

Solving a Mystery From the Thirty Years' War

Karel Rabenhaupt ze Suché's Encrypted Letter to Landgravine Amalie Elisabeth

Eugen Antal

Slovak University of
Technology in Bratislava
Slovakia
eugen.antal@stuba.sk

Pavol Zajac

Slovak University of
Technology in Bratislava
Slovakia
pavol.zajac@stuba.sk

Jakub Mírka

The State Regional Archives
in Pilsen
Czech Republic
mirka@soaplzen.cz

Abstract

In 2013, an unsolved encrypted message was presented in a Czech cryptogram solving competition. This message was sent by Karel Rabenhaupt ze Suché to Amalie Elisabeth von Hanau-Münzenberg, Landgravine of Hessen-Kassel at the end of the Thirty Years' War. During the following years, many crypto enthusiasts tried to solve the cipher without success. Finally, in 2020, the authors of this paper were able to reveal the content of the encrypted message. Here we present the decryption of the encrypted message, including the historical background of the communication. We also present an analysis of the used encryption system.

1 Introduction

The history of the European nations is deeply interconnected. European aristocratic families played crucial roles in military and international diplomacy. Through a web of correspondence, the historical mosaic can be reconstructed and presented in various aspects.

Archives of European aristocratic families still contain many unsolved secrets. In our project, we focus on historical archives of families who lived in the former Austro-Hungarian Monarchy. The nobility had strong ties in the whole Central European region. As such, the study of encrypted correspondence found in any middle-European archive is not self-contained, but instead requires additional materials from many different archives in multiple countries (Hungary, Austria, Czechia, Poland, Germany, ...).

In the present paper, we focus on a story of a specific encrypted message. We want this story to demonstrate the need for interconnected research in historical cryptography, and the need to have

a platform for efficient sharing of encrypted (and decrypted) materials and keys.

2 Historical Background

Our focus is an encrypted message created during the Thirty Years' War in the Rhine region and now deposited in The State Regional Archives in Pilsen (SOA v Plzni, FA Trauttmansdorff, inv. nr. 125) in the Czech Republic.

The encrypted message is a part of the correspondence of Karel Rabenhaupt ze Suché with Amalie Elisabeth von Hanau-Münzenberg, Landgravine of Hessen-Kassel. In this section, we briefly summarize the historical background of the sender of the encrypted message.

Karel Rabenhaupt ze Suché (see Figure 1), was born in 1604 as the son of the Bohemian Protestant nobleman Zikmund Rabenhaupt (Robmháp) ze Suché, the owner of the land estates Lichnice and Třemošnice,¹ and Kateřina Žehušická z Nestajova (Engelbrecht, 1989; Genealogical-heraldic collection of Wunschvitz, inv. nr. 921). In 1620 he took part in the defense of Bautzen against the army of John George II, Elector of Saxony. After the defeat of the Bohemian Revolt on Bílá Hora he emigrated to the Netherlands because of his faith. He began to study fortress construction at the Leiden University (Woringer, 1913; Engelbrecht, 1989).

He fought in the Dutch army, and he was promoted to the rank of lieutenant in 1627 after the siege of Groenlo. Later on, he became famous in his military service. He joined William V, Landgrave of Hessen-Kassel. From 1633 he was the commander of the Schaarkopf cavalry regiment. After the death of William V in 1637, **Amalie Elisabeth** (see Figure 2) took over the government as the regent of William VI (Engelbrecht, 1989;

¹Town in the Czech Republic near Pardubice, approx. 90 km eastwards from Prague.



Figure 1: Karel Rabenhaupt ze Suché (Wikipedia Commons, 2020)

Warlich, 2021). In the 1640s he was engaged in the fights on the left bank of Rhine.

After the Thirty Years' War Rabenhaupt stayed in Hessian service and gained high military posts there. In 1668 he left the service and moved to his estates in the Netherlands. Rabenhaupt became a national hero in the Netherlands in 1672, after defending the city of Groningen.² He not only defended Groningen against the Münster army, but he was also able to break through and recapture one of the most modern and powerful fortresses of its time, Coevorden. He became Coevorden's governor. In 1673 he was promoted to the status of a baron by the Emperor, now an ally of the Netherlands, for his services in defending the Netherlands. He died on August 12, 1675 (Woringer, 1913; Engelbrecht, 1989).

2.1 Rabenhaupt on the Rhine

In 1640, Count Kaspar von Eberstein became the commander-in-chief of the army of Hessen-Kassel. In the same year, Rabenhaupt, in Eberstein's presence, conquered the town of Kalkar, which lies on the lower Rhine near the border with

²The Dutch province of Groningen offered Rabenhaupt the position of the commander of the army.



Figure 2: Amalie Elisabeth von Hanau-Münzenberg, Landgravine of Hessen-Kassel (Wikipedia Commons, 2020)

the Netherlands. From there he made raids along the Rhine to the south (Warlich, 2021).

In 1642, the Protestants conquered Kempen, Linn, and Neuss. The city of Neuss, near Düsseldorf, fell to the Hessians. The same year, Rabenhaupt became military commander of Neuss, and made the city his base for military actions, especially on the left bank of the Rhine. On the opposite side, one of the important Imperial strongholds in this area was the fortified city of Zons, which belonged to the Electorate of Cologne, and was located about 14 km southeast of Neuss. In the following years, neither side of the rivals gained a significant advantage, and the fighting devolved into smaller skirmishes, partial raids and tactical shifts (Löhrer, 1840). Rabenhaupt was captured in April 1644 but was released again in the summer (at the latest). In the autumn of the same year, Eberstein died, and after

his death, Johann von Geysso temporarily became the head of the Hessian troops (Warlich, 2021).

In 1645, Rabenhaupt tried unsuccessfully to conquer Zons (Woringer, 1913; Warlich, 2021). He was more successful in the autumn when the Hessian army managed to conquer the city of Euskirchen, which belonged to the Duchy of Jülich-Berg and was located about 60 km south of Neuss. From there, the Hessians controlled the entire adjacent area (Hofmann, 1882).

At the beginning of 1646, Colonel Rabenhaupt was appointed major general³ (HLA-HStAM, Best. 4 h, Kriegssachen, Nr. 1810). The Hessian army on both sides of the Rhine was again engaged mainly in smaller battles. During February, Rabenhaupt managed to occupy numerous settlements in Jülich-Berg and later moved to the right bank of the Rhine for a time, as he was to be in Wipperfürth on March 2. From the west, however, the allied French army approached, led by Marshal Henri de La Tour d’Auvergne de Turenne, and from the east and north, the Swedes. The two armies tried to unite. The enemy forces were led by Imperial General Peter Melander von Holzappel, who changed sides during the war. It is interesting that until 1640 he was the commander in chief of the Hessian army. After his resignation, he was replaced by the aforementioned Count Kaspar von Eberstein. Melander’s deputy was Otto Christoph von Sparr. He was also at this time the main opponent of Rabenhaupt, and also successfully prevented Marshal de Turenne from crossing the Rhine (von Schroetter, 1899; Warlich, 2021).

Rabenhaupt has been preparing for the siege of Zons since the summer or maybe has even besieged it directly for some time, as Rommel (1843) states. In early July, Rabenhaupt made a military move against Bonn to ease the pressure on Euskirchen. Rabenhaupt has described this successful operation in details in his report, which was preserved in a manuscript in the library of Wolfenbüttel (Löhner, 1840; HAB, Cod. Guelf. 11.8 Aug. 2°, ff. 368-369).

In this situation, an encrypted letter, which is the main subject of this article, was created. Thanks to its decipherment (see Section 5), we know that Rabenhaupt’s main goal at this time was indeed the conquest of Zons and that he probably hoped for the help of Marshal de Turenne (SOA in Pilsen, FA Trauttmandorff, inv. Nr. 125). We know from

other sources that de Turenne eventually refused to help Rabenhaupt with the siege of Zons. Apparently, he did so because it would keep him from the main task of uniting with Swedish troops, in which he succeeded at the turn of July and August 1646. Although he could not cross the Rhine in the south, he went north to Wesel and met the Swedes in Hessen. This operation was very swift. Sources show, that while he was supposed to be at Ahrweiler on July 12, he had managed to cross the Rhine at Wesel on July 15. Even after de Turenne’s departure from the area, Rabenhaupt continued to dominate the left bank of the Rhine. General Melander, therefore, tried to get the Hessians from the Rhine by making a diversionary assault against their capital Kassel. However, at the end of September, Rabenhaupt attacked Zons again, forcing Melander to return (von Rommel, 1843; von Schroetter, 1899; Salm, 1990).

The siege of the city began on September 24, 1646, and on September 28, heavy artillery was launched, which greatly damaged the city. According to some sources, the walls had already been broken and negotiations for a possible surrender had been initiated. On October 6, however, Melander crossed the Rhine and the Hessians had to withdraw to Neuss. Melander then went on to conquer Euskirchen. Later in October, Rabenhaupt was reported to be with Geysso in Wesel. As early as 1647, Rabenhaupt operated in Neuss, but was then assigned to General Königsmarck’s Swedish army and left with him. In May he was already with Königsmarck near Vechta in northern Germany (Wassenberg, 1647; von Rommel, 1843; Hofmann, 1882; Warlich, 2021).

The area of Karel Rabenhaupt ze Suché’s operations on the Rhine is marked in Figure 11 (in the Appendix).

3 An Unsolved Cryptogram From the Thirty Years’ War

In 2013 an unsolved encrypted message was presented in a Czech journal (Mírka, 2013) as part of a cryptographic competition. Here, we summarize the most important facts known at that time:

The object of the competition was an encrypted message (see Figure 12), which is now deposited in The State Regional Archives in Pilsen (SOA v Plzni, FA Trauttmandorff, inv. nr. 125). The encrypted message was a part of a correspondence of Karel Rabenhaupt ze Suché with Amalie Elisabeth

³General-Wachtmeister

von Hanau-Münzenberg, Landgravine of Hessen-Kassel, from 1646.

Beside the encrypted message, a second (unencrypted) message was found.

These two messages were intercepted near Arnsberg and were never delivered. After the interception, the encrypted message was directly investigated by the military commander Alexandre de Bournonville, but he was unable to solve it. Alexandre de Bournonville, on July 20, sent a copy of the messages from Hamm to Maximilian von Trauttmansdorff, who was the envoy of Emperor Ferdinand III to peace talks in Münster. He hoped that somehow Maximilian von Trauttmansdorff would be able to find the corresponding encryption key.

The encrypted message is dated to 11 (or 13)⁴ of June 1646. The second (not encrypted) is dated July 13, 1646. Both messages were written in German language and were sent from Neuss. The date of the encrypted message is probably not correct. Due to the fact that both messages were intercepted together in the same place, it is more possible that the encrypted message was also written in July. It is also probable that Alexandre de Bournonville would not have sent the report about the encrypted message a month after the interception. So it is more probable that Bournonville's scribe made a mistake copying the message (Mírka, 2013; SOA v Plzni, FA Trauttmansdorff, inv. nr. 125).

The unencrypted letter tells about movements of Marshal de Turenne's troops, that were presumably referenced in the previous letter sent on July 11th. The unencrypted letter also references other army movements in the Rhine valley around Zons and Wesel. The encrypted letter contains cleartext parts, but the important information is encrypted with numbers and symbols. The preliminary analysis points to the possibility that a nomenclator encryption scheme was used.

4 Nomenclator Encryption System

A nomenclator is a special encryption system consisting of several different simpler encryption systems used together during the encryption.

⁴11 is rewritten to 13 in the document. Supporting evidence for July 13 is also that according to sources, de Turenne was at Ahrweiler on July 10, and thus could not have been at Euskirchen, as mentioned in the letter.

A nomenclator⁵ mostly contains a monoalphabetic or homophonic substitution in a combination with bigram and/or trigram substitution, code word substitutions and nulls (Mírka, 2012; von zur Gathen, 2015; Antal and Mírka, 2018). The basic encryption key of a nomenclator is frequently represented in a table. Additional codes used in a nomenclator can grow its size to several pages. The cipher text alphabet is very often represented by numbers (mostly due to the large number of possible code words and homophones).⁶ In addition to digits/numbers, special symbols/glyphs were used as well⁷ (Antal and Mírka, 2018; Dunin and Schmech, 2020). This type of encryption was very popular and was used for a long time period from the fourteenth to the nineteenth century (Dunin and Schmech, 2020; Meister, 1906; Lasry et al., 2020).

After taking a closer look at some available nomenclator constructions (Mírka and Vondruška, 2013; Antal and Mírka, 2018; Dunin and Schmech, 2020) we can conclude that many nomenclators were poorly designed: cipher text numbers (or letters) were assigned in an alphabetical or numerical order (see Figures 3, 4 and 5). The nomenclator key could be also used incorrectly (Dunin and Schmech, 2020). Another possible drawback of some nomenclator keys was that they have been used for a long time period, and have been reused by several different persons. On the other hand, this means that some nomenclator copies have survived in various archives.

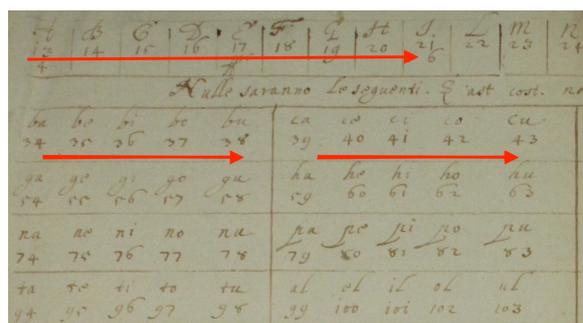


Figure 3: Poor nomenclator design. SOA v Plzni, FA Windischgrätz, inv. nr. 1403.

⁵Based on the authors' experience from research in archives.

⁶In many cases, a special separator is required such as dot, comma, or space between cipher text units. This separator is used to correctly split the digits into ciphertext numbers.

⁷Mostly for the monoalphabetic/homophonic substitution parts, but there are also examples of nomenclators with glyphs representing code words.

A	B	C	D	E	F	G	H	I	K	L	R
1500	1600	1700	1800	1900	2000	2100	2200	2300	2400	2500	2600
62	63	64	65	66	67	68	69	70	71	72	73
74	75	76	77	78	79	80	81	82	83	84	85
86	87	88	89	90	91	92	93	94	95	96	97
98	99	100	101	102	103	104	105	106	107	108	109
110	111	112	113	114	115	116	117	118	119	120	121

A	B	C	D	E	F	G	H	I	K	L	R
1500	1300	1200	1100	1000	900	800	700	600	500	400	300
57	58	59	60	61	62	63	64	65	66	67	68
69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90	91	92
93	94	95	96	97	98	99	100	101	102	103	104
105	106	107	108	109	110	111	112	113	114	115	116
117	118	119	120	121	122	123	124	125	126	127	128

Figure 4: Poor nomenclator design (homophonic substitution part). HLA-HStAM Best. 4d Nr. 1218.

A	B	C	D	E	F	G	H	I	K	L	R
1500	1300	1200	1100	1000	900	800	700	600	500	400	300
57	58	59	60	61	62	63	64	65	66	67	68
69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90	91	92
93	94	95	96	97	98	99	100	101	102	103	104
105	106	107	108	109	110	111	112	113	114	115	116
117	118	119	120	121	122	123	124	125	126	127	128

Figure 5: Poor nomenclator design (homophonic substitution part). HLA-HStAM Best. 4d Nr. 1227.

5 The Solution of the Cryptogram

The cryptogram was made publicly available in 2013 as a part of a Czech cryptogram solving competition. Antal and Zajac (2013) tried to solve it within the competition but without success. Despite to additional popularization of the encrypted message in conferences and blogs, nobody was able to directly solve this mystery. In fact, a correctly used nomenclator scheme can remain unbreakable even with modern computing power, especially if the analyzed cipher text is short. However, there was still a hope that the nomenclator key may have been preserved in some archive.

We have searched for additional documents related to Karel Rabenhaupt in the Hessian State Archives in Marburg. Unfortunately, the studied collections did not contain nomenclator keys. After the cipher challenge was published on Klaus Schmech's site (Klausis Krypto Kolumne, 2020), one of his readers (using the Thomas nickname) directed us to the HStAM 4d collection in this archive. The collection contains a lot of different nomenclator keys from the seventeenth and eighteenth century, and as we found out, it also

contains the key that was used to encrypt Rabenhaupt's letter.

In fact, there are three almost identical nomenclator keys, which fit our cryptogram (one of the keys in Figure 13). Two of them have also an inverse key.⁸

To date the keys, we use the fact that they contain notes with names. Probably the first of the series is from 1641 and was created as a new key to communicate with Lieutenant-General Count von Eberstein. In original: "Neuer (=neuer) Clavis Mit dem Herrn General Lieutenant Graven von Eberstein des 4./14. t[en] Aprilis a[nn]o 1641 ufgerichtet (=aufgerichtet)". The second key is probably the updated version of the previous one, where additional "users" of this nomenclator were gradually added (different names written with different handwriting). The first name is von Eberstein ("Clavis mitt H[ern] General Lieut[enant] Graven von Eberstein"), then the added ones: "Herrn Wicqueforten, Herrn Obrist Lieut[enant] von KroBieg, Obersten Karpffen, Herrn Gen[eral] Wachtmeister Geyso". On the third version of the key there is a different name mentioned - Hans Heinrich G#unterode, Court Marshal and Obrist of Hessen-Kassel ("Clavis ahn Herrn Obristen G#unterode").

Interestingly, the name of Karel Rabenhaupt is not present on these keys.⁹ There is also a possibility that there were even more users of this nomenclator than mentioned on the nomenclator itself. Note that the latter story of Rabenhaupt's letter shows that the Emperor's agents were unable to read the encrypted parts of the letter in 1646, and perhaps later. This means that even with multiple users of the key, the key management was relatively secure.

Having found the (correct or related?) nomenclator key, we used it to decipher the encrypted parts of the letter. The obtained result contains dozens of typos/mistakes. Such mistakes can also make potential decryption harder. These mistakes could have been caused either by Rabenhaupt or more probably by a scribe while copying the original document.

After the corrections, the final version of our solution is the following (the deciphered parts in the

⁸We also found another inverse key that fits our cryptogram and that does not belong to the previous ones. So there are six versions of these keys preserved in total.

⁹We have found a different cipher key from 1646 with the name Rabanhaupt, but this one does not fit our cryptogram.

text are marked in bold):

Copia
*Durchleuchtige, Hochgeborne Fürstin, Gnädige Frau. Dießen Morgen empfang ich Andtwortschreiben von **Mareschall de Turenne**, so gestern in **Eusskirchen gewesen undt daherumb gelegen, dass er heute marchiren undt also morgen vor Zoons sich setzen wolte.** Alß mache ich meine Rechnung **fünffzehen Hundert Mann Fuessvolck nebst ein Batterie Stückgeschütz und einen Fewermörsel**¹⁰ undt negst Gottes Hülff **einen kurtzen Proces damitt zu machen**, undt weil[e]n ich gute Hoffnung habe, daß die Aliirten in ihren Vortheil lenger alß andere werden können stehen pleiben, undt vielleicht waß geschehen solle, ehe **der Mareschall dahin kommen kan wird, geschehen sein.** So hette Eu[er] Fürst[lichen] Gn[aden] underthenig zu bitten, die schleunige Verordnung zu thun, daß **di[e] Ostfrieslandsche commendirte Völcker, auch die gelehnete Stückgeschütz zu Wesel mir ausgefolget werden möchten.** Vielleicht möchte ich etwas wichtiges verrichten und gute Winterquartier machen. Eu[er] Fürst[lichen] Gn[aden] hi[e]rmit [Gedelicher] Obhuet empfehlend verpleib
Eu[er] Fürst[lichen] Gnaden underthänig, gehorsahmer, pflichtschuldig Diener Rabenhaupt
Neuß den 13 Juny 1646, ahn die Landtgravin zu Hessen Amalie Elisabet*

We have created a rough translation of the deciphered message to English, presented in Appendix B. The original text is difficult to translate, and without further context, some passages can be interpreted in various ways. We tried to preserve the nuances of the original text to avoid potential shifts in the meaning of the text.

6 Analysis of the Cryptogram

In this section, we revise to and extend the preliminary analysis of the cryptogram from Antal and Zajac (2013), and point out some weaknesses of the used encryption method.

The encrypted message contains both encrypted and unencrypted parts. The whole text consists of 34 rows: 13 rows are fully encrypted, 13 rows are encrypted partially and 8 rows contain only plain text (not encrypted) parts.

¹⁰= Feuermörsel

Rows containing both encrypted and unencrypted passages are very valuable. This property can be useful to guess the content of the encrypted part. As an example, the second row starts with the German sentence "Dießen Morgen empfang ich Andtwortschreiben von ..." (This morning I received a letter of reply from ...) and continues with cipher symbols. From the meaning of this passage, it is clear, that the text should continue with a name of a person. From section 2.1 we know that Rabenhaupt was in Neuss at the time of the writing of the document (in July 1646) and the army of Vicomte de Turenne operated nearby Rabenhaupt. His name is also present in the second (not encrypted document). In fact, the solution of the first encrypted passage is directly "MARESCHALL DE TURENNE" (see section 5).

The encrypted part of the document consists of numbers, letters (uppercase and lowercase), and special symbols/glyphs.¹¹ These units are mostly divided by dots.¹² Dots were commonly used in nomenclators as separator chars. In the document, a dot is the most frequent symbol and really serves as a separator char. The transcription of the cipher text is in Appendix A. After splitting the text by the separator char,¹³ the encrypted part of the document contains 118 unique cipher text units and is 369 symbols/letters/numbers long.¹⁴ There are:

- 145 numbers (51 unique),
- 105 symbols (30 unique),
- 72 lower case and 24 upper case letters (24 unique),
- and 23 double letters (13 unique).

Based on a large number of cipher text units and on the relatively flat frequencies (Figure 6), Antal and Zajac suggested (2013) that the nomenclator consists of a homophonic substitution, bigrams, codes, and nulls. The possible way of solving such

¹¹The first row contains the word *Copia*, the document is probably only a copy of the original document. This is the reason why many transcription errors (typos) occurred during the copy, see section 5.

¹²In some cases the dot separator is missing, but there is a wide space between the cryptogram units so they can be distinguished.

¹³We added several dots in case it was not present to unify the structure of the cipher text.

¹⁴Numbers and double letters are counted as one cipher text unit, e.g. 110, pp.

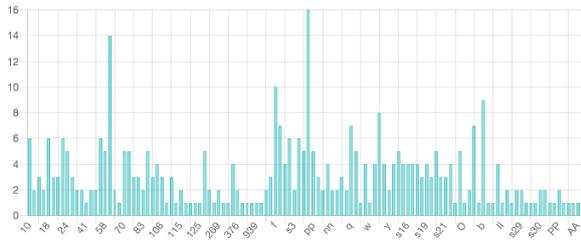


Figure 6: Frequency characteristic of the cipher text

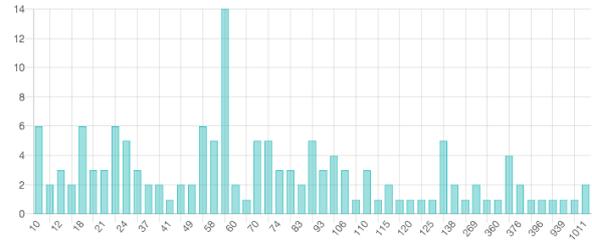


Figure 8: Frequency characteristic of numbers in the cipher text

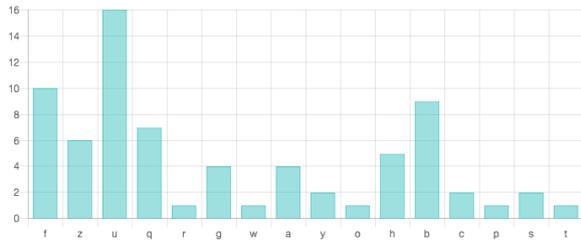


Figure 7: Frequency characteristic of lower case single letters

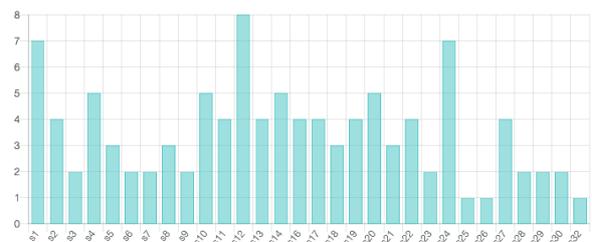


Figure 9: Frequency characteristic of symbols in the cipher text

a complicated nomenclator is to guess/separate the nomenclator sub-ciphers, guess the most frequent cipher text units, or try to find something that was incorrectly used during the encryption.

If we examine the frequency characteristic separately for numbers, symbols, and letters we can find some interesting properties. The frequency characteristics of the lower case letters (Figure 7) is similar to a frequency distribution of a simple substitution (the index of coincidence of these letters is also high). This means it can also be a row in a homophonic substitution table. The letter *u* has the highest frequency and can stand for the plain text letter *e*.

The number frequencies (Figure 8) are relatively flat, only the number 59 has a relatively high frequency. If 59 is also obtained in the homophonic cipher, it can stand for a frequent letter such as *e*. From the symbol frequencies (Figure 9) we were unable to find any useful details.

In (Antal and Zajac, 2013) the authors also investigated the cyclic structure of homophones.

Although the used nomenclator is relatively strong, we can see that there are some mistakes that allowed Antal and Zajac (2013) to correctly guess that

- one row in the homophonic substitution table consist of lower case single letters (Figure 10),

- letter *u* stands for plain text letter *e*,
- number 5 (that is in fact a symbol very similar to number 5) stands for plain text letter *n*,
- number 59 also stands for plain text letter *e*.

Figure 10: Letters in the homophonic substitution table. HLA-HStAM Best. 4d Nr. 1218.

Unfortunately, these suggestions are not enough to solve the cipher by analysis. The used nomenclator key is complicated and was designed carefully. The letters are used as homophones and nulls as well. The numbers are used to encrypt homophones, code words, and nulls. The symbols are used both as homophones and to encrypt common bigrams.

The used homophonic substitution is very strong - each set of homophones (assigned to a plain text letter) consist of 8 to 11 elements and consist of numbers, lower case single letter, upper case double letters, and symbol. The fre-

quency characteristic of the used cipher text elements is flat (except for few elements from the homophones). We expect that to solve such a homophonic substitution an impractically large number of cryptograms would be required.

7 Conclusions

Nomenclator encryption systems were used extensively in European warfare and diplomacy. Some of them were used and designed incorrectly (see section 4), so they could be solved. On the other hand, correctly designed (and used) nomenclators provide strong encryption which is almost impossible to solve correctly.

Our case study shows that historians and historical cryptography enthusiasts have an alternative method of solving encrypted historical documents. We can try to "connect the dots" and search for original keys (or their copies and related documents) in historical archives.

In our present paper, we focused on the story of a specific encrypted message, that resisted classical cryptanalytic attempts. As we have shown in the paper, the nomenclator used in the communication between Karel Rabenhaupt ze Suché and Amalie Elisabeth von Hanau-Münzenberg, Landgravine of Hessen-Kassel was designed carefully (see sections 5 and 6). It contains a strong homophonic cipher, common bigram encryption, code words, and a large selection of nulls. Despite the presence of unencrypted parts between the encrypted parts of the document, the cipher text does not contain enough information for relevant cryptanalysis.

The search for the decryption key was quite complicated as well. The encrypted document was found in the State Regional Archives in Pilsen, Czech Republic. However, the correct nomenclator key was preserved in the Hessian State Archives in Marburg, Germany. This particular situation was caused by the fact that the encrypted message was intercepted during the Hessian war and sent for analysis to Emperor's envoy von Trauttmansdorff, who has stored the (unsolved) letter in his family archive. This situation might not be unique, and archives of one side of a war can contain intercepted messages of the other side, with keys remaining in the opposite archives. Furthermore, documents in family archives were passed down during centuries and moved to different locations.

The goal of our story was to demonstrate the need for interconnected research in historical cryptography. To efficiently analyze and solve historical cryptograms, researchers need to have a platform for efficient sharing of encrypted (and decrypted) materials and keys. We hope that collaboration efforts such as the *DECODE*¹⁵ (Megyesi et al., 2020) database and the *HCPortal Cryptograms*¹⁶ (Antal and Zajac, 2020) database can result in further joint projects and connected open data platforms and tools available for both researchers and crypto and history enthusiast all over the world.

Acknowledgments

This work was supported by grant VEGA 2/0072/20.

We thank Ingo Niebel for his help with the initial search in the Hessian State Archives in Marburg, Klaus Schmeh for publishing the challenge on his blog, Thomas for the pointers, Jiří Kubeš for his help with the translation, Dušan Kováč for his help with the documents from the Herzog August Bibliothek, and Pavel Vondruška, who has initiated the cryptographic challenge leading to this article.

References

- Eugen Antal and Jakub Mírka. 2018. Selected encrypted messages found in Slovak and Czech archives. In *HistoCrypt 2018 Workshop: Solving codes rather than ciphers. Is there a software challenge?*
- Eugen Antal and Pavol Zajac. 2013. Analýza Rabenhauptovho zašifrovaného dopisu (Analysis of Rabenhaupt's encrypted message). In *Crypto-World*, 11-12.
- Eugen Antal and Pavol Zajac. 2020. HCPortal Overview. In *Proceedings of the 3rd International Conference on Historical Cryptology, HistoCrypt 2020*, pages 18 - 20. Linköping University Electronic Press.
- Elonka Dunin and Klaus Schmeh. 2020. Codebreaking: A Practical Guide. Robinson. Great Britain.
- Wilken Engelbrecht. 1989. Flüchtling im fremden Lande. Weißenberger Exulanten in niederländischen Quellen. In *Sborník příspěvků. IV. setkání genealogů a heraldiků*, Ostrava.

¹⁵<https://cl.lingfil.uu.se/decode/database>

¹⁶<https://cryptograms.hcportal.eu>

- Wilhelm Hofmann. 1882. *Peter Melander Reichsgraf zu Holzappel. Ein Charakterbild aus der Zeit des dreißigjährigen Krieges*. Bibliographisch-Artistisches Institut, München.
- George Lasry, Beáta Megyesi and Nils Kopal. 2020. Deciphering papal ciphers from the 16th to the 18th Century. In *Cryptologia*. Taylor & Francis.
- Friedrich J. Löhner. 1840. *Geschichte der Stadt Neuß von ihrer Gründung an bis jetzt, nach gedruckten und handschriftlichen Quellen verfaßt*. Druck u. Verlag von L. Schwann, Neuß: 314–325.
- Beáta Megyesi, Bernhard Esslinger, Alicia Fornés, Nils Kopal, Benedek Láng, George Lasry, Karl de Leeuw, Eva Pettersson, Arno Wacker and Michelle Waldspühl. 2020. Decryption of historical manuscripts: the DECRYPT project. In *Cryptologia*, volume 44, number 6, pages 545-559. Taylor & Francis.
- Aloys Meister. 1906. *Die geheimschrift im dienste der Päpstlichen kurie von ihren anfängen bis zum ende des XVI. Jahrhunderts*.
- Jakub Mírka. 2013. Dosud nevyluštěný dopis českého pobělohorského emigranta Karla Rabenhaupta ze Suché z doby třicetileté války. (Unsolved message of Czech emigrant Karel Rabenhaupt ze Suché from the Thirty Years' War). In *Crypto-World*, 7-8.
- Jakub Mírka. 2012. Raně novoněká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni (Early modern encrypted correspondence in the fonds of the aristocratic family archives in the State Regional Archive in Pilsen). In *Západočeská archivy 2012*, also published in three parts in *Crypto-World*, 11-12/2012, 1-2/2013 and 3-4/2013.
- Jakub Mírka and Pavel Vondruška. 2013. Nomenklátory 17. a 18. století (Nomenclators from the 17. and 18. century). In *Crypto-World*, 11-12.
- Christoph von Rommel. 1843. *Neuere Geschichte von Hessen. Vierter Band*. Verlage von Friedrich und Andreas Perthes zu Hamburg und Gotha, Cassel: 701, 704.
- Hubert Salm. 1990. *Armeefinanzierung im Dreißigjährigen Krieg Der Niederrheinisch-Westfälische Reichskreis 1635-1650*. Aschendorff. Münster: p. 71.
- Klaus Schmeh. 2020. *Klausis Krypto Kolumne (Cipherbrain)* <http://scienceblogs.de/klausis-krypto-kolumne>.
- Friedrich von Schroetter. 1899. Otto Christoph von Sparr, der erste brandenburgische Generalfeldmarschall. *Hohenzollern-Jahrbuch. Forschungen und Abbildungen zur Geschichte der Hohenzollern in Brandenburg-Preußen*, 3: 163–187.
- Joachim von zur Gathen. 2015. CryptoSchool. Springer.
- Bernard Warlich. Der Dreißigjährige Krieg in Selbstzeugnissen, Chroniken und Berichten. Entries: Rabenhaupt, Karl; Sparr zu Trampe, Ernst Georg; Eberstein, Kaspar. Available online (accessed 27. 1. 2021), <https://www.30jaehrigerkrieg.de/>.
- Eberhard Wassenberg. 1647. *Der Erneuerder Teutsche Florus Wassenberg: mit Animadversionem Addition und Correctionen deren in vorigen eingeruckten ungleichen Hystorien verbessert der Wahrheit restituirt und biss Anno 1647 continuirt*. Bey Antoni Hummen, Frankfurt am Main: 692.
- August Woringen. 1913. Ausländer als Offiziere im hessischen Heere. *Hessenland*, 27: 60–61.
- Herzog August Bibliothek /HAB/ (Herzog August Library in Wolfenbüttel), manuscript Cod. Guelf. 11.8 Aug. 2°, ff. 368-369.
- Hessisches Landesarchiv – Hessisches Staatsarchiv Marburg /HLA-HStAM/ (The Hessian State Archives – Hessisches Staatsarchiv Marburg), archival fond Politische Akten nach Philipp dem Großmütigen: Kanzlei- und Geheimeratskorrespondenz (4d), Nr. 1218; Kriegssachen (4h), Nr. 1810.
- Národní archiv /NA/ (National Archives in Prague), Sbíрка genealogicko-heraldická Wunschwitzova (Genealogical-heraldic collection of Wunschwitz), inv. nr. 951.
- SOA v Plzni. Státní oblastní archiv v Plzni /SOA v Plzni/ (State Regional Archive in Pilsen), archival fond Rodinný archiv Trauttmansdorffů (Family Archive Trauttmansdorff), inv. nr. 125.
- Wikipedia Commons. 2020.

Appendices

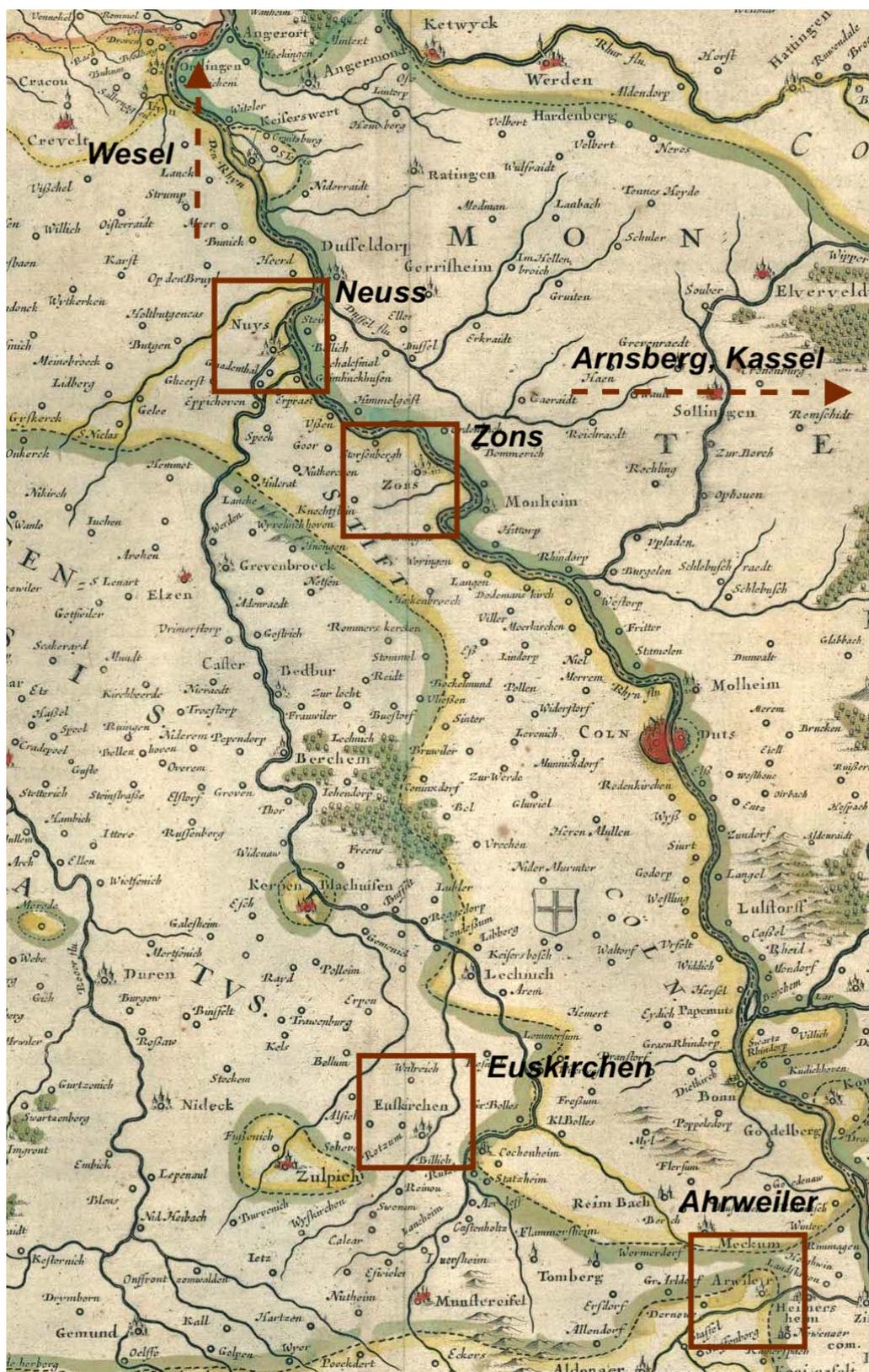


Figure 11: Area of Karel Rabenhaupt ze Suché's operations on the Rhine (Wikipedia Commons, 2020)

1646 Jun. 18.

Copia

Amsternische, Jagoborus Buch in quodam Praxo

Dießes meyn Quersfang, in antwort schreib, v. N. N. 110.
 f. #. d. 3. f. w. o u pp. 5. 10. p. 59. φ. 72. 369. 269. P. 27.
 jagoborus in φ. p. q. 18. p. 59. 22. 28. 24. 20. 72. 9. 49
 21. vnt w. f. f. u f 10. a y θ. 59. 7. 57. 111. 72. 74. 269.
 in pp. 377 φ 3 f. pp. # 18. f. φ. 59. d. 3. f. θ. p. f. 9.
 18. 49. 22. vnt all. N. N. 90. f. 28. 59. 21. φ 58. 14. 37. 6.
 w. 66. 90. 58. 41. 4. d. p. 60. 93. 70. N. 4. u. 129. 4. 59.
 74. 2. 58. 0. 8. 38. φ All. maß in mein darsumy
 396. p. 4. 10. 5. 4. 4. u. 70. 2. f. 5. f. 42. 115. 100. 72. 106
 129. 3. f. φ. 939. 6. u. y. θ. 11. a. 5. 33. 3. f. 59. f. d
 1011. 10. 5. 12. m. 21. 26. 38. 22. Δ 57. 2. 24. 18. a
 90. 14. 9. u. 7. vnt vnt gathel fult d. 26. 59. 22. 369
 w. d. 117. f. 4. 59. 22. B. B. θ. c. p. u. f. d. 37. 68. 9. f. 66
 11. d. B. 123. 107. 138. 83. 21. 376. vnt wach in gute
 festumy fult das die allix, in ison vnt schil lenger
 als andan warden könnig schy plaidy, vnt vnt allix
 was garstosy sell, φ. auf n. N. N. 7. 8. u. d. f. f. m. 100.
 110. 70. 9. 5. φ. 90. p. u. s. p. 37. 115. 2. q. f. 100. θ. 59. d. 24
 f. #. 6. #. 26. 369. w. pp. 277. φ. sell. f. w. schy gine
 vnt schy in litle, die schy in vnt vnt vnt die schy
 das m. 360. pp. 0. 9. N. 7. 975. d. u. w. 22. 90. f. 4. 5
 100. 60. f. 5. 59. φ. 58. 9. f. #. 106. auf die φ u 7. f. 6.
 59. h. 57. 1011. c. c. 10. 913. w. a. 77. 119. p. φ. 7. 5. u.
 f. 58. 28. 83. 129. 20. 24. 18. 12. 59. 22. a. c. p. f. h. #
 6. 2. vnt allix in ison p. p. 93. 70. d. #. 129. 2. 5. f. 20. 77.
 p. f. 5. 9. 59. φ u 77. 93. 238. 120. 57. 74. p. φ. 6. 12. φ
 42. p. 57. 77. pp. 11. 5. 57. 106. f. f. 103. f. 129. φ. 18
 φ. 110. 125. 70. 72. 6. 369. N. d. d. 260. f. w. schy gine
 damit gathel fult darsumy fult vnt schy

ARCHIV MUSEA KRAL. CES.

Wirt da is gine 246
 auf die landgravin di' l' d' y
 amelin Elisabeth

Schy gine
 vnt schy in ison
 schy gine
 schy gine
 schy gine

Figure 12: Encrypted message. SOA v Plzni, FA Trauttmansdorff, inv. nr. 125.

A Cryptogram Transcription

NN.110.f.s1.s2.z.s3.W.s4.u.pp.s5.10.f.59.s6.72.369.269.P.nn.s7.s8.s9.q.18.s10.r.59.22.28.24.20.72.g.49
.21.w.s11.s12.u.f.10.a.y.s13.59.s14.57.111.72.74.269.M.pp.377.s4.z.s8.pp.s1.18.s12.s7.s16.59.D.s17.s1
1.s18.s10.s12.q.18.49.22.NN.90.f.28.59.21.s19.58.14.376.W.CC.90.58.41.s20.D.g.60.93.70.N.s20.u.12
9.s21.59.74.s22.58.o.h.38.O.396.P.s23.10.s24.s25.s21.u.70.24.s24.s12.42.115.100.72.106.129.s17.s11.s
6.939.b.u.y.s26.ll.s27.s24.II.z.s16.59.f.s28.1011.10.s24.12.M.nn.s27.b.38.22.s23.57.s22.24.18.a.90.14.
g.u.s14.s27.b.59.22.369.W.s9.11.f.h.s21.59.22.BB.s18.c.s10.u.s20.s4.37.68.q.s16.CC.11.D.s17.123.107
.138.83.21.376.s4.u.f.NN.z.s18.u.s2.s11.s3.M.100.110.70.q.s24.59.90.s29.u.s24.p.37.115.s22.q.f.100.s
13.59.s2.24.s12.s1.b.s20.s27.b.369.W.pp.277.M.360.pp.s4.q.N.T.975.s2.u.W.ZZ.90.s29.u.s24.100.60.f.
h.59.s19.58.s14.s30.s1.106.s13.u.s14.s1.s12.b.59.h.57.1011.CC.10.913.W.a.77.119.P.s30.s20.s.u.t.58.s
14.28.83.129.20.24.18.12.59.22.a.c.s10.s12.h.s1.b.Q.PP.93.70.D.s1.129.s22.z.s8.20.77.s10.s12.s5.q.s.u.
g.s19.u.s32.77.93.138.120.57.74.P.s19.b.12.s13.42.s16.57.XX.PP.LL.s5.57.106.AA.10.z.f.129.s28.18.s
17.110.125.70.72.b.369.N.dd.260

Note: Elements starting with letter *s* in a combination with numbers (starting with *s1*) represents the symbols.

B English Translation of the Deciphered Message

Copia

Enlightened, highly noble Princess, a gracious Lady. This morning I received an answer from Marshal de Turenne, who was in Euskirchen yesterday and had a camp nearby. He wanted to march today and settle in front of the Zons tomorrow. So I do my math, I have 1,500 infantry with one battery of cannons and one mortar. With God's help, we'll do a short process with that [Zons]. And because I firmly believe that it is an advantage of the Allies that they endure [in the siege] longer than others, perhaps what is to happen will happen before the Marshal gets there. Therefore, I would like to ask your Princely Grace to order immediately that the levies from East Frisia and the borrowed cannons be sent to Wesel. I would like to do something important and arrange [for the army] good winter quarters. I hereby commend myself to the beneficial protection of Your Princely Grace and remain

a subject to Your Princely Grace, an obedient servant Rabenhaupt

Neuss, June 13th, 1646, to Landgravine of Hessen, Amalia Elizabeth