

# On the Combination of Cryptography and Steganography in 17th Century Germany

Eveline Szarka

University of Heidelberg

Grabengasse 1

69117 Heidelberg, Germany

eveline.szarka@uni-heidelberg.de

## Abstract

Assessing and averting possible interception lies at the heart of cryptology. In handbooks printed in 17th century Germany, the authors suggested combining steganography and cryptography to increase information security. This article discusses several techniques for concealing ciphers and demonstrates that the authors of instructional literature had to consider complex interplaying factors when it came to combining cryptography and steganography. Overall, these examples show that the cryptological literature of the 17th century mirrors an increased discussion about the visibility of ciphers.

## 1 Introduction

The history of early modern cryptology is first and foremost a history of alphabetical and numerical encryption techniques. Historians have been primarily interested in the invention and evolution of polyalphabeticity, which, according to scholarship, peaked in the 15th and 16th centuries (Strasser, 2007, p. 297, 321, Kahn, 1967, p. 154). For this reason, the cryptological literature of the 17th century, especially those printed in Germany, received relatively little scholarly attention.<sup>1</sup> However, the authors of handbooks on secret communication showcase the skillful use of diverse resources to develop ever more sophisticated techniques. Applying polyalphabeticity was not the only way to increase information security.

Steganography is another blind spot in the history of secret communication. In contrast to cryptography (text encryption), steganographic techniques hide messages entirely so that they escape the attention of unauthorized persons. In the early modern era, this form of secret communication was more diverse and important than is assumed today.

To achieve an even higher level of information security, early modern scholars also suggested combining cryptography and steganography. The aim of this article is to offer an insight into multiple historical techniques concerned with the concealment of a ciphertext. To create an adequate basis of understanding, I will briefly discuss early modern steganography and its relevance for the history of cryptology. It will be argued that, when it came to the combination of cryptography and steganography, scholars had to consider multiple interplaying factors such as the knowledge of interceptors, the naturalness of the steganotext, the choice of the steganotext, the complexity of the cipher, as well as the encryption process on the receiver side.

On a broader level it will be shown that these techniques reflect a broader historical change in cryptology that began around 1600. Although alphabetical and numerical substitutions remained important, 17<sup>th</sup> century sources mirror an increased discussion about the visibility of ciphers.

## 2 Early Modern Steganography

The field of steganography (from the Greek word *στεγανός*, ‘hidden’ and *γραφία*, ‘writing’) dates back to antiquity. Steganography is a form of secret communication that seeks to hide messages in innocuous texts, objects, art works etc. There are two forms of steganography:

---

<sup>1</sup> Gerhard F. Strasser examines 17th century handbooks published in Germany, although with a focus on universal languages schemes, see Strasser (1988). For England see Ellison (2017).

Linguistic steganography is the term used to describe methods by which a text is hidden in a set of data. Writing with invisible inks or hiding slips of information in objects, on the other hand, are examples of technical steganography. This article discusses linguistic steganography.

*Semagrams* were a popular means of hiding information in early modern Europe. Here, the secret message is embedded into an inconspicuous message (*steganotext*). The semagram relies on visual cues such as tiny ink dots placed above certain letters or a slightly different appearance of a character to denote the relevant letter of a secret message. The advantage of this technique is that the sender does not have to compose a text, but can also send, for example, journals or books to the receiver to convey clandestine intelligence. Due to the use of visual cues, however, detection is still possible.

*Null ciphers* work similarly, but the plaintext is inserted into a larger text body based on a rule. Despite their name, null ciphers are not concerned with encryption, but the significant text is surrounded by insignificant data (*nulls*). An example would be to only read the first (*acrostic*) or last (*telestich*) letters of each word.<sup>2</sup> Depending on the complexity of the rule, null ciphers are a safe way to convey clandestine messages. In contrast to semagrams, the sender would have to compose a text that might sound constructed.

Since steganographic techniques ideally do not arouse suspicion, they are also prone to escape the historians' gaze. This is probably the reason why there is hardly any historical research on this topic.<sup>3</sup> Invisible inks have been found in early modern letters (Britland, 2018, p. 208, Rous, 2011, p. 250), but other forms are much harder to spot. For this reason, cryptological handbooks are – besides metatexts that attest for its application<sup>4</sup> – the only valuable source to gain insight into early modern steganography.

---

<sup>2</sup> For example, the *Steganographia* (c. 1499) penned by Johannes Trithemius' applies the null cipher to hide the secret behind the names of spirits.

<sup>3</sup> Despite having surveys on steganography covering the time from antiquity to modern times (Schmeh, 2009 or Macrakis, 2014), there is still a lack of in-depth studies on the early modern era.

<sup>4</sup> Strasser writes that the so-called *Cardano Grille*, a physical steganographic key, "was employed from the 16th well into the 18th centuries in the diplomatic correspondence of a number of countries." (Strasser, 2007, p. 291).

Many cryptological works of the 16th century mention forms of linguistic steganography. However, in the 17th century, steganographic techniques take up more space in cryptological handbooks; a trend that correlates with changing attitudes towards the visibility of ciphers. The Nuremberg professor Daniel Schwenter, military expert<sup>5</sup> and author of the first cryptological handbook in the German language, the *Steganologia & Steganographia nova* (1617)<sup>6</sup>, writes (p. 250):

"Hingegen aber ist es nicht rahtsam inn Brieffen mit verborgenen Charactern zu schreiben / in dem die sach voller argwohn / und man solche Brieff nit allein auffangen / sondern auch verstehen möchte [...]."<sup>7</sup>

The polymath Georg Philipp Harsdörffer states in the *Delitiae Mathematicae et Physicae* (1653) that during sieges, letters containing indecipherable characters, numbers, or images will not pass the guards.<sup>8</sup> He also advises to hide messages altogether (p. 56). The risk of a death penalty for messengers who carried encrypted information (Harsdörffer, 1653, p. 56, Francisci, 1673, p. 176) was not limited to the 17th century, but also a relevant factor. Moreover, it is likely that rising literacy rates and the dissemination of cryptological knowledge increased the amount of people who were able to break ciphers.<sup>9</sup> It seems then, that the mastering of steganographic techniques became increasingly important in the 17th century.

Still, little is known about the value of steganography in cryptological literature, the authors' receptions, and improvements of existing methods as well as inventions after 1600. What factors did scholars like Schwenter assess to guarantee information security? What additional security measures did they apply? And what about the advantages and disadvantages

---

<sup>5</sup> Several parties asked Schwenter for advice during the Thirty Years' War. Mährle (2000), p. 375. Schwenter also published a work on war fortification, see Gärtner (1999), p. 244.

<sup>6</sup> Much ink has been spilled about the exact publication date of Schwenter's handbooks. However, it seems likely that the first edition with the *nova*-title was published in 1617, as on p. 50 Schwenter refers to a book that had been published two years earlier, namely Franz Kessler's *Secreta* (1615). The publication dates of the second and third editions remain unresolved.

<sup>7</sup> "However, it is not advisable to write with secret characters in letters / as the matter is full of suspicion / and one can not only intercept these letters / but also understand them."

<sup>8</sup> Post espionage in general and the extent of interception remains to be examined. In a survey on early modern Saxony, Rous counted eleven boxes with intercepted letters from the Thirty Years' War. Rous (2022), p. 380.

<sup>9</sup> According to the writer Erasmus Francisci everyone had become so clever, that it was almost impossible to come up with secure ciphers. Francisci (1673), p. 173.

when it came to decide on the one or the other method? Regardless of whether or not these techniques were applied, handbooks are a crucial source for the history of science and technology, as they demonstrate how changes in communication culture spurred the invention of new ways to protect intelligence.

Information security could, for example, be increased by the combination of cryptography and steganography. In simple terms, a plaintext is transformed into a ciphertext and hidden as / in a steganotext.

plaintext	ciphertext	steganotext
hello →	ALFFC →	<u>A</u> nd <u>L</u> inda <u>f</u> ed <u>f</u> eral <u>c</u> ats.

Table 1: Example of a concealed cipher, based on a simple monoalphabetic substitution and acrostic null cipher.

Concealed ciphers were known before 1600,<sup>10</sup> however, 17th century handbooks contain more variations and innovations thereof. The following examples demonstrate that hiding ciphertexts required the assessment of various interplaying factors.

### 3 Secret Alphabets

In addition to common alphabetical or numerical ciphers, handbooks often include secret alphabets consisting of alchemical, zodiac, or geometrical symbols. We know that in 17th century Germany symbols were used for encryption, although they were not supposed to be hidden.<sup>11</sup> Overall, the use of secret alphabets was not a secure method to conceal a message, as the cipher could be cracked easily just like other encryptions based on a monoalphabetic substitution.

Schwenter assesses several commonly known alphabets in the fifth book of the *Steganologia* (1617), such as Cabbalistic alphabets discussed by Cornelius Agrippa in the third volume of *De occulta philosophia* (1533), all of which Schwenter deems to be impractical as they are difficult and slow to write (p. 146). He also examines several geometric alphabets consisting of rectangles, triangles, or circles.

<sup>10</sup> Trithemius' *Ava Maria Cipher* presented in his *Polygraphia* (1518) is a prime example on how to hide an enciphered text. The letters of the alphabet are encrypted by Latin nouns, verbs, and adjectives that should read like innocuous religious texts or prayers. See also a recent study by Paolo Bonavoglia (2020) on a technique used in late 16<sup>th</sup> century Italy, as well as Strasser (2007), p. 317.

<sup>11</sup> See for example Stützel (1963).



Figure 1: Triangle Alphabet (Schwenter, 1617, p. 152). Bayerische Staatsbibliothek München, Res/Path. 801#Beibd.4, urn:nbn:de:bvb:12-bsb10926734-6.

Unfazed by the existing techniques, Schwenter introduces his own cunning alphabet (p. 154). As a professor of Oriental languages at the Altdorf Academy near Nuremberg, he took inspiration from the Hebrew, Syriac, and Arabic writing systems. According to the key, the symbols substitute consonants and dots signify vowels. As figure 2 shows, the dots are placed below or above the preceding consonants. The first symbol from the right is to be used as a proxy consonant in case a word starts with a vowel. Additionally, Schwenter proposes to change the writing direction.

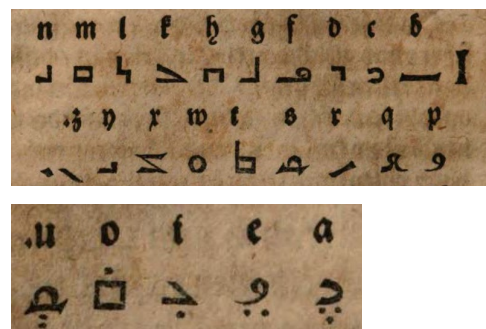


Figure 2: Schwenter's Secret Alphabet (Schwenter, 1617, p. 154). Bayerische Staatsbibliothek München, Res/Path. 801#Beibd.4, urn:nbn:de:bvb:12-bsb10926734-6.

Schwenter then encrypts the sample text "Saliter / Schwefel und Weinstein angezündet / zerschmelzen etliche Metall fast im augenblick."<sup>12</sup>

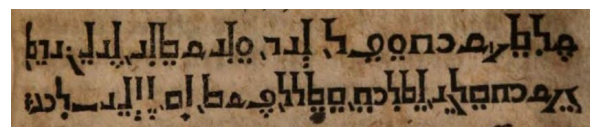


Figure 3: Example of Schwenter's Secret Alphabet (Schwenter, 1617, p. 155). Bayerische Staatsbibliothek München, Res/Path. 801#Beibd.4, urn:nbn:de:bvb:12-bsb10926734-6.

This alphabet is a simple monoalphabetic substitution, but the secret message disguises

<sup>12</sup> "Salpeter / sulfur and wine scale ignited / immediately melt all kinds of metals."

itself as an innocuous text; using this method, interceptors would ideally assume a text written in a foreign language and therefore refrain from attempting to break the cipher. In this case, the ciphertext and the steganotext are identical.

It can be assumed that Schwenter proposed to encrypt only certain passages and not an entire letter. In that case, the relationship between the script and the surrounding text would have been of utmost importance. The letter would have had to refer to languages or scripts. The specific communication context should also have legitimized the exchange of information related to this topic.

The key to using secret alphabets was to find a middle ground between something that looked familiar, but not too familiar. In contrast to the triangle letters or other secret alphabets, this way of writing could be mistaken for a foreign script in use. It was still better to encrypt a text with Greek letters than with an invented alphabet, but in 17th century Germany, there was still the possibility that the correspondence could fall into the hands of scholars who were able to read Greek. The chance of someone being fluent in Oriental languages was smaller. Thus, the success of this technique depended on the interceptors' language skills.

To protect the message even in the event of detection, Schwenter adds another layer of security by suggesting a right-to-left-script as is usual in the Arabic, Syriac, or Hebrew writing systems. While *inversion* – the technical term for writing backwards – is usually not a safe way to disguise a message, it somewhat improves the safety of an enciphered text as cryptanalysis heavily depends on the recognition of linguistic patterns such as frequent diphthongs, pre- or suffixes, or parts of words. This process is already complicated by the fact that the vowels are substituted by diacritics. Schwenter proudly declares his invention to be the best, swiftest, and safest of all secret alphabets (p. 155).

#### 4 Musical notes

Musical note ciphers were already used in the Middle Ages (see for example de Luca / Haines, 2018, or Code, 2022, p. 13). However, it is unclear if the ciphers were supposed to be visible. Musical note ciphers were particularly

popular in 17th century handbooks.<sup>13</sup> Gustavus Selenus (Duke August II of Brunswick-Lüneburg) discusses several musical ciphers in his *Cryptomenytices* (1624), which he attributes to Count Friedrich of Oettingen-Wallerstein.<sup>14</sup>

These techniques are based on the *Polybius Square*. In its original form, the square, first introduced by the Greek historian Polybius in the second century BC, consists of five rows and five columns with spaces for up to 26 letters of the alphabet. Thus, all letters are represented by a two-digit number, depending on which cell they are located in. The first digit signifies the row, the second the column. Although by using the square the ciphertext is twice as long as the plaintext, from a combinatorial perspective it comes handy in situations when cryptographic knowledge is transferred from basic alphabetical substitutions to other symbolic representations or media. For example, Polybius applied the square to encrypt a message by operating five torches at two places ( $5^2 = 25$  letters of the alphabet) (Polybius, 1925, p. 215ff.).

To simplify and speed up the encryption process, Selenus reduces the alphabet to 16 letters as is shown in table 2.

	1	2	3	4
1	a	b	c	d
2	e	f	g	h
3	i	l	m	n
4	o	r	s	u

Table 2: Selenus' version of the *Polybius Square* (Selenus, 1624, p. 321).

Now the sender draws five lines that serve as note lines as is common in musical sheets, although only four are to be used. These four lines correspond to the numbers of columns and rows ( $4^2$  positions to signify 16 letters). The letter “g” as is shown in Selenus sample text “Gustavus” is therefore encrypted by the number 23 (second row and third column). The sender must therefore place the first note on the second line and the second note one on the third.

<sup>13</sup> For an overview of various musical ciphers of the 17th century see Code (2022).

<sup>14</sup> The Count penned a cryptological manuscript in 1601 that was possibly offered to emperor Rudolf II. Strasser (1997), col. 784. See also Strasser (1982), p. 86f.

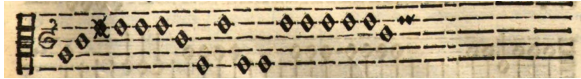


Figure 4: Selenus' example of a musical cipher (Selenus, 1624, p. 321). Staats- und Stadtbibliothek Augsburg, 2 H 336, urn:nbn:de:bvb:12-bsb11197933-2.

However, the application of this technique produces odd melodies; depending on the knowledge of interceptors, this could have posed a problem. Selenus therefore presents another technique with polyphonic vocals and in which only the tenor is encrypted, resulting in a somewhat harmonious musical piece.<sup>15</sup> Although this method is quite secure, also because the ciphertext is surrounded by nulls, it would have been very tedious to compose this kind of music, not to mention the skill that it required.

In the *Cryptographia* (1684), the second cryptological handbook published in the German language, Johann Balthasar Friderici<sup>16</sup> suggests an easier cipher. According to the key shown in figure 5, the letters are substituted by three notes each, however, the tone is irrelevant. Instead, the letters are encrypted by a combination of whole, half, and quarter notes. To even out an odd rhythm, Friderici proposes to add nulls in the form of inverted quarter notes.

While at first, this technique might look like the solution to avert detection, there are two issues. First, just as with the last example discussed by Selenus, the sender of the secret message would have to know how to compose a coherent melody. Second, in music composition, the rhythm is just as important as the melody, and this case, it could look funny to the trained eye. Nonetheless, from a cryptographic perspective, this was still safer than methods that relied on the note height, which seem to have been more commonly known. The more natural the music “looked”, the better.

<sup>15</sup> According to Selenus, it was composed by a musician from Luneburg named Friedrich Hollandt (p. 325). In 2017, the piece was played by Pennsylvania State University's orchestra on behalf of Gerhard F. Strasser. See Klaus Schmech's upload: <https://youtu.be/XjHtiXE8Iys>.

<sup>16</sup> To this day, it is unknown if this was the author's real name or a *nom de plume*. Friderici plagiarized a lot of his material, although the extent of his plagiarism remains to be examined.



Figure 5: Key for a musical cipher (Friderici, 1684, p. 181). Bayerische Staatsbibliothek München, Res/4 Graph. 19, urn:nbn:de:bvb:12-bsb10897281-3.

Overall, di- or trigraphic ciphers were a bit safer than musical notes that relied on monographic substitutions.<sup>17</sup> Similar to the use of secret alphabets, the success of the technique furthermore relied on the surrounding text. The cipher could remain obscured if the sender wrote about music. Of course, it was also possible to only transmit a musical sheet without additional information. Lastly, the context would have to justify why two people exchanged musical sheets or information about music.

## 5 Invoices

In the second volume of the *Delitiae Mathematicae et Physicae* (1651), Georg Philipp Harsdörffer presents a cryptological technique for people in besieged cities who want to convey intelligence to persons outside the city walls (p. 6ff.). The numerical ciphers are inserted to a merchant's invoice. As is shown in table 3, the consonants b-m are signified by the numbers 1-

<sup>17</sup> See Porta, 1602, p. 156 or Schwenter, s.d., p. 303. We know, for example, that by the end of the 16th century, complex musical ciphers using di- and trigraphs were used by the papal cryptographic service (Strasser, 1997, col. 784), although it is unclear whether the cipher was supposed to be hidden.

10, the letters n-z by 20-100 and the vowels by zeros.

1	2	3	4	5	6	7	8	9	10
b	c	d	f	g	h	j	k	l	m
20	30	40	50	60	70	80	90	100	
n	p	q	r	s	t	v	x	z	

0	00	000	0000	00000
a	e	i	o	u

Table 3: Key for a cipher to be used in an invoice (Harsdörffer, 1651, p. 6ff.).

Harsdörffer’s example message “Ich kan den Ort drey Tage halten”<sup>18</sup> is encrypted by numbers that are then listed as the debts of certain people. As the first and fourth word begin with a vowel, he advises his readers to attach the vowels to the preceding names, as demonstrated here with Claus Pfitz and Moritz Curz:

Claus Pfitz	26	Jch
Conrad Groß	8020	kan
Friederich Beerlin	30020	den
Moritz Curz	5070	Ort
Friederich Demm	35027	drey
Dieterich Plock	7005	Tag
Georg Schwetz auf 3 mal	6097020	halten.

To increase the complexity of the cipher, the encryption operates with one, two, three, four, and five-digit numbers to make cryptanalysis even more difficult. Unfortunately, Harsdörffer failed to take the recipient into account, as the ciphertexts result in multiple plaintexts. For example, the number “30020” encrypts the plaintext “den”, but also “daan” “daaca”, “deca”, “pan”, or “paca”. Therefore, this is not a practical technique.

Another example of an encrypted invoice is included in Friderici’s *Cryptographia* (1684) (p. 166ff.). A variation of the *Polybius Square* serves as the base.

I	a	b	c	d	e	f	g	h
II	i	k	l	m	n	o	p	q
III	r	s	t	u	w	x	y	z
	1	2	3	4	5	6	7	8

Table 4: Friderici’s version of the *Polybius Square* (Friderici, 1684, p. 166).

The ciphers are merged into four-digit numbers (quadgraphs), while the number 9 marks a word ending. To hide the message “Dein Verwalter ist dir nicht getrew / schaffe ihn ab”<sup>19</sup>, Friderici composes a letter asking the recipient for the correction of an erroneous invoice. The recipient first jots down the numbers listed in the first column from top to bottom and so on, splits up the numbers into two-digits (leaving out the number 9) and consults the square to decrypt the secret message.

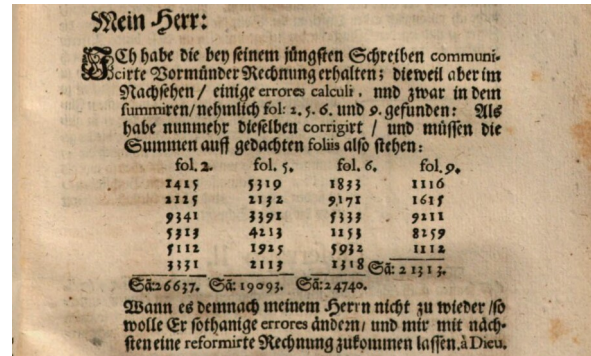


Figure 6: Friderici’s encrypted invoice (Friderici, 1684, p. 167). Bayerische Staatsbibliothek München, Res/4 Graph. 19, urn:nbn:de:bvb:12-bsb10897281-3.

Unlike common numerical ciphers, the surrounding text and the appearance of an invoice legitimates the presence of numbers. In contrast to secret alphabets and musical notes, the knowledge of the interceptor would have been irrelevant as long as the amount of money made sense. Moreover, digraphic encryptions presented as quadgraphs as well as the addition of nulls significantly increases information security.

## 6 Encrypted Null Ciphers

Secret alphabets, musical ciphers, and numerical ciphers in invoices feigned to be something else which ideally resulted in an undetected exchange of information. The downside was that the choice of the steganotext was somewhat limited, as the sender of a message would have to reference languages/scripts, music, or amounts of money. Techniques for concealed ciphers that utilized the Latin alphabet had two advantages: The knowledge of possible interceptors was irrelevant, and they allowed the flexibility to choose any kind of steganotext.

<sup>18</sup> “I can hold this place for three days.”

<sup>19</sup> “Your steward is disloyal to you / get rid of him.”

According to a technique discussed in Friderici's *Cryptographia* (1684), the letters of the secret message are encrypted by words that are then embedded into a larger body of non-significant text (p.111). In that sense, this method is similar to Trithemius' *Ava Maria Cipher*, although there are more word types, which are also unrelated to the nature of the information.<sup>20</sup> Friderici uses the key shown in figure 7. The letters of the alphabet are divided into three groups, each of which is assigned a different word beginning ("UN-", "AL-", or "WE-").

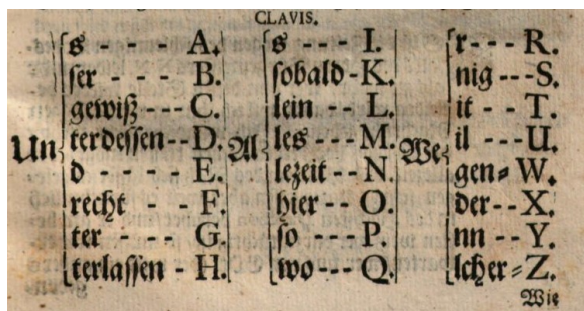


Figure 7: Friderici's key for an encrypted null cipher (Friderici 1684, p. 111). Bayerische Staatsbibliothek München, Res/4 Graph. 19, urn:nbn:de:bvb:12-bsb10897281-3.

The sample message "wir sind verrathen"<sup>21</sup>, is encrypted by the ciphertext:

"WEGEN ALS WER WENIG ALS ALLEZEIT  
UNTERDESSSEN WEIL UND WER WER UNS WEIT  
UNTERLASSSEN UND ALLEZEIT."<sup>22</sup>

According to Friderici, the sender would now have to integrate these words into a coherent message in the right order. He continues that this technique is especially convenient for the recipient, as they can skim the letter searching for words starting with "UN-", "AL-", and "WE-". However, he acknowledges that, in order to avert confusion, the sender would have to refrain from using any of the above listed words in the text surrounding the cipher. In sum, Friderici states that while this technique is rather tedious, it is also "sehr sicher und darzu von allem Verdacht befreyet"<sup>23</sup> (p. 112).

<sup>20</sup> The *Ava Maria Cipher* also made use of nulls, but the syntactic structure remained somewhat fixed. Additionally, the choice of steganotext (prayers, religious texts) was limited. For this cipher, see Gamer (2022), p. 148.

<sup>21</sup> "We have been betrayed."

<sup>22</sup> "BECAUSE AS WHO LITTLE AS ALWAYS MEANWHILE BECAUSE AND WHO WHO US FAR REFRAINED AND ALWAYS."

<sup>23</sup> "Very secure and, in addition, free from any suspicion."

## 7 Encrypted Semagrams

In the second half of the 17th century, the Jesuit scholar Caspar Schott introduced in the *Schola Steganographica* (1665) a technique that, according to him, could be used for correspondence with princes and governors. He uses a *Tabula Recta* and a keyword as introduced by Blaise de Vigenère in his *Traicté des chiffres* (1586), although Schott refers to Athanasius Kircher's *Abacus Numeralis* using numbers instead of letters.

Figure 8: The *Abacus Numeralis* (Schott, 1665, p. 77). Staatliche Bibliothek Regensburg, 999/4Art.31, urn:nbn:de:bvb:12-bsb11060024-5.

The key, as shown in figure 8, consists of a table with letters of the alphabet both in a vertical and horizontal order as well as numbers from 1-24 allowing for polyalphabeticity. First, the sender writes the secret message onto a piece of paper for reference. The note shall be:

"State cauti, cras hora decima noctis venient hostes, ut invadant urbem ex parte orientalis plagae."<sup>24</sup>

Then, they must decide on a keyword; Schott uses the sentence (p. 79):

"Omnia sunt hominum tenui pendentia filo."<sup>25</sup>

The sender now composes a text in any language with any kind of information. To encrypt the message, they locate the first letter of the keyword, "O" in the top row. Then they move down to where the first letter of the secret

<sup>24</sup> "Be careful, tomorrow at ten o'clock at night the enemy will invade the city from the eastern quarter."

<sup>25</sup> "All men are hanging by a thin thread."

message “S” is located on the far-right column and finds the number 7. Thus, the first letter is encrypted by the number 7. To encrypt the second letter of the secret, the sender finds the number located between “M” (second letter of the keyword) and “T” (second letter of the secret), which is the number 6, etc.

So far, this is nothing new. But, to “write” the first letter of the secret message (“S”), one should not jot down the number 7, but rather place a small dot or line below the seventh letter of the steganotext. To signify the following letter “T”, which is encrypted by the number “6”, the sender starts from the first mark, counts six letters, and places a dot on the thirteenth letter of the steganotext, etc. This technique was quick and easy to use. Moreover, the sender of a secret message could apply it to any kind of steganotext. The language sounded natural, and the parties could disregard any concerns relating to the communication context or knowledge of possible interceptors.

The writer and poet Erasmus Francisci paid reverence to this method in the third volume of *Die lustige Schau-Bühne* (1673), which contains six fictional conversations between six friends (Helduser 2011),<sup>26</sup> providing valuable insight into contemporary communication culture. The fictional friends state that letters containing ciphers would be confiscated immediately, which is why it would be better to hide a secret message (Francisci 1673, p. 173). This is followed by a story about a French diplomat named De la Haye who was supposedly incarcerated after “the Turks” had intercepted one of his letters that contained some ciphers (p. 177). One of the characters – or rather Francisci – deems Schott’s method to be the safest technique of all and adds that it would be even more secure to make the dots with invisible ink. To this date, it is the only known early modern technique to combine complex cryptography (polyalphabeticity and keyword) with linguistic and technical steganography.

## 8 Conclusion

As this article has shown, skills for hiding messages became increasingly important during the 17th century. To ensure the highest possible level of information security, scholars combined cryptography and steganography. Although the

simultaneous application of these two forms of secret communication fanned out the possibilities of hiding information, they also required a lot of skill and consideration.

The authors of cryptological handbooks had to consider the knowledge of possible interceptors, the naturalness of the language or data, and flexibility in choosing an adequate steganotext. The scholars even made sure that they increased the complexity of the ciphers through the application of inversion, polygraphic substitution, as well as keywords and polyalphabeticity. The techniques presented in this paper varied in sophistication, and were sometimes not very practical, but they all exemplify the scholars’ ability for computational thinking and creative problem-solving strategies.

As a next step, it would be interesting to see if and to what extent the techniques discussed have been applied in correspondences. However, since steganography obscures the presence of a secret message, this will prove to be a difficult task. In sum, historians still have a lot to discover as far as 17th century cryptology – and hiding information in specific – is concerned. This paper offers only a small glimpse into early modern steganography, which, just like the messages it seeks to conceal, is still hiding in plain sight.

## Acknowledgements

This article results from a project kindly funded by the Swiss National Science Foundation (grant no. 210981). Warmest thanks to Theresa Bayer for her helpful suggestions regarding the structure of the text.

## References

- Cornelius Agrippa. 1533. *De occulta philosophia*, vol. 3. Cologne.
- Paolo Benavoglio. 2020. A Partenio’s Stegano-Crypto Cipher. *HistoCrypt 2020. Proceedings of the 3rd International Conference on Historical Cryptology*:36-45.
- Karen Britland. 2018. “What I Write I Do Not See.” Reading and Writing with Invisible Ink. Katherine Ellison, Susan Kim (ed.). *A Material History of Medieval and Early Modern Ciphers. Cryptography and the History of Literacy*, Routledge, New York

<sup>26</sup> He also refers to Hardsörffers method hiding ciphers in invoices as a secure way to convey information, p. 175.



- (Material Readings in Early Modern Culture):208-222.
- David Løberg Code. 2022. Can musical encryption be both? A survey of music-based ciphers. *Cryptologia*. <https://doi.org/10.1080/01611194.2021.2021565>.
- Katherine Ellison. 2017. *A Cultural History of Early Modern English Cryptography Manuals*. Routledge, Abingdon.
- Erasmus Francisci. 1673. *Die lustige SchauBühne von allerhand Curiositäten*, vol. 3. Nuremberg.
- Johann Balthasar Friderici. 1684. *Cryptographia*. S.l.
- Maximilian Gamer. 2022. *Die Polygraphia des Johannes Trithemius nach der handschriftlichen Fassung. Edition. Übersetzung und Kommentar*, vol. 1. Brill, Leiden (Mittellateinische Studien und Texte 56/1).
- Barbara Gärtner. 1999. Daniel Schwenter (1585-1636). Ein barocker Mathematiker. Rainer Gebhardt (ed.). *Rechenbücher und mathematische Texte der frühen Neuzeit*. Adam-Ries-Bund, Annaber-Buchholz:241-247.
- Urte Helduser. 2011. Erasmus Francisci: Die lustige Schau-Bühne von allerhand Curiositäten. Nikola Roßbach, Thomas Stäcker (ed.). *Welt und Wissen auf der Bühne. Die Theatrum-Literatur der Frühen Neuzeit. Repertorium*. Herzog August Bibliothek, Wolfenbüttel. <http://www.theatra.de/repertorium/ed000043.pdf>.
- Georg Philipp Harsdörffer. 1651. *Delitiae Mathematicae et Physicae*, vol. 2. Nuremberg.
- Georg Philipp Harsdörffer. 1653. *Delitiae Mathematicae et Physicae*, vol. 3. Nuremberg.
- David Kahn. 1967. *The Codebreakers. The Story of Secret Writing*. Macmillan Publishing Co. Inc., New York.
- Franz Kessler. 1615. *Unterschiedliche bißhero mehrern Theils Secreta*. Oppenheim.
- Elsa de Luca, John Haines. 2018. Medieval Musical Notes as Cryptography. Katherine Ellison, Susan Kim (ed.). *A Material History of Medieval and Early Modern Ciphers. Cryptography and the History of Literacy*, Routledge, New York (Material Readings in Early Modern Culture):30-47.
- Kristie Macrakis. 2014. *Prisoners, Lovers, and Spies. The Story of Invisible Ink from Herodotus to al-Qaeda*. Yale University Press, New Haven.
- Wolfgang Mährle. 2000. *Academia Norica. Wissenschaft und Bildung an der Nürnberger Hohen Schule in Altdorf (1575-1623)*. Franz Steiner Verlag, Stuttgart (Contubernium 54).
- Polybius. 1925. *The Histories*, vol. IV. Ed. by the Loeb Classical Library, transl. by Paton, W.R. Harvard University Press, London, New York.
- Giambattista della Porta. 1602. *De furtivis literarum notis*. Naples.
- Anne-Simone Rous. 2011. Geheimschriften in sächsischen Akten der Neuzeit. *Neues Archiv für sächsische Geschichte*, 82:243-253.
- Anne-Simone Rous. 2022. *Geheimdiplomatie in der Frühen Neuzeit- Spione und Chiffren in Sachsen 1500–1763*. Franz Steiner Verlag, Stuttgart.
- Klaus Schmeh. 2009. *Versteckte Botschaften. Die faszinierende Geschichte der Steganografie*. Heise, Hannover.
- Klaus Schmeh. 2017. Selenus' musical cipher played by the orchestra of the Pennsylvania State university on behalf of Gerhard F. Strasser. <https://youtu.be/XjHtiXE8Iys>.
- Caspar Schott. 1665. *Schola Steganographica*. Nuremberg.
- Daniel Schwenter. [1617]. *Steganologia & Steganographia nova*. Nuremberg.
- Daniel Schwenter. s.d. *Steganologia & Steganographia aucta*. Nuremberg. (2nd edition).
- Gustavus Selenus. 1624. *Cryptomenytices*. Luneburg.
- Gerhard F. Strasser. 1982. Die kryptographische Sammlung Herzog Augusts: Vom Quellenmaterial für seine „Cryptomenytices“ zu einem Schwerpunkt in seiner Bibliothek. *Wolfenbütteler Beiträge* 5:83-121.
- Gerhard F. Strasser. 1988. *Lingua Universalis. Kryptologie und Theorie der Universalsprachen im 16. und 17.*

*Jahrhundert*. Otto Harrassowitz, Wiesbaden (Wolfenbütteler Forschungen 38).

Gerhard F. Strasser. 1997. Musik und Kryptographie. Ludwig Finscher (ed.). *Die Musik in Geschichte und Gegenwart, Sachteil* 6:783-790.

Gerhard F. Strasser. 2007. The Rise of Cryptology in the European Renaissance. Karl de Leeuw, Jan Bergstra (ed.). *The History of Information Security. A Comprehensive Handbook*. Elsevier, Amsterdam:277-325.

Hermann Stützel: Chiffrierwesen im Dreissigjährigen Krieg. 1963. *Württembergisch Franken* 47, *Neue Folge* 37: 109-115.

Johannes Trithemius. c. 1499. *Steganographia*. First published in 1606. Frankfurt.

Johannes Trithemius. 1518. *Polygraphia*. [Reichenau].

Blaise de Vigenère. 1586. *Traicté des chiffres*. Paris.