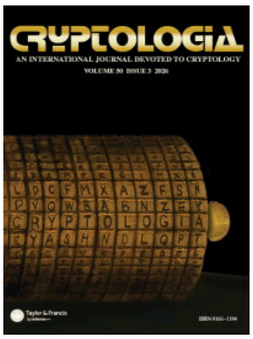

Cryptologia

ISSN: 0161-1194 (Print) 1558-1586 (Online) Journal homepage: www.tandfonline.com/journals/ucry20

Development of obfuscation techniques in Vienna during the early modern era

Eugen Antal, Jakub Mírka & Dušan Kováč

To cite this article: Eugen Antal, Jakub Mírka & Dušan Kováč (2026) Development of obfuscation techniques in Vienna during the early modern era, Cryptologia, 50:3, 191-221, DOI: 10.1080/01611194.2025.2457096

To link to this article: https://doi.org/10.1080/01611194.2025.2457096

CRYPTOLOGIA
2026, VOL. 50, NO. 3, 191–221
https://doi.org/10.1080/01611194.2025.2457096

Taylor & Francis
Taylor & Francis Group

Development of obfuscation techniques in Vienna during the early modern era

Eugen Antal, Jakub Mírka, and Dušan Kováč

ABSTRACT

Nomenclator, one of the main encryption systems used before the twentieth century, consists of several different simple (mainly substitution) encryption systems combined. To increase the cipher's security, various obfuscation techniques were also employed. However, the real-life use of these techniques is not well known. One of the few sources of information about obfuscation techniques are the preserved cipher key instructions. We investigate and study a large amount of instructions from the Vienna Cipher Office, deposited in the Staatskanzlei key collection in the Österreichisches Staatsarchiv in Vienna. We present detailed information about the investigated cipher keys with instructions and about the obfuscation techniques, as well as their typology. All the identified obfuscation technique categories—nulls, annullants, and false separators—are supported with visual examples. Additionally, a case study is presented to demonstrate the creation of a strong cipher using various advanced obfuscation techniques. We believe our findings add new knowledge and details about the development of obfuscation techniques in Vienna during the early modern era.

KEYWORDS

black chamber; cipher keys; historical cryptology; instructions; nomenclator cipher; obfuscation techniques; Vienna Cipher Office

1. Introduction

The history of encryption systems (ciphers) goes back a long way. The first ciphers were very simple. Alongside the creation of ciphers came the development of cryptanalysis, or the breaking of ciphers. At the time, the two main goals of cryptanalysis were to decipher the encrypted message without the cipher key and to reconstruct the corresponding cipher key from the plaintext and ciphertext pairs.[1]

CONTACT Eugen Antal eugen.antal@stuba.sk Institute of Computer Science and Mathematics, Slovak University of Technology in Bratislava, Ilkovicova 3, Bratislava 84104, Slovakia

[1]Cipher key reconstruction can help decrypt other intercepted messages that were encrypted with the same cipher system and the same cipher key.

Over time, ciphers evolved (Megyesi et al. 2021), and various techniques were added to make cryptanalysis more difficult. One of the first techniques was the use of *nulls* (Meister 1906; Dunin and Schmeh 2020; Antal and Mírka 2022; Láng et al. 2024). Nulls evolved and eventually became more sophisticated. Because the nature (operational principle) of these techniques changed over time, it is necessary to introduce the obfuscation technique terminology in the context of historical ciphers.

In this work, we focus on a special encryption system called nomenclator (see Section 2) and on the obfuscation techniques (see Section 6) designed to enhance the security of this encryption system.

In modern cryptology, the encryption system should be secure even if the algorithm is publicly known; the security of the encryption system depends only on the secrecy of the cipher key. This principle was formulated by Auguste Kerckhoffs in 1883. In effect, this means that knowledge of both the ciphertext and the plaintext should not allow the cipher key to be revealed. However, this principle did not apply to most historical ciphers. For early modern ciphers, if both the ciphertext and the plaintext are known, it is usually relatively easy to reconstruct the cipher key or at least a substantial part of it. This has generally been our experience. Recently, however, we encountered a cipher for which this observation did not apply. During our research, a certain Central European historical cipher got our attention. We found several ciphertexts with the corresponding plaintexts from a communication between Count Nicolaus Esterházy and Count Wenzel Anton von Kaunitz-Rietberg in the years 1756 and 1757 (Antal et al. 2023). However, we were unable to reconstruct the cipher key from the ciphertext (Figure 1) and plaintext (Figure 2) pairs without knowledge of the obfuscation technique used (false ciphertext unit separators in this case; see Section 6). Thanks to Láng (2020), we were able to obtain the corresponding cipher key with detailed instructions, including a description of the obfuscation techniques used. More information about this cipher, our preliminary analysis of the ciphertexts, and a description of the instructions can be found in Appendix C.

This finding motivated us to investigate a large number of preserved cipher instructions and to study the obfuscation techniques designed. The main goal of this work is to present the development of various obfuscation techniques from a specific geographic location. To this end, we analyzed several cipher keys and their instructions deposited in the Staatskanzlei key collection in the Österreichisches Staatsarchiv in Vienna (Láng 2020). This work partially covers the cipher instructions presented by Megyesi, Láng, et al. (2024) and Láng et al. (2024). However, we focus on the description of advanced obfuscation techniques. In Sections 2 and 3 we briefly describe the nomenclator cipher and provide the historical context of this research.

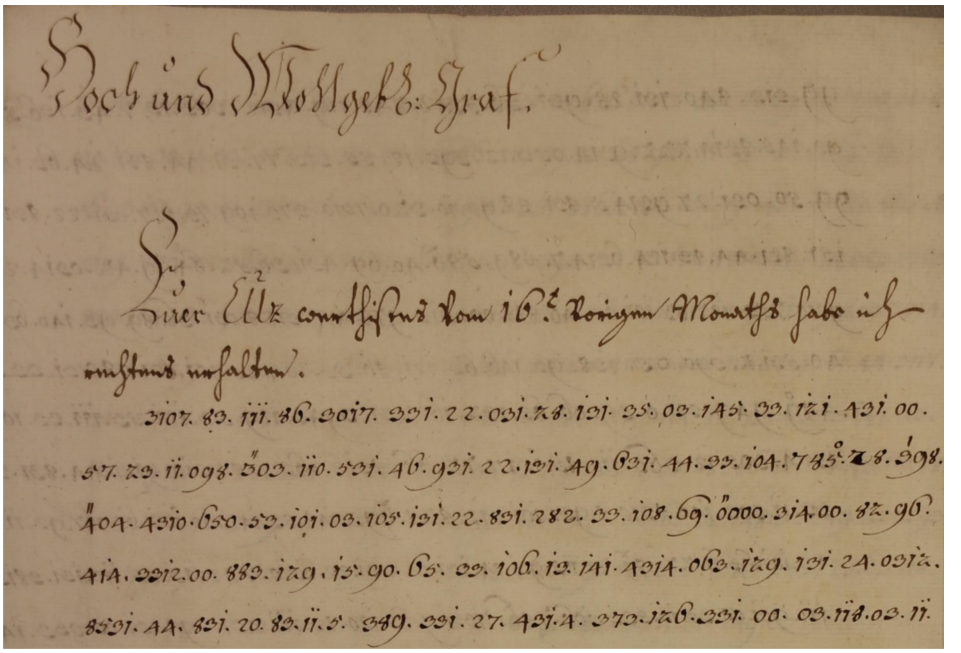

Figure 1. Ciphertext example (Ministry of Interior of the Slovak Republic, Slovak National Archives, fond Esterházi-čeklíska vetva, box no. 634).

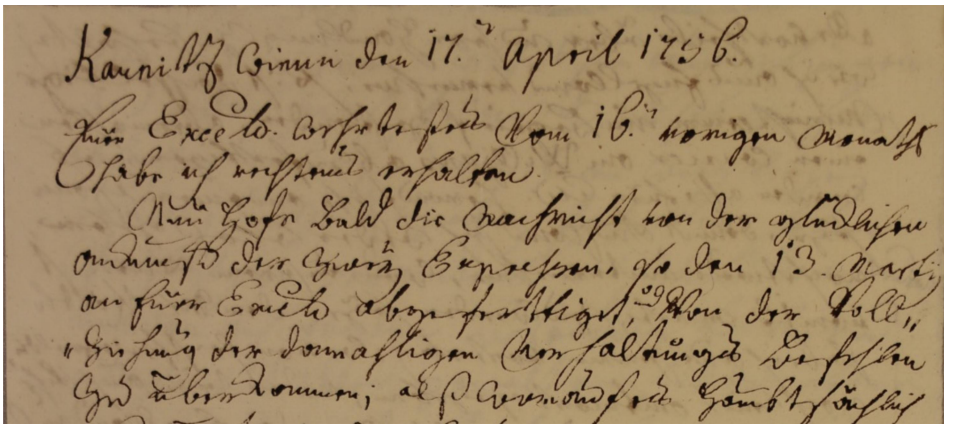

Figure 2. Plaintext example (Ministry of Interior of the Slovak Republic, Slovak National Archives, fond Esterházi-čeklíska vetva, box no. 634).

The methodology we used is described in Section 4, and the analyzed cipher keys and instructions are presented in Section 5. An overview of the analyzed obfuscation techniques is provided in Section 6.

2. Nomenclator encryption system

Historically, one of longest used encryption systems is the nomenclator. It was one of the main encryption systems used before the twentieth century

and was employed extensively in European warfare and diplomacy.[2] Nomenclator consists of several different simple (mainly substitution) encryption systems combined (Meister 1906; Dunin and Schmeh 2020; von zur Gathen 2015; Antal and Mírka 2022; Antal, Zajac, and Mírka 2021). It contains a monoalphabetic or homophonic letter substitution[3] in combination with *n*-grams (bigram and/or trigram substitution),[4] codes,[5] and nulls (or other obfuscation techniques; see Section 6). The encryption rules (different subencryption parts) are represented by the corresponding cipher key. Because of the nature of a substitution, the cipher key contains mainly pairs of plaintext and ciphertext units. If the elements in the key are sorted by the plaintext units, the cipher key is designed for (faster) encryption.[6] If the elements in the key are sorted by the ciphertext units, the cipher key is designed for (faster) decryption.[7]

The ciphertext alphabet of a nomenclator encryption system varies. It may contain letters, symbols (glyphs), numbers, and special markups (Megyesi et al. 2021; Antal et al. 2023). When the elements (mainly the code) in the cipher keys started to grow rapidly, the simplest way to extend the ciphertext alphabet was to switch to numbers only. Some nomenclator ciphers were designed to be used with or without a separator character, which is a special character (most commonly a dot) inserted between ciphertext units to clearly indicate the division of the ciphertext elements.

Early examples of this cipher system were simple, and the cipher key (encryption rules) could be drawn on one large sheet of paper (see Section 5 and Figure 5), with the subencryption parts separated graphically. Antal and Mírka (2022) describe the characteristics of this type of cipher key in more detail. Later, as the codes used in a nomenclator grew to several pages, a different visual format for the encryption key became popular. In this format, which is similar to codebooks, the plaintext and ciphertext elements are shown in a list, sorted into sections according to the first letter of the plaintext elements (see Section 5 and Figure 6). Dunin and Schmeh (2020) discuss the similarities and differences between codebooks and nomenclator systems. A more detailed analysis of the nomenclator encryption system is beyond the scope of this paper. For more information about nomenclator ciphers, their typology, and

[2]Nomenclator was in use from the fourteenth to the nineteenth centuries.

[3]It is not widespread, but some nomenclators contain a polyalphabetic substitution too (Antal and Mírka 2022).

[4]There is often a section for the substitution of syllables, but from a structural point of view, the *n*-grams category is better suited (Antal and Mírka 2022).

[5]In some of the literature, codes are called nomenclatures (Megyesi et al. 2021). However, we use the term *code* to avoid confusion with the term *nomenclator*.

[6]Often marked as *Chiffrant* in the cipher key (Láng 2020).

[7]Often marked as *Déchiffrant* in the cipher key (Láng 2020).

statistics, we recommend Meister (1906), Dunin and Schmeh (2020), von zur Gathen (2015), Megyesi et al. (2021), and Megyesi, Láng, et al. (2024).

3. Historical context

Most of the instructions analyzed in this paper are from the Vienna Cipher Office. It is known that the emperors of the Holy Roman Empire and their official apparatus used encryption as early as the sixteenth century (Walder 2015; Stix 1937; Hubatschke 1975b). The modern office dealing with encryption and cryptanalysis, which is usually called the "black chamber" in the literature (Kahn 1996; Leeuw 2015), probably originated at the court of Emperor Charles VI. During the eighteenth century, and especially in the second half of that century, the Vienna Cipher Office (Ziffernkanzlei)[8] became probably the most efficient black chamber in Europe. Its history has been the subject of several works. Some mention it only in a broad context (Kalmus 1937; Mayr 1935a, 1935b; Reinöhl 1963; Kahn 1996; Auer, 2015), but Stix (1937) made it his main subject. The most important work so far is Harald Hubatschke's unpublished dissertation, especially volumes 5 and 6 (Hubatschke 1975a). That work is based on both his own thorough study of the historical sources and a synthesis of the above-mentioned works. An extract from the dissertation was published in a separate paper (Hubatschke 1975b). Since the history of the office is described in detail in the cited literature, only a brief overview is provided here.

The exact date of the founding of the Cipher Office is not known, but it was probably sometime around the first or second decade of the eighteenth century. Its first head was Rochus Stella a Santa Croce (until 1722); he was followed by von Neuff[9] (1722–1734), Johann Theodor von Imbsen (1734–1742), Ignaz von Koch (1742–1763), Karl Joseph von Püchler (1763–1786), Joseph Franz Stephan von Kronenfels (1786–1812), Michael Bösler von Eichenfeld Jr. (1812–1838), and finally Adalbert von Zaremba (1838–1849) (Hubatschke 1975a).

At first, the office had only three staff members. In 1721, three copyists were added. Already, the results of the office were said to be incredible, and almost nothing was considered indecipherable. Close cooperation with the Imperial Reichspost developed gradually. In the 1730s, it is said that

[8]The name Geheime Ziffernkanzlei dates back to the nineteenth century. Stix (1937) and Hubatschke (1975a, b) used this name in their works. In this paper, we use the broad English equivalent of Cipher Office. In fact, the office has undergone several organizational and name changes. In earlier times, for example, it was known as the Geheymbes Zyffer-Weesen, the Zyffer-Secretariat, the Cabinet-Secretariat, and the Visitations- und Interceptions-Geschäft; after 1750 it was called the Geheime Kabinets-Kanzlei; and in the nineteenth century it was known as the Geheime Kabinets-Kanzlei, Geheimes Chiffrekabinett, Geheimes Ziffernkabinett, and Geheime Ziffernkanzlei.

[9]His first name has not been determined.

the Dutch, English, and French embassies could not send anything by ordinary mail that was not allowed to fall into foreign hands. At that time, the office had ten employees. In the 1740s, the number of employees was reduced, and in 1763, there were still only seven staff members. However, this apparently did not affect its performance. During the time Ignaz von Koch was in charge of the office, its ability to intercept and decipher foreign ciphers was renowned. Koch's successor, Karl Joseph von Püchler, had worked in the office since Koch's arrival in 1742. During Püchler's time, the staff began to increase again, and by the 1780s, there were more than twenty people working in the office, including twelve or thirteen who dealt directly with ciphers. A large number of very advanced key designs and instructions from Püchler's time have survived (more on these in the next section). The office experienced a decline in the early nineteenth century, when only simple ciphers were supposedly made and solved. A revival of its former glory occurred under Chancellor Metternich (Stix 1937; Hubatschke 1975a, 1975b).

Since the time of Emperor Joseph II, the Cipher Office cooperated not only with the postal lodges but also with the police. It thus became an instrument used to monitor the empire's own citizens. This practice intensified under Chancellor Metternich and was eventually one of the main reasons the office was abolished in the aftermath of the revolutionary events of 1848. In the following period, the cipher service operated as part of the Foreign Ministry (Stix 1937; Hubatschke 1975a, 1975b).

4. Sample of instructions and methodology

There is a large collection of cipher keys from the sixteenth through nineteenth centuries in the Österreichisches Staatsarchiv in Vienna (ÖStA/HHStA/Staatskanzlei Interiora/Chiffrenschlüssel, boxes 13–21, 1500–1900). Many were either created or collected by the Cipher Office over the years, but there are also keys from other sources. This collection was briefly described by Hubatschke (1975a), who also presented some interesting ciphers, and in more detail by Láng (2020). The latter states that only the first six of the nine boxes contain about 480 keys.

We examined the entire collection and selected keys that were accompanied by instructions for their use. We then translated and analyzed the selected instructions.

There is no clear definition of a cipher "instruction". Megyesi, Láng, et al. (2024) adopted a broad interpretation, but we define a cipher key instruction as textual information provided for a cipher that contains information about one or more of the following items:

1. how to use the cipher (key) in general;
2. number of encryption tables and how to switch between them;
3. separator characters;
4. how to deal with diacritical marks;
5. how to express numbers and some special phrases;
6. how to use nulls and other obfuscation techniques.

Some instructions may also contain restrictions—such as not mixing the encrypted and unencrypted text parts in the message—to increase the cipher's security. However, there are few limitations of this type in our sample instructions. Most of the investigated instructions were presented on a separate sheet of paper,[10] or they were sometimes written directly on the cipher key.

We first identified 98 instances of textual descriptions in the collection, from which we removed 33 entries consisting of duplicated entries, instructions for polyalphabetic ciphers, and cases in which, after further investigation, the document did not satisfy our definition of a cipher key instruction. This left us with 65 instructions. In almost all cases, the corresponding cipher key was preserved alongside the instruction (the cipher key was missing in only two cases).

The largest subset in this sample consists of the keys and instructions that immediately catch the eye not only because of their similar design but also because of the multiple obfuscation techniques used. They appear throughout the collection. Most of these similar keys have instructions attached. In total, we counted 37 such similar keys with instructions attached, which represents approximately two-thirds of all the instructions examined.[11] Most of them are numbered in red (usually in the lower right corner), but this numbering was probably added at a later time. There are at least two incomplete series of numbers.

All the keys are anonymous, but they were probably the work of one or, more likely, several authors. Unfortunately, we have not discovered any comparative materials that would allow us to identify the scribe. Of course, even if we could, we could not infer that this person was the main or only author of the keys. Of these 37 keys, only 11 were subsequently used in practice. Thus, we believe the Cipher Office was essentially creating designs for sophisticated cipher keys and keeping them in reserve. When a cipher was needed, the selected one was usually given a number (different from the red numbers mentioned above), and the names of the persons or places of the diplomatic missions for which the cipher was intended were written

[10]This often included a plaintext and ciphertext example.

[11]See Appendix E for an overview.

on the front. At the same time, codes for the names of relevant persons who might appear in correspondence were added to the key. These names were quite logically not included in the key designs themselves because it was not yet known when and for what purpose the key would be selected.

On the basis of an analysis of their content, we estimate that this predominantly uniform type of cipher key and instructions was created and used from the early 1770s to the 1790s at least. The method of dating them is discussed in more detail in Appendix D.

Other undated keys with instructions were dated similarly. The oldest key with instructions was created around 1593, and the youngest is dated 12 November 1860. Apart from the aforementioned set of 37 keys with instructions, the sample does not contain any other large set of similar keys. However, it is worth mentioning that the cipher keys from the 1740s and 1750s were mostly of a very high level. We divided all 65 instructions into four time periods:

1. up to 1742 (until Ignaz von Koch took office);
2. 1742–1763 (corresponding to von Koch's leadership);
3. 1763–1800 (most of the keys from this period were created before 1786, when Karl Joseph von Püchler was head of the office; however, this period was extended to the end of the eighteenth century because it was not always possible to determine whether the 37 similar keys were created before or after 1786, and it would not be appropriate to divide them);
4. after 1800.

Based on this division, the vast majority of keys could be assigned to a specific period with near certainty. However, for a few borderline cases whose dating could only be estimated, we chose the most likely period.

Figure 3 shows the distribution of instructions in the specified periods.

It should be emphasized that this time division applies only to the keys with instructions, not to all the keys in the collection. For the keys themselves, regardless of whether instructions were attached, the ratio of numbers in time periods could be different. Thus, Figure 3 tells us only from which period most of the instructions survived.

Considering the provenance of the collection, it is not surprising that most of the keys or instructions are written in German. Fifty-one of the 65 are written only in German, 1 in both German and Latin, 1 in both German and Italian, 1 in Latin only, and 11 in French.

Except for two instructions, they all contain information about nulls and other obfuscation techniques.

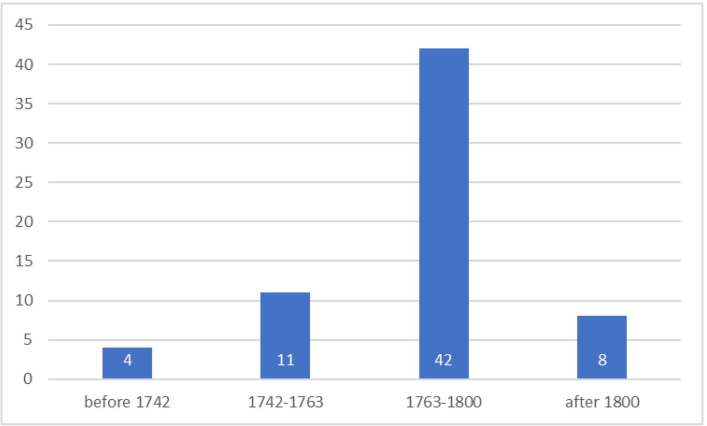

Figure 3. Number of keys with instructions by time periods.

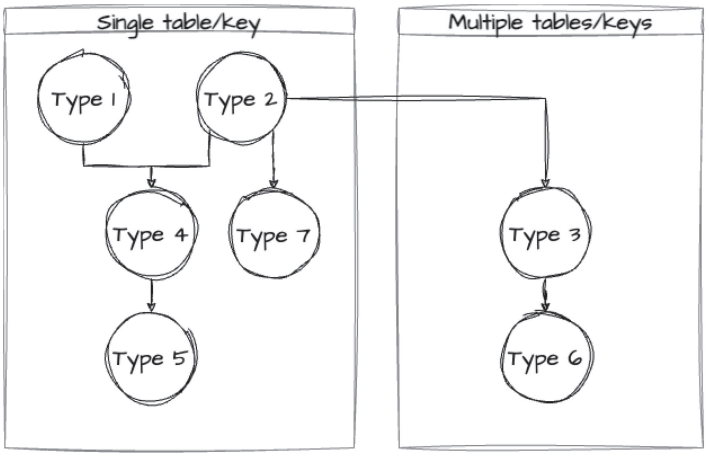

Figure 4. Typology of cipher key types.

The 65 analyzed instructions can be divided into two main categories, based on the location of the instructions. In 60 cases, the instructions were written outside the range of the cipher key, on a separate sheet of paper. In 5 cases, the instructions were present on the same sheet of paper, alongside the cipher key. Some instructions were titled with a header such as Note, Information, Instruction, Belehrung, Weisung zum Ziffer-Schlüssel, or Gebrauch des Ziffer-Schlüssels. However, in many cases, the instructions had no heading.

In the next step, we created a typology based on the cipher keys' visual characteristics and divided them into seven categories (described in Section 5). Then we analyzed the textual information and the corresponding cipher keys. We identified the main properties of the obfuscation techniques employed and divided them into three main categories. Due to the

large variety of obfuscation techniques, we split the main categories into smaller subcategories (see Section 6). We described the main properties of the ciphers,[12] based on the available cipher key and instruction.

5. Overview of cipher keys

We analyzed the cipher keys that relate to the 65 instructions and divided them into several categories based on their properties and visual representation (see Figure 4). Each type is described in more detail below (on cipher key morphology, see Megyesi et al. 2021). Some of the ciphers used a single key (table); in other cases, multiple different cipher keys (tables) were employed during encryption.

5.1. Single key table

One of the basic cipher key types (Type 1, Figure 5) consists of one sheet of paper,[13] where the subencryption parts are graphically separated. Most commonly, the letter substitution table and the *n*-gram substitutions are in a separate table, followed by a list of nulls and a list of codes. The order and location of the subencryption parts are not strictly uniform; however, the letter substitutions are often displayed at the beginning, and the codes are displayed at the end. This type was popular mainly before the eighteenth century. In the set of analyzed cipher keys, we found only four keys of this type; however, many Type 1 cipher keys can be found in other archives, such as in the Hessian State Archives from the time of the Thirty Years' War (Antal and Mírka 2022). Until the seventeenth century, this was probably the most common type of cipher key. Many examples can be found in Meister (1906) and in the DECODE Database (Héder and Megyesi 2022).

The second basic type (Type 2, Figure 6) consists of a list of the plaintext and ciphertext pairs, commonly sorted alphabetically and divided into subsections based on the first letter of the plaintext element. Type 2 often appears in booklet form, depending on the number of elements used. In the investigated collection, we found 23 instances of Type 2. In this type, the subencryption parts are not separated graphically. In both Type 1 and Type 2, there may be additional separated sections containing only selected entries (e.g., persons' names, geographic locations, numbers). Type 2 is the most common cipher key type in the collection from Vienna. List-type cipher keys that have additional, visually separated parts are designated

[12]Cipher key type, number of different cipher tables used, ciphertext alphabet, plaintext elements, details of the obfuscation techniques, etc.

[13]Or multiple sheets, depending on the length of the code.

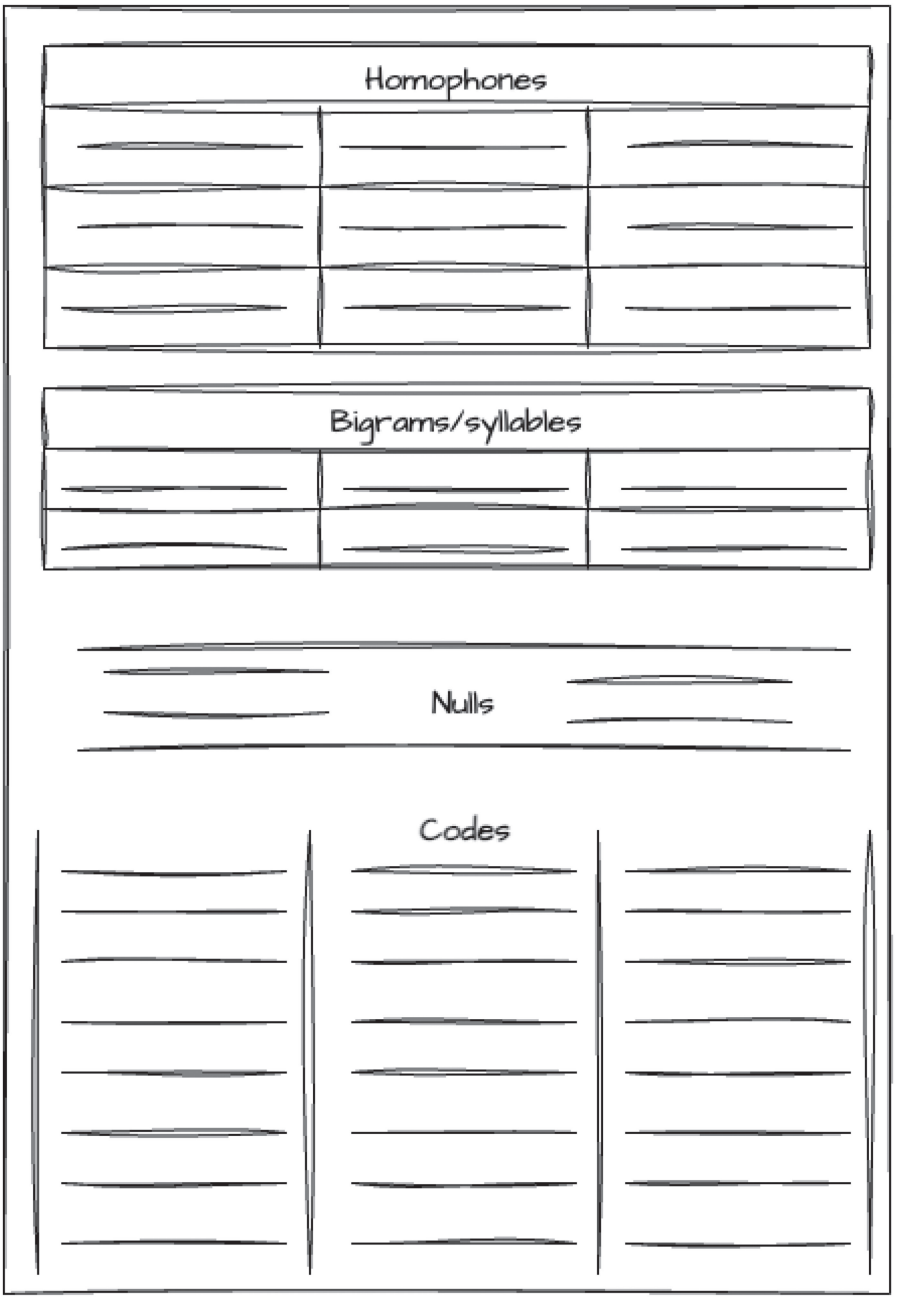

Figure 5. Cipher key Type 1.

Types 4 and 5. Type 4 (Figure A3) contains a special header in the upper part of the sheet where obfuscation techniques and special characters are separated (nine cases found). A slightly different version is Type 5 (Figure A4), where the header from Type 4 is located (usually on a separate sheet

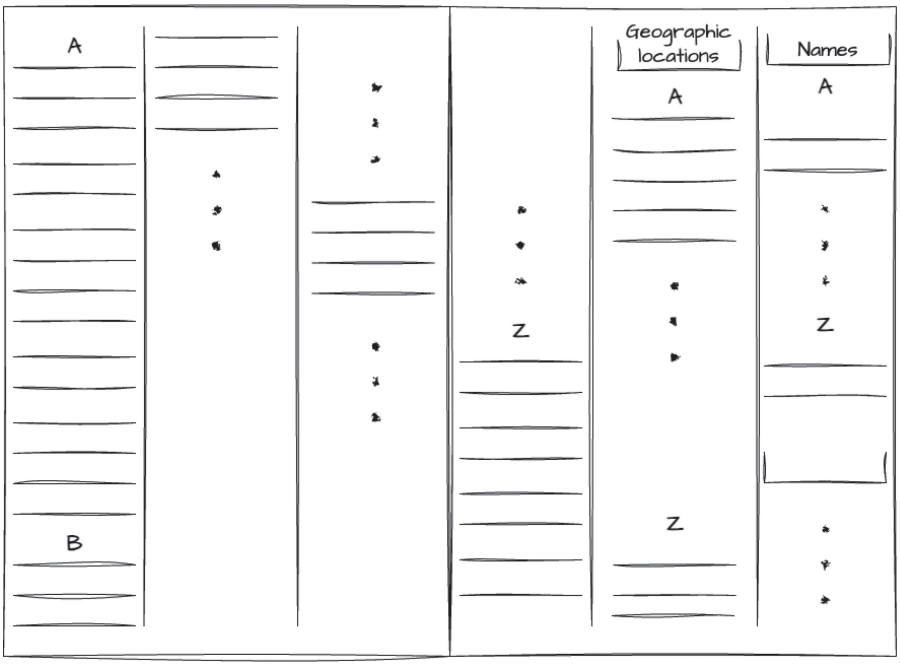

Figure 6. Cipher key Type 2.

of paper) at the beginning or end of the cipher key (two cases found). Types 4 and 5 are a mixture of Types 1 and 2.

Type 7 (Figure A5) is a variation of Type 2 in which the cipher key consists of several pages, and additional markings are drawn on the right side of each sheet of paper. These markings contain information about the plaintext unit groups (first letters) and the ciphertext unit ranges. The markings were probably intended to increase the speed of using the cipher key. We found only one instance of this type.

Examples of these types found in ÖStA/HHStA/Staatskanzlei Interiora/Chiffrenschlüssel (boxes 13–21) are: box 14, fasc. 20, f. 159 (Type 1); box 15, fasc. 21, f. 26–29 (Type 2); box 15, fasc. 21, f. 38–46 (Type 4); box 17, fasc. 24, f. 1–29 (Type 5); and box 20, fasc. 27 (Varia), f. 10–11 (Type 7).

5.2. Multiple key tables

Some cipher keys were designed to use multiple cipher key tables.[14] The length of the ciphertext units may differ for each table. Most commonly, two to ten tables were used per cipher key. The tables were switched using special *table switch indicator* elements, reserved from the ciphertext alphabet in each cipher key table. Type 3 (Figure A1) is an extension of Type 2 adapted to allow the use of multiple tables. In Type 3, additional markings

[14]Commonly marked as key 1, 2, … (Clavis 1, 2, …).

are drawn on the right side of each sheet of paper to identify the cipher key table. Commonly, there is one cipher key per page. We found 22 instances of Type 3. Examples of this type are box 15, fasc. 21, f. 2–13 (10 tables), and box 15, fasc. 21, f. 54–57 (2 tables) in ÖStA/HHStA/Staatskanzlei Interiora/Chiffrenschlüssel (boxes 13–21).

We also found specially modified Type 3 cipher keys in which the basic Type 2 properties are slightly different, designated Type 6 (Figure A2). This cipher type is applicable only when the ciphertext elements start with the same sequence (at least in the corresponding sections or columns). Probably to increase the speed of encryption or decryption, each column has a special header containing the beginning of the cipher unit (the sequence is the same for each element in the column). This sequence is omitted from the rest of the column and is available only in the header. We found six instances of Type 6. An example of this type is box 19, fasc. 26, f. 127–141, in ÖStA/HHStA/Staatskanzlei Interiora/Chiffrenschlüssel (boxes 13–21). In Láng et al. (2024, p. 19, instruction text in German), this cipher type is called the "polyalphabetic nomenclature cipher".

6. Overview of obfuscation techniques

In the context of this paper, an obfuscation technique of a nomenclator cipher system is a technique used to make cryptanalysis more difficult by modifying parts of the ciphertext. This modification can be performed:

- in the ciphertext by adding new elements that do not have a predefined mapping in the plaintext alphabet;
- in the ciphertext by adding new elements, which changes other elements at a different position (see Figure B1 for further details):
  - in the ciphertext before decryption,
  - in the plaintext after decryption;
- in ciphertext units by removing or modifying part of a cipher unit or by adding new elements to it.

From the instructions and the plaintext cipher examples, we were able to identify and describe a large variety of obfuscation techniques. Based on their characteristics, we divided the obfuscation techniques into three main categories: *nulls*, *annullants*, and *false separators* (see Figure 7). We then split nulls and annullants into subcategories. The individual techniques are described in more detail in the following subsections.

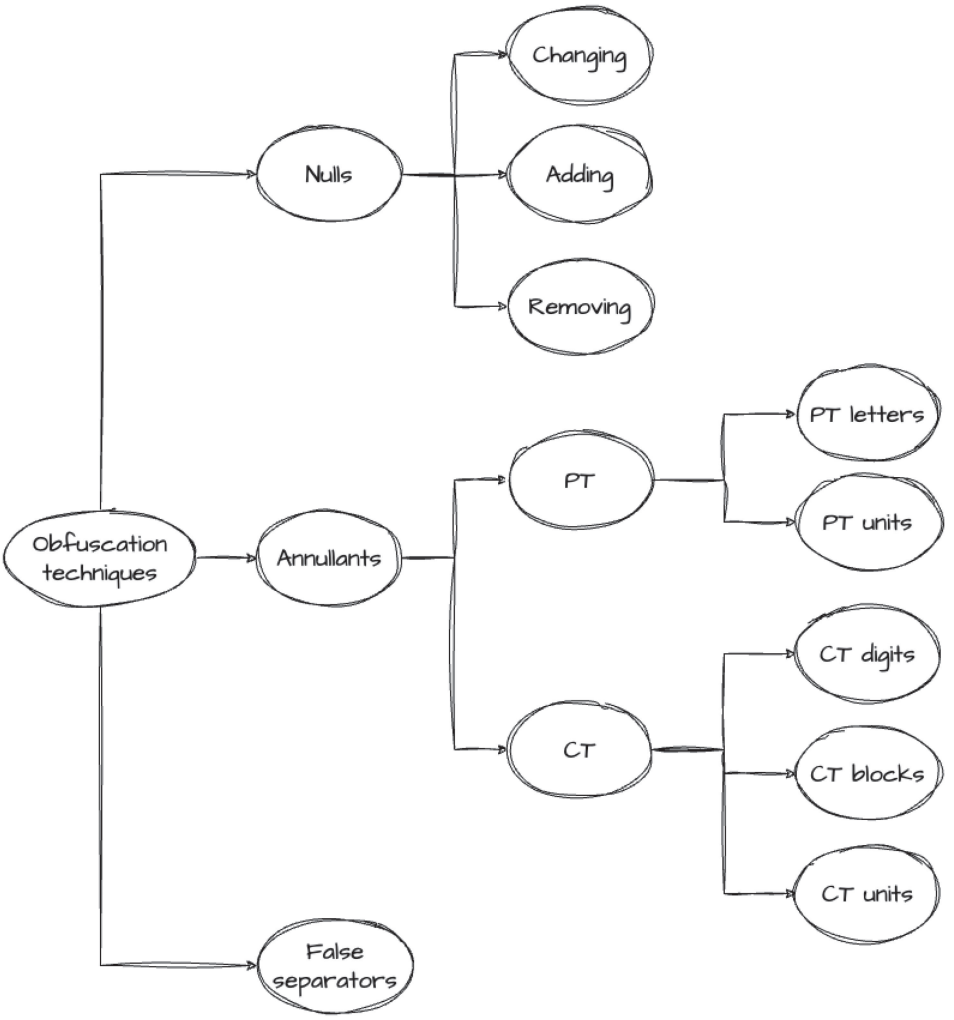

Figure 7. Typology of obfuscation techniques.

6.1. Nulls

Nulls[15] (or null characters) are special characters added to the ciphertext during or after the encryption process. These characters have no meaning, and the message's legitimate recipient has to remove the nulls from the ciphertext before or during decryption. Nulls are generally listed in the cipher key. However, in some cases, they are not listed directly but are described in the instructions. Here, we use the term *null* for both cases. In our collection, the ciphertext alphabet was mostly numerical; therefore, the described techniques are based primarily on a numerical representation.

[15]Errantes/err., nonvaluers, etc.

In the analyzed collection, we found several different types of nulls. The most common were:

- one specific entry (ciphertext unit);[16]
- multiple entries listed directly in the cipher key;
- unused entries in the key;
- defined interval(s) of numbers;
- entries not present in the ciphertext alphabet (e.g., if only numbers are used, any added letter or symbol is a null).

There were also special cases of nulls, applicable only to a specific cipher key structure:

- homophonic cipher:
  - during the encryption of one letter, multiple elements are inserted from the same group of homophones,[17] but during decryption, only the first occurrence is kept;
- ciphertext with separators:
  - if the ciphertext entries (separated by a separator character) have a fixed length in the cipher key, additional numbers can be inserted as nulls at the end of any ciphertext unit, but for ciphertext elements longer than the fixed length, these additional characters must be removed during decryption;
  - all numbers containing a specific digit (at any position) are nulls;
  - all numbers starting with a specific digit or digits, plus an additional condition (e.g., the number must be a certain length), are nulls;
- ciphertext without separators:
  - randomly inserted elements in random positions, but these elements have to be marked visually;
- ciphertext units with a fixed length:
  - some digits at a specific position (e.g., first) can be duplicated as a null digit;
  - addition of a specific (e.g., odd or even) digit before or after a ciphertext unit (number);
  - one or more random digits inserted in every ciphertext unit (number) at a specific position;

[16]There may be some restrictions. For example, if digit 0 is selected as null, it can be an exception from null (i.e., must be kept) if it occurs after a special digit 1 (e.g., number 10).

[17]A group of homophones represents a set of ciphertext elements belonging to exactly one plaintext element.

    - if the ciphertext units have a specific structure (e.g., the first two digits are the same), null is any number without this structure; this is also applicable in the opposite way;
    - if the ciphertext units have a specific structure (e.g., the first two digits are the same), nulls are any (multiple) digits inserted between the identical digits in the number;
    - a fixed number of random or specific digits added before or after all entries;
    - any number longer than the fixed length;
- multiple cipher key tables:
    - if the ciphertext entries are different in the key tables (different length or value), all elements in one key table are nulls during use of a different key table, and vice versa;
    - all entries from the first table with a given structure (e.g., the same digits at the first two positions) used in a different table are nulls; this also works in the opposite way for another key table with a different structure;
    - elements in the second table are created in such a way that a random (specific) digit is inserted before the element (or at a fixed position) in the first table (only the added digits are nulls);
    - the cipher key table id can be used as null;
- other specific structures:
    - if the cipher key consists of only even numbers, all odd numbers are nulls, and vice versa;
    - if all entries in the cipher key start with even digit, all entries starting with odd digits are nulls, and vice versa.

The general interpretation of a null is that it *adds* a meaningless element to the ciphertext. In previous cases, nulls were added based on defined rules. However, the nature of a null character may vary, and we found several instances in which the null (meaningless) character was created in a different way. Based on the key structure, some digits in the entries may be redundant (e.g., the same digit is at a specific position for all entries), so a digit at a specific position can be *removed* without losing information. A similar technique can be used for cipher keys with the same structure. If some digits are redundant, they can be *changed* to any other (random) digit at a specific position. If entries are used in the base form in combination with the reduced or modified form, this can increase the variability of the cipher key (similar to a homophonic cipher) and can flatten the frequency characteristics.

See Figure B1 (first row) for visual examples.

6.2. Annullants

Annullants (or cancelation signs, as used by Megyesi, Láng, et al. 2024) are more advanced versions of null characters with a slightly different interpretation. Annullants invalidate a fixed-length sequence of elements located before or after the place where the annullant is inserted into the ciphertext. The invalidated elements have to be removed during or after decryption. The annullant can invalidate both plaintext and ciphertext elements. In the case of plaintext elements, letters or larger plaintext units (n-grams or words) are most commonly invalidated (canceled). In the case of ciphertext elements, ciphertext units, a block of ciphertext units, or smaller parts (digits in the case of numerical representation) are invalidated. See Figure B1 (second and third rows).

In the analyzed collection, we found several different types of annullants. Annullants could be unmapped ciphertext elements, specially constructed elements (e.g., a random number starting with a special digit, such as 0), or directly listed in the cipher key or instructions.

The most commonly used annullants invalidate the following ciphertext elements:

- a certain number (n) of previous or following ciphertext units (numbers); if numbers are used without a separator character, the ciphertext unit has a fixed length (number of digits);
- a certain number (n) of previous or following digits in the ciphertext;
- a certain number (n) of following lines;
- everything up to the end of the current line;
- everything up to the end of the current page;
- a digit at a fixed position in the following n numbers.

In the case of plaintext units, most commonly used annullants invalidate a certain number of letters in the plaintext sequence located before or after the annullant's position. There may be variations in which letters are invalidated from the end of the decrypted word. If multiple entries are invalidated (in both plaintext and ciphertext), n mostly stands for $\{1, 2, 3, 4, 5\}$.

There may be special cases regarding the interpretation of annullants. We found an example in which inserting one annullant meant deleting one ciphertext unit after that position, but inserting two annullants meant deleting one ciphertext unit before and one ciphertext unit after the annullants' position.

6.3. False separators

False separators are separator characters (e.g., dots) inserted in the ciphertext that do not indicate the correct division of the elements; see Figure B1 (third row). The aim is to confuse any illegitimate reader of the encrypted message and make cryptanalysis more difficult. These separators must be ignored during decryption. False separators may be used in combination with other obfuscation techniques to increase the cipher's security (see Appendix C).

When cipher elements consist of fixed-length numbers, inserting false separators at random positions makes it appear that the cipher uses numbers of various lengths.

When cipher keys use various-length numbers, a specific element (e.g., a digit) can be used as a legitimate separator character to divide the ciphertext elements, and other symbols (e.g., dots) can be inserted at random positions to create confusion.

We found a specific cipher key in which three- and four-digit numbers were used as cipher elements, and every element contained a dot at a predefined position (dividing the numbers into $1+2$, $2+1$, and $3+1$ digit parts). These dots were false separators used as an obfuscation technique. These elements were separated with an additional dot character during encryption. If the structure of the cipher key is known, the cipher elements and the real separators can be identified.

7. Summary

The nomenclator is one of the oldest encryption systems. The security of this type of cipher varies, based on its design and its correct usage. There are real-life ciphers preserved in archives that are resistant to all of today's modern computerized approaches to cryptanalysis. The security of this cipher type can be enhanced using special obfuscation techniques such as nulls, anullants, and false separators. Most commonly, the ciphertext is expanded by adding nulls (meaningless elements). However, ciphertext units can also be changed (removed or modified). By using annullants (cancelation signs), ciphertext or plaintext elements of varying lengths (letters, blocks, lines, paragraphs) can be removed. If this technique is used correctly, the difficulty of cryptanalysis is increased. Security can be increased even more with the use of false separators to confuse any illegitimate reader. Even if the ciphertext contains no obvious separators or contains only false separators, it often consists of codes of varying lengths, and there are techniques to recognize the number of characters in a code. One method of making cryptanalysis more difficult is to create multiple tables with the same plaintext words but different codes. The tables are then switched, using indicators for which special codes were created. If these techniques are combined, well designed, and correctly used, the cipher is very hard (or almost impossible) to solve from only ciphertext.

About the authors

Eugen Antal is an assistant professor at the Slovak University of Technology in Bratislava. He specializes in modern cryptanalysis of classical ciphers. His interest in classical ciphers is motivated by the famous Zodiac killer's Z340 cipher. Currently, he is investigating historical ciphers from the Central European countries and leads the HCPortal (https://www.hcportal.eu/) project.

Jakub Mírka is an archivist at the State Regional Archives in Pilsen, where he manages the family archives of the nobility and the archival fonds of their land estates. He specializes in the Bohemian social and economic history and the development of cryptology in Central Europe in the early modern era.

Dušan Kováč is an emeritus fellow of the Institute of Historical Research, Slovak Academy of Sciences. His main field of research is Slovak and Central European History in the 19th and first half of the 20th centuries and the history of historical thinking. He published more than 200 historical studies and articles. In the years 1989–1998, he was director of the Institute of Historical Research, Slovak Academy of Sciences. He is a member of the Slovak, Hungarian, and Austrian Academy of Sciences and a member of the Royal Historical Society London.

Acknowledgements

We would like to thank Tünde Lengyelová, Diana Duchoňová, and Zuzana Šedová for their help. We also thank Benedek Láng for his helpful comments and suggestions.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This research was supported by Ministry of Education, Science, Research, and Sport of the Slovak Republic through grant VEGA 2/0054/24 and by the project Artificial Intelligence for Encrypted Handwritten Document Processing, 09I05-03-V02-00031 of Support of Research Projects Aimed at Digitization of the Economy in TRL Levels 1–3, Call. No. 09I05-03-V02, managed by the Research Agency and funded by the Recovery and Resilience Facility of the Slovak Republic.

References

Antal, E., P. Marák, P. Zajac, T. Lengyelová, and D. Duchoňová. 2023. Encrypted documents and cipher keys from the 18th and 19th century in the archives of aristocratic families in Slovakia. In Proceedings of the 6th International Conference on Historical Cryptology, HistoCrypt 2023, 1–12. Linköping University Electronic Press.

Antal, E., and J. Mírka. 2022. Wrong design of cipher keys: Analysis of historical cipher keys from the Hessisches Staatsarchiv Marburg used in the thirty years' war. In Proceedings of the 5th International Conference on Historical Cryptology, HistoCrypt 2022, 1–11. Linköping University Electronic Press.

Antal, E., P. Zajac, and J. 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, 12–24. Linköping University Electronic Press.

Auer, L. 2015. Die Verwendung von Chiffren in der diplomatischen Korrespondenz des Kaiserhofes im 17. und 18. Jahrhundert. Der letzte Ritter als erster Verschlüsser im Reich. In *Geheime Post Kryptologie und Steganographie der diplomatischen Korrespondenz europäischer Höfe während der Frühen Neuzeit*, ed. A.-S. Rous and M. Mulsow, 153–69. Berlin: Duncker & Humblot.

Dunin, E., and K. Schmeh. 2020. *Codebreaking: A practical guide*. Robinson. London: Great Britain.

Héder, M., and B. Megyesi. 2022. Database of historical ciphers and keys: Version 2. In Proceedings of the 5th International Conference on Historical Cryptology, HistoCrypt 2022, 1–11. Linköping University Electronic Press.

Hubatschke, H. 1975a. Ferdinand Prantner (Pseudonym Leo Wolfram) 1817-1871. Die Anfänge des politischen Romans sowie die Geschichte der Briefspionage und des geheimen Chiffredienstes in Österreich. Unpublished diss., Universität Wien.

Hubatschke, H. 1975b. Die amtliche Organisation der geheimen Briefüberwachung und des diplomatischen Chiffrendienstes in Österreich. *Mitteilungen des Instituts für Österreichische Geschichtsforschung* 83(3-4):352–413. doi: 10.7767/miog.1975.83.34.352.

Kahn, D. 1996. *The codebreakers: The comprehensive history of secret communication from ancient times to the internet*. New York: Scribner.

Kalmus, L. 1937. *Weltgeschichte der Post. Mit besonderer Berücksichtigung des deutschen Sprachgebietes*. Wien: Verlag für Militärwiss. & Fachliteratur.

Láng, B. 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, 87–95. Linköping University Electronic Press. doi: 10.3384/ecp2020171012.

Láng, B., B. Megyesi, N. Kopal, V. Mikhalev, C. Tudor, and M. Waldispühl. 2024. Cipher key instructions in early modern Europe: Analysis and text edition. *Cryptologia*. Taylor & Francis. doi: 10.1080/01611194.2024.2396800.

Leeuw, K. 2015. Books, science, and the rise of the Black chambers in early modern Europe. In *Geheime Post Kryptologie und Steganographie der diplomatischen Korrespondenz europäischer Höfe während der Frühen Neuzeit*, ed. A.-S. Rous and M. Mulsow, 87–99. Berlin: Duncker & Humblot.

Mayr, J. K. 1935a. *Geschichte der österreichischen Staatskanzlei im Zeitalter des Fürsten Metternich. Inventare österreichischer staatlicher Archive, V. Inventare des Wiener Haus-, Hof- und Staatsarchivs, Band 2*. Wien: Selbstverlag des Haus-, Hof- und Staatsarchivs.

Mayr, J. K. 1935b. *Metternichs geheimer Briefdienst. Postlogen und Postkurse. Inventare österreichischer staatlicher Archive, V. Inventare des Wiener Haus-, Hof- und Staatsarchivs, Band 3*. Wien: Selbstverlag des Haus-, Hof- und Staatsarchivs.

Megyesi, B., B. Láng, N. Kopal, V. Mikhalev, T. Crina, and W. Michelle. 2024. A typology for cipher key instructions in early modern times. In Proceedings of the 7th International Conference on Historical Cryptology, HistoCrypt 2024, 183–193. Tartu University Library.

Megyesi, B., C. Tudor, B. Láng, and A. Lehofer. 2021. Key design in the early modern era in Europe. In Proceedings of the 4th International Conference on Historical Cryptology, HistoCrypt 2021, 121–30. Linköping University Electronic Press.

Megyesi, B., C. Tudor, B. Láng, A. Lehofer, N. Kopal, K. de Leeuw, and M. Waldispühl. 2024. Keys with nomenclatures in the early modern Europe. *Cryptologia* 48 (2):97–139. Taylor & Francis. doi: 10.1080/01611194.2022.2113185.

Meister, A. 1906. *Die geheimschrift im dienste der Päpstlichen kurie von ihren anfängen bis zum ende des XVI. Jahrhunderts*. Paderborn: Druck und Verlag von Ferdinand Schöningh.

ÖStA. 1500–1900. Österreichisches Staatsarchiv, Haus-, Hof- und Staatsarchiv, Staatskanzlei Interiora, Chiffrenschlüssel, Karton (box) 13–21.

Reinöhl, F. 1963. *Geschichte der k.u.k. Kabinettskanzlei*. Mitteilungen des Österreichischen Staatsarchivs, Ergänzungsband 7. Wien, Druck und Verlag Ferdinand Berger: Horn, N.-Ö.

Stix, F. 1937. Zur Geschichte und Organisation der Wiener Geheimen Ziffernkanzlei. *Mitteilungen Des Instituts Für Österreichische Geschichtsforschung* 51 (JG):131–60. doi: 10.7767/miog.1937.51.jg.131.

von zur Gathen, J. 2015. *CryptoSchool*. Berlin, Heidelberg: Springer.

Walder, A. 2015. Der letzte Ritter als erster Verschlüsser im Reich. In *Geheime Post Kryptologie und Steganographie der diplomatischen Korrespondenz europäischer Höfe während der Frühen Neuzeit*, ed. A.-S. Rous and M. Mulsow, 121–35. Berlin: Duncker & Humblot.

Winter, O. F., ed. 1965. *Repertorium der diplomatischen Vertreter aller Länder seit dem Westfälischen Frieden (1648). III. Band (1764-1815)*. Graz-Köln: Verlag Hermann Böhlaus Nachf.

Appendix A. Cipher key types

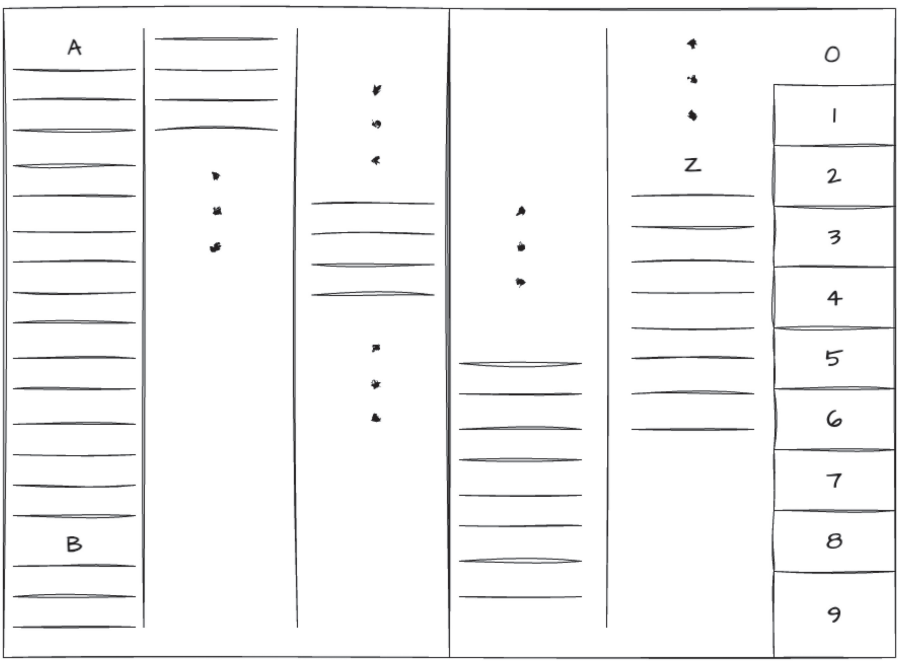

Figure A1. Cipher key Type 3 (multiple tables/keys).

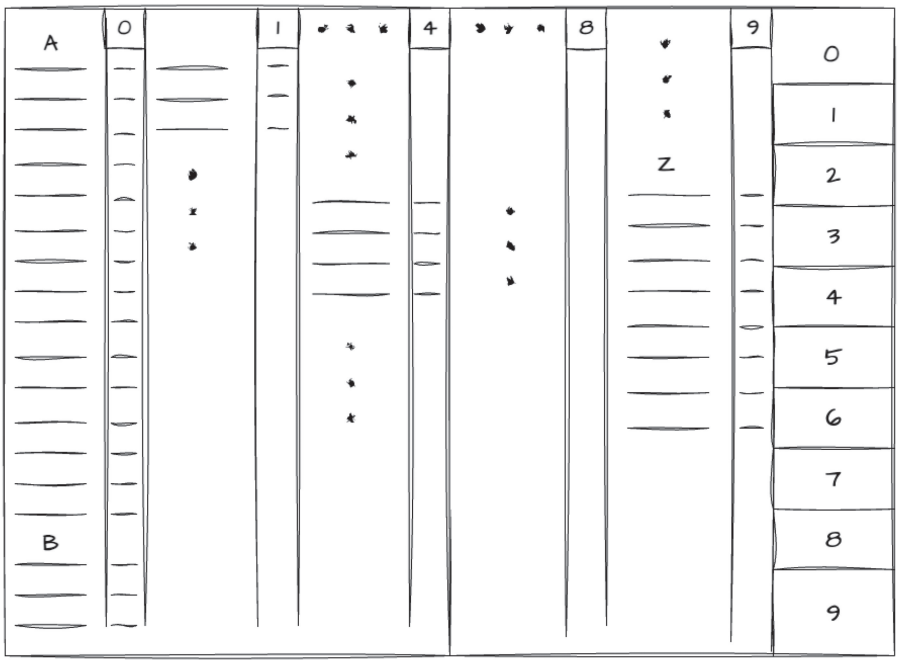

Figure A2. Cipher key Type 6 (multiple tables/keys).

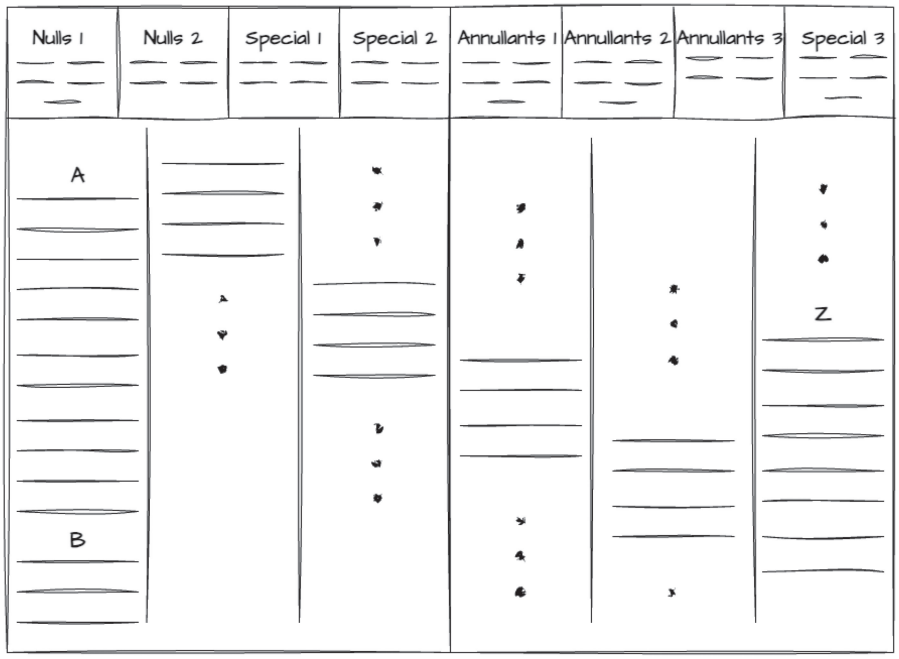

Figure A3. Cipher key Type 4 (single table/key).

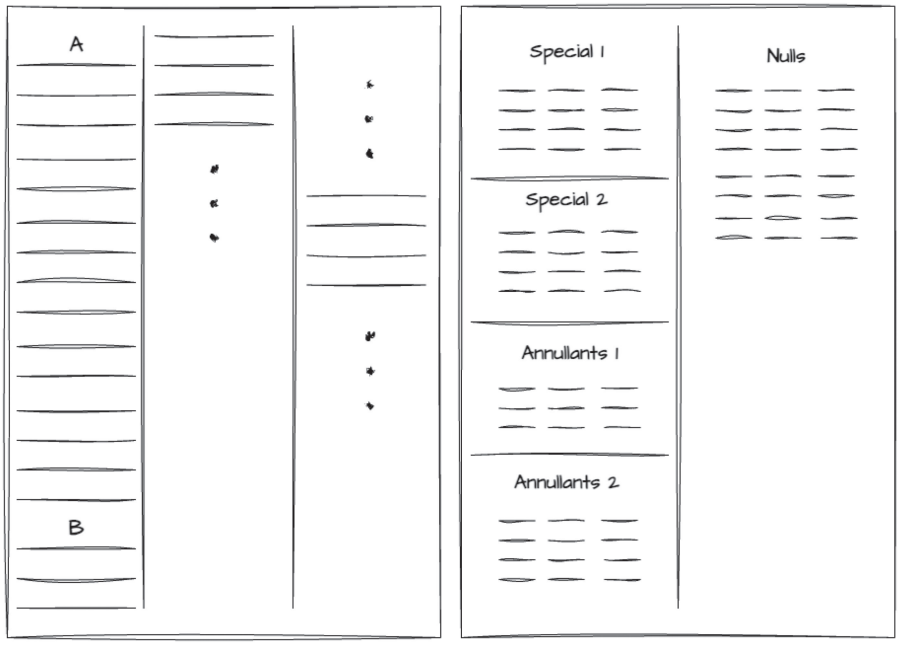

Figure A4. Cipher key Type 5 (single table/key).

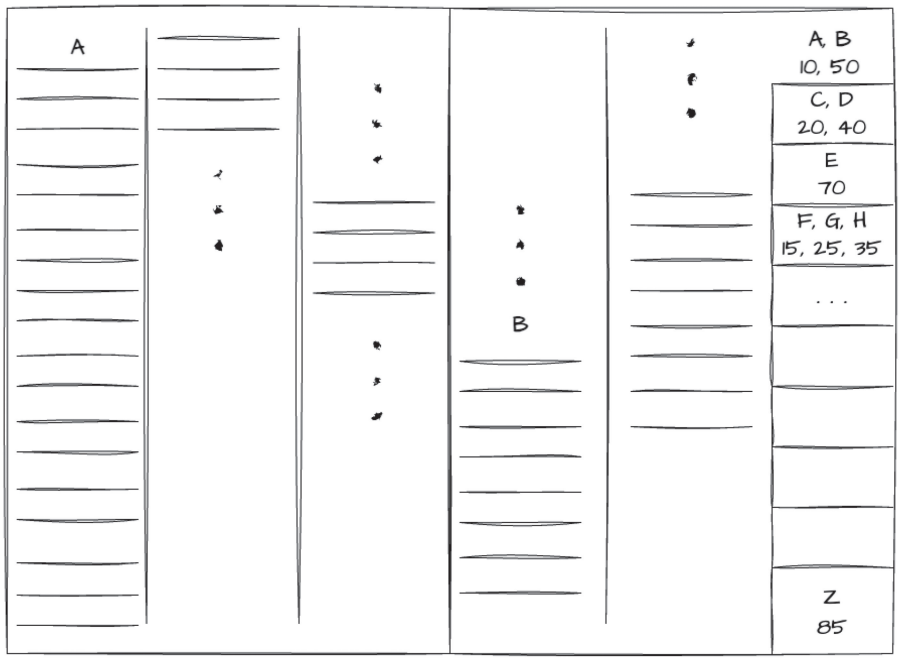

Figure A5. Cipher key Type 7 (single table/key).

Appendix B. Examples of obfuscation techniques

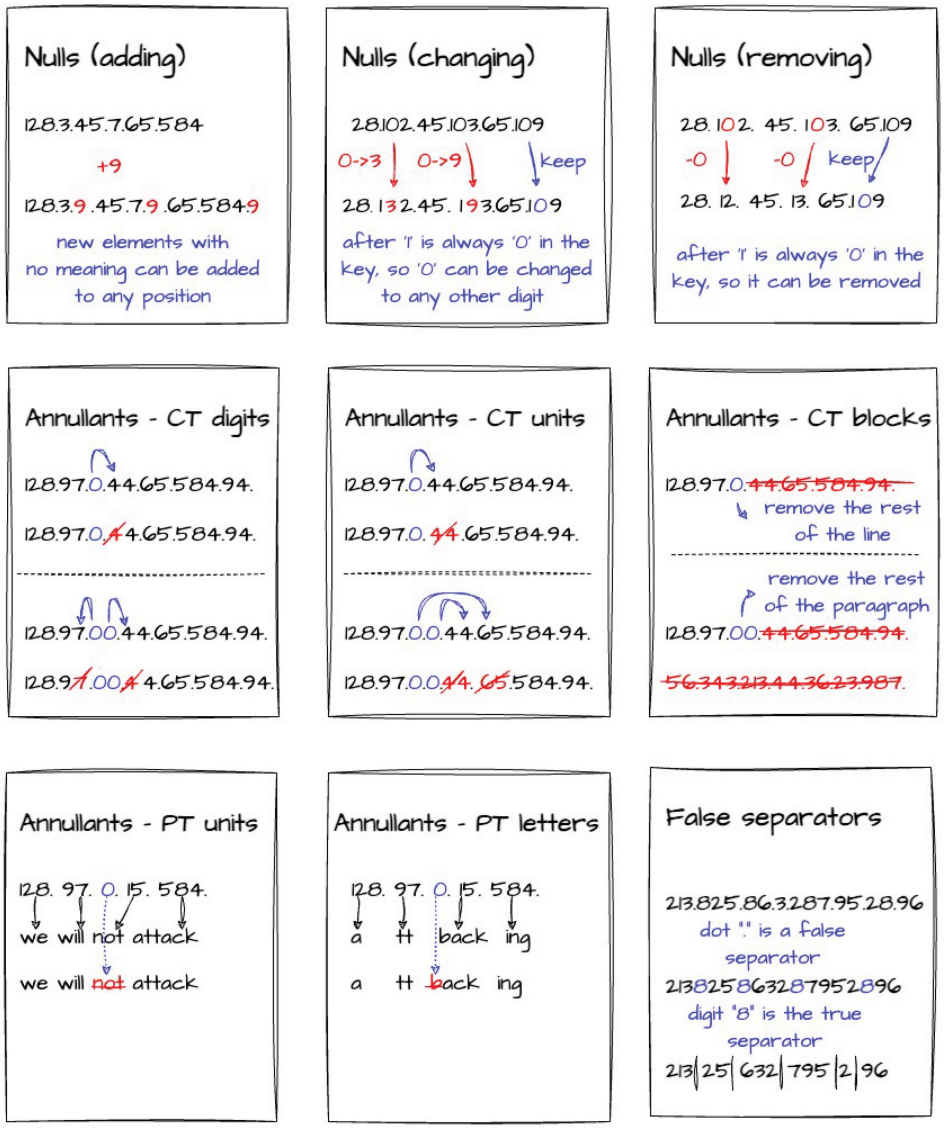

Figure B1. Examples of obfuscation techniques.

Appendix C. Example of an advanced obfuscation technique

The Slovak National Archive in Bratislava, Esterházy family archive (Čeklís family branch), card box no. 634 contains, among others, sixteen encrypted messages sent between Count Nicolaus Esterházy and Count Wenzel Anton von Kaunitz-Rietberg beginning in 1756. The whole communication is in the German language. Based on the ciphertext characteristics, all these messages were encrypted with the same key. The plaintexts (decrypted messages) were also preserved for all the ciphertexts. Unfortunately, the collection does not contain the cipher key.

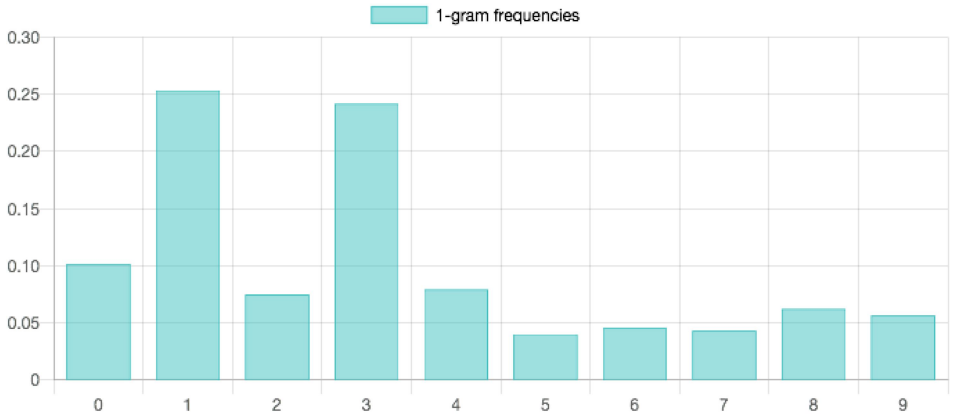

Figure C1. Relative frequency of digits.

In the first step, we transcribed some selected ciphertexts and the corresponding plaintexts. Our primary goal was to reconstruct the cipher key used.

Next, we analyzed the ciphertext and performed a frequency analysis of the ciphertext elements. The ciphertext consists of numbers of various lengths, separated by dots. This is a strong indication that a nomenclator cipher was used. We must therefore assume that the cipher consists of a (homophonic) letter substitution, *n*-gram substitution, codes, and probably nulls.

We split the ciphertext into numbers based on the separator character to obtain the ciphertext elements.[18] Our goal was to match the plaintext elements (letters, *n*-grams, words) and ciphertext symbols (numbers). We focused on the beginning and ending sequences of the documents because it was easier to align the plaintext and ciphertext elements in those parts.

We searched for repeated plaintext words (and other sequences) in the messages and tried to find ciphertext units (unit sequences) that also repeated. If a code was used for the name of a king or some other important person, it is highly probable that the same ciphertext unit would also appear. But because the codes could also be homophonic, there was no guarantee that the same ciphertext unit would appear for the code element. If a word was encrypted by letters and *n*-grams or syllables with a homophonic cipher, some ciphertext units might repeat. If the scribe used the homophonic cipher incorrectly (or the cipher was not homophonic), the ciphertext sequences must repeat. We marked several possible plaintext and ciphertext pairs, but the results were insufficient to reconstruct enough elements of the cipher key.

We used the full transcription of selected ciphertexts (more than 11,000 digits) and performed a frequency analysis of digits. As shown in Figure C1, the frequency of digits 1 and 3 was more than twice the frequency of any other digit. Also, the sequence 31 was the most frequent bigram in the numbers separated by a dot (in the ciphertext units).

It was also obvious from a visual check of the ciphertext that digits 1 and 3 may have some special meaning. One possibility is that the cipher was designed so that most of the ciphertext elements start or end with 31. We also assumed that the sequence 31 could be either a null or a separator (instead of a dot). If 31 was a separator, we needed to remove all the dots and replace all occurrences of sequence 31 with a space (or some other

[18] It later became clear that this was the main mistake we made.

separator) and re-create the ciphertext units. Unfortunately, we were still unable to reconstruct the cipher key. Although we were able to identify a few codes, it became clear that trying to obtain the complete key would be very time-consuming.

Later, based on Láng (2020), we found the correct cipher key and instructions in Vienna (ÖStA/HHStA/Staatskanzlei Interiora/Chiffrenschlüssel, box 16, fasc. 23, fol. 13–16). The cipher key is from 1752. It showed that the cipher system was much more complex than

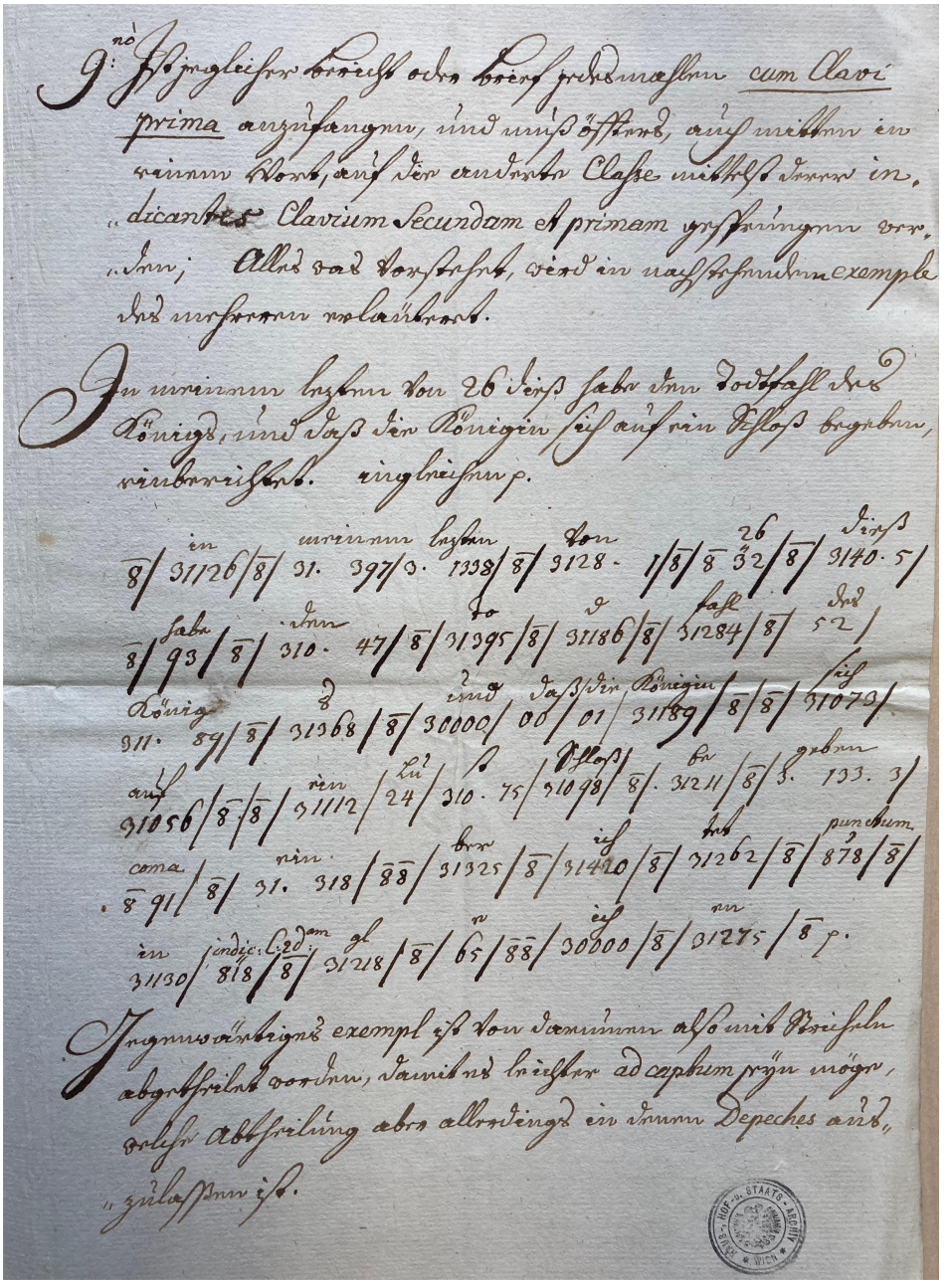

Figure C2. Example of decrypting a message from an instruction (ÖStA/HHStA/Staatskanzlei Interiora/Chiffrenschlüssel, box 16, fasc. 23, fol. 16).

Figure C3. Clavis secunda (second table) of the cipher key described in the text of Appendix C (ÖStA/HHStA/Staatskanzlei Interiora/Chiffrenschlüssel, box 16, fasc. 23, fol. 17).

we thought. The cipher key consists of two separate cipher tables (Clavis Prima and Clavis Secunda). Both can be used as two-digit, three-digit, or four-digit codes. Both also contain a digit 8 null and a digit 3 indicator of four-digit codes. However, both these digits also serve as real separators, while the dots are false separators. Until the digit 3 appears, all codes are only two-digit, and the digit 8 can be used to separate them. However, if a number 3 appears at the beginning of a new code, it is always followed by a four-digit code. If the digit 3 or 8 appears between the next four digits, they do not activate their special function described above and are considered numbers like any other. The number 3 also behaves the same way if it appears at the end of a two-digit code. Its special function is activated only when its position is at the beginning of a new code. Three-digit codes are used only for days, months, years, and numbers. To recognize them, a special mark must be written above the middle digit. Also, in the three-digit codes, the digits 3 and 8 do not activate their special functions, even if they are at the beginning of the code. Each message starts with Clavis 1, switches to Clavis 2, and then reverts to Clavis 1 using special indicators (*indicantes clavium secundam et primam*), as shown in the example of message deciphering (Figures C2 and C3).

Appendix D. Examples of dating undated cipher keys and instructions

Most of the analyzed instructions and corresponding cipher keys were not dated by their authors. Therefore, all undated instructions and keys had to be dated at least approximately based on an analysis of their content. The codes for the personal names given in the keys are usually most useful for this purpose. However, often only the surnames or titles of individuals are given in cipher keys. It is therefore necessary to identify the persons and determine when they lived and during what time they held important positions, often in the diplomatic service. In most cases, it is not possible to determine the exact year of the key's creation or use. However, it is usually possible to date the key to within five or ten years.

In this example, we look at a set of 37 similar keys with instructions, described in Section 4. First, we describe the dating method for the keys that were actually in use. Unlike the designs that were not being used, these keys contain codes for the names of persons, and their users' names are often written on them. The oldest dated key in this set indicates that it was used from 30 April 1770 (box 15, fasc. 22, fols. 1–4). The names of the users can be found directly on the key: first "H[err] Graf Wilczek" (later crossed out), and below that, "H[err] Veigl." Both were imperial ambassadors in Milan.[19] At least one of the keys was used until 1799 (box 15, fasc. 22, fols. 25–26). It was used for correspondence with "Baron van Suieten," then "Rewizki" (both names crossed out), and finally "Reuss."[20] It is noted that after the death of Prince Reuss in 1799, the key is no longer secure.[21] It seems that the key was used exclusively for correspondence with ambassadors in Prussia, probably from 1777 until 1799. Another example is the key marked simply "Dänemark," which was probably used for correspondence with the ambassador in Denmark (box 15, fasc. 21, fols. 26–27). This key has no user names on it, so we had to date it by using codes for personal names. There are 61 codes for the names, mostly just surnames, of various

[19] Johann Josef von Wilczek (1738–1819) was ambassador in Milan in 1771–1773. He was followed by Joseph Veigl, who was ambassador there from 1773 until at least 1798 (Winter 1965). The key was probably made before Count Wilczek officially took office.

[20] These were most likely the following imperial ambassadors in Berlin: Gottfried Baron van Swieten (1733–1803), in Berlin 1770–1777; Károly Imre Sándor Reviczky von Revisnye (1737–1793), in Berlin 1779–1785; and Heinrich XIV, Prince Reuss of Greiz (1749–1799), in Berlin 1785–1799 (Winter 1965).

[21] In the original, Verdächtig seit dem Todfall des Fürsten v[on] Reuss Anno 1799.

persons. The codes are in alphabetical order. This means that they were all added at the same time. Most of the codes did not provide a clear identity. The most useful names were "Segur Mr." and "Stutterheim Mr." The first person was most likely Louis Philippe, comte de Ségur (1753–1830), who was French ambassador to St. Petersburg from 1784 and had previously pursued a military career. In 1783 he was serving in the war in America. The second person was probably the Saxon minister Heinrich Gottlieb von Stutterheim (1718–1789). It is therefore likely that the key started to be used between 1784 and 1789.

For the 37 similar keys with instructions, it is more difficult to date those that were never used in practice (or at least we have no evidence of their use) because they do not contain any codes for the names of persons. Nevertheless, in some cases it is possible to determine a terminus post quem for them. The instructions often contain examples that can be related to specific historical events. For example, in one instruction (box 18, fasc. 25, fols. 124–125), the example mentions that the Congress of North American States[22] notified France that it had entered the war with England. Thus, the instruction was probably not created until the mid-1770s. Another instruction (box 18, fasc. 25, fols. 58–59) contains text noting that the London riots caused about a million florins worth of damage. This is probably related to the famous Gordon Riots of 1780. Finally, in one of the instructions (box 19, fasc. 26, fol. 71) it is written, "*in Paris … die sogennanten Jacobiner oder Terroristen die Oberhand gewonnen haben.*" So this instruction was probably not created before 1793.

During the analysis of the 37 keys with instructions, we could not find any examples that definitively referred to events before 1770. However, we cannot rule out the possibility that some were created before 1770. Nor can we exclude the possibility that some of these keys may have been in use during the nineteenth century, although we found no clear evidence that this was the case. These questions could be answered by a more detailed analysis of the content of the keys and instructions, but that is beyond the scope of this article. The rest of the 65 instructions were dated in similar ways (see Table 1), unless they were already dated by their authors or users.

[22]In the original, Congress von den Nordamerikanischen Staaten.

Appendix E. Overview of the analyzed cipher keys

Table 1. Overview and dating of the analyzed cipher keys.

Box	Fasc.	Fol.	Key type	Date of origin/use	Language	Subset of 37 similar keys
13	20	2	1	[1622]–[1633]	GER; LATIN	
14	20	159	1	[1593]	GER	
14	20	277	1	[1640]–[1650]	LAT	
14	20	11 (in file fol. 1–16)	2	1764-06-26	GER; ITA	
15	21	2–3	3	[1780]–[1785]	GER	YES
15	21	20–21	2	1750-09-18	FRA	
15	21	26–27	2	[1770]–[1800]	GER	YES
15	21	34–35	2	[1770]–[1800]	GER	YES
15	21	38	4	1824-02-23	FRA	
15	21	54–55	3	1753-06-16	GER	
15	21	66–67	3	[1770]–[1800]	GER	YES
15	21	68–69	3	[1745]–[1755]	GER	
15	21	75	4	1749-09-05	GER	
15	21	84	4	1746-09-20	GER	
15	21	111–112, 120–121	2	1745	GER	
15	21	126	6	[1770]–[1800]	GER	YES
15	22	1–4	2	[1770]–[1800]	GER	YES
15	22	10	3	[1770]–[1800]	GER	YES
15	22	25–26	6	[1770]–[1800]	GER	YES
15	22	38–39	2	[1740]–[1750]	FRA	
15	22	58–59	2	[1770]–[1800]	GER	YES
15	22	77	4	1795	FRA	
15	22	91	3	[1770]–[1800]	GER	YES
16	23	13–16	3	1752-09-03	GER	
16	23	47–48	4	1763-08-10	GER	
16	23	52–53	4	1761	FRA	
16	23	71–74	4	1770-11-15	GER	
17	24	3–4	5	1772-01-15	GER	
17	24	41–42	6	1780	GER	YES
17	24	43–44, 47–48	3	1780-09-29	GER	YES
17	24	61–62	2	[1740]–[1750]	FRA	
17	24	105	4	1790	FRA	
17	24	140	4	1805	FRA	
17	24	192–193	5	1812-06-10	FRA	
17	24	200	2	[1805]–[1809]	GER	
18	25	38–41	3	[1770]–[1800]	GER	YES
18	25	58–59	3	[1770]–[1800]	GER	YES
18	25	78–81	3	[1770]–[1800]	GER	YES
18	25	102–105	3	[1770]–[1800]	GER	YES
18	25	115–116	2	[1770]–[1800]	GER	YES
18	25	124–125	3	[1770]–[1800]	GER	YES
18	25	132–135	2	[1770]–[1800]	GER	YES
18	25	140–141	3	[1770]–[1800]	GER	YES
19	26	12–15	3	[1770]–[1800]	GER	YES
19	26	33–36	3	[1770]–[1800]	GER	YES
19	26	53, 55	3	[1770]–[1800]	GER	YES
19	26	71	2	[1770]–[1800]	GER	YES
19	26	86–89	3	[1770]–[1800]	GER	YES
19	26	93–94	2	[1770]–[1800]	GER	YES
19	26	99–100	2	[1770]–[1800]	GER	YES
19	26	109–112	3	[1770]–[1800]	GER	YES
19	26	119–122	2	[1770]–[1800]	GER	YES
19	26	127–130	6	[1770]–[1800]	GER	YES
20	27 (Varia)	—	2	[1800]–[1815]	GER	
20	27 (Varia)	128–129	?	[1800]–[1815]	FRA	
20	27 (Varia)	24 (red)	3	[1770]–[1800]	GER	YES

(*continued*)

Table 1. Continued.

Box	Fasc.	Fol.	Key type	Date of origin/use	Language	Subset of 37 similar keys
20	27 (Varia)	25 (red)	3	[1770]–[1800]	GER	YES
20	27 (Varia)	26 (red)	2	[1770]–[1800]	GER	YES
20	27 (Varia)	27 (red)	2	[1770]–[1800]	GER	YES
20	27 (Varia)	28 (red)	2	[1770]–[1800]	GER	YES
20	27 (Varia)	29 (red)	3	[1770]–[1800]	GER	YES
20	27 (Varia)	—	1	[1700]–[1740]	GER	
20	27 (Varia)	10 = 11	7	[1770]–[1800]	GER	YES
20	27	Lit: C	2	[1800]–[1815]	FRA	
21	27	Nro. 478/3	2	1860-11-12	GER	

Note: Square brackets indicate approximate dates.