New Ciphers and Cryptanalysis Components in CrypTool 2

Nils Kopal
University of Siegen, Germany
nils.kopal@uni-siegen.de

Bernhard Esslinger
University of Siegen, Germany
bernhard.esslinger@uni-siegen.de

Abstract

In this paper, we discuss new additions (components) for cryptography and cryptanalysis added to the CrypTool 2 (CT2) software over the course of the last two years. We mainly focus on components for classical and historical ciphers, but also keep an eye on other updates of CT2, e.g. the CrypConsole, which allows the users to execute CT2 workspaces in the Windows command prompt. The Chaocipher as well as Josse's cipher were added to CT2. The Symbol Cipher component already allows the user to create musical ciphers. We implemented a new Playfair Analyzer as well as a Josse Cipher Analyzer. The Enigma Analyzer component has been rewritten completely and now features six different computerized attacks on Enigma. Two historical ciphers were successfully deciphered with the help of CT2: five ciphertexts from and to the Holy Roman Emperor Maximilian II as well as the Ramanacoil transcript. Both ciphers from the 16th and 17th century were analyzed and deciphered using the Homophonic Substitution Analyzer component as well as the substitution component. Finally, we take a brief look at how CT2 is used for teaching and e-learning cryptology.

1 Introduction

CrypTool 2 (CT2) is an open-source software for cryptography and cryptanalysis developed in a sub project of the overall CrypTool project. (Kopal et al., 2014). Although initially developed with the intention of creating an e-learning software to support the teaching and learning of cryptology, CT2 increasingly became a software for supporting the cryptanalysis of ciphers in real historical manuscripts. Examples for successfully analyzed and broken historical ciphertexts are encrypted letters of the Holy Roman Emperor Maximilian II, which we were able to decipher using the Homophonic Substitution Analyzer of CT2. Parallel to the Maximilian letters, together with Dinnissen, we were able to easily decipher the Ramanacoil transcript using CT2's Substitution component. Therefore, since 2020, CT2 is also officially used within the DECRYPT project (Megyesi et al., 2020) to publish cryptanalytic prototypes each developed by different members of the project.

All implemented cryptography and cryptanalysis components of CT2 are available in regularly built "nightly builds" as well as in stable release versions, which we aim to publish twice a year. In 2021, we therefore released two stable versions, one in April and one in December.

In this paper, we give a brief and general overview of the most important new components integrated in CT2 over the course of the last two years. Two previously published HistoCrypt articles ((Kopal, 2019) and (Kopal, 2018)) already deal with specific c omponents, e .g. t he Homophonic Substitution Analyzer, and how to use CT2 to cryptanalyze historic ciphers.

The rest of the paper is structured as follows: Section 2 introduces new and updated components which are used to decrypt and cryptanalyze classical and historical ciphertexts. Then, Section 3 shows two examples of successful cryptanalyses performed with CT2. After that, Section 4 shows how CT2 is used for teaching and e-learning cryptology. Finally, Section 5 concludes the paper and gives a brief overview of what will be implemented in CT2 in the future.

2 New and Updated Components

CT2 implements a powerful graphical programming language that allows the connection of different **components** with each other on a virtual

workspace via drag&drop. Components implement ciphers, cryptanalytic algorithms, and also possibilities to enter and view texts, numbers, and other types of data. In order to combine components, each component has **input connectors** and **output connectors** which can be connected using **connection** lines. Furthermore, components offer different **parameters** (settings) which can be changed by the user. In cryptanalysis components, such a parameter is the type of cryptanalysis algorithm, e.g. hillclimbing or brute-force. Finally, many components offer **presentations**, which show the internal operations of the implemented algorithms or allow the user to manually engage in the performed cryptanalysis. For example, with the Homophonic Substitution Analyzer component the user is able to (re-)assign the mappings from homophones to plaintext letters.

In order to ease the usage, CT2 contains over 250 different templates which are pre-constructed, ready-to-run scenarios.

2.1 Cryptography

This section presents three different newly implemented classic ciphers. The Chaocipher and Josse Cipher components have been already available in the last release version released in December 2021. The Symbol Cipher component is currently being developed.

2.1.1 Chaocipher

The Chaocipher (Rubin, 2011) is a manual encryption method designed by John F. Byrne in 1918. Byrne believed that his cipher was unbreakable and unsuccessfully tried to sell it to U.S. government agencies. He created different challenges and provided these to the officials to prove that his cipher is unbreakable. He also published the challenges in his autobiography "Silent Years". In contrast to common practice, he kept the cipher's specification secret. Byrne was never able to sell his cipher. In 2010, the specifications were made public after his family donated all of his material to the National Cryptologic Museum in Fort Meade. Subsequently, all challenges could be solved, many of them by (Lasry et al., 2016), and the cipher itself proved to be much weaker than Byrne always believed. In a 2021 bachelor's thesis, Chaocipher was implemented in a new component in CT2. It allows the encryption and decryption of texts using Byrne's specification of his cipher. The component includes a presentation, which shows the internal states during en- and decryption. To further ease the understanding of the cipher, it also contains a log of each single step performed during the execution. Figure 1 shows a workspace containing the newly implemented Chaocipher component in CT2.

2.1.2 Josse Cipher

The Josse's code or Josse's cipher is a polyalphabetic substitution cipher developed by the French Major Josse Hippolyte Désiré around 1889. (Géraud-Stewart and Naccache, 2020). The cipher is based on a keyed substitution alphabet. Each letter is connected to the previous letters using modular arithmetic. Consequently, the cipher can be regarded as some type of autokey cipher. Lasry published an attack in (Lasry, 2021) that can recover the key and the plaintext from ciphertexts with only 75 letters. In a 2021 bachelor's thesis, a Josse cipher component as well as a Josse cipher analyzer component have been implemented. Figure 2 shows a workspace containing the newly implemented Josse cipher component. The component's presentation shows the alphabet in a table. The internal computations of the cipher are displayed in a text output component to the user. This eases the understanding of the cipher.

2.1.3 Symbol Cipher

Until now, CT2 mainly worked on text data (with classical ciphers) or binary data (with modern ciphers). Many historical ciphers nevertheless do not encrypt into standard Latin letters but into different kinds of character or symbol systems. Therefore, in December 2021 we started working on a component which we call the "Symbol cipher" component. The Symbol cipher component allows the encryption of plaintext into e.g. musical notes. We also plan to implement other types of symbols, like astrological symbols, etc. So far, we implemented two types of musical cipher notations: The first notation is based on a scheme developed by Daniel Schwenter, a German orientalist, mathematician, and cryptologist from the 17th century. The second notation is based on the scheme invented by John Wilkins, an Anglican clergyman, natural philosopher, and an author also from the 17th century. Figure 3 shows a CT2 workspace encrypting text to notes using the Symbol cipher component. The output format is set to the Daniel Schwenter scheme. All created ciphertexts are images and can easily be exported and

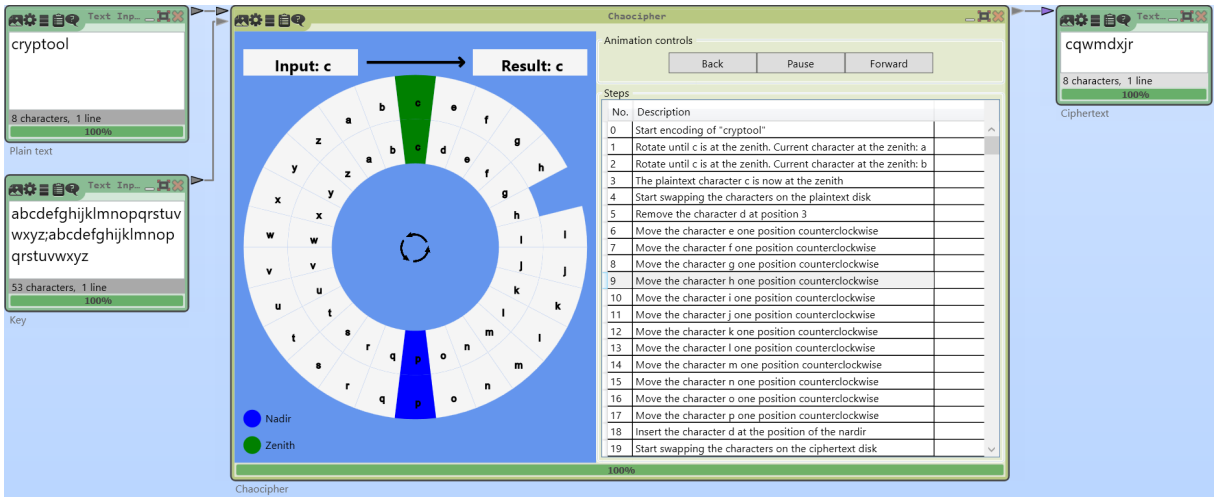

Figure 1: A CrypTool 2 workspace showing the newly implemented Chaocipher component. The cipher consists of two alphabet discs which are rotated. The letters of each disc are exchanged during en- and decryption.

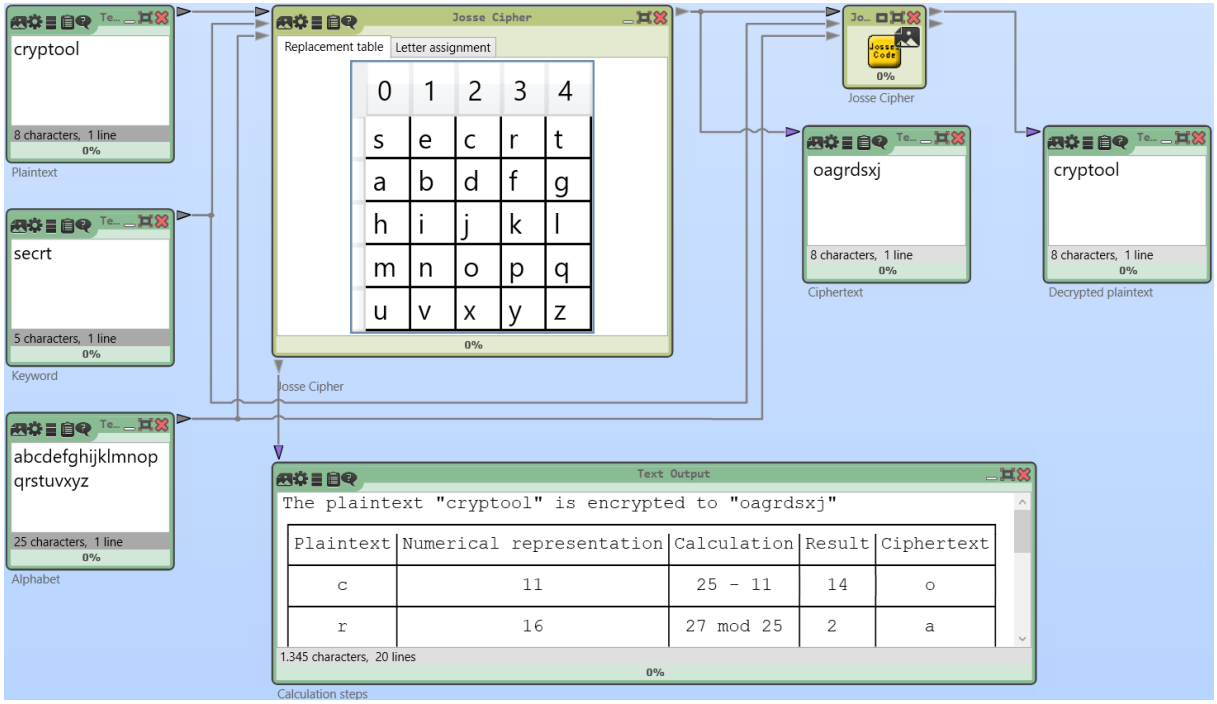

Figure 2: A CrypTool 2 workspace with the newly implemented Josse cipher component. The component's presentation view shows the keyed alphabet, and the component produces an output log with all computations performed during en- and decryption.

stored outside of CT2.

2.2 Cryptanalysis

This section presents two cryptanalysis components (Playfair Analyzer and Josse Cipher Analyzer) implemented over the course of the last two years. Additionally, the Enigma Analyzer was completely reimplemented.

2.2.1 Playfair Analyzer

The first new cryptanalysis component is the "Playfair Analyzer" component, which allows the cryptanalysis of the Playfair cipher. Based on cryptanalytic algorithms developed by Lasry (Lasry, 2019), we implemented the component's internal analysis algorithm. It allows the user to cryptanalyze Playfair ciphers down to a ciphertext length of 40 characters. It implements a known-plaintext as well as a ciphertext-only attack. In order to use the component, the user has to download a 590 MiB sized language statistics file (English hexagram statistics). Currently, this statistics file is only available in English.

2.2.2 Josse Cipher Analyzer

The second new cryptanalysis component is the "Josse Cipher Analyzer" component. It allows the cryptanalysis of ciphertexts encrypted using the Josse cipher (see Section 2.1.2). The internal cryptanalysis algorithm is also based on algorithms developed by Lasry (Lasry, 2021). The algorithms are based on hillclimbing and simulated annealing.

2.2.3 Enigma Analyzer

The last component for cryptanalysis we describe in this paper is the completely reimplemented Enigma Analyzer component. While the old analyzer was no longer state-of-the-art (it used one of the first cryptanalytical algorithms invented by Gillogly (Gillogly, 1995)) the new "Enigma Analyzer" component implements six different types of attacks (the "classical" Gillogly attack, hillclimbing, simulated annealing, Index of Coincidence Search, Trigram Search, and an implementation based on the famous Turing Bombe (Deavours and Kruh, 1990)). All newly implemented attacks are based on research results and implementations by Lasry (Lasry et al., 2019).

2.3 Miscellaneous

In addition to working on cryptography and cryptanalysis, we have also improved the overall CT2 application by making it more stable, powerful, and user friendly. Since many users suggested it would be helpful that CT2 workspaces could be executed in a console application without having to start up a full-blown CT2, we implemented "CrypConsole". CrypConsole is a Windows console app which allows the execution of CT2 workspaces in the Windows terminal. Thus, it can be combined with and included in shell scripts and other console applications. Figure 5 shows a screenshot of the CrypConsole executing a Caesar cipher in the Windows command prompt. The CrypConsole is currently still being developed.

Further examples for more modern cryptography visualized in new components are the Keccak hash function component (Bertoni et al., 2013), the Chacha cipher, the visual cryptography component (Naor and Shamir, 1994), and the steganography component which implements the Bit-Plane Complexity Segmentation Steganography algorithm (Kawaguchi and Eason, 1999). Figure 6 shows a CT2 workspace which contains the visual cryptography component. With visual cryptography, an input text is encrypted into two separated images. Only by overlaying the two images can the original plaintext image be revealed. Figure 7 depicts the ChaCha cipher's visualization. Here, the user is able to view all internal state values of the ChaCha cipher while it is encrypting or decrypting.

3 Work on Historical Ciphers Using CT2

This section presents two successful decryptions of historical ciphers which used CT2. First, a collection of ciphertexts of Maximilian II was deciphered within the DECRYPT project. The second ciphertext is the Ramanacoil transcript. Here, we briefly s how t he c omponents u sed f or t he cryptanalysis of the manuscripts.

3.1 Maximilian II Ciphers

Maximilian II was the Holy Roman Emperor from 1564 to 1576. In 1574 and 1575, Maximilian tried to obtain the Polish-Lithuanian crown. Poland-Lithuania was an electoral monarchy, where the nobility was able to elect their king. Within the DECRYPT project, five encrypted letters from and to Maximilian II relating to the election could be successfully deciphered using CT2's Homophonic Substitution Analyzer. The results were published

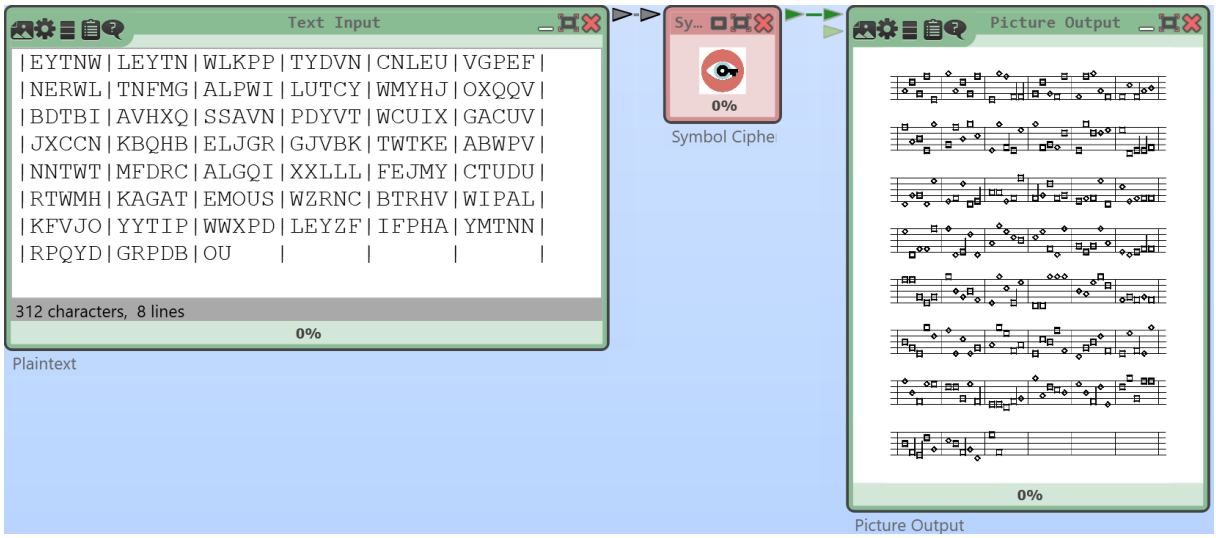

Figure 3: A CrypTool 2 workspace showing the work-in-progress component "Symbol cipher". The component's parameters are set to create a musical cipher based on the scheme by Daniel Schwenter. The result is an image containing the ciphertext formatted as notes.

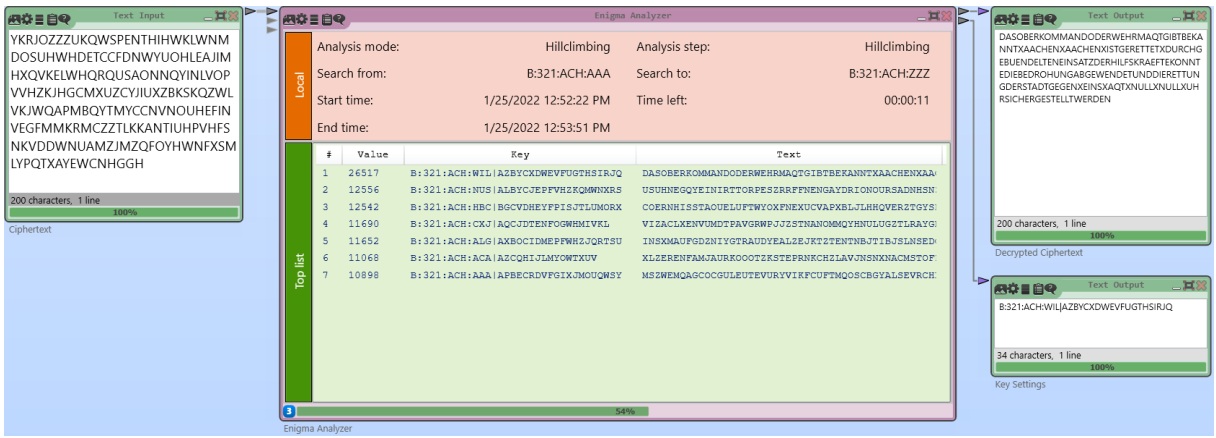

Figure 4: A CrypTool 2 workspace showing the newly implemented "Enigma Analyzer" component in action. It performs a hillclimbing attack on a short Enigma message consisting of 200 characters. On the right side, the deciphered German message can be seen.

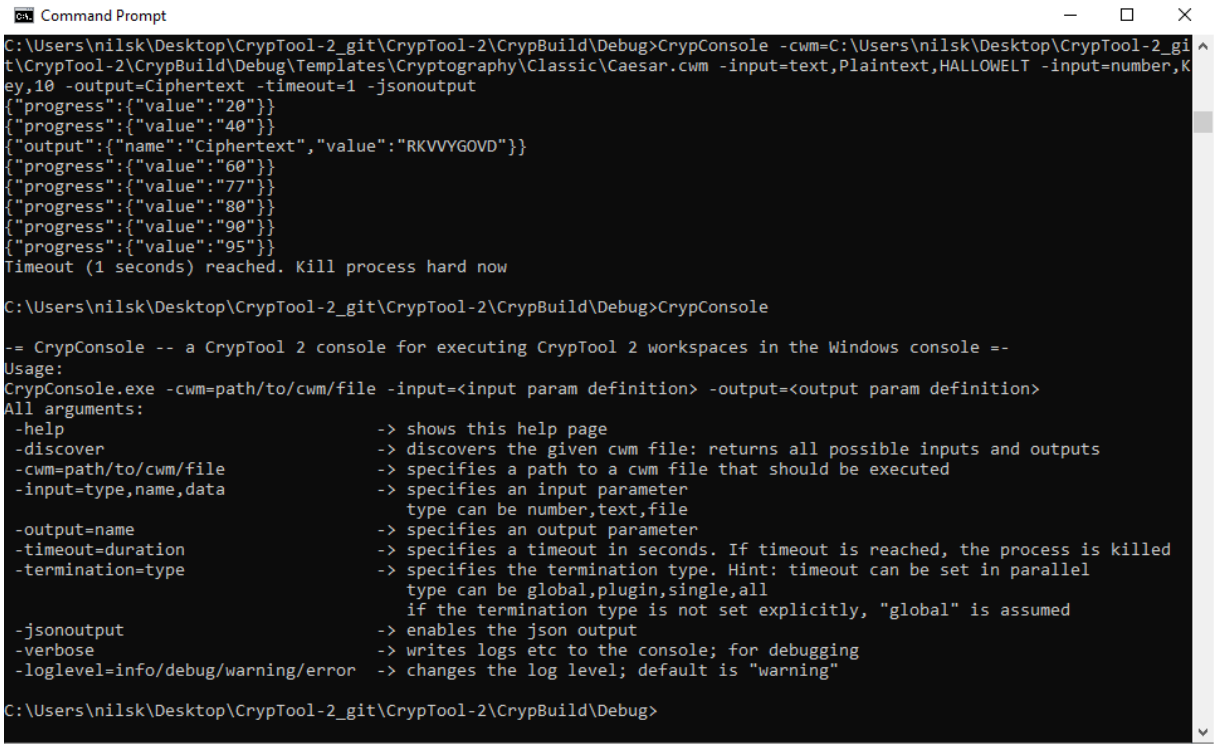

Figure 5: A Windows command prompt showing the CrypConsole executing a Caesar cipher.

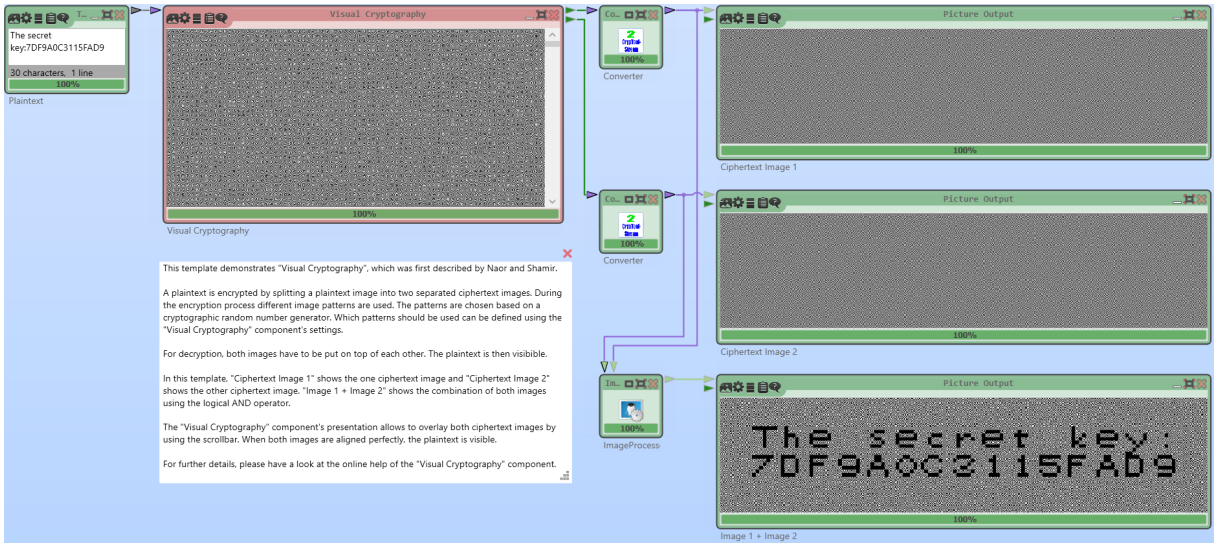

Figure 6: A CT2 workspace showing the Visual Cryptography component encrypting a text and creating two images. The images are overlayed to produce the original plaintext.

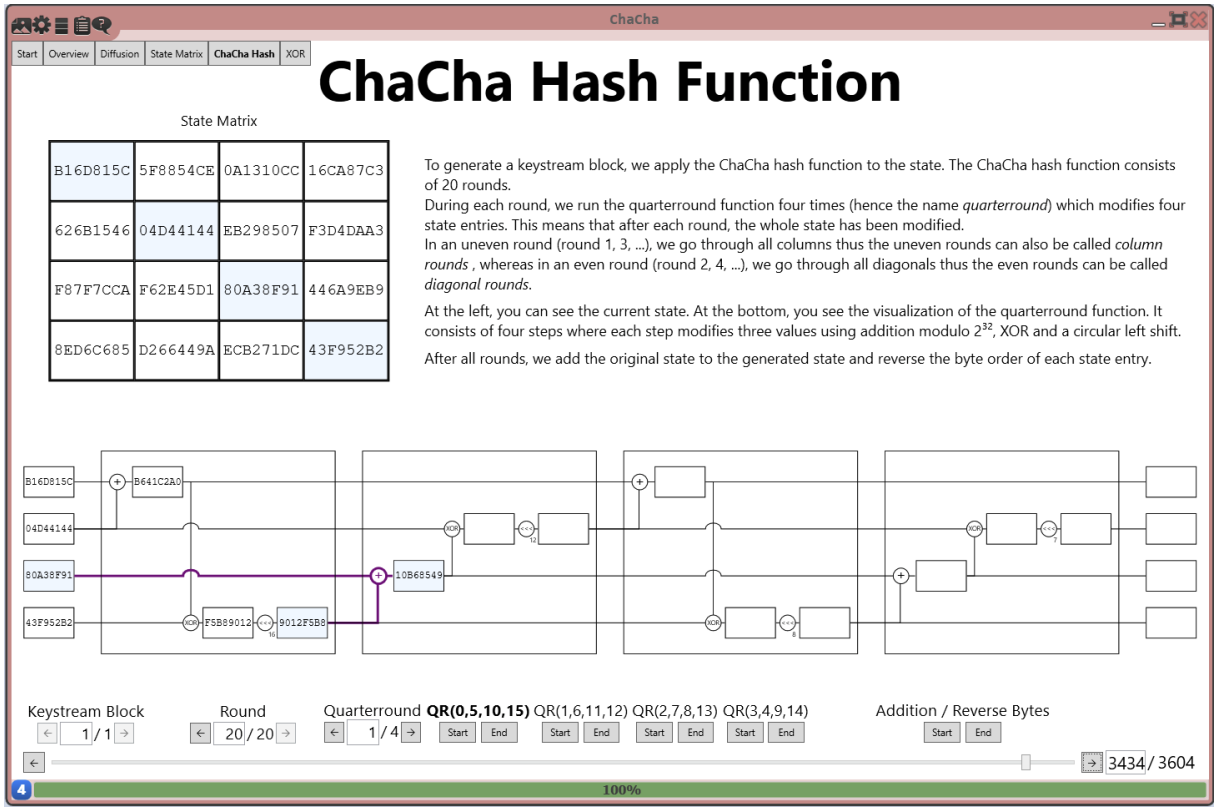

Figure 7: A CT2 workspace showing the Chacha cipher component's visualization.

in two research papers, see (Kopal and Waldispühl, 2020) and (Kopal and Waldispühl, 2021).

The Homophonic Substitution Analyzer component allows the cryptanalysis of homophonic substitution ciphers with the help of hillclimbing. The user is able to change the assignments of plaintext letters found to homophones in a semi-automated way. He does so by stopping the currently running cryptanalysis process and assigning new letters to the homophones by exchanging these using the analyzer's presentation. Figure 8 shows a CT2 workspace containing the Homophonic Substitution Analyzer which is used to decipher one message from Maximilian II.

3.2 Ramanacoil Transcript

The Ramanacoil ciphertexts are two encrypted Dutch East India Company letters from 1674. The first letter was sent by Van Goens Senior from Sri Lanka to the Lords Seventeen (leaders of the East India Company) in The Netherlands. Letter two, which has 33 pages, was addressed to the governor general of Indonesia.

The original copies of the transcript are stored in the National Archives of The Netherlands. Photos of the ciphertexts are stored in the DECODE database (Megyesi et al., 2019), which is the largest database of historical ciphers and keys. Besides the ciphertexts, the original key is also kept in the National Archives. Using CT2, we were able to decipher a self-made transcription created by members of the DECRYPT project. Then, together with Dinnissen the decryption of the Dutch plaintext was improved. Finally, a publication about the transcript's content as well as its deci-pherment was published in a research paper (Din-nissen and Kopal, 2021). Figure 9 shows a CT2 workspace containing a Substitution component, the transcribed Ramanacoil ciphertexts, and a dig-itized key. The Substitution component is used to decrypt the contents of the letters.

4 CrypTool 2 for Teaching and E-Learning

Parallel to using CT2 for solving real-world ciphers, another intention is and always was to establish an e-learning framework for cryptology allowing students, pupils, and everyone else to teach and learn cryptology. Good examples are the evaluated courses at the Singidunum University (Adamovic et al., 2018). Classical and historical ciphers help to motivate students for the fascinating topics of cryptology and information se-

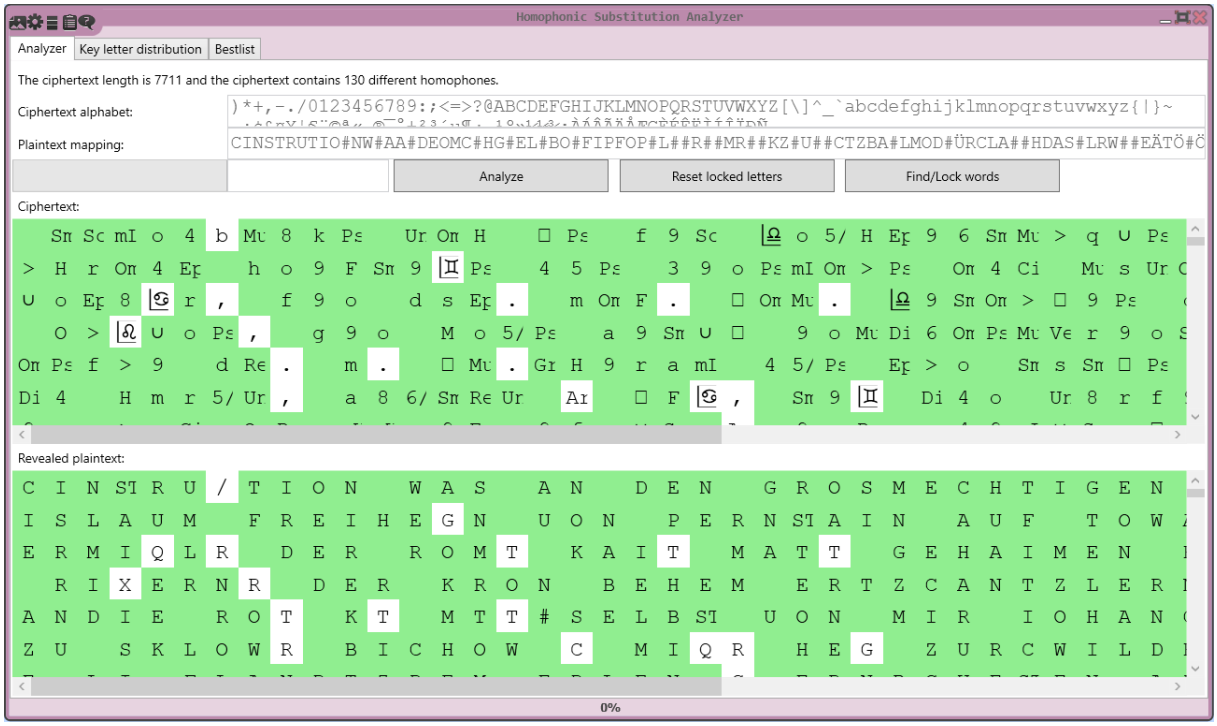

Figure 8: The Homophonic Substitution Analyzer component of CrypTool 2. Here, the analyzer is used to cryptanalyze one of the letters sent by Maximilian II in 1575.

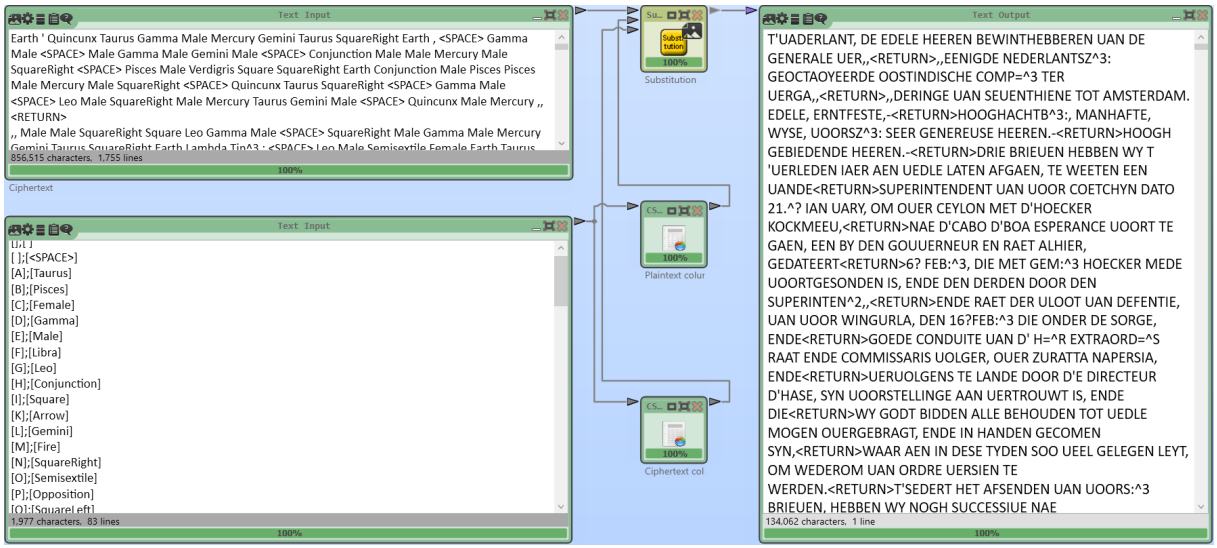

Figure 9: The Substitution component decrypting the Ramanacoil ciphertext using the digitized version of the original key found besides the transcript.

curity. CT2 takes students through the different phases of cryptologic history by providing an all-inclusive set of classical but also modern ciphers. Starting from the Caesar cipher, over the Vigenère cipher, the Enigma machine and other important ciphers and machines from the past, CT2 also includes state-of-the-art cryptanalysis algorithms implemented in various analysis components (for example the Enigma Analyzer as described in Section 2.2.3). A presentation with cryptographic challenges, which gives a good introduction to CT2 and modern cryptography is available on the future forces forum website.[1]

To further assist people in learning cryptology, we established a YouTube channel[2] two years ago dealing especially with cryptologic-related topics. There, we also use CT2 to further explain classical as well as modern ciphers and cryptanalysis techniques. Thus, besides being able to test each cipher and method on their own, students are able to watch guided tours and introductions to different CT2 components.

Before the COVID19 pandemic forced people to keep their distance we organized various "pupils' cryptos", i.e. events in schools and universities where students were introduced to mathematics, science, and especially cryptology. Students were taught the very basics of cryptography and cryptanalysis in one-day events consisting of a secret-agent story with lectures and hands-on exercises. The student's feedback was very positive and CT2 helped to ease their entry into the world of cryptography. We believe that courses like pupils' cryptos helped that students later decided to study math and science. We will continue to carry out such events in the future, as soon as it is possible again.

5 Conclusion and Future Work

This paper presented six new components implemented over the last two years in CrypTool 2 (CT2) using three cipher components and three cryptanalysis components as examples. CT2 is actively used within the DECRYPT project to cryptanalyze ciphers: We successfully solved letters from Maximilian II from the 16th century as well as the Ramanacoil transcript from the 17th century. Finally, we gave a brief insight in how we use CT2 to further support e-learning, e.g. using YouTube, as well as in lectures and the so-called pupils' cryptos, where students are introduced to cryptology in order to motivate them to study math and science.

In the future, we plan to implement more modern cryptanalysis algorithms and methods for both classical and modern ciphers. We currently implement all ciphers defined by the American Cryptogram Association. As part of the DECRYPT project, we aim to implement all newly developed cryptanalytic algorithms in CT2 to make them available to a wider audience.

Also, we are currently working on the implementation of a Hagelin component, which includes simulations of all mechanical Hagelin cipher machines, e.g. the M-209 and the CX-52.

Due to a rework of the DECODE database, the current interface between CT2 and DECODE is non-functional. We plan to update the DECODE components to allow CT2 to connect to the new DECODE database in the near future.

Finally, we also want to use CT2 to analyze more historical encrypted manuscripts stored in the DECODE database that have not yet been deciphered. Based on this, we want to improve our analysis methods and components, e.g. the Homophonic Substitution Analyzer.

[1] `http://www.future-forces-forum.com/download/Workshop-IntroductionToCrypTool.pdf`

[2] "Cryptography for everybody, YouTube channel: `https://www.youtube.com/c/CrypTool2`

Acknowledgments

This work was supported by the Swedish Research Council, grant 2018-06074.

References

Sasa Adamovic, Marko Sarac, Dusan Stamenkovic, and Dalibor Radovanovic. 2018. The importance of the using software tools for learning modern cryptography. *International Journal of Engineering Education*, 34(1):256–262.

Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. 2013. Keccak. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 313–314. Springer.

Cipher A Deavours and Louis Kruh. 1990. The Turing Bombe: was it enough? *Cryptologia*, 14(4):331–349.

Jörgen Dinnissen and Nils Kopal. 2021. Island Ramanacoil a Bridge too Far. A Dutch Ciphertext from 1674. In *International Conference on Historical Cryptology*, pages 48–57.

Rémi Géraud-Stewart and David Naccache. 2020. A French cipher from the late 19th century. *Cryptologia*, pages 1–29.

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

Eiji Kawaguchi and Richard O Eason. 1999. Principles and Applications of BPCS Steganography. In *Multimedia systems and applications*, volume 3528, pages 464–473. International Society for Optics and Photonics.

Nils Kopal and Michelle Waldispühl. 2020. Deciphering three diplomatic letters sent by Maximilian II in 1575. *Cryptologia*, pages 1–25.

Nils Kopal and Michelle Waldispühl. 2021. Two Encrypted Diplomatic Letters Sent by Jan Chodkiewicz to Emperor Maximilian II in 1574-1575. In *International Conference on Historical Cryptology*, pages 80–89.

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

Nils Kopal. 2018. Solving classical ciphers with CrypTool 2. In *Proceedings of the 1st International Conference on Historical Cryptology HistoCrypt 2018*, number 149, pages 29–38. Linköping University Electronic Press.

Nils Kopal. 2019. Cryptanalysis of homophonic substitution ciphers using simulated annealing with fixed temperature. In *Proceedings of the 2nd International Conference on Historical Cryptology, HistoCrypt*, pages 107–16.

George Lasry, Moshe Rubin, Nils Kopal, and Arno Wacker. 2016. Cryptanalysis of Chaocipher and solution of Exhibit 6. *Cryptologia*, 40(6):487–514.

George Lasry, Nils Kopal, and Arno Wacker. 2019. Cryptanalysis of Enigma double indicators with hill climbing. *Cryptologia*, 43(4):267–292.

George Lasry. 2019. Solving a 40-Letter Playfair Challenge with CrypTool 2. In *Proceedings of the 2nd International Conference on Historical Cryptology, HistoCrypt 2019, June 23-26, 2019, Mons, Belgium*, number 158, pages 87–96. Linköping University Electronic Press.

George Lasry. 2021. Analysis of a late 19th century French cipher created by Major Josse. *Cryptologia*, pages 1–15.

Beáta Megyesi, Nils Blomqvist, and Eva Pettersson. 2019. The DECODE database: Collection of historical ciphers and keys. In *The 2nd International Conference on Historical Cryptology, HistoCrypt 2019, June 23-26 2019, Mons, Belgium*, pages 69–78.

Beáta Megyesi, Bernhard Esslinger, Alicia Fornés, Nils Kopal, Benedek Láng, George Lasry, Karl de Leeuw, Eva Pettersson, Arno Wacker, and Michelle Waldispühl. 2020. Decryption of historical manuscripts: the DECRYPT project. *Cryptologia*, 44(6):545–559.

Moni Naor and Adi Shamir. 1994. Visual Cryptography. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 1–12. Springer.

Moshe Rubin. 2011. John F. Byrne's Chaocipher Revealed: An Historical and Technical Appraisal. *Cryptologia*, 35(4):328–379.