Two Encrypted Diplomatic Letters Sent by Jan Chodkiewicz to Emperor Maximilian II in 1574-1575

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

Michelle Waldispühl
University of Gothenburg
Sweden
michelle.waldispuhl@sprak.gu.se

Abstract

This paper presents the work on two encrypted diplomatic letters sent by the Lithuanian nobleman Jan Chodkiewicz to emperor Maximilian II in 1574 and 1575. It describes the decipherment process as well as the content and the context of the letters. Furthermore, it provides linguistic aspects of the used plaintext language. It continues our previous work on Habsburg ciphers where we analyzed and contextualized three diplomatic letters sent by Maximilian II. All presented and analyzed letters relate to the Polish-Lithuanian election in 1575, where Maximilian II, his son Ernst, and his brother Ferdinand were amongst the candidates. The deciphered German plaintexts of all five letters can be accessed via the DECODE database, a storage for historical encrypted manuscripts, which is maintained by members of the DECRYPT project.

1 Introduction

This paper presents a new direct outcome of the DECRYPT project which collects, transcribes, and analyzes historical original encrypted manuscripts in an international and interdisciplinary team of researchers. The final project goal is to research and develop methods and tools which can be used by any researcher, e.g. historians, for free to decipher encrypted material they found in archives all over the world.

In early 2020 three Austrian diplomatic encrypted letters caught our attention for being cryptanalyzed. Photos of the letters were made previously by our project colleagues Anna Lehofer and Benedek Láng in the ”Haus-, Hof- und Staatsarchiv – Österreichisches Staatsarchiv” (HHStA), a unit of the Austrian State Archive, in Vienna. They uploaded the photos into the DECODE database, a storage infrastructure for encrypted historical manuscripts. In the course of the year, we managed to decipher all three letters. The letters were written in German and sent in the 16th century. The sender was Maximilian II, a Habsburg emperor. The letters were sent in July and December 1575. Receivers were delegates of Maximilian II in Poland and Lithuania. The content of the letters related the Polish-Lithuanian royal election in 1575, where Maximilian II was among the candidates. He gave direct orders in favor of his position. Despite all his effort, Maximilian II did not succeed in obtaining the Polish-Lithuanian crown and died soon after in October 1576.

After finishing the cryptanalytical work on the three diplomatic letters by Maximilian II, we turned our attention at the end of 2020 to two other encrypted manuscripts, which equally had been collected in the HHStA by Benedek Láng and Anna Lehofer. The visual writing style is similar to the three encrypted letters previously deciphered. Upon request, student assistants who work for DECRYPT at the University of Uppsala provided transcriptions of the two ”new” letters. After that, we started analyzing the two letters. The experiences we obtained analyzing the first three letters helped us cryptanalyzing the additional letters that turned out to be sent likewise in the time of Maximilian II. While writing this paper in early 2021, we are still in the process of cryptanalyzing and contextualizing the two additional letters. Nevertheless, this paper here gives an overview of the findings which could be of interest to the HistoCrypt audience.

The rest of the paper is structured as follows: Section 2 gives a brief summary of the previously deciphered letters sent by Maximilian II in 1575. After that, Section 3 contains preliminary results of the cryptanalysis of the two recently found letters. Then, Section 4 gives a brief overview of the historical context as well as of the content of the letters. Section 5 presents some aspects of the plaintext language. Finally, Section 6 concludes this paper.

2 Deciphering three diplomatic letters sent by Maximilian II in 1575

This section briefly summarizes the previous findings on the three Habsburg letters sent by Maximilian II in 1575 (letters A-C). While letters A and B both consist of eight full pages of ciphertext symbols and a ninth page with only a few lines of ciphertext, letter C only consists of two full pages and a third page with a few lines of ciphertext symbols.

We published a detailed article about the decipherment, content, and linguistic analysis of the letters A-C in (Kopal and Waldispühl, 2021). In the same article, we also present the historical background of the happenings referred to in the letters in more detail and give an overview on previous work on Habsburg cryptography (e.g. Láng, 2020). Table 1 shows an overview of the meta data of all five letters.

In early 2020, when the work started on letter A, we were not aware of the fact that a set of three letters share the same encryption key. Not knowing the original key used for encryption, we firstly had to perform a ciphertext-only attack on the cipher to reconstruct the used key as well as to decipher the plaintext.

While working on the decipherment of letter A, we found a photo of the original key from 1572, named "Cyffra nova ad Poloniam" in the DECODE database. Shortly after finding the original key, we found two other letters (B and C) sharing the same key. Finally, we found a second copy of the original key in the DECODE database. Having both copies of the original key helped to decrypt the first line of letters A and B, which contained a multitude of null symbols making the decipherment challenging. These lines contain in plaintext "MAXIMILIAN", thus, identify him as the sender. Moreover, the sending dates were similarly "hidden" between nulls at the end of the letters. Only after having obtained the original key these sending dates could be identified.

The used cipher is a homophonic substitution cipher with nomenclature elements and null symbols. Used symbols are a mixture of astrological signs, Greek letters, and esoteric symbols.

The letters contain a total of about 80 distinct ciphertext symbols (homophones). These encrypt single letters and multiple letters. "I" and "J" and "U" and "V" share the same ciphertext symbol, respectively. There are symbols for duplices (bigrams) like "NN" or "ST", as well as a homophone for the frequently used word "UND" (English: 'and'). For each of these, at most two different homophones are used. Embedded in the ciphertext are Latin words written in clear, e.g. "Benigni" or "Ater", which turned out to be nomenclature elements (code words) of the cipher. For example "Benignus" encrypts Archduke Ernest of Austria, which we could only find out by finding the original key.

To decipher letter A, we firstly used the Homophonic Substitution Analyzer component implemented in our open-source software CrypTool 2 (Kopal, 2018). For details on the analyzer, we suggest reading Kopal (2019). In short, the analyzer uses hill climbing and simulated annealing to incrementally improve the decryption key (mapping of homophones to plaintext letters). The user is able to manually improve the automatically generated results of the analyzer. Thus, it was possible to decipher 80% of the letter without having the original key. After finding the original key and entering it into CrypTool 2, it was easily possible to decrypt letters A-C by 95%. Only the code for a few nomenclature elements is still unknown, since these are not described in the original key. Therefore, we assume that there has to be another original key which we have not been able to find so far. Until then, only assumptions can be made about the meaning of these nomenclature elements, e.g. by their usage within the plaintext.

3 Cryptanalysis of the two additional letters

Encouraged by the success with deciphering the first three Maximilian II letters, we started in December 2020 (crypt-)analyzing the two additional letters, which are also stored in the DECODE database. Letter D consists of five full pages of ciphertext symbols and eight lines of ciphertext symbols on a ninth page. Letter E consists of three and a half pages of ciphertext letters as well as three lines of ciphertext on a fifth page.

At first, we compared the ciphertext symbols

Letter	Key	Sender	Receiver(s)	DECODE database (name)	Sending date	Sent from
A	Cyffra Nova Ad Poloniam	Maximilian II	Johan Kochtitzky	Chiffrenschlüssel_fasc 20_kt_14_200-204	7 July 1575	Prague
B	Cyffra Nova Ad Poloniam	Maximilian II	Ambassadors	Chiffrenschlüssel_fasc 20_kt_14_194-198	24 December 1575	Vienna
C	Cyffra Nova Ad Poloniam	Maximilian II	unknown receivers	Chiffrenschlüssel_fasc 20_kt_14_174	23 December 1575	(probably) Vienna
D	unknown name	Johan Chodkiewicz	Maximilian II	Chiffrenschlüssel_fasc 20_kt_205-208	15 November 1574	Vilnius
E	unknown name	Johan Chodkiewicz	Maximilian II	Chiffrenschlüssel_fasc 20_kt_210-212	22 February 1575	Sklow

Table 1: Metadata of all five letters. The column ”Key” contains the names as written on the original key. The column ”DECODE database (name)” is the name used in the database based on the location in the HHStA.

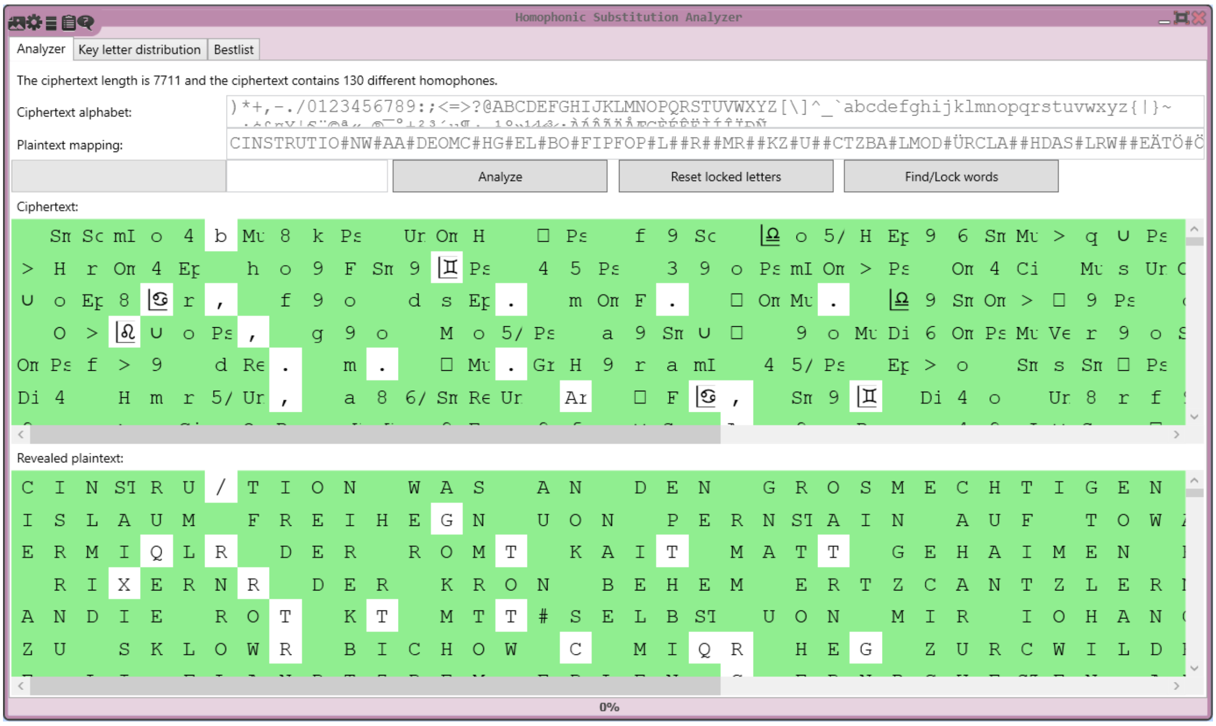
used in the letters D and E with the symbols of the already analyzed letters A-C. Despite of a few ciphertext symbols looking familiar, the used key turned out to be a different one. Therefore, we also searched the key records in the DECODE database for a possible original key. But to our regret we could not find any key suitable for deciphering letters D and E. Therefore, we started to perform a ciphertext-only attack on letter D. We used the Homophonic Substitution Analyzer component implemented in CrypTool 2 to semi-automatically decipher letter D. Figure 1 shows this process. After that, it turned out that letter E was encrypted using the same key. The cryptanalysis of letters D and E was more difficult than the cryptanalysis of the first three letters. Here, we give a short summary of challenges we had in deciphering as well as helpful properties of the two additional letters:

Spaces between words are clearly visible As in letters A-C, spaces between words are (mostly) clearly visible. This eased the decipherment work, since frequently used short German words, like ”DER/DIE/DAS” (English: ’the’) could be spotted and deciphered easily.

Usage of nulls similar to usage in letters A-C Null symbols are rarely used within the ciphertexts. Exceptions are the endings and beginnings of the letters, where multiple nulls are used to confuse an attacker trying to decipher these. The same practice was employed in letters A-C. In addition, in the beginning of letter E, nulls are used between different words in the salutation formula. Moreover, the digits of the sending year (1574) were written as plaintext digits embedded in null symbols. Since we also saw this usage in the first three letters, spotting the sending dates in the additional letters was quite easy.

Usage of Latin words as nomenclature elements Similar to letters A-C, nomenclature elements (code words) used for enciphering persons and places are cleartext Latin words embedded in the ciphertext. Nomenclature elements are, however, only used in letter D. We found a key similar to the two keys used in letters A-E in a collection of letters issued by Andreas Dudithius in 1575 edited in Dudith and Kotońska (1998). In the introduction to the edition, the key of the cipher Dudithius used in his correspondence with the Habsburg is given. However, the source for this key is not indicated. Thus, it remains unclear if it was reconstructed by the author on the basis of the edited letters only, or if it represents a transcription of an original key document. Further investigation of key documents in archives are needed to clear this question. Luckily for us, the published key contains all nomenclature elements used in letter D which facilitated their encoding. This case shows that two keys used in different geographical places and by different persons shared the same nomenclature elements in that time. While that practice opens security issues for keys, it facilitates and accelerates the practicability of keys for encoding and decoding, cf. (Ernst, 1992).

Homophones encoding frequently used words In letters A-C the frequently used German word ”UND” (English: ’and’) was encrypted using its own homophone. Also, we assume that homophones for the words ”Poland” and ”Lithuania” were used. In the additional letters, we found another homophone that encrypts a frequently used word. Based on its positions and usages in the plaintext, we assume that this homophone



The ciphertext length is 7711 and the ciphertext contains 130 different homophones.

Ciphertext alphabet:)*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~

Plaintext mapping: CINSTRUTIO#NW#AA#DEOMC#HG#EL#BO#FIPFOP#L##R##MR##KZ#U##CTZBA#LMOD#ÜRCLA##HDAS#LRW##EÄTÖ#C

Ciphertext:

```
  Sn Sc mI o  4  b  Mu 8  k  Ps    Ur On H     □  Ps    f  9  Sc    |♎ o  5/ H  Ep 9  6  Sn Mu >  q  ∪  Ps
>  H  r  On 4  Ep    h  o  9  F  Sn 9  |♊ Ps    4  5  Ps    3  9  o  Ps mI On >  Ps    On 4  Ci    Mu s  Ur
∪  o  Ep 8  |♋ r  ,     f  9  o     d  s  Ep .     m  On F  .     □  On Mu .     |♎ 9  Sn On >  □  9  Ps
   O  >  |♌ ∪  o  Ps ,     g  9  o     M  o  5/ Ps    a  9  Sn ∪  □     9  o  Mu Di 6  On Ps Mu Ve r  9  o
On Ps f  >  9     d  Re .     m  .     □  Mu .  Gr H  9  r  a  mI    4  5/ Ps    Ep >  o     Sn s  Sn □  Ps
Di 4     H  m  r  5/ Ur ,     a  8  6/ Sn Re Ur    Ar    □  F  |♋ ,     Sn 9  |♊    Di 4  o     Ur 8  r  f
```

Revealed plaintext:

```
C  I  N  ST R  U  /  T  I  O  N     W  A  S     A  N     D  E  N     G  R  O  S  M  E  C  H  T  I  G  E  N
I  S  L  A  U  M     F  R  E  I  H  E  G  N     U  O  N     P  E  R  N  ST A  I  N     A  U  F     T  O  W
E  R  M  I  Q  L  R     D  E  R     R  O  M  T     K  A  I  T     M  A  T  T     G  E  H  A  I  M  E  N
   R  I  X  E  R  N  R     D  E  R     K  R  O  N     B  E  H  E  M     E  R  T  Z  C  A  N  T  Z  L  E  R
A  N  D  I  E     R  O  T     K  T     M  T  T  #  S  E  L  B  ST    U  O  N     M  I  R     I  O  H  A  N
Z  U     S  K  L  O  W  R     B  I  C  H  O  W     C     M  I  Q  R     H  E  G     Z  U  R  C  W  I  L  D
```

Figure 1: Letter D being analyzed using the Homophonic Substitution Analyzer component of CrypTool 2. The top of the analyzer displays the encrypted ciphertext. The bottom of the analyzer displays the deciphered plaintext.

encrypts a royal title, e.g. ”Majestät” (English: ’Majesty’). Additionally, the homophone for encrypting ”UND” in German plaintext parts is also used to encrypt ”ET” in Latin plaintext parts.

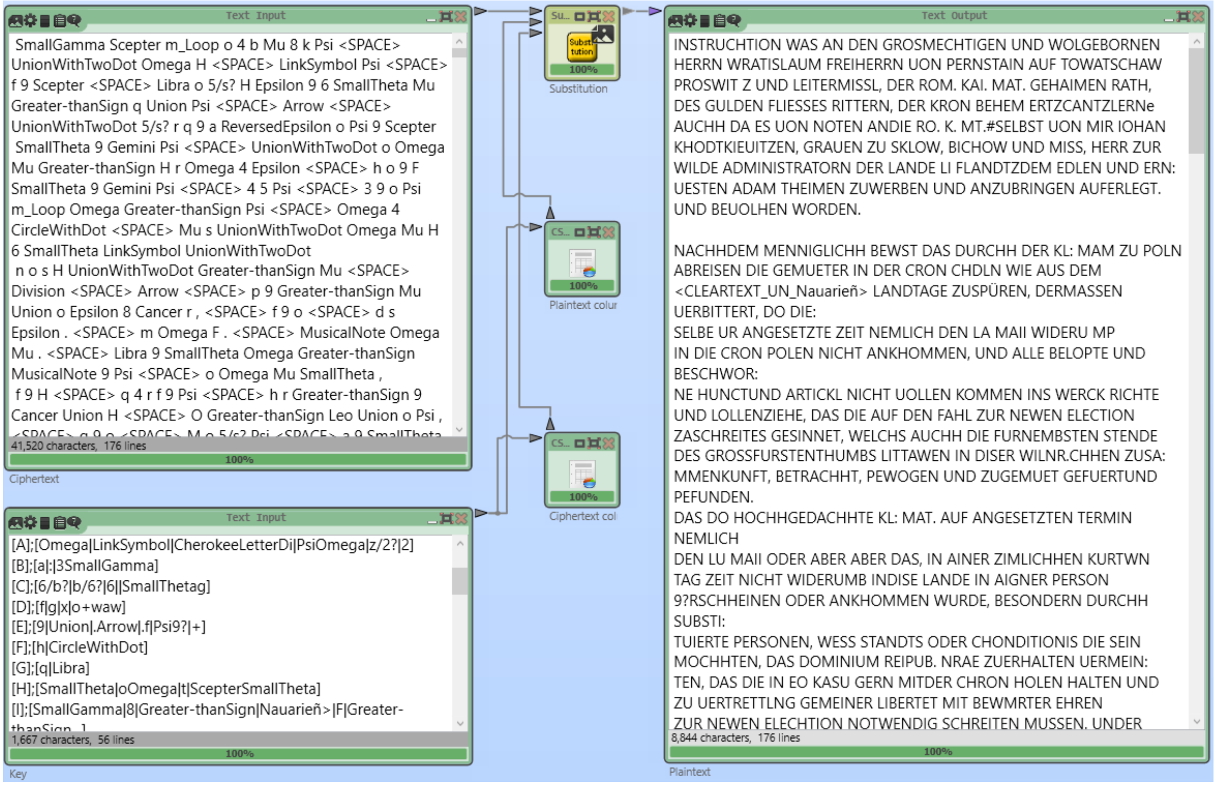
Usage of abbreviations in the plaintext We found several constructions in the plaintext that are abbreviations. For example, we found ”KAY.” (= ”kaiserliche”, English: ’imperial’) and ”E.” (= ”Eure”, English: ’Your’). Such abbreviations can be easily spotted already in the ciphertext, since the used dots are not encrypted.

Usage of interpunction The interpunction, as already shown above, is (mostly) clearly visible in the ciphertexts. Endings of sentences are marked with a dot. Enumerations and abbreviations are also constructed with dots.

Encryption of umlauts The German umlauts are also encrypted in the same manner as in the first three letters. At many positions (but not at all), the homophones for A, O, and U have two small dots on top, meaning, these are the German umlauts Ä, Ö, and Ü.

Non-encrypted cleartext digits When dates are given (such as typically at the end of the letters, but also within the texts) the numbers of the day are presented in non-encrypted digits, e.g. the numbers ”12” on page 1, line 13 in letter E in the date ”12 MAII”. Since the digits might possibly also function as homophones or nomenclature elements, we could only definitely decipher them and disambiguate their meaning in the context of the plaintext. However, at the end of the letters it was easier to spot the digits and identify them as numbers indicating the sending year (1574 and 1575, respectively) since we saw the same usage in letters A-C.

After reconstruction the mappings of homophones to plaintext letters using the Homophonic Substitution Analyzer, the complete ciphertexts could be decrypted easily using the Monoalphabetic Substitution component of CrypTool 2. Figure 2 shows the decryption of letter D using CrypTool 2. As an example decipherment, Figure 3 presents the first paragraph of letter D. Above each line of ciphertext the corresponding deciphered line of German plaintext is shown in red letters. We were able to decipher both letters (D and E) completely. Table 2 contains all homophones used in the first paragraph of letter D.



SmallGamma Scepter m_Loop o 4 b Mu 8 k Psi <SPACE>
UnionWithTwoDot Omega H <SPACE> LinkSymbol Psi <SPACE>
f 9 Scepter <SPACE> Libra o 5/s? H Epsilon 9 6 SmallTheta Mu
Greater-thanSign q Union Psi <SPACE> Arrow <SPACE>
UnionWithTwoDot 5/s? r q 9 a ReversedEpsilon o Psi 9 Scepter
SmallTheta 9 Gemini Psi <SPACE> UnionWithTwoDot o Omega
Mu Greater-thanSign H r Omega 4 Epsilon <SPACE> h o 9 F
SmallTheta 9 Gemini Psi <SPACE> 4 5 Psi <SPACE> 3 9 o Psi
m_Loop Omega Greater-thanSign Psi <SPACE> Omega 4
CircleWithDot <SPACE> Mu s UnionWithTwoDot Omega Mu H
6 SmallTheta LinkSymbol UnionWithTwoDot
n o s H UnionWithTwoDot Greater-thanSign Mu <SPACE>
Division <SPACE> Arrow <SPACE> p 9 Greater-thanSign Mu
Union o Epsilon 8 Cancer r , <SPACE> f 9 o <SPACE> d s
Epsilon . <SPACE> m Omega F . <SPACE> MusicalNote Omega
Mu . <SPACE> Libra 9 SmallTheta Omega Greater-thanSign
MusicalNote 9 Psi <SPACE> o Omega Mu SmallTheta ,
f 9 H <SPACE> q 4 r f 9 Psi <SPACE> h r Greater-thanSign 9
Cancer Union H <SPACE> O Greater-thanSign Leo Union o Psi ,
<SPACE> q 9 o <SPACE> M o 5/s? Psi <SPACE> a 9 SmallTheta

41,520 characters, 176 lines

Ciphertext

[A];[Omega|LinkSymbol|CherokeeLetterDi|PsiOmega|z/2?|2]
[B];[a|:|3SmallGamma]
[C];[6/b?|b/6?|6||SmallThetag]
[D];[f|g|x|o+waw]
[E];[9|Union|.Arrow|.f|Psi9?|+]
[F];[h|CircleWithDot]
[G];[q|Libra]
[H];[SmallTheta|oOmega|t|ScepterSmallTheta]
[I];[SmallGamma|8|Greater-thanSign|Nauarieñ>|F|Greater-thanSign]

1,667 characters, 56 lines

Key

INSTRUCHTION WAS AN DEN GROSMECHTIGEN UND WOLGEBORNEN
HERRN WRATISLAUM FREIHERRN UON PERNSTAIN AUF TOWATSCHAW
PROSWIT Z UND LEITERMISSL, DER ROM. KAI. MAT. GEHAIMEN RATH,
DES GULDEN FLIESSES RITTERN, DER KRON BEHEM ERTZCANTZLERNe
AUCHH DA ES UON NOTEN ANDIE RO. K. MT.#SELBST UON MIR IOHAN
KHODTKIEUITZEN, GRAUEN ZU SKLOW, BICHOW UND MISS, HERR ZUR
WILDE ADMINISTRATORN DER LANDE LI FLANDTZDEM EDLEN UND ERN:
UESTEN ADAM THEIMEN ZUWERBEN UND ANZUBRINGEN AUFERLEGT.
UND BEUOLHEN WORDEN.

NACHHDEM MENNIGLICHH BEWST DAS DURCHH DER KL: MAM ZU POLN
ABREISEN DIE GEMUETER IN DER CRON CHDLN WIE AUS DEM
<CLEARTEXT_UN_Nauarieñ> LANDTAGE ZUSPÜREN, DERMASSEN
UERBITTERT, DO DIE:
SELBE UR ANGESETZTE ZEIT NEMLICH DEN LA MAII WIDERU MP
IN DIE CRON POLEN NICHT ANKHOMMEN, UND ALLE BELOPTE UND
BESCHWOR:
NE HUNCTUND ARTICKL NICHT UOLLEN KOMMEN INS WERCK RICHTE
UND LOLLENZIEHE, DAS DIE AUF DEN FAHL ZUR NEWEN ELECTION
ZASCHREITES GESINNET, WELCHS AUCHH DIE FURNEMBSTEN STENDE
DES GROSSFURSTENTHUMBS LITTAWEN IN DISER WILNR.CHHEN ZUSA:
MMENKUNFT, BETRACHHT, PEWOGEN UND ZUGEMUET GEFUERTUND
PEFUNDEN.
DAS DO HOCHHGEDACHHTE KL: MAT. AUF ANGESETZTEN TERMIN
NEMLICH
DEN LU MAII ODER ABER ABER DAS, IN AINER ZIMLICHHEN KURTWN
TAG ZEIT NICHT WIDERUMB INDISE LANDE IN AIGNER PERSON
9?RSCHHEINEN ODER ANKHOMMEN WURDE, BESONDERN DURCHH
SUBSTI:
TUIERTE PERSONEN, WESS STANDTS ODER CHONDITIONIS DIE SEIN
MOCHHTEN, DAS DOMINIUM REIPUB. NRAE ZUERHALTEN UERMEIN:
TEN, DAS DIE IN EO KASU GERN MITDER CHRON HOLEN HALTEN UND
ZU UERTRETTLNG GEMEINER LIBERTET MIT BEWMRTER EHREN
ZUR NEWEN ELECHTION NOTWENDIG SCHREITEN MUSSEN. UNDER

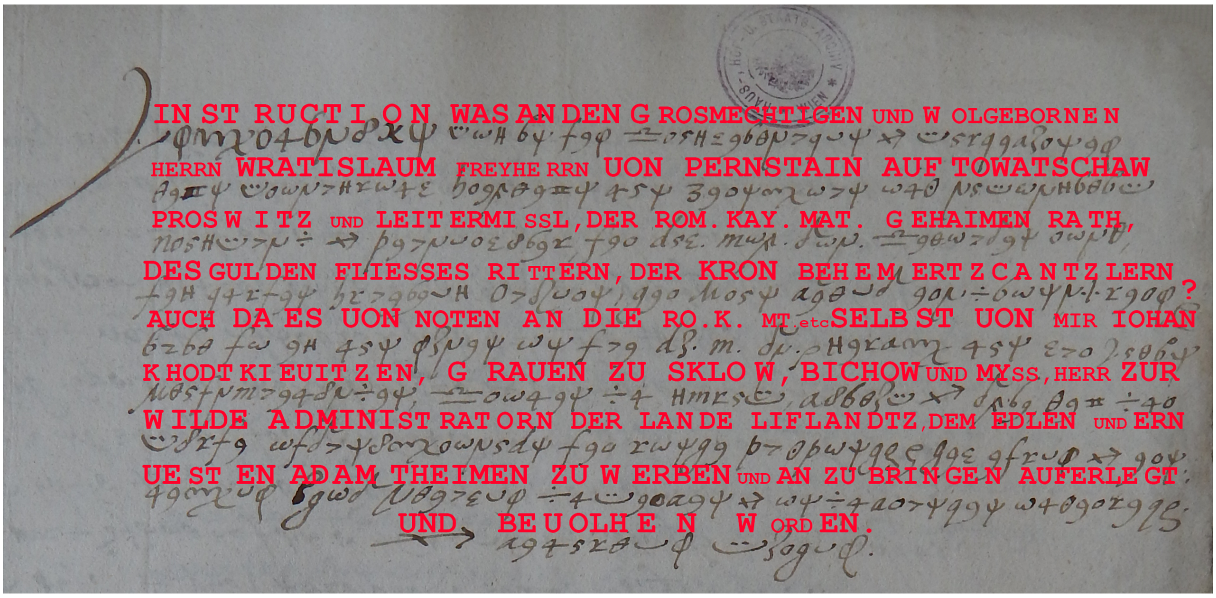
8,844 characters, 176 lines

Plaintext

Figure 2: Letter D decrypted using the Monoalphabetic Substitution component of CrypTool 2 and the reconstructed key.

Plaintext symbol(s)	Ciphertext symbol(s)	Plaintext symbol(s)	Ciphertext symbol(s)
A	ω ☍	R	o d
B	a	S	H
C	6 b	T	ϻ 5
D	f g	U / V	4 ƶ
E	9 ∪	W	∪̈
F	⊙ h	Y	Ʌ
G	♎ q	Z	÷
H	θ		
I / J	> 8 ɣ	UND/ET	↗
K	m M		
L	⊤ p	ST	♏
M	ε ☍		
N	Φ Ψ	RR	♊
O	3 S	SS	♋
P	3 n	TT	♌

Table 2: Partially reconstructed key (showing only homophones used in the first paragraph of letter D).



INSTRUCTION WAS AN DEN GROSMECHTIGEN UND WOLGEBORNEN
HERRN WRATISLAUM FREYHERRN UON PERNSTAIN AUF TOWATSCHAW
PROSWITZ UND LEITERMISSL, DER ROM. KAY. MAT. GEHAIMEN RATH,
DES GULDEN FLIESSES RITTERN, DER KRON BEHEM ERTZCANTZLERN ?
AUCH DA ES UON NOTEN AN DIE RO. K. MT. etc SELBST UON MIR IOHAN
KHODTKIEUITZEN, GRAUEN ZU SKLOW, BICHOW UND MYSS, HERR ZUR
WILDE ADMINISTRATORN DER LANDE LIFLANDTZ, DEM EDLEN UND ERN
UESTEN ADAM THEIMEN ZU WERBEN UND AN ZU BRINGEN AUFERLEGT
UND BEUOLHEN WORDEN.

Figure 3: Original first paragraph of letter D with deciphered German plaintext shown in red letters above each line of ciphertext. English translation: ”Instruction about what I, Johan Khodtkievitz, Count of Shklow, Bichow and Miss, Castellan at Vilnius [and] governor of the land Livonia have imposed and ordered to Adam Theim that should be advertised and promoted to the mighty and honorable baron Vratislav (II.) baron z Pernštejna of Tovačov, Prostějov and Litomyšl, the imperial Roman Majesty‘s privy counsellor, knight of the Golden Fleece, archchancellor of the Crown Bohemia, and also, because there is need, to the imperial Roman Majesty etc. himself.”

4 Historical context and content of the letters

Both letters form part of the same broad historical context as the previously presented letters A-C: the election of the ruler of the Polish-Lithuanian Commonwealth in 1575. The Commonwealth (originally ”Crown of the Kingdom of Poland and the Grand Duchy of Lithuania”) included areas of today’s Poland, Ukraine, Estonia, Latvia, Lithuania, and Belarus. The Polish-Lithuanian crown had been vacant from June 1574 and the election of a successor started in November 1575. In the Polish-Lithuanian Commonwealth, the monarch ruler was elected by the nobility which in 1574-1575 included more than 50,000 persons. The Habsburg were interested in gaining the crown and nominated several candidates, among them the emperor Maximilian II himself and his son Ernst (cf. Rhode (1997), Augustynowicz (2001), Roşu (2017). In the *interregnum* period when the crown was vacant, the Habsburg put intensive efforts into diplomatic correspondence to make campaign for its candidacy. The main supporters of the Habsburg were the members of the Lithuanian higher nobility and the clerics while the nobility of Lesser Poland had an anti-Habsburg attitude and favored a local candidate. This divide eventually led to a double election in December 1575 of both Maximillian II. and the Polish princess Anna Jagiellon, giving her Stefan Báthory, the Prince of Transylvania, for husband (cf. ibid.). Eventually, the latter candidates succeeded in claiming the throne and got married and crowned in May 1576.

While letters A-C presented in Kopal and Waldispühl (2021) were sent by Maximilian II to his Polish and Lithuanian delegates in July 1575 (letter A) and on 23 and 24 December 1575 (letter C and B), respectively, the current letters D and E are dated earlier and were sent by the Lithuanian nobleman, Grand Marshal of Lithuania, Johan Chodkiewicz. They show the perspective and interests of the Lithuanian higher nobility in late 1574 and early 1575 as presented to Maximilian II.

In the following is a short summary of the content of the two letters and report on open problems regarding source criticism and the historical contextualization.

Letter D: LEGATIO IOANNI KHODTKIEUITI[1], sent from Vilnius, 15 November 1574 This letter dated on 15 November 1574 is indicated as a message (LEGATIO) by Johan Chodkiewicz and was addressed to Maximilian II. The letter was sent from Vilnius (ZUR WILDE[2]) where Johan Chodkiewicz was castellan.

In the first paragraph, Johan Chodkiewicz makes himself known and says that he gives an instruction on what he has ordered to his servant Adam Theim to report to Vratislav (II.) z Pernštejna and also to the emperor himself. In the following he advises Maximilian to win supporters and prepare for the election of a new king of Poland and Grand Duke of Lithuania before the gathering on 12 May. He informs the emperor about the divide between the Lithuanian and Prussian senators who back the Habsburg candidacy on the one side and the Polish senators who refuse to take Archduke Ernst as their king and ruler on the other side. Chodkiewicz then recommends Maximilian to mobilize his allies in Hungary, Moravia, and other places. He expresses his wish that, if "in the lucky case" Ernst will gain the thrown, the privileges of the Lithuanian Grand Duchy will be restored. He advises Maximilian to send envoys to Lithuania at the latest by March to negotiate certain privileges with the local nobility and make a resolution. In the last two paragraphs he gives his allegiance and loyalty and concludes the letter.

Letter E: Copy of Johan Chodkiewicz' letter to Maximilian II, sent from Sklow (Sjkloŭ), 22 February 1575 This letter was filed as "ABSCHRIFT IOHANN CHODTKIEUIZ SCHREIPENS AN DIE MAJESTÄT" ('copy of Johan Chodtkieviz letter to the Majesty') and was sent from Sjkloŭ (Chodkiewicz' Duchy in today's Belarus) on 22 February 1575.

In contrast to letter D, this exemplar is introduced with a salutation formula addressing the emperor. Chodkiewicz then confirms the receipt of Maximilian's message and reassures his loyalty to the emperor. In a humble tone he utters his doubts about what Maximilian mentioned in his earlier letter. Unfortunately, we lack the whole context to understand what Maximilian's suggestions exactly were. However, Chodkiewicz fears these matters might lead to "all sorts of repulsive thoughts [...] all kinds of confusions and splits". He suggests to send out his own envoy, Adam Theim, in order to bring the Lithuanian electorate on the emperor's side and he thinks that in the following, it would equally be possible to attract several Polish nobles as supporters of the Habsburg candidacy. Uttering his loyalty to the emperor, he reassures that it would be impossible for the emperor to achieve common consensus among the voters without supporters like him. He suggests Maximilian to make a contract first with the higher nobility only who then would communicate it further to other electors. The letter concludes with a declaration of loyalty and a humble excuse for bringing up a suggestion that might annoy Maximilian.

Open problems In the course of research on the historical background, we found a reference to the content of letter D in Augustynowicz (2001) who even cites parts of the letter in note 106 on page 50. The text given corresponds to five lines in letter D, however, it shows some deviations in orthography, e.g in the use of more double consonants (*auff, dessenn* vs. AUF, DESSEN in letter D) or *meinung* instead of MAINUNG. In addition, for this passage, Augustynowicz refers to two documents with the shelf marks "HHStA Wien, Polen I, 23, D, 44r" and "ebenda, Ungarn, 105, C, 20r-v". These documents are different from the ones we are dealing with here. Thus, the same text content seems to be represented in different physical documents in the State Archive of Vienna. It is the task of future investigation to compare these three documents and determine their relation both with regard to content and textual representation. For instance, there might even be the possibility that one of these documents cited in Augustynowicz (2001) contains the plaintext of the here analyzed ciphertext.

The content of letter E, on the other hand, seems not to form part of (Augustynowicz, 2001)'s work. However, it is filed as a copy, which implies that there must be an original. In future work, the possible transmission of this letter in other documents likewise has to be clarified.

5 Language

The plaintext language of letters D and E is German with short passages in Latin. In 16th cen-

[1] Here and in the following, we use capital letters to represent plaintext passages of the two deciphered documents.

[2] The place name "Wilde" for Vilnius was used in historical German from 14th century onwards.

tury Lithuania, many languages were used simultaneously. German was one of the languages for communication with foreigners (next to Latin and Church Slavonic) while Polish (for nobleman) and Lithuanian (for peasants) were the main means of spoken communication. For written correspondence within Lithuania a local chancery language labeled ”Old White Russian” was used (Niendorf, 2006). With regard to this diversity of different languages and the German speaking addressee, Johan Chodkiewicz’ use of German is not surprising.

Written dialect The main linguistic characteristics of the written dialect can be defined as very similar to the Austrian-German office language we found in the letters A-C sent by Maximilian II’s chancery. There is, for instance, the differentiation of the spelling <ai> for an old Germanic diphthong *ai (e.g. AINER ’one’, BAIDE ’both’) and the spelling <ei> for a younger diphthong from an older long vowel *ī (e.g. ZEIT ’time’, FLEISS ’diligence’, SCHREIBEN ’letter, writing’). However, this use is less consistent in letters D and E than in letters A-C. Letter D, for instance, shows variation of <ei>- and <ai>-spellings in some instances (MEINUNG and MAINUNG ’opinion’ or GEMEIN and GEMAIN ’general’). Additionally, the use of <p> for an older *b is more common in the two current letters than in the letters sent by Maximilian and also found in the prefix *be-* (e.g. PEWOGEN, PEFUNDEN in letter D) which is usually not the case in Austrian German (Wiesinger, 2012). The syntax is typical of the chancery style used in the 16th century and the sentences show a similar complexity to what we found in letters A-C. Additionally, some main features, such as the dropping of auxiliary verbs in subordinate clauses, are equally present in the letters sent from Lithuania.

German-Latin code switching The plaintexts of both letters include some smaller parts in Latin embedded into the German text. This is a linguistic feature we did not observe in letters A-C. The code switching includes both shorter passages, such as example 1 and longer passages, such as example 2.

1. ”EO KASU” in the sentence DAS DIE IN *EO KASU* GERN MIT DER CRON POLEN HALTEN UND ZU VERTRETUNG GEMEINER LIBERTET

2. DAS ALLE DENEN SO E. [EURE] M [MAIESTET] GEWOGEN, AUCH MEINER PERSON *SINE ISTIS MEDIIS IMPOSSIBILE [EST], OMNIUM ANIMOS IN EODEM KONSENSU* ZU ERHALTEN

It is interesting to note that the Latin passages are always embedded syntactically into German sentences. There is no entire Latin sentence standing on its own. Moreover, the Latin parts involve both formulaic language (e.g. example 1) but also more freely formulated passages (example 2).

The homophone used for the German word UND (English: ’and’) is also used in the Latin passages which means it performs its semantic function irrespective of the language-specific context. One example is the passage DE OMNIBUS [ET] SINGULIS in letter E, where [ET] is represented by a homophone (see Table 2).

Punctuation marks In contrast to the earlier analyzed letters A-C, the punctuation marks were included in the transcriptions of letters D and E which allows for some observations of the use of punctuation. Generally it can be noted that punctuation marks are not encrypted and function exactly in the way they would be employed in a cleartext. This concerns, for instance, dots that were used consistently in abbreviations (e.g. ROM. KAY. MAT.), as already mentioned in Section 3, but also commas that separate clauses and dots at the end of sentences and paragraphs. Since dots are easily visible in the ciphertext they imply a security flaw. This is equally the case for the use of colons at the end of a line as a separator when the word continues on the next line (e.g. DIE:SELBE or ZUSA:MMENKUNFT in letter D).

These observations clearly show that it is worth transcribing punctuation marks in ciphertexts since they give information about linguistic structures and may not only facilitate the decryption of the ciphertext but also the comprehension of the content.

6 Conclusion and future work

This paper is a new direct outcome of the DECRYPT project. It describes how we transcribed, analyzed, and deciphered two additional diplomatic letters sent in the time of Maximilian II in the years 1574 and 1575. The work on these letters is the continuation of the previous work on the decipherment of letters sent by Maximilian. The letters presented here were sent by the nobleman Johan Chodkiewicz to the emperor in November 1574 and February 1575. The letters were encrypted with a different key as the one used for encrypting Maximilian's letters. In contrast to Maximilian's letters, where we were able to find the original key in the DECODE database, we currently do not have knowledge about the original key used in Chodkiewicz' letters.

However, in the course of working on this paper in early 2021, we found an edition of letters of Andreas Dudith, a Hungarian nobleman, bishop, humanist, and ambassador of Maximilian II in Kraków where the key used in Dudith's correspondence is presented (Dudith and Kotońska, 1998). This key contains, besides additional homophones, the same homophones as used in the letters A-C sent by Maximilian II. Moreover, it contains nomenclature elements that fit for letter D written by Chodkiewicz. Therefore, in future work, we will compare the Dudith nomenclature to the keys stored in the DECODE database and to the key which we reconstructed for the decipherment of the Chodkiewicz letter. As a preliminary result, we can say that it seems that the same nomenclature elements were used among different cryptographic keys at that time. Clearly, this introduced a potential threat since being in possession of one key enables an adversary to also decipher nomenclature elements of other (similar) keys. On the other hand, this practice facilitated the work for the encoders and decoders because they probably knew the code words by heart.

Review of previous literature has likewise shown that the HHStA holds other documents that have a close relation to some of the cryptographic letters presented here. Hence, another future task is to visit the HHStA and gather material in the folders "Polen I" for further analyses and comparison.

The main new cryptographic findings of and differences between the Maximilian's letters (Letters A, B, and C) and Chodkiewicz' letters (Letters D and E) are:

- Letters D and E are encrypted using the same key, but it was a different key than the one used in the Maximilian letters (A, B, and C).
- However, in general it can be said that knowledge of text structure and cryptographic practice from other letters written in the same historical context are useful for deciphering newly found encrypted manuscripts. In our case, the comparison of the use of nulls, the placing of names (of sender and addressee), and the placing and execution of dates we have seen in letters A-C facilitated the decipherment of letters D-E.
- Chodkiewicz used abbreviations in the ciphertext, while in the Maximilian letters no abbreviations can be found.
- In contrast to the Maximilian letters, where a lot of nulls were used, these can only rarly be found in Chodkiewicz' letters. Only the dates at the endings are embedded in nulls similar to the practice in Maximilian's letters.
- As described above, nomenclature elements were shared among different keys at that time in the Habsburg Empire.
- Chodkiewicz switches between German and Latin (code switching) in the plaintext. Latin was not recognized in the automatic cryptanalysis and therefore, transcription and deciphering errors were assumed in the beginning of the cryptanalysis. After Latin had been identified in the linguistic analysis, the decipherment could be verified.
- Interestingly, the same ciphertext symbol (homophone) was used for the conjunction "UND"/"ET" in the ciphertext, irrespective of the plaintext language German or Latin.

The decipherment of the five Maximilian II letters using the homophonic substitution analyzer in CrypTool 2 helped us to further enhance our cryptanalytical algorithms as well as to improve the general handling of our tools. Furthermore, having all letters as transcriptions that follow the DECRYPT transcription guidelines, proved to ease and speed up the cryptanalysis. This confirms that the common standards developed within the DECRYPT project and the cooperation between experts from different scientific fields can be very helpful and fruitful.

Additionally to performing cryptanalysis to decipher the Chodkiewicz letters, we analyzed linguistic aspects of the letters. Our main findings here are that the written dialect is similar to the one employed by Maximilian's chanceries detected in letters A-C. However, the letters sent from Lithuania seem to show more orthographic variation and make use of German-Latin code switching. Moreover, since punctuation is not encrypted, it brings linguistic structures to the fore and facilitates both decipherment and text comprehension.

The decipherments of the three letters of Maximilian II to his chamberlain Johann Kochtitzky and ambassadors (letters A-C) and the letters from the Lithuanian nobleman Jan Chodkiewicz to Maximilian II (letters D and E) provide insight in the (secret) Habsburg views and actions before the free election in 1575. They show the deep division between the Polish and Lithuanian noblemen, the Lithuanian side pro and the Polish side contra the Habsburg empire's candidates. Because of that division, Maximilian made efforts to achieve his goal of convincing the Polish electors to vote for his position. Besides the offer of money and rights he even considers war efforts in case his wishes are not fulfilled. Clearly, a deeper and more profound historical analysis and contextualization of the revealed content in the diplomatic letters by historians is needed in future work. To allow this, we uploaded the complete decipherments of all of the discussed letters to the DECODE database.

Acknowledgments

This work was supported by the Swedish Research Council, grant 2018-06074. We would like to thank our DECRYPT project colleagues Crina Tudor, for managing the work on the transcriptions, and Bernhard Esslinger for valuable feedback on our work. Moreover, we are very grateful to Leopold Auer for important references on the historical contextualization he shared with us. Lastly, we would like to thank the experts from the State archive of Vienna for their fruitful comments on the decipherment.

References

Christoph Augustynowicz. 2001. *Die Kandidaten und Interessen des Hauses Habsburg in Polen-Litauen während des Zweiten Interregnums 1574-1576*. WUV-Univ.-Verl., Wien.

András Dudith and edited by Catharina Kotońska. 1998. *Epistulae 4: 1575*, volume 13,4 of *Bibliotheca scriptorum medii recentisque aevorum: Series Nova*. Akadémiai Kiadó.

Hildegard Ernst. 1992. Geheimschriften im diplomatischen Briefwechsel zwischen Wien, Madrid und Brüssel 1635–1642. *Mitteilungen des Österreichischen Staatsarchivs*, 42:102–126.

Nils Kopal and Michelle Waldispühl. 2021. Deciphering three diplomatic letters sent by Maximilian II in 1575. *Cryptologia*, pages 1–25.

Nils Kopal. 2018. Solving Classical Ciphers with CrypTool 2. In *Proceedings of the 1st International Conference on Historical Cryptology HistoCrypt 2018*, 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.

Benedek Láng. 2020. Was it a Sudden Shift in Professionalization? Austrian Cryptology and a Description of the Staatskanzlei Key Collection in the Haus-, Hof-und Staatsarchiv of Vienna. In *Proceedings of the 3rd International Conference on Historical Cryptology HistoCrypt 2020*, pages 87–95. Linköping University Electronic Press.

Mathias Niendorf. 2006. *Das Großfürstentum Litauen. Studien zur Nationsbildung in der Frühen Neuzeit (1569-1795)*. Harrassowitz Verlag, Wiesbaden.

Maria Rhode. 1997. *Ein Königreich ohne König. Der kleinpolnische Adel in sieben Interregna*. Deutsches Historisches Institut Warschau. Quellen und Studien. Harrassowitz, Wiesbaden.

Felicia Roşu. 2017. *Elective monarchy in Transylvania and Poland-Lithuania, 1569-1587*. Oxford University Press, Oxford, 1st edition.

Peter Wiesinger. 2012. Bairisch-österreichisch – Die Wiener Stadtkanzlei und die habsburgischen Kanzleien. In Albrecht Greule, Jörg Meier, and Arne Ziegler, editors, *Kanzleisprachenforschung. Ein internationales Handbuch*, pages 415–439. de Gruyter, Berlin.