Wrong Design of Cipher Keys:
Analysis of Historical Cipher Keys From the Hessisches Staatsarchiv Marburg Used in the Thirty Years' War

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

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

Abstract

Nomenclator is a complex encryption system consisting of several different simpler encryption systems used together during the encryption. It is one of the main encryption systems used before the twentieth century. In some cases, there are large collections of historical ciphers preserved in archives. Those from a particular time period or geographic location are very valuable and can bring insights to the cipher design from a specific time/location. This paper provides the first detailed empirical analysis of historical cipher keys from the Thirty Years' War deposited in Hessisches Staatsarchiv Marburg. We describe a large variety of analyzed keys with a focus on those properties (poorly designed keys) that can decrease the security of the cipher. We further show that these properties alone do not imply a bad design, sometimes a combination of several properties is needed and at the same time a bad use of the encryption key.

1 Introduction

The study of historical ciphers is essential for understanding how ciphering evolved in the past. In this paper, we examine a special encryption system called *Nomenclator*. It is one of the main encryption systems used before the twentieth century and used extensively in European warfare and diplomacy. Many encrypted documents and cipher keys have survived[1] in archives around the world. In some cases, also as large collections from a particular time period or geographic location (Láng, 2020; Antal et al., 2021). Studying such a collection of ciphers can help to better understand some aspects of historical cryptography.

Research in this field is progressing in recent years. Projects, like the *DECRYPT*[2] (Megyesi et al., 2020) and the *HCPortal*[3] (Antal and Zajac, 2020; Antal and Zajac, 2021), are mainly focusing on the digitization and processing of encrypted documents and cipher keys, and developing new methods to solve these ciphers. Gaining new knowledge about how these ciphers were designed and used is necessary for a better understanding of these ciphers and for developing effective and sophisticated solving methods. It is therefore necessary to investigate the design and structure of historical cipher keys (Tudor et al., 2020; Megyesi et al., 2021).

If a nomenclator system is correctly constructed and used, it is very hard (or impossible) to crack. On the other hand, many of them were designed and used incorrectly (Dunin and Schmeh, 2020; Antal et al., 2021). In the available literature, to the knowledge of the authors, there is no comprehensive study of the poor design of encryption keys. This paper provides the first detailed empirical analysis of the weak cipher key design from a specific time period. We investigated a collection of cipher keys from the Thirty Years' War deposited in Hessisches Staatsarchiv Marburg.

2 Nomenclator Encryption System and Cipher Key Design

Nomenclator is a special encryption system consisting of several different simpler encryption systems used together during the encryption. This type of encryption was very popular and was used for a long time period. It was used from the fourteenth to the nineteenth century (Dunin and Schmeh, 2020; Meister, 1906; Lasry et al., 2020). The design of these systems was very variable. It is possible to find examples from small (very sim-

[1] There are thousands of ciphers preserved in archives. Many of the encrypted documents are still unsolved.

[2] https://de-crypt.org/

[3] https://hcportal.eu

ple) instances to very complex ones. We recall the main characteristics of this type of encryption system summarised from Antal et al. (2021):

A *nomenclator* mostly contains a substitution of *letters* (monoalphabetic or homophonic substitution) in a combination with substitution of $n - grams$ (bigram and/or trigram substitution),[4] *codes* and *nulls*. It is not widespread, but some nomenclators contain a polyalphabetic substitution, too.

The sub-encryption systems (encryption rules) are described by a cipher key, which is very characteristic:

- Cipher key is mostly drawn on a large paper sheet.
- The individual sub-encryption systems are mostly graphically separated.
- Codes used in a nomenclator can grow its size to several pages. In that case, it is often organized as a small book.
- The cipher text alphabet is often represented by (combinations of) letters, numbers, and special symbols/glyphs.[5]
- Cipher key sometimes contains a part not only for encryption but also for decryption (where the elements are ordered by the cipher text units).

An example of a good cipher key design is visible in figure 1. This nomenclator contains a large homophonic substitution, bigram substitution, and many nulls and codes (codes are not visible on this image). If the text encrypted with this key is not too long, and the key is correctly used,[6] it is almost impossible to solve such a cipher without additional information or without finding the correct key (Dunin and Schmeh, 2020; Antal et al., 2021).

However, many cipher keys were also poorly designed (Mírka and Vondruška, 2013; Antal and Mírka, 2018; Dunin and Schmeh, 2020; Antal et al., 2021).

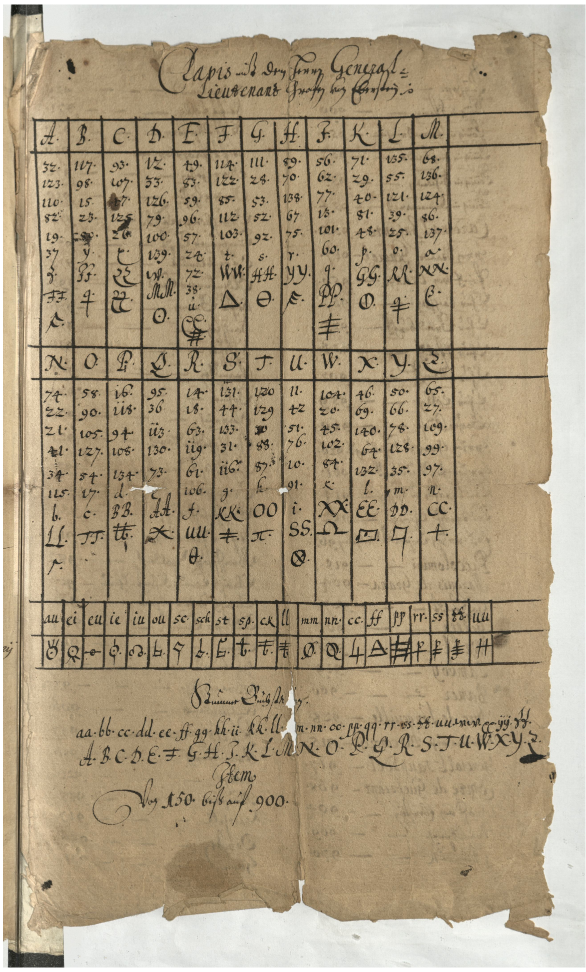

Figure 1: Cipher key example (part of the key). HLA-HStAM Best. 4d Nr. 1218.

We introduce a less formal definition of the weak (wrong/poor) cipher key:

A cipher key is weak if it contains one or more properties, that decrease the security of the cipher.

The security of a cipher (nomenclator) is decreased, when:
a) at least one sub-encryption part of the cipher can be distinguished from other sub-encryption parts, and as a consequence, it is significantly easier to (partially) solve at least one sub-encryption part; or
b) the symbols of the cipher alphabet are assigned according to some regular patterns, and as a consequence, it is significantly easier to (partially) solve at least one sub-encryption part.

In the next section, we will describe some properties of poorly designed keys that can decrease the security of the cipher. We further show that these properties alone do not imply a bad design. Sometimes a combination of several properties

[4]There are often section for substitution of syllables, but from the structural point of view the *n*-grams category is more suited.

[5]In many cases, a special separator is required such as a dot or comma. This is necessary to clearly distinguish/split the cipher text units.

[6]In fact, incorrect usage of a strong cipher key (e.g. not using nulls/using a small number of nulls, or not using all possible homophones from the table) can lead to the depreciation of the strength of the key.

and/or a bad use of the encryption key are necessary for successful cryptanalysis.

3 Empirical Analysis of Wrong Key Designs

Complex encryption systems are problematic in many ways. The design of a nomenclator cipher key and writing it on a paper requires a lot of effort and patience. From the preserved archival documents (mainly from cipher keys), it is obvious that often not enough attention was paid to the design of the key. After a more detailed examination of the preserved keys, it is possible to identify various properties in the encryption keys which in some cases significantly reduce the security.

We investigated a collection of cipher keys deposited in Hessisches Staatsarchiv Marburg (HLA-HStAM Best. 4d Nr. 1218). The collection contains 126 keys from the Thirty Years' War. Because we focus mainly on nomenclator encryption systems, some keys do not fit our requirements. We excluded[7] all cipher keys which were:

- consisting of only a monoalphabetic substitution,
- consisting of only a polyalphabetic substitution,
- drafts/incomplete key reconstructions,

but kept cipher keys consisting of only codes or homophonic substitution.[8] Please note that some keys were repeated (or were very similar),[9] in that case, we kept/counted all instances. The remaining 93 cipher keys have the following structure:

- 78 are nomenclator[10] systems (83.87%),
- 82 contain a homophonic substitution part (88.17%),
- 13 are only homophonic substitutions (13.98%),
- 74 contain a code part (79.57%),
- 2 are only codes (2.15%).

Because our collection mainly consists of cipher keys only (encrypted documents were not preserved for all keys), we directly focus on the analysis of the structure of these keys, trying to identify some specific properties. We divide the investigated cipher key properties into two main categories: properties that can *distinguish* the sub-encryption parts, and properties that describe some regularities in the key that can help to *crack* (at least partially) the cipher.

3.1 Distinguishing the Nomenclator Parts

In this section, we focus on the 78 cipher keys, which consist of at least two sub-cipher parts. The most commonly used symbol set in the cipher keys were numbers (with an increasing tendency through the centuries) (Megyesi et al., 2021). This also corresponds with our case, we identify 66 cipher keys from the 78 (84.615%), where numbers were used in at least two sub-cipher parts. Our goal is to figure out if it is possible to distinguish[11] these sub-cipher parts - separate the numbers into intervals.

In figure 2 there is an example of a cipher key where numbers were used in the homophonic table and in the code part. In this case, the used numbers can be easily divided into three groups: numbers from 2 to 121, numbers from 300 to 2600 (increasing by 100), and numbers 8000+ (increasing by 1000). Assigning numbers in a special format (e.g. large numbers increasing with a constant step) is one of the worst strategies in the cipher key design. If there is a sufficient number of occurrences of the numbers in a cipher text, it is clearly visible from a statistical analysis. This example is a bit special. Since three different intervals appeared, one would assume that they were used in the case of three different sub-cipher parts. But in our case, these three parts belong only to two sub-cipher parts. With a little luck, we can assume that such a trick and can try to assign the 300-2600 interval to the letters (or to codes). Sometimes this is obvious after applying frequency analysis.

Similar example is on figure 3 where the homophonic part (numbers 10-85) is clearly distinguish-

[7] We excluded 33 cipher keys.

[8] Despite the fact that in this case there are no multiple sub-ciphers used, we evaluated these keys too. Codes and homophonic substitutions are the most common part of a classic nomenclator. It is also hard to determine the exact boundary between e.g. a code and a nomenclator (Dunin and Schmeh, 2020).

[9] In some cases there are different key users written on similar/equal keys.

[10] Based on section 2, we define a nomenclator as a cipher consisting of at least two different simple encryption systems.

[11] In Dunin and Schmeh (2020) there is present a nice example where the numbers used in the homophonic substitution part of the nomenclator can be easily separated from those numbers used for code groups.

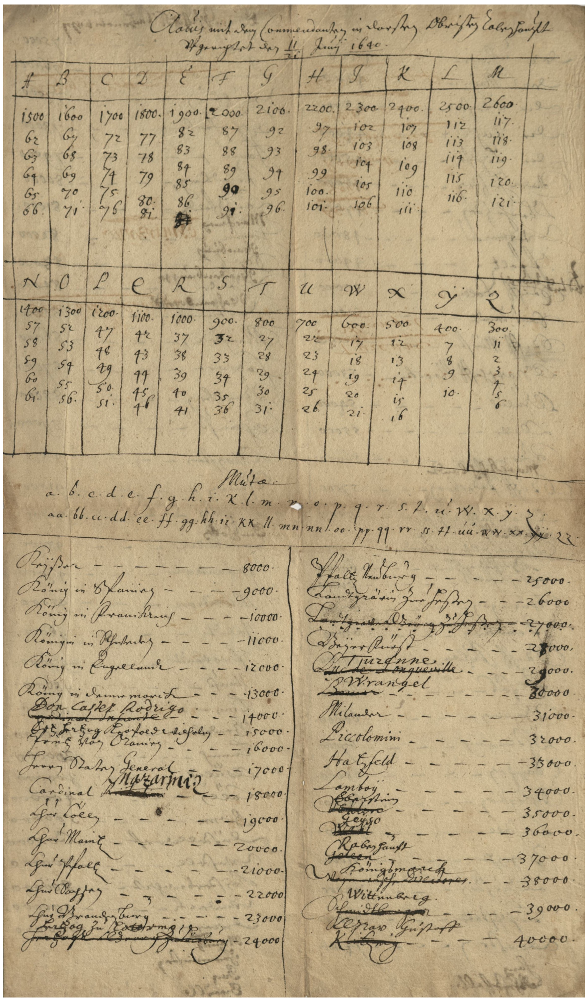

Figure 2: Cipher key with easily distinguishable number intervals. HLA-HStAM Best. 4d Nr. 1218.

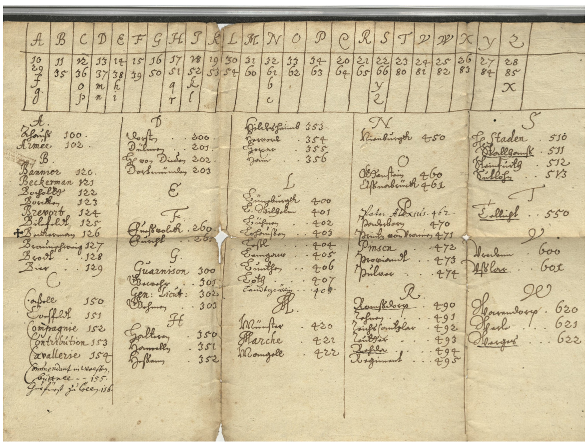

Figure 3: Cipher key with easily distinguishable number intervals. HLA-HStAM Best. 4d Nr. 1218.

able from codes (numbers 100+).

If the numbers for each sub-cipher part were assigned in clear intervals (e.g. two-digit numbers for homophones, three-digit numbers for bigrams, and four-digit numbers as code groups or in a similar way) we can easily separate them, as it was shown in the previous examples. It is also possible to do it if there are no large gaps between these intervals, however, this does not have to be trivial. On figure 4 the used numbers are divided into four groups: numbers 1-11 are nulls, numbers 12-90 are homophones, numbers 91-100 are common bigrams, and numbers above 100 are code groups. Separating the sub-cipher parts is not impossible in that case, but in general, we do not know the exact number of used sub-cipher parts before/during the analysis.[12]

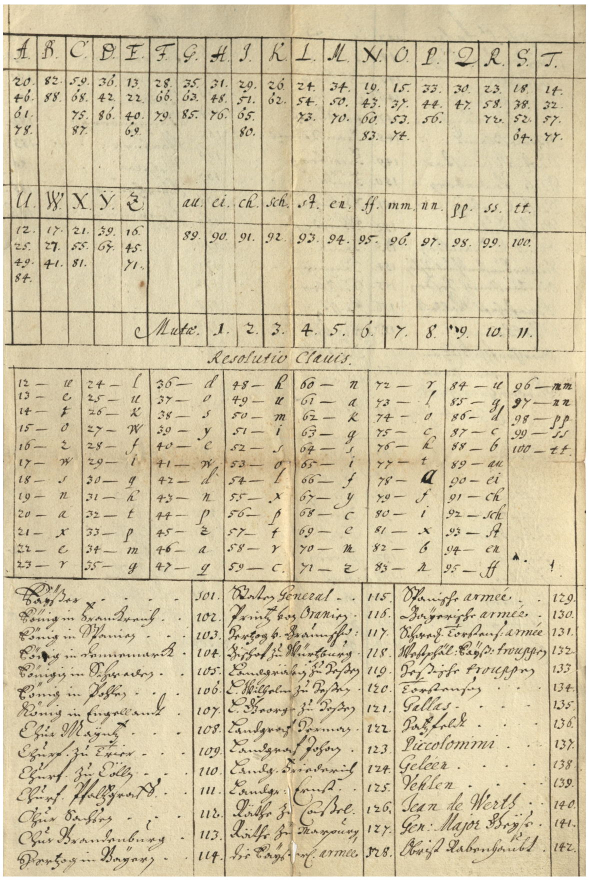

Figure 4: Cipher key with distinguishable number intervals. HLA-HStAM Best. 4d Nr. 1218.

It is recommended, as the first step of the analysis, to calculate the frequency of each number in the ciphertext as provided in an example in Dunin and Schmeh (2020) on page 143. However, the

[12] Many cipher keys were constructed in such a way that increasing number intervals were assigned in a specific order (e.g. (nulls), homophonic substitution, bigrams, codes, (nulls)).

frequency analysis does not necessarily lead us to the right assumptions. It highly depends on the key structure (e.g. the number of used homophones, number of entries in the code part, number of nulls used) and if the key was used correctly.[13] It also depends on the length of the analyzed encrypted text.

Totally, in 75.76% of the investigated cipher keys (from the 66 cipher keys where numbers were used in multiple sub-cipher parts) can be the numbers in the sub-cipher part separated into clear intervals. Moreover, in 91.53% of cases (from the 59 cipher keys where substitution and code parts were present), the interval used in the substitution part contained smaller numbers than in the code's part. Thus, we can expect that the substitution tables would almost always contain smaller numbers than the codes.

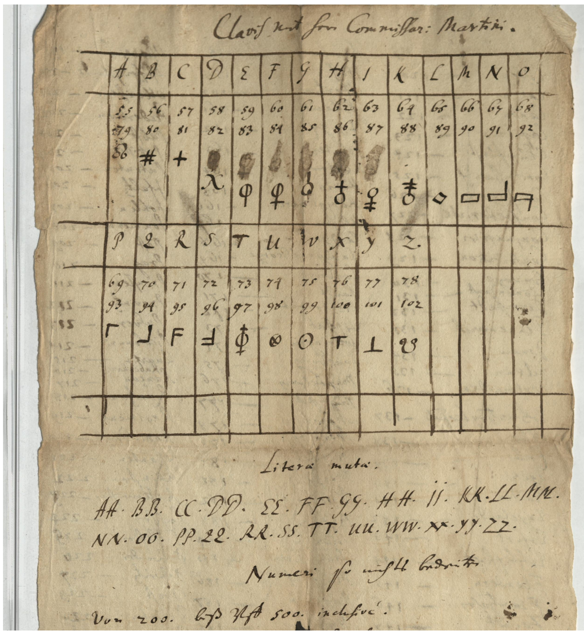

Figure 5: Cipher key with special rows. HLA-HStAM Best. 4d Nr. 1218.

We can summarize our findings in the chart visible on figure 7.

In many cases, there are sub-cipher parts where multiple symbol sets were used (not only numbers). These parts can contain a special *row* of letters (*a-z*/*A-Z*), or double letters (*aa-zz*/*AA-ZZ*) or numbers/symbols[14]. On figures 1 and 6 there is

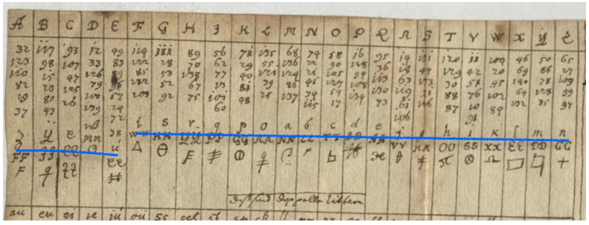

Figure 6: Homophonic substitution containing a row of letters. HLA-HStAM Best. 4d Nr. 1218.

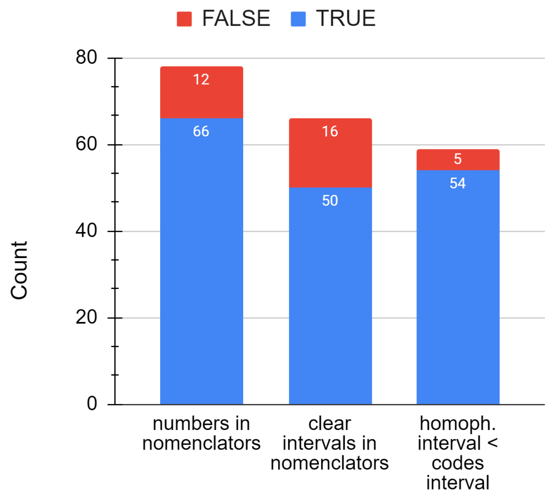

Figure 7: Statistics of selected cipher key properties

one row of lower case letters in the homophonic substitution. In figure 2 the nulls consist of a row of letters and double letters. In figure 5 the homophonic substitution contains a row of symbols, and the symbols are used only in that part; nulls also contain double upper case letters. This property can be also available in codes. In such a case we can deal with these rows separately (assigned to one specific sub-cipher part). It will not necessarily solve the whole sub-cipher part but can help in the cryptanalysis. If a special row is present in the homophonic substitution (as in figure 6) and there is sufficient occurrence of these symbols in the ciphertext, we can solve this part as a simple substitution. In Antal and Zajac (2013) and Antal et al. (2021) the authors were able to correctly assign[15] the row of numbers to the homophonic part based on statistical analysis, however, the length of the analyzed text was too short to break the ci-

[13] An example of incorrect key usage is choosing the same homophone when others are available (Dunin and Schmeh, 2020).

[14] This property can be used only when the mentioned rows (or symbols/numbers) are used only in one sub-cipher part.

[15] In that example the key from figure 1 was used. The lower case letters occur 72 times in the cipher text and have a large *index of coincidence* producing the properties of simple substitution.

pher.

In 36.56% of the all investigated cipher keys (from the total 93) there is a special row in at least one of the sub-cipher parts.[16]

These explained properties can be used to help to separate/distinguish the sub-cipher parts in the nomenclator cipher key. These properties can be mostly used only to simplify the solving process, and are not necessarily enough to solve the whole cipher. However, this kind of simplification can increase the chance of successfully solving many times.

3.2 Solving the Nomenclator Parts

After separating the sub-cipher parts (see section 3.1) we can try to solve each of the sub-part of the cipher separately. If we are not dealing with a nomenclator system (e.g. only with a homophonic substitution), and there is enough information in the text, we can use well-known automated/statistical approaches to solve the cipher. However, if several different ciphers were used together, and gradually swapped - even, identifying and separating a sub-cipher part is not enough to break the cipher. In many cases, as described in Dunin and Schmeh (2020), the key may contain a sorted part in an easy-to-determine alphabetical or numerical order. In this section, we will investigate these kinds of properties in the homophonic and code parts of the cipher keys.

Poorly designed homophonic substitutions

The major part (88%) of the investigated cipher keys contain a homophonic substitution. There are available well-designed ones, consisting of a large number of homophones that can be assigned to each letter and without any visible drawbacks in the design. A lot of keys contain some very specific properties that can significantly reduce the security of the cipher. We identify four properties:

1. the rows of the homophonic table contain continuous numbers,
2. the columns of the homophonic table contain continuous numbers,
3. there is a specific pattern how were the numbers filled in the homophonic table,
4. each column consists of a fixed/same number of elements.

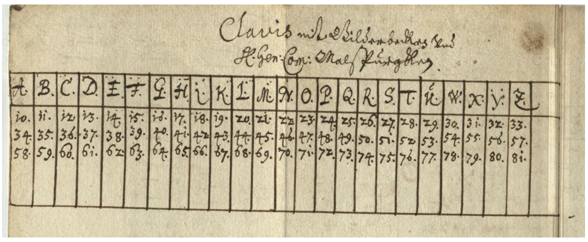

Figure 8: Continous numbers in the rows of a homophonic substitution. HLA-HStAM Best. 4d Nr. 1218.

A very weak design of a homophonic substitution is shown in figure 8. The rows are filled with increasing numbers (interval 10-81) starting in the first row from the left. This key also contains the fourth property - all columns consist of exactly 3 elements. During the cryptanalysis, if we can guess these properties, or can estimate (based on a frequency analysis of the cipher text), we can easily fill the table (or we can use a simple helper computer program if we need to check some combinations). Similar example is visible on figure 5. There are two rows of numbers filled in the same way as before (starting from the number 55), but the third row consists of symbols. In this case, the symbols are not used in any other sub-cipher part of the nomenclator, so we can solve it separately as a simple substitution. After solving the numeric rows, it is highly probable that the symbol row can be easily determined.

Some keys contain an ordered sequence in the rows of the homophonic table only partially. In figure 3 we can see continuous number sequences of different lengths altered in the rows. In this example, there are mainly sequences of length 5 and 10 numbers. In such a case, we can write a helper computer program and check some predefined sequences/lengths. Another example of partially ordered sequences in the rows is in figure 9. In addition, there are nulls (marked as *Literae mutae*) inserted to break the sequences. However, there is a fixed pattern of how it was done (sequence of four numbers, two nulls, sequence of four numbers, ...). We can try several variations as before. Even if we hit only partially the correct structure, it can help a lot in the solving process.

Another very weak design of a homophonic substitution is shown in figure 10. In that case,

[16]This kind of row in the homophonic substitution part was probably intended by the authors to strengthen substitution, but paradoxically it could often weaken it as a result.

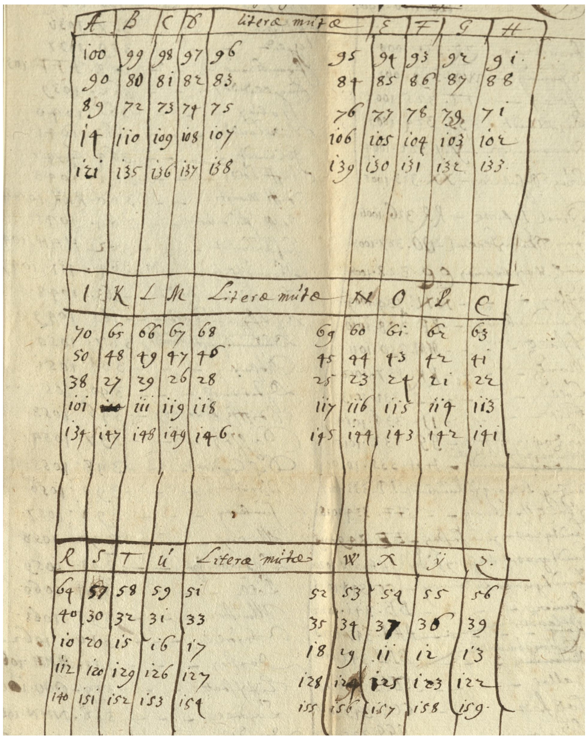

Figure 9: Continous numbers in the rows of a homophonic substitution. HLA-HStAM Best. 4d Nr. 1218.

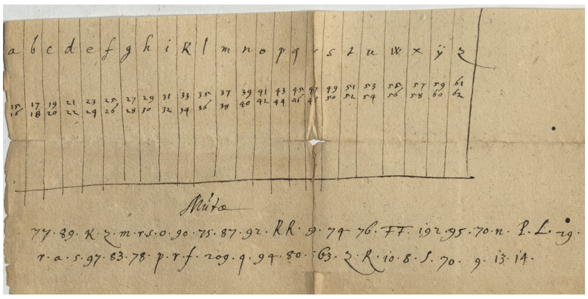

Figure 10: Continous numbers in the columns of a homophonic substitution. HLA-HStAM Best. 4d Nr. 1218.

the columns are filled with increasing numbers (interval 15-62) starting in the first column from the top. This is the same situation as in the first example. We can easily try to fill the table. In some cases, like the key in figure 11 the columns contain ordered sequences, however, the length of the columns differs and the column does not continue from the number ended in the previous column. This key design is also weak, but it requires more effort during the solving process.

Some cipher keys may contain a combination of the first, second, and fourth weakness, as visible on figure 2 and highlighted on figure 12. There

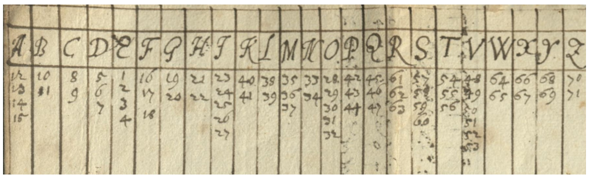

Figure 11: Continous numbers in the columns of a homophonic substitution. HLA-HStAM Best. 4d Nr. 1218.

are continuous numbers in the columns starting in the last column and continuing to the left. Each of these columns consists of five elements (continuous numbers) except for the column *Y*. In addition, there is a row that consists of increasing elements (fixed-step 100). On figure 13 there is even worse design present. The first column starts with a low number and the column numbering continues to the right without skipping any number. There is one row in addition with increasing elements (fixed-step 100). It is highly probable that we can separate the first row in both cases. We can try to fill the rows and columns of fixed length with continuous numbers using a computer program.

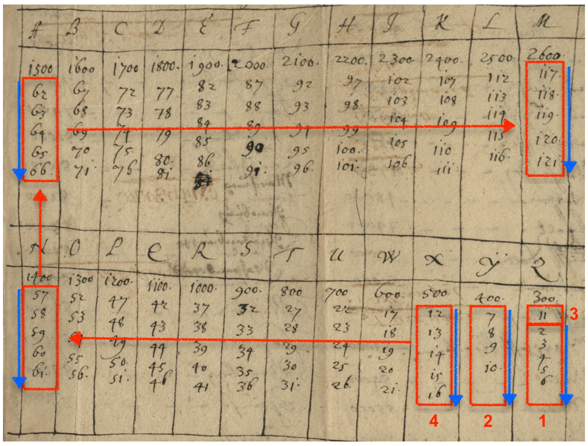

Figure 12: Continous numbers in the rows and columns of a homophonic substitution. HLA-HStAM Best. 4d Nr. 1218.

There were also used other - less simple and harder to detect - ways of filling the table with numbers. In general, there is a huge variety of patterns how we can fill/construct the homophonic table. We will show a few of them. On figure 14 there is a simple pattern. The homophonic table consists of two rows consisting of odd numbers only. If we look at the first two columns, we can see that there are numbers 3,5,7,9 (fixed dif-

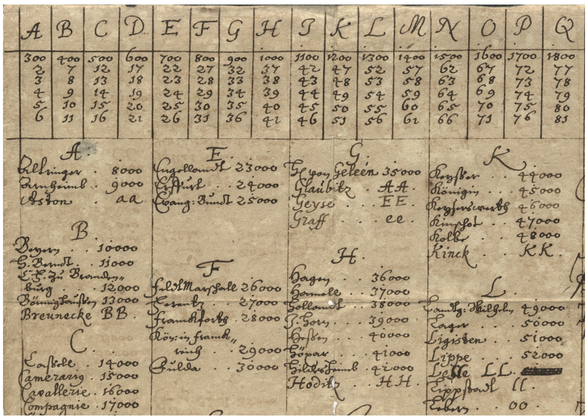

Figure 13: Continous numbers in the rows and columns of a homophonic substitution. HLA-HStAM Best. 4d Nr. 1218.

ference 2). And the pattern of the filling is: first row/first column, first row/second column, second row/first column, and second row/second column. This pattern continues on the next two neighboring columns and so on. Similar example is on figure 15 with the same constant step. In this case, the table is divided into two parts (for letters *A*-*M* and for letters *N*-*Z*) and the pattern is applied in the same row but between the first and the second part of the table (instead of the first/second rows). This specific pattern can be also seen as follows: some of the neighboring columns in the same row have a different offset of four. Finding these *patterns* may be complicated.

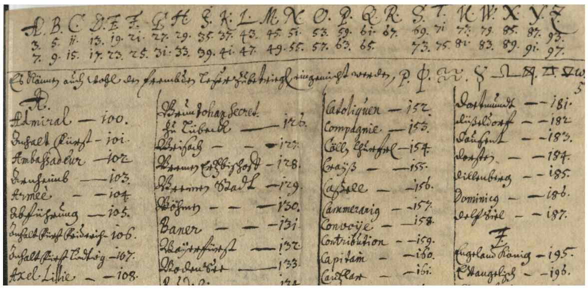

Figure 14: Specific pattern in a homophonic substitution. HLA-HStAM Best. 4d Nr. 1218.

We can summarize our findings in the chart visible on figure 16. Totally, 82 cipher keys were analyzed where a homophonic substitution was present.

In this subsection, we focused on some flaws in the design of a homophonic substitution which is most commonly used also in nomenclators in the

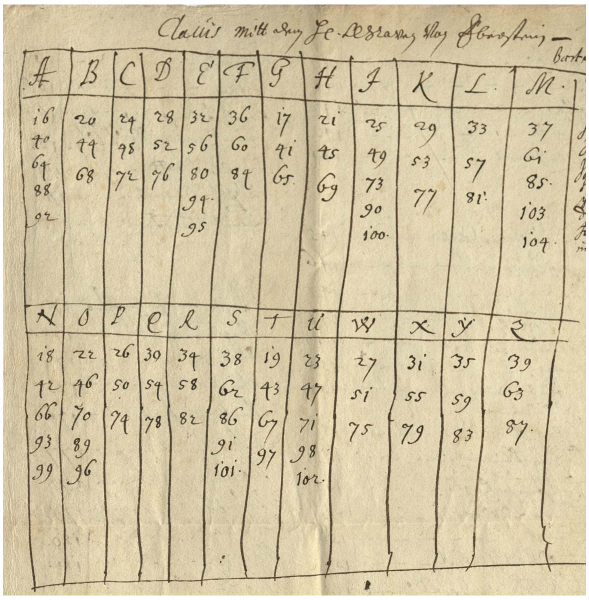

Figure 15: Specific pattern in a homophonic substitution. HLA-HStAM Best. 4d Nr. 1218.

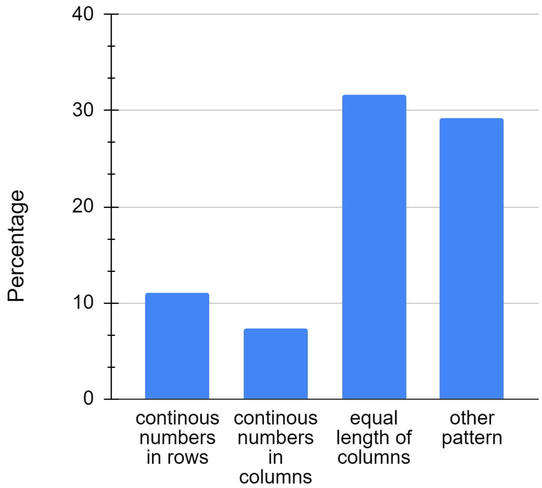

Figure 16: Statistics of selected cipher key properties

analyzed cipher keys. It is clear that there are regularities and easy to detect patterns in many cases. Some of the shown patterns can be used directly to break the cipher. In some cases, it is needed to be present more properties (like the combination of the first/second property with the fourth one) to be able to successfully solve the cipher. During the cryptanalysis of a given cipher text, it is recommended to first perform a statistical analysis and in addition, we recommend trying to separate the sub-cipher parts (if we are dealing with nomenclators) and start the solving process with a special analysis of the homophonic parts. Several different and commonly used patterns/regularities with different parameters can be checked using a computer program within a few minutes.

Poorly designed codes

The second most frequent part of the available sub-cipher type is a code.[17] The length and the structure of codes vary. Some keys contain only a few code words, some may contain thousands. In some cases also multiple code groups are assigned to each plain text word/phrase forming a homophonic code system. The code groups may contain only numbers, sometimes a combination of letters, double letters, numbers, and symbols. If only numbers were used and these numbers are assigned in a specific order to words (also sorted alphabetically), we have got a one-part code. In many cases, if a one-part code is used, it is easier to solve (Dunin and Schmeh, 2020) than the two-part (shuffled order) ones. Nice examples of easily distinguishable one-part codes are on figures 3 and 13. On figure 17 we can see a special construction of a one-part code. The words are grouped based on the first letter of the word, ordered alphabetically, the code groups are generated with a specific prefix (upper case letter) for each group, and increasing numbers are assigned starting from 10. Similar example is on figure 3. The code is a one-part code divided into sub-groups based on the starting letter in the word. For each code word, a three-digit number was used. It is also visible that the sub-groups are based on a two-digit prefix (all words starting with letter *a* starts with a fixed prefix 10, all starting with letter *b* starts with a fixed prefix 12, starting with letter *c* starts with a fixed prefix 15). This prefix is different for each group (starting letter).

On figure 18 we can see a one-part homophonic code, however there are exactly two adjacent numbers assigned to each word/phrase.

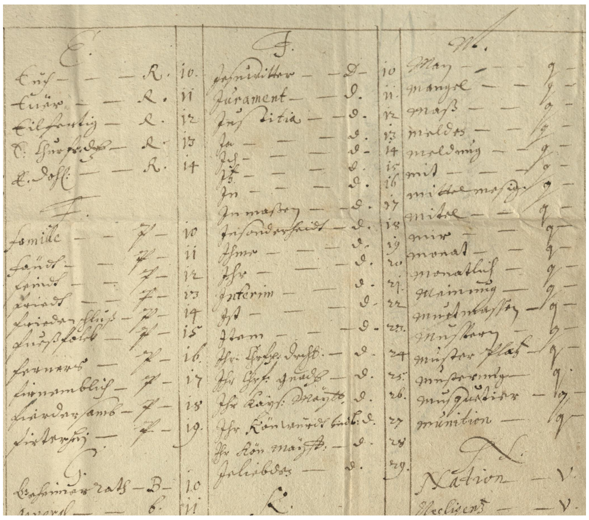

Figure 17: One-part code with a prefix. HLA-HStAM Best. 4d Nr. 1218.

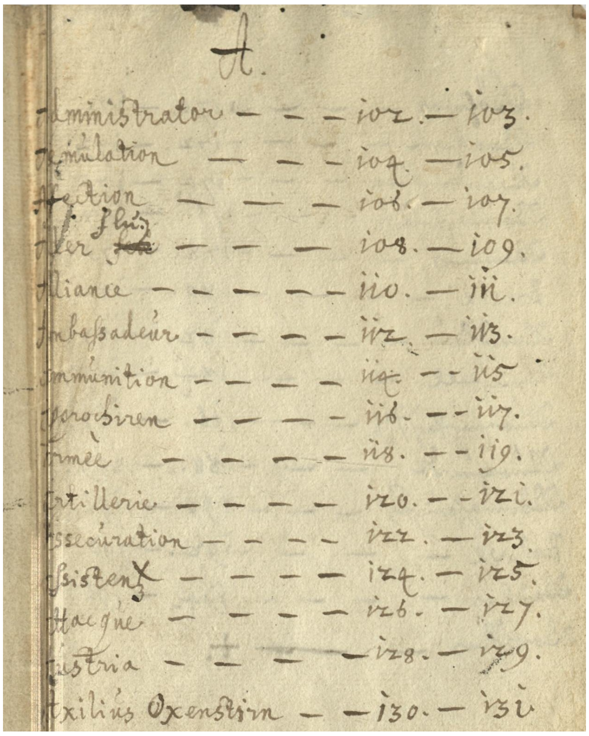

Figure 18: One-part homophonic code. HLA-HStAM Best. 4d Nr. 1218.

4 Conclusions

In this paper, we have shown that many of the analyzed cipher keys were poorly designed. We identified several specific properties of the cipher keys (key parts) which represent a possible security flaw. We divide these properties into two large categories. One that can help to separate the nomenclator sub-parts, and one that is more suited to cryptanalysis. However, in many cases, these properties can be successfully used in a combination. Finding such a property alone does not imply a bad design. There could be well-designed cipher keys where some of the properties are present but cannot be exploited (see the example on figure 1). If we are solving a nomenclator (and have a long enough cipher text available), we can simply

[17] Please note that for codes a qualitative analysis is given only.

check if there is any of the described properties present. If the cipher key was designed (also used) correctly, we have still a chance[18] that the used cipher key is preserved somewhere.

Acknowledgments

This work was supported by grant VEGA 2/0072/20. We thank Pavol Zajac for his help.

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?* Available online: `https://www2.lingfil.uu.se/histocrypt2018/Antal_HCC18.pdf`.

Eugen Antal and Pavol Zajac. 2013. Analýza Rabenhauptovho zašifrovaného dopisu (Analysis of Rabenhaupt's encrypted message). In *Crypto-World*, 11-12. Available online: `http://crypto-world.info`.

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.

Eugen Antal and Pavol Zajac. 2021. HCPortal Modules for Teaching and Promoting Cryptology. In *Proceedings of the 4th International Conference on Historical Cryptology, HistoCrypt 2021*, pages 1 - 11. Linköping University Electronic Press.

Eugen Antal, Pavol Zajac and Jakub Mírka. 2021. Solving a Mystery From the Thirty Years'War: Karel Rabenhaupt ze Suché's Encrypted Letter to Landgravine Amalie Elisabeth. In *Proceedings of the 4th International Conference on Historical Cryptology, HistoCrypt 2021*, pages 12 - 24. Linköping University Electronic Press.

Elonka Dunin and Klaus Schmeh. 2020. Codebreaking: A Practical Guide. Robinson. Great Britain.

George Lasry, Beáta Megyesi and Nils Kopal. 2020. Deciphering papal ciphers from the 16th to the 18th Century. In *Cryptologia*. Taylor & Francis.

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.

[18] A complex nomenclator can be solved also in such a way as described in Antal et al. (2021).

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. In *Cryptologia*, volume 44, number 6, pages 545-559. Taylor & Francis.

Beáta Megyesi, Crina Tudor, Benedek Láng and Anna Lehofer. 2021. Key Design in the Early Modern Era in Europe. In *Proceedings of the 4th International Conference on Historical Cryptology, HistoCrypt 2021*, pages 121 - 130. Linköping University Electronic Press.

Aloys Meister. 1906. Die Geheimschrift im Dienste der Päpstlichen Kurie von ihren Anfängen bis zum Ende des XVI. Jahrhunderts. Paderborn, F. Schöningh.

Jakub Mírka and Pavel Vondruška. 2013. Nomenklátory 17. a 18. století (Nomenclators from the 17. and 18. century). In *Crypto-World*, 11-12.

Crina Tudor, Beáta Megyesi and Benedek Láng . 2020. Automatic Key Structure Extraction. In *Proceedings of the 3rd International Conference on Historical Cryptology, HistoCrypt 2020*, pages 146 - 152. Linköping University Electronic Press.

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.

Appendices

A Additional information about cipher key examples

- Figure 1 – Nomenclator used for the correspondence of the chancellery of Landgravine of Hesse-Kassel with Kaspar von Eberstein, Joachim de Wiquefort, Adolph Wilhelm von Krosigk, Hans Adam von und zu Karpf and Johann von Geyso in the 1640s.
- Figure 2 - Nomenclator used for the correspondence of the chancellery of Landgravine of Hesse-Kassel with Karel Rabenhaupt ze Suché, created in June 1640.
- Figure 3 - Nomenclator used for the correspondence of unspecified persons probably in the 1630s.
- Figure 4 – Nomenclator used for the correspondence of the chancellery of Landgravine of Hesse-Kassel with the commander of Ziegenhain Justinus Ungefug probably in the 1640s.
- Figure 5 – Nomenclator used for the correspondence of the chancellery of Landgravine of Hesse-Kassel with not otherwise specified commissioner Martini in 1640s.
- Figure 6 – Nomenclator used for the correspondence of the chancellery of Landgravine of Hesse-Kassel and Kaspar von Eberstein, created in April 1641.
- Figure 8 – Cipher key used for the correspondence of unidentified persons.
- Figure 9 – Nomenclator used since May 1639 for the correspondence of the chancellery of Landgravine of Hesse-Kassel probably with James King of Birness and Dudwick and since December 1639 also with Peter Melander von Holzappel.
- Figure 10 – Nomenclator used for the correspondence of the Electorate of Cologne with Gottfried Huyn von Geelen, intercepted in 1640 in Lippstadt.
- Figure 11 – Nomenclator used for the correspondence of the chancellery of Landgravine of Hesse-Kassel with English resident William Curtius probably in 1639.
- Figure 12 – Nomenclator used for the correspondence of the chancellery of Landgravine of Hesse-Kassel and Karel Rabenhaupt ze Suché, created in June 1640.
- Figure 13 - Nomenclator used for the correspondence of the chancellery of Landgrave of Hesse-Kassel with (Franz Ulrich?) Wasserhuhn, created for his mission to Alexander Leslie probably in 1636.
- Figure 14 – Nomenclator used for the correspondence of the chancellor Christoph Deichmann with Johannes Vultejus and (Moritz Otto?) von Günterode probably at the turn of the 1630s and 1640s.
- Figure 15 – Nomenclator used for the correspondence of the chancellery of Landgraves of Hesse-Kassel and Kaspar von Eberstein probably in the 1630s.
- Figure 17 - Nomenclator used for the correspondence of Duke Maximilian I of Bavaria with Gottfried Huyn von Geelen and the commander of the fortress Wolfenbüttel, intercepted in 1636 by Daniel Rollin de Saint-André.
- Figure 18 – Nomenclator used for the correspondence of the chancellery of Landgraves of Hesse-Kassel probably with Reinhard Scheffer and with the commander of Dorsten in the 1630s/1640s.