Decipherment of a German encrypted letter sent from Sigismund Heusner von Wandersleben to Axel Oxenstierna in 1637

Michelle Waldispühl
University of Oslo
Norway
michelle.waldispuhl@ilos.uio.no

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

Abstract

We present our work on an encrypted letter from the Thirty Years' War written by the ally of the Swedish Empire, Sigismund Heusner von Wandersleben in 1637 and sent from Kassel to the Swedish High Lord Chancellor Axel Oxenstierna. We describe our analysis of the ciphertext including information on the cipher type, the process of cryptanalysis and challenges for the decipherment. We include the edition of the letter in the current state of decipherment and summarize its content.

1 Introduction

It is not unusual that encrypted sources are stored in archives without having been deciphered. It is a laborious process to decrypt historical ciphers and oftentimes, historians and archivists working with these documents do not have the resources to perform a cryptanalysis of unknown ciphers. This fact may lead to sensational finds such as the recent discovery of unknown letters by Mary Stuart in the Bibliothèque Nationale de France (Lasry et al., 2023). For cryptanalysts interested in historical ciphers, searching archives systematically for undeciphered material is not always straightforward. However, with the help of specific search entries, such as ”undeciphered”, ”unknown writing”, and more effectively, by talking to experienced archivists, such documents can be found (Megyesi et al., 2024). Assisted by computer-based tools such as those provided by the DECRYPT project[1] undeciphered documents can be cryptanalyzed and deciphered on the own computer in a (semi-)automatic way.

In this brief paper, we present the decipherment and cryptanalysis of an encrypted letter from the Swedish National Archives, which has not been deciphered before. It is a letter sent by Sigismund Heusner von Wandersleben, an ally of the Swedish Empire, to the Swedish High Lord Chancellor, Axel Oxenstierna, in 1637.

2 The letter

The letter is three pages long and includes cleartext in German and ciphertext. Additionally, there is an attachment to the letter also including ciphertext passages. We show the first page in Figure 1; for the other pages see the entry in the DECODE database (Heusner von Wandersleben, Sigismund, 1637).

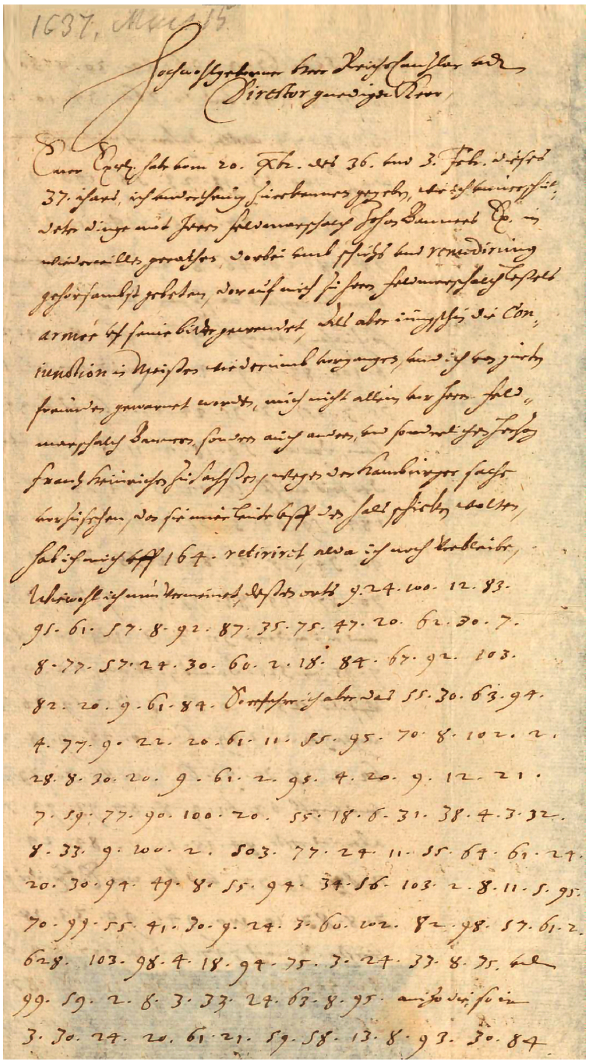
The document is stored at The Swedish National Archives in the Oxenstiernska samlingen, volume E 622 A. It is included in a collection containing 14 letters written by Sigismund Heusner von Wandersleben in the years 1632–1638. Only this one letter is encrypted. The ciphertext was collected in fieldwork by Beáta Megyesi and uploaded to the DECODE database. We ordered digitations of all 14 letters from the Swedish National Archives.

3 The cipher

The encrypted passages are written in a homophonic substitution cipher using digits as ciphertext code elements. We have identified 85 homophones for the plaintext alphabet letters. The homophonicity is uneven with a maximum of eight homophones for the letter 'e' and a minimum of one code element for the letters 'k' and 'p'. The digits used as code elements for the alphabet letters range between 4 and 202. In the ciphertext, each code element is separated using dots.

In addition to the encoding of the alphabet letters, there is also a nomenclature in use where three-digit code elements encode lexical plaintext elements. From several syntactic contexts we can deduce that we here mainly have to do with place

[1] www.de-crypt.org (Megyesi et al., 2020).



1637, Mai 15

[illegible]

[illegible] hab ich mich vff 164. retiriret, [illegible]

[illegible] 9. 24. 100. 12. 83.
95. 61. 57. 8. 92. 87. 35. 75. 47. 20. 62. 30. 7.
8. 77. 57. 24. 30. 60. 2. 18. 84. 67. 92. 103.
82. 20. 9. 61. 84. [illegible] 55. 30. 63. 94.
4. 77. 9. 22. 20. 61. 11. 85. 95. 70. 8. 102. 2.
28. 8. 30. 20. 9. 61. 2. 95. 4. 20. 9. 12. 21.
7. 59. 77. 90. 100. 20. 55. 18. 6. 31. 38. 4. 3. 32.
8. 33. 9. 100. 2. 503. 77. 24. 11. 55. 64. 61. 24.
20. 30. 94. 49. 8. 55. 94. 34. 56. 103. 2. 8. 11. 5. 95.
70. 99. 55. 41. 30. 9. 24. 3. 60. 102. 82. 98. 57. 61. 2.
62. 8. 103. 98. 4. 18. 94. 75. 3. 24. 33. 8. 35. [illegible]
99. 59. 2. 8. 3. 33. 24. 63. 8. 95. [illegible]
3. 30. 24. 20. 61. 21. 59. 58. 13. 8. 93. 30. 84.

Figure 1: Page 1 of Heusner von Wandersleben's letter from 1637. (Heusner von Wandersleben, Sigismund, 1637)

names and personal names, e.g., the passage 'hab ich mich vff 164. retiriret' (*I have withdrawn myself to* 164.) on page 1. The complete key can be found in the entry for the record in the DECODE database (Heusner von Wandersleben, Sigismund, 1637).

4 Transcription

We transcribed the collection of 14 letters using the automatic text recognition tool *Transkribus* (https://readcoop.eu/transkribus/, accessed 25 September 2023). The decision for this tool lied in the high amount of cleartext in German "Kurrentschrift" for which Trankribus' transcription models are well trained. Furthermore, the cipher alphabet contains only digits which is a symbol set also covered by Transkribus' models — in contrast to other rare scripts used in e.g. the Copiale cipher. For these symbol sets, *Transcript Tool* has been developed (Szigeti and Héder, 2022) and is a more suitable choice.

The transcription output provided by the Transkribus tool was manually validated, and special care was taken to correct any mistranscribed digits in the encrypted passages. Subsequently, the ciphertext was extracted from the first letter to further process for cryptanalysis.

5 Cryptanalysis

Due to the high number of distinct code elements, we hypothesized that the cipher is homophonic. Since the cleartext passages were written in German, we assumed that the plaintext language was also German, a hypothesis that was confirmed during the cryptanalysis. We cryptanalyzed the letter using two components from the cryptanalysis tool CrypTool 2 (CT2) (Kopal, 2018): (1) the Homophonic Substitution Analyzer (HSA) (Kopal, 2019), which enables to perform (semi-)automatic cryptanalysis, and (2) the Substitution component, which allows for the decryption of a given ciphertext when the key is (partially) known. Initially, we utilized the HSA's automatic cryptanalysis algorithm, which, after several restarts, yielded partially correct words. Subsequently, we iteratively refined the generated output and restarted the algorithm to further enhance the automatic discovery of more plaintext segments. Additionally, we performed a frequency analysis in CT2 on the code elements. This allowed to identify the frequency distribution of the code elements, e.g., the two most frequent represent the letter 'e' (despite the high amount of homophones) and code elements occurring only once are candidates for nomenclature elements.

5.1 Close-reading and writer-specific dictionary

After the first round of cryptanalysis, we reintegrated the decrypted passages into the cleartext passages and applied a manual close-reading method. First, obvious false letters were corrected, i.e., in the passage HERRUNDKNECIT *Herr und Knecht* 'master and servant' where the last I must be H. After several rounds of further improving the key applying this method, the homophonic cipher could be broken entirely.

Our plan to incorporate a writer-specific dictionary based on Heusner Wandersleben's other 13 letters in order to find his specific spelling patterns turned out not to be useful in our analysis because the material consisting of 4,067 tokens was too limited.

5.2 Search for the original cipher key

Upon deciphering significant parts of the homophones and subsequently revealing portions of the key, we searched for the original key. Since the cipher has similarities with other keys used in Swedish correspondence in the 30 Years' War, such as the Camerarius key or the Beaumont key (Stålhane, 1934; Waldispühl, in press), we examined the documentation of seventeenth-century keys from the Swedish National Archives in the DECODE database. We also reviewed keys from the 1600s in the Hesse State Archives based on the fact that the letter was sent from Kassel, Germany. Sometimes, one is fortunate enough to find the original key (Kopal and Waldispühl, 2022), but in this case, we were not. That is why we have not been able to decipher the nomenclature elements of the cipher.

5.3 Challenges during the decipherment

The ciphertext contained a high number of homophones relative to its length, complicating the cryptanalysis. For instance, the letter 'e' is represented by seven homophones. Some homophones occurred only once or twice in the whole text, which was problematic for automatic decryption. However, this challenge could be met by manual cryptanalysis. An open problem is the absence of a key for the nomenclature elements which keeps them indecipherable. The lack of punctuation and word separation in the ciphertext obscures syntactic structures, complicating sentence delineation and interpretation initially. Furthermore, in historical alphabets, I/J and U/V are not separated and share identical code elements. Since CT2 uses the modern alphabet as a starting point in the automatic analysis, the analyzer has to decide either to use e.g. U or V, and based on the decision, half of the words are decrypted in a "wrong" way (Waldispühl et al., in press). Lastly, the key seems to show a certain pattern in how the code elements are distributed for the plaintext letters, i.e., 12-A, 11-C, 10-B, 9-D. However, we did not fully understand the system to exploit it for cryptanalysis.

6 Decrypted letter

In the following, the plaintext is rendered in capital letters and remaining undeciphered nomenclature code elements are given as they appear in the original text. To facilitate reading, word separators are introduced in the plaintext. Words followed by a question mark are cleartext passages difficult to read.

```
  Page 1:  1637, Mais-15
Hochwohlgeborner Herr Reichchanzlar
vndt Director gnediger Herr
Eurer Excell.  habe vom 20.  Xmbr.
des 36.  vnd 3.  Febr.  dieses 37.
ihars ich vnderthenig zuerkennen
gegeben, wie ich vnuerrichtetdeter
dinge mit Herrn Feldmarschalch Johan
Banners Ex.  in wiederwillen gerathen,
darbei vmb schutzs vnd remedirung
gehorsambst gebeten, darauf mich zu
herrn Feldmarschalch Leßels armée
vf seine bitte gewendet, Als aber
iüngsthin die Coniunction in Meißen
wiederumb vorgangen, sond ich von
gueten freunden gewarnet worden, mich
nicht allein vor herrn Feldmarschalch
Bännern, sondern auch anderen, vnd
sonderlichen Hern frantz heinrichen
zu sachßen, wegen der Hamburger sache
vorzusehen, da sie mier leute vff den
hals schicken wolten, hab ich mich
vff 164.  retiriret, alda ich noch
verbleibe, Wiewohl ich nun vermeinet,
deßen orts DIE ALTE DEUOTION GEGEN DIE
CRON ZU FINDEN. So erfahre ich aber
das HERR UND KNECHT SEHR GEENDERT UND
AM GANZEN HOFE AUSSER DER 503.  NICTT
EINER MEHR UFFRECHT SCHWEDISCH IA DER
628.  FAUORISIREI vnd CARESRIRET aizo
die so in SEINEM ABWESEN

  Page 2:  dem 503.  ZUWIEDER GEWESEN
vnd die 764.  UBERGEBEN wollen, daher
ich mich nicht wenig Verwundert wie
L.EWOLFF DERORTEN NEGOCIIREN SONNEN
deme es furwahr an nottieftigen
vnderhalt, in?  sogar das ich darfur
erschrocken, höchlichen gebracht?, UON
EINEM FELDZUG wirdt geredet, WOHIN IST
STILL. es kan aber nichts großes sein,
dan die FORCE nicht alda, vnd man der
```

Zeit nicht BASTANT 808. 385. 184. AUS DEM LANDT ZU TREIBEN da 503. SOLL IN DAS FELD vnd ein anderer AUS DEM LANDT in 321. damit ist es ein KUCHEN Vff die 255. BESTALLUNG ingleichen die 289. GELDER machet man GROSSES HERANTZ vnd viehl REDENS UON. Es ist aber das erste NOCG NICHT CLAR vnd kan was E. Ex. die sache mit SELBER CRON dero hohen verstandt nach 747. vnd den 617. RECHT IM DIRECTORIO FASSEN schon alles dergestalt ge-

Page 3: machet werden, das man DOCH DIE CRON 708. SUCHEN vnd von derselben DEPENDIREN UND BITTEN muss von deren MAN SICH SONSTEN AUSZUHALFETERN GEMEINET Wegen des andern ist kein vberflues, vnd erfolget sparsam genug, das sich also die sachen wohl geben, Euer Ex. habe meiner schuldigkeit nach ich dieses mit wenigen gehorsamlichen anfuegen wollen, die ich des allerhöchsten schvzs? vnd dero zu beharrlich gnaden mich vnderthenig empfehle vnd dero resolution mit sachßen erwarte, Vol. CASSEL den 15. May 1637. Eurer Excelz. Werthiger gehorsamer diener 384.
ich habe mich des EWOLFREN seines Comptorii? et?

Page 4: Man hat hier in der aller größen geheimb etlich 385. CENTNER METALLISCHE SPEISSE ZUSAMMEN GESCHMELZET vnd solche verdecket auf 147 gefüret, daselbst etliche schon hierzu gemachte STUCKE ZU TAUSCHEN vnd werden mit dem UFFBRUCH wie ich in vertrauen vernommen den nechsten sich eihlen vndt ALLE ABWERTS GEHEN. Alhier wie ich Vermercke wirdt IOHAN UON UFFELN COMMENDANT 571. GUNTEROT aber GEHET MIT ANDEREN ZU FELDT varleßet sich mercken, ob seye etwas UON 703. ALHIER wie auch ANDERE vnd haben GROSSE HOFFNUNG
dieses wird gleich bey schließung meines schreibens ahn? EWOLFFEN bey einem gueten ort geschrieben.

7 Some historical context and summary of the content

The author of the letter, Sigismund Heusner von Wandersleben, served as a Swedish counselor and general war commissioner 1631–1638. Born 1592 in Coburg, he entered a diplomatic career after his studies first as a counselor of Herzog Wilhelm IV. of Sachsen-Weimar and then as a Swedish General War Commissioner (Warlich, 2011).

The letter is addressed to Axel Oxenstierna who served as the High Lord Chancellor of Sweden before, during, and after the Thirty Years' War, from 1612 until his death in 1654.

The text discusses various diplomatic and military matters in spring 1637, i.e., the time when the Swedish army had to flee North to Pommern after they had defeated the Saxon army in Wittstock in autumn 1636 (Murdoch et al., 2012). Heusner von Wandersleben mentions personal conflicts with leaders such as Johan Banér, Franz Heinrich of Saxony, and others. There are concerns about potential threats. He also talks about his own actions, including a retreat, and he seeks guidance and support of Oxenstierna. Towards the end, there are discussions about military forces, territories, and financial matters.

8 Conclusion

We have presented the methods and results of our partly successful decipherment of a hitherto undecrypted letter written by Heusner von Wandersleben to Oxenstierna in 1637. Our work lays the ground for historians to further analyze the letter's content and contribute contextual knowledge in order to address the undeciphered nomenclature elements. The fact that the nomenclature elements remained obscure to us means in turn that they make the cipher secure. However, the switching between cleartext and ciphertext had an opposite effect and contributed significantly to our successful cryptanalysis. Another aspect strengthening the cipher's security is its high number of homophones that were varied extensively in the ciphertext. Further research into a possible systematic ways of the homophone variance as well as the patterns of cleartext-ciphertext switching would reveal more knowledge about how keys were applied in practice.

Acknowledgments

We are grateful to our colleagues in the DECRYPT project for valuable feedback on our ongoing work. We want to thank especially Beáta Megyesi for collecting the ciphertext letter and sharing it with us. We are also indebted to the archivists at the Swedish National Archives for digitizing and openly sharing their materials. This work has been supported by the Swedish Research Council, grant 2018-06074, DECRYPT – Decryption of Historical Manuscripts.

References

Heusner von Wandersleben, Sigismund. 1637. The National Archives of Sweden, Oxenstiernska samlingen, volym E 622 A, fols. 1-4, DECODE ID 4332, link: https://de-crypt.org/R/4332.

Nils Kopal and Michelle Waldispühl. 2022. Deciphering three diplomatic letters sent by Maximilian II in 1575. *Cryptologia*, 46(2):103–127.

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.

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, Norbert Biermann, and Satoshi Tomokiyo. 2023. Deciphering Mary Stuart's lost letters from 1578-1584. *Cryptologia*, 47(2):101–202.

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.

Beáta Megyesi, Alicia Fornés, Nils Kopal, Benedek Láng, Michelle Waldispühl, Vasily Mikhalev, and Bernhard Esslinger. 2024. Historical Cryptology. In Bernhard Esslinger, editor, *Learning and Experiencing Cryptography with CrypTool and SageMath*, pages 97–138. Artech House, Norwood.

Steve Murdoch, Kathrin Margarete Gertrud Zickermann, and Richard Adam Marks. 2012. The Battle of Wittstock 1636: Conflicting Reports on a Swedish Victory in Germany. *Northern Studies*, 43:71–109.

Henning Stålhane. 1934. *Hemlig skrift. Coder och chiffrermaskiner*. Lindfors, Stockholm.

Ferenc Szigeti and Mihály Héder. 2022. The TRANSCRIPT tool for Historical Ciphers by the DECRYPT project. In *Proceedings of the 5th International Conference on Historical Cryptology, HistoCrypt22*, pages 208–211.

Michelle Waldispühl, Beáta Megyesi, Nils Kopal, and Alicia Fornés. in press. Grapholinguistic features of historical ciphers and challenges for computer-based transcription and cryptanalysis. In Kerstin Kazzazi, Michael Schulte, and Gaby Waxenberger, editors, *From the Maya Script to the Germanic Runes – Case Studies on the Typology of Scripts and Research on Writing Systems*. Reichert, Wiesbaden.

Michelle Waldispühl. in press. Verschlüsselte Briefe im Schwedischen Reich: Mehrsprachigkeit und Geheimschrift während des Dreißigjährigen Kriegs. In Dessislava Stoeva-Holm and Michael Prinz, editors, *Praktiken der Mehrsprachigkeit im Schwedischen Reich (1611–1721)*. Harrossowitz Verlag.

Bernd Warlich. 2011. Der Dreißigjährige Krieg in Selbstzeugnissen, Chroniken und Berichten. Heusner von Wandersleben, Sigismund, link: https://www.30jaehrigerkrieg.de/heusner-von-wandersleben-sigismund-2/.