext letter and k_1 and k_2 are the known keybits from the registers 1 and 2).

CT	D	P	I	F	E	R	U	O	B	K
k_1	0	0	1	1	0	1	0	1	0	0
k_2	1	1	1	0	0	0	0	1	0	0
	S	V	V	**A**	E	G	U	N	B	K
	A	B	**B**	H	**S**	V	X	R	**O**	N
	U	T	P	Z	A	B	X	C	**O**	N
	C	L	R	O	U	X	S	**D**	G	**R**
	X	Z	D	M	E	I	I	F	**O**	C
	K	O	O	G	X	**S**	E	J	M	D
	I	**M**	M	V	A	O	S	K	G	F
	E	G	G	B	I	M	**A**	T	V	J

The boldface letters show that here the word **AMBASSADOR** is possible.

If the word has a sufficient length only correct positions are found. (Almost) every plaintext letter that is found in this way fixes a keybit in the registers 3, 4 and 5. In the example above that is the case for all ciphertext letters, except the ciphertext letter B, for which there are three possible decryptions as O.

As soon as enough independent keybits have been found, the initial content of the registers 3, 4 and 5 can be found by solving a set of linear equations for each register.

5 Conclusion

The cryptographic algorithm that has been described could very well have been invented in the 1970's, when new ideas in cryptography were generated by the new electronic components that became available. The paper shows that although the algorithm meets a number of design criteria, it still could have been broken using an idea that was published in 1989.

References

Solomon W. Golomb. 1967. *Shift Register Sequences*. Holden–Day.

Auguste Kerckhoffs. 1883. La cryptografie militaire. *Journal des Sciences Militaires*, IX:5–38, jan.

Willi Meier and Othmar Staffelbach. 1989. Fast Correlation Attacks on certain Stream Ciphers. *Journal of Cryptology*, 1(3):159–176.

Author Index

Published by

NEALT Proceedings Series 34
Linköping University Electronic Press, Sweden
Linköping Electronic Conference Proceedings No. 149
ISSN: 1650-3686
eISSN: 1650-3740
ISBN: 978-91-7685-252-1
URL: http://www.ep.liu.se/ecp/contents.asp?issue=149