Real Life Cryptology

Published by Amsterdam University Press

Real Life Cryptology: Ciphers and Secrets in Early Modern Hungary.
Amsterdam University Press, 2018.
Project MUSE. muse.jhu.edu/book/66424.

For additional information about this book
https://muse.jhu.edu/book/66424
6. Ciphers in action

6.1. Sharing the key

A recurrent theme in early modern Hungarian military, political, and diplomatic correspondence is the use, or improvement, of cryptography and all the entailing problems. These topics are usually covered at the very beginning or end of a letter in a few explicit remarks, and it is mentioned here which cipher worked and which did not, what letters they had sent or received. Such an example can be found in the second sentence of a 1662 letter sent to the Transylvanian politician Mihály Teleki, where his correspondent reported that he had earlier received both the letter and the cipher key. “As to a good-willed lord, I am at your service. An officer handed me your letter together with the clavis a few days ago.”

Ciphered correspondence did not work in the early modern period if the corresponding partners had not previously exchanged a cipher key or clavis. The key was usually not more than a folded paper. Since at least two claves were needed for a ciphered correspondence to work, one for the sender and one for the addressee, and because often it was the secretaries who did the administrative tasks around the correspondence, it is not surprising that some keys have survived in several copies.

Political actors often noted that without a proper cipher key, they were not able or not willing to write about things that really mattered. The Transylvanian magnate, Dénes Bánffy, who was writing to Mihály Teleki, noted that “Since I have no clavis, I do not dare to write, because if my letter were caught, they would know that we were betraying our lord and our nation, and that we are asking for money for this reason.” Bánffy writes again, in another letter, “Do not fail to send the clavis because there is no correspondantia without it.” Prince Ferenc Rákóczi II wrote to his correspondent in 1711 from Gdansk, “I do not dare to write without a clavis...” Chancellor of Transylvania, János Bethlen emphasizes in a 1667 letter that “we can trust a letter with private information if it is written with a clavis”.

It is no surprise, then, that people regularly asked each other to write their letters with a clavis, or, if they had no clavis, they requested one,

1 Teleki 2. 253–254, 186.
2 Teleki 4. 297–98.
3 Teleki 4. 461–463.
4 AR, I. vol. 3. 698–701.
5 Teleki, 4. 47–49.
usually the less important person from the more important one. Mihály Teleki is writing to János Nemes in 1678. “Dear brother, please write to me better and more truthfully with a clavis.”6 Miklós Bethlen is writing in 1678, “therefore I suggest that you only write about significant topics with the clavis.”7 Mihály Teleki in 1678, “Because Lord Rédei was also there, I have used a clavis to make this more secret. We pray to God that it would remain secret.”8 Ferenc Rákóczi II is writing to Antal Esterházy in 1710, “Please write to me by post via couriers, in casu necessitatis using the clavis of Újvár.”9 Ferenc Palkovics is sending a letter to General Bercsényi from Simontornya in 1709, “As the enemy is going to encircle us more, I advise my Lord to have some claves made and use them in writing to us here.”

István Dalmady, childhood friend of Teleki is asking for a clavis from him: “If it is not too much of a trouble, please make a clavis with secret letters so we could write to each other with bigger confidentia.”10 The lawyer István Vitnyédi makes the same request to his patron, the magnate Miklós Zrínyi: “It would be good if Your Lordship could send a clavis that I could trust because I think things will occur that I will need to write to Your Lordship about.”11

A similar letter from the same correspondence: “As I see it I will soon need to have a secret writing to Your Lordship, so I am asking Your Lordship to send me a clavis as Your Lordship promised to do when we parted from each other so I could write without fear in case a servant reports something that I need to tell Your Lordship about, or if I hear some other news.”12 People asked for a clavis from a higher dignity because they wanted to share private and sensitive information with them, in other words, they wanted to offer their services to a more preeminent politician, this time for example, to Zrínyi. Though Vitnyédi wished to send ciphered letters to the lord, he was not in a position to ask Zrínyi to use a clavis that he, as his inferior, had made.

Requests for a clavis were often granted and claves were exchanged, as Rákóczi writes in the last sentence of his letter to Antal Eszterházy, sent from the fort of Senthe in 1706, “In order that we can be more confident

6 Teleki 8. 4–5. 4.  
7 Teleki 8. 216–217, 178.  
8 Teleki 8. 78. 68.  
11 Teleki 1. 311–312.  
12 Magyar Történelmi Tár (Hungarian Historical Records, MTT) (Pest, MTA, 1855 – 1934) II/3. 237–239.  
13 MTT II/4. 37–41.
in the correspondentia, I am sending to Your Lordship a clavis with which Your Lordship could cipher if not the whole letter, in casu interruptae et periculosae correspondentiae, the most relevant pieces of information.”

Márton Kászoni says goodbye at the end of his letter in 1663, “Please find attached the new clavis. (...) You can be securus that I am going to report any news, as I am asking you to do the same. May God bring you back to us with good news.”

György Lippay starts his letter to Prince György Rákóczi I in 1637 in this way, “I have written to you recently and have sent it by a man of the voivode. I have also sent a clavis. He must have been delayed because I should have received a reply from you by now.”

There were several ways to exchange a clavis. They were often sent together with the ciphered letter, sometimes by a separate courier, or occasionally a personal meeting was arranged, this being the most secure option, of course.

Archbishop György Lippay sent the clavis in an attachment to his letter to Prince György Rákóczi in 1637 from Vienna. The clavis itself has survived too: “...in order to carry it out more appropriately, I am sending Your Lordship the clavis too. There are things I would be happy to share with Your Lordship. If Your Lordship had received this clavis, I might be able to write more.”

Rákóczi reacts assuring that he has received the key, noting that “I took the letter and the clavis included in it from the man of the voivode four days ago...” Then once more a few days later, “We received your letter four weeks ago from the man of the voivode dated from 16 July, together with the clavis.”

It was vital to indicate that a clavis had been successfully delivered to the addressee as Mihály Teleki writes on the back of a monoalphabetic clavis this polite request, “Rogo responsum an reciperit hanc cartam nisi duo verba.” A similar request can be read on the back of one of the biggest nomenclature dictionaries of our period, a table with one thousand and three hundred items that survived in Vienna, “Please write me recipisset.”

14 AR I. vol. 563–565, 82.
15 Teleki 2. 660–661, 453.
16 MTT III/5. 147, 35.
17 MTT III/5. 146, 34.
18 MTT III/5. 144–146, 34.
19 MTT III/5. 280–281, 37.
20 MTT III/5. 283–284, 39.
21 MNL OL P 1238 Teleki Mihály Collection, Miscallenous documents, Cipher keys
The first lines of another letter to Teleki make us think that the clavis was delivered by a separate messenger. “I have replied to your letter. If it was not taken elsewhere, it must have been delivered to you by now. I have been delivered the clavis.”

Despite being complex and confused, the letter of László Rédei from Hust, Ukraine (Huszt) in 1660 nicely illustrates how difficult it was to arrange a ciphered correspondence: “I have often regretted that I did not take information concerning the clavis when I was at His Lordship, but I had not expected these things to happen; although I did not know about it so far, I am only learning it, but to no avail, if my lord does not know my clavis. You might have a copy, and if you do not, you might write these words with a clavis, but if you do not have a key, and you cannot write to His Lordship using a clavis, you might take the courage to send my letter to His Lordship, you may succeed because I have written only that much to His Lordship, but I have not written to His Lordship where you should be, because I cannot. So His Lordship may not understand a word from my letter, but if you could either send this letter to His Lordship, or write to him in clavis these few words...”

After the appropriate claves were sent, delivered or exchanged, the corresponding partners put them into use. That was when a new problem arose. How should one name the different cipher keys? They evidently had to be differentiated since a high-ranking political figure had several significant relationships in which he used ciphered letters, to which end he used a number of different keys.

Ciphers were often named after the sender or the addressee, supposing (rightly or not) that the given person was only using one ciphered channel of correspondence. The writer would sometimes specify below the signature and the date at the bottom of the page which cipher was used for encoding the letter, or part of the letter. “We have written this letter with the clavis that Lord Szalai has.” “We have written to you this letter with the clavis of His Lordship.” “I have used the clavis of Lord Absolon.” “I have written to Your Lordship with the clavis of Lord Fajgel.”

In other cases the keys are described less precisely. Teleki notes that “I have written to Lord Simon Kemény the names with the clavis that Your

23 Teleki 2. 259–260, 189.
24 MTT II/5. 101., 25. sz.
25 Teleki 8. 249, 222.
26 Teleki 8. 265–266, 238.
27 Teleki 8. 433–435, 413.
28 Teleki 8. 68–69, 63.
Lordship has sent me, I wonder if you know which one I am talking about.”

“My brother has written to Your Lordship using the clavis that Your Lordship had made for me for the alphabet, so when Your Lordship is writing to me, please use only that.”

Jónás Mednyánszky’s instructions on his message for the Transylvanian noble (later prince) János Kemény were hardly explanatory: “Your Lordship can understand it using the clavis that our lord owns.” Since the ciphered parts of this letter had not yet been decoded, one suspects that the one-time addressee could make no sense of the faint reference either.

Sharing the key was a need often discussed in the letters, but its usage was hardly problem-proof. In a 1710 letter to his general, Miklós Bercsényi, Prince Rákóczi brings up the topic of claves twice. First he scorns his commander-in-chief that he did not use the cipher frequently enough in his previous letter, making it accessible to unsolicited readers (“you could have used more encoded text in the letter where you write about negotiations, for it is peasants who deliver these messages from Szolnok (...) and they are not safe from robbers”) and then he goes on to lament that he could not “decipher a letter because the key was left somewhere else”.

Rákóczi mentions such problems several times – he obviously had a great deal of experience exchanging keys. In 1711 he sends the following letter: “Since Your Lordship has written to me once again with a clavis that previously I have told Your Lordship about that Károlyi also has a copy, I am not sure whether the clavis that Lord Vay had resigned to you in a table is not lost. Until I hear confirmation that Your Lordship has received it, I cannot write any more particularities.”

Archbishop György Lippay and Prince György Rákóczi could not successfully share the key either, according to their 1637 correspondence – the prince finds a mistake in the clavis he was sent by the archbishop upon which Lippay, who cannot find any fault with it, asks him somewhat indignantly to mend it quickly so they can use it. “Your Majesty did not wish to use the clavis I had sent and had found some fault in it that I still cannot see,” he writes, “but if there was one, Your Majesty could correct it and send me a copy, perhaps my humble service had not been useless to Your Majesty, I do not wish to be of nuisance to Your Majesty. I remain to be full of good intentions.”

29 Teleki 2. 262–264, 193.
30 Teleki 1. 389–390, 342.
31 MTT II/6, 86–89.
32 AR I. vol. 3. 133–137, 84.
33 AR I. vol. 3. 673–674, 68.
34 MTT III/5, 286–90, 41.
later he repeats the request: “I have written about that clavis by the courier, please, Your Majesty, correct it and *cum correctione* send me a copy.”

It is impossible to prevent all complications, but it is exemplary how careful Chancellor Miklós Bethlen is when he gives orders on sharing the key as well as about what to do if the addressee happens to pass away. “I have sent Harsányi a clavis too, in case he will need it,” he instructs. Continuing, he notes that “I have told my messenger whom he should deliver the letter to in case Harsányi had died in the meantime. Your Lordship may see the short *instructio* that I have given to him. *Pro sua prudentia* instructs Your Lordship too. All about these *coram plura*.”

### 6.2. Replacing the cipherkeys

After a key was successfully shared and smoothly used for a while, it was time to think about how to replace it with a newer one. Naturally, a cipher key cannot be in service forever. The longer it was used, in more letters and in more relationships, the easier the job of the potential codebreaker was, who would have more materials to identify breaking points. One would expect the expert cipher users of the early modern period to do all they could to avoid this danger.

It is surprising, however, that the issue of replacing a cipher is rarely mentioned in the letters. Updating it in order to prevent enemy eavesdropping seems to have been of little interest to early modern Hungarian political actors. Security was surprisingly neglected in this respect. Correspondents were not careful to use a clavis with one particular person only, and they did not aim at replacing the claves at least yearly, either.

For example, Ferenc Rákóczi II’s envoys to Constantinople, János Pápai and Ferenc Horváth, had written several dozen almost completely enciphered letters to the prince during the year 1706. For these, they had used a table that was so important that it has survived in several copies both in the secret archives of the prince and in the Ráday Archives. If one looks at this pack of letters closely, one sees that three of them begin with similar combinations of numbers. The two following letters, almost completely enciphered, are particularly long, more than ten pages. Had a Turkish codebreaker captured the

---

35 MTT III/5. 291–292. 42.
38 Ráday Archives C64-4d2-25, 12, no., MNL OL G 15 Caps. C. Fasc 43.
package, he would have found ample resources to use the appropriate analyses and locate regularities that would aid codebreaking. Pápai even used the same table when writing to another correspondent, Ádám Vay. What is more, the envoys were still using this key—not once or twice, but dozens of times—in the following three years from Belgrade and Constantinople, despite the change in the diplomatic circumstances.

Enciphered report from a Constantinople envoy for the Prince from 1 May 1706

41 MNL OL G 15 Caps. C. Fasc 33, fol 35–38.
43 MNL OL G 15 Caps. C. Fasc 33, fol. 19–20
This clavis was undoubtedly one of the most important ones in the eight-year-long freedom fight. This can be known not only from the fact that Rákóczi's diplomatic relationship with Constantinople was a highlighted relation, but also because only three tables survived the freedom fight that were copied onto parchment, Pápai's table being one of these.\textsuperscript{44} The other such table signals Rákóczi's most distinguished diplomatic goal, because it was used in the correspondence with Louis XIV and his court, and the third one, bearing no name, was not used for political purposes, rather with Rákóczi's secret love in Poland (to be discussed below). However central Pápai's table could have been in the prince's correspondence, it was still highly dangerous to use it for five long years in several cities and with several partners. With this knowledge in hand, we should hardly be surprised to learn that after his freedom fight terminated and he was forced to leave the country for Poland, the fleeing prince took this key out once again, when he was hard pressed without ciphers that the addressees would also have a copy of. Wanting to share private information in letter, he suddenly remembered that he could start using Pápai's table again in his correspondence with Ádám Vay, too: “Although I would have liked to inform You \textit{circumstantialiter}, I did not dare to write without a clavis, but then I was reminded by Pápai's letter that we can use his old clavis from Constantinople, which I am using right now; and since I do not doubt his faithfulness, he could decipher this message himself.”\textsuperscript{45}

Pápai's clavis was undeniably overused, even though several other tables were available and efforts were made not to overcharge this or any other clavis. András Bay, envoy to Constantinople in 1706,\textsuperscript{46} Mihály Henter, envoy to Constantinople from Transylvania in 1707,\textsuperscript{47} and Ferenc Ládonyi Horváth, another envoy to Constantinople in 1708 all used different claves – in fact, three different ones,\textsuperscript{48} despite being at the same place, in the same period, in the similar function as János Pápai. Pápai himself used another different cipher method in 1707, when writing to József Voynovich.\textsuperscript{49} In cases, attitudes towards ciphers were cautious, in other cases not the least.

\textsuperscript{44} MNL OL G 15 Caps. C. Fasc 43.
\textsuperscript{46} MNL OL G 15 Caps. D. Fasc 81.
\textsuperscript{47} MNL OL G 15 Caps. D. Fasc 80. fol. 38, 40, 46.
\textsuperscript{48} MNL OL G 15 Caps. E. Fasc 109.
\textsuperscript{49} MNL OL G 15 Caps. D. Fasc 80. fol. 28.
A good example for irresponsible behavior is described in the 1706–1707 correspondence of László Vetési Kökényesdi, who was Rákóczi’s advocate at the Bavarian prince elector and who sometimes wrote under the pseudonym Casimirius de Miloftzky. Kökényesdi used the same clavis with Ráday and Rákóczi in Hungarian that he used with Chamillard, secretary of the French ambassador Des Alleurs in Latin and in French. Even Jakab Kray, another supporter of Rákóczi, applied this very cipher to write to Ráday.

6.3. The tiresome work of enciphering

In a particularly long letter Prince Rákóczi apologizes to Marquis Bonnac, “I am going to make my letter shorter so you are not as bored reading it as your secretary is when deciphering the clavis, because these are matters of seemingly low importance.”

Parties involved in enciphered correspondences often complained that encryption and decryption were time-consuming and tedious tasks. It is easy to experience what they meant with a simple encoding exercise involving an average homophonic table of about three to four hundred items, and a message of average length (made up of four or five paragraphs) waiting to be encrypted. Looking up and noting the corresponding numbers to every and each letter and one by one is a monotonous job that can take a long time even with a shorter letter. Decryption is an even longer process, most of all because the clavis usually lists the letters of the open text in alphabetical order, aiding the encryption but not so much the decryption. This is the reason why certain writers only encrypted some of the words or parts of the sentences.

Mihály Teleki wrote: “I had no time to decipher our lord’s letter since I only received it in the evening and I had to leave early at dawn.” Rákóczi writes to his general, Bercsényi: “I could hardly wade through all these claves.” And in another letter: “I realized at last that you must have found

50 Ráday Archives C64-4d2-10.
51 Ráday Archives C64-4d2-25. 6.
52 Ibid. 27.
53 Ibid. 23.
54 Ibid. 24.
55 Ibid. 44.
56 Köpeczi, II. Rákóczi Ferenc, no. 39.
57 Teleki 8. 228–229, 195.
58 AR I. vol. 3. 113–114.
deciphering these letters very boring, since even their summary is annoyingly long for me to read.”

A month later Bercsényi laments the lack of time needed for decryption, “Having finished my letter, an honest captain has just arrived who has brought the golden lamb for His Majesty the Prince, and he has also brought long ciphered letters that take a long time to decipher, especially since they are in French which I am not familiar with, so I am rather sending out this letter to you now.”

Rákóczi asks Sándor Nedeczky, his envoy to Russia, in vain to use the clavis properly and not to mix coded and un-coded letters in the same word. Without a secretary, Nedeczky finds this work too tiresome and asks his partners not to “ruin him in the future”, and “only encipher secretum, leaving the rest as open text.” This angry request was aimed at Ráday, who knew precisely that the partial use of a cipher saves a lot of time for the addressee, since he had written this to Prince Rákóczi in a previous letter, “I did not wish to burden Your Majesty by enciphering all of my humble letter, I only used that for the secret parts and I am writing about the other things explicitly.”

Many years earlier Simon Kemény makes a similar request to Teleki: “By God, I am asking Your Lordship to write only what is important, and only breviter, and not to write such horribly long pandechta, enciphered, and with a lot of mistakes, because with the ambassador being here we have so much to do we can hardly get any sleep.” György Udvarhely, summarizing the content of other enciphered letters for Teleki, closes his letter: “I was working all night on the claves.” The leader of the anti-Habsburg uprising, Imre Thököly, writes in his diary: “I have spent most of the night deciphering texts, and when I have finished revising them, I called for the French lord.” Deciphering required a long night’s work more than once.

6.4. The cryptologist

This last example is informative not only because it contains the usual complaint about the tiresome work of enciphering, but also because of
its (lack of) reference to the cryptologist. Normally, decryption was a skill practiced by a specialist, a servant or a secretary. Dániel Esterházy writes to Rákóczi in 1711, "Please forgive me that I did not write myself, I have been very sick for the last eleven days, but my servant who wrote this letter and who assists in all my secret communicatio, is a true Hungarian, I trust him very much because I have known him for a long time, this is why I share all my private matters with him." Sometimes the name of the specialist who, as it is said in the sources, “translates” the clavis, is revealed within the correspondence. Ferenc Rákóczi warns István Sennyei: “do the clavisatio yourself, if your illness allows, if it does not, trust it to Butler György Körösy.”

Miklós Bercsényi, in his letter to the prince, makes a reference to a person deciphering the secret signs, a certain Jánoki, who seems not only a secretary decoding the ciphers with the clavis, but also a codebreaker expert.

All in all, one cannot quite expect powerful politicians to labor for hours on the arduous job of deciphering. It is all the more surprising to read that noble leaders of different anti-Habsburg movements, such as Imre Thököly and Ferenc Rákóczi II, regularly did so.

Thököly mentions claves and ciphering a lot in his diary, they seemed to have been laborious part of his everyday life: “My Polish mail has arrived from Drinápoly, big packets of letters, and I spent the whole day looking through them, yet I could not finish with them, because they contained so many claves.” Similarly, though Rákóczi had several trusted secretaries assisting his extensive correspondence and the ciphering work involved, still, his letters quoted above obviously imply that the prince considered ciphering tiresome because he often did it himself. This is confirmed by what Gáspár Beniczky wrote in his diary, “His Majesty, having had the mail delivered to him, retreated to his room privately, and was diligently working on deciphering the letters containing a clavis.”

6.5. Cautious and reckless encryption

A general experience of the history of cryptography is that cipher systems are broken successfully not because they are weak but because they have

---

69 AR I. vol. 3. 602, 22.
70 AR I. vol. 5. 280–283, 141.
71 Nagy, Késmárki Thököly Imre naplója, 298.
72 Révay, II. Rákóczi Ferenc rejtjelezése, 60.
not been used properly. The options they offer are not exploited fully, and they are used carelessly or incorrectly.73 The Hungarian sources contain a number of direct and indirect information about how clerks were aware of the danger threatening ciphered content, how they tried to protect their ciphers from being found out, or how they made them withstand the attempts of the codebreakers. However, such information from the sources is highly ambiguous: there are many signs implying that cipherers were careful, and there are also signs that they did not have the faintest idea how they were making their ciphered texts vulnerable.

Some of the signs of carefulness have already been noted. A number of homophonic tables assigned a special sign for the numbers and the names of the months. This was wise because almost every message contains dates, which are in a special place (at the end or beginning of the letter), and if a codebreaker finds several letters, regularities can be identified as easy breaking points. If information had been also gained from traffic analysis (showing which letter was mailed in which month), the codebreaker would have had a reliable anchor with which to identify the months. If, however, the names of the months are not coded letter by letter, but each month gets a number code, then the codebreaker cannot use this as a breaking point. The same goes for salutations, greetings, or the name of the addressee, all of which can be easily identified by traffic analysis. Assigning separate characters to these in the code table is a sign of cautious and wise behavior. A similarly conscious cipher use is when the numbers are not in alphabetical order in the nomenclature tables, but are positioned vertically – as was described above.

For example, Mihály Teleki enciphered his letter to Mihály Apafi completely, but left the date as an open text.74 Why bother enciphering the date and the signature when a potential codebreaker knows who had sent the letter and when? There is no danger in giving the reader information already known, but it would be unwise to offer a part of the text that would be easy to guess because that would also open a path into identifying certain characters. Teleki realized the paradox: leaving certain parts open actually increases the level of security.

Besides such indirect references showing the users’ level of awareness when it comes to danger, explicit comments about their cautiousness can also be found. They were trying to protect the code key, often burning them

---


74 Teleki 8, 240–241, 212.
upon reading. Dénes Bánffy asked Teleki in 1660 if he is allowed to give a copy of his clavis to someone else, “I have not yet seen one note from Your Lordship, although I have learned that you have sent one, but it was intercepted by Lord Gáspár Barcsai and he still has it. He asked for the clavis, but I did not give it to him because I did not know what Your Lordship was writing about in this note. So please let me know what was written in it, because they are suspicious about it.”\textsuperscript{75} Two years later, in a richly ciphered letter between the same people, Bánffy notes that Captain István Ébeni asked him to burn the letters that were with him for security reasons.\textsuperscript{76} Two weeks later they exchange letters again, and Bánffy talks about the vulnerability of the information that the letters contain, “Please send my letter to Lord Ébeni with proper securitas, it would be bad if Germans or others had found it because I had written about these things a lot, and did not always use a clavis.”\textsuperscript{77}

While there are numerous examples of ciphering with a careful attitude, there are also as many signs of reckless and senseless behavior. Hungarian fugitives writing to Teleki for example acted quite inconsistently. It is typical of them to code only a small part of their letters. In the following case they only enciphered the words in italics, “He also completely destroyed places under Turkish rule around Dévény and Torna”. What does the enemy see of this? “He also completely destroyed places xxxx xxxx xxxx xxxx Dévény and Torna” Some information is lost, but not much, and if someone is familiar with the recent military events, he may even know exactly what places the writer of the message had in mind.\textsuperscript{78}

Dániel Absolon is characterized by frequent but economical cipher use. He does try to pick wisely what he will cover from prying eyes, which may be a clever thing in itself, if well applied. The following excerpt shows an unlucky choice of ciphered text from 1678, “I have humbly received Your Lordship’s 12. letter praesentis from Kővár, and I have sorrowfully taken the reproach to my heart. If I wanted to excuse myself, there would be many words in this letter. I need to make this reply short, the disconsolate spirit indeed does not allow me to be longer.”\textsuperscript{79} One should try reading the text leaving the italicized words out and see that hardly any crucial information is lost.

\textsuperscript{75} Teleki 1, 555–556, 475.
\textsuperscript{76} Teleki 2, 398–399, 295.
\textsuperscript{77} Teleki 2, 398–399, 295.
\textsuperscript{78} Teleki 8, 428–429.
\textsuperscript{79} Teleki 8, 179–186, 154. and MTT III/6. 6–13.
The following paragraph from the same letter is not much better: "What deficiencies and numerous peculiar obstacles there have been on this part, I have written to you. To go on specificatio I have judged to be neither good nor necessary. Rather, whatever deficiencies there had been, I endeavoured to repair and mend – thinking that to frighten away minds with defects that are to be repaired is contra rationem status et interesse publicum, I was about to build, not to destroy." He consistently codes the words “deficiencies” and “defects”, but not “peculiar obstacles”, which is their synonym, as one can clearly see from the sentence structure. It seems that in this case Absalon had a hard time thinking with the head of his possible adversaries.\(^{80}\)

János Pápai, Rákóczi’s ambassador in Istanbul – a center partly, but not entirely in alliance with the fighting Hungarian prince – changed the key of his letters to Rákóczi dangerously seldom – as we have seen above. However, he wrote quite a lot to the prince with abundant ciphering. It would not have been the least surprising if the Turkish secretaries had stopped and copied his letters. Had they compared only three successive letters, which the key indicates all begin with the greeting “Your Lordship,” they would surely have discovered that the number sequences at the beginning of the letters are always almost the same, and it would not have been a difficult task to guess what they mean.

Ke. gy. el. me. s. Ur. am.
133. 39. 32. 273. 80. 205. 61\(^{81}\)

Ke. gy. el. me. s. Ur. am.
133. 39. 364. 32. 273. 308. 205. 61\(^{82}\)

Ke. gy. el. me. s. Ur. am.
133. 39. 32. 273. 80. 205. 61\(^{83}\)

Ke. gy. el. me. s. Ur. am.
133. 39. 32. 273. 80. 205. 61\(^{84}\)

\(^{80}\) Ibid.
\(^{81}\) MNL OL G 15 Caps. C. Fase 36, fol. 3–4.
\(^{82}\) MNL OL G 15 Caps. C. Fase 36, fol. 9–10.
\(^{83}\) MNL OL G 15 Caps. C. Fase 36, fol. 11–12.
\(^{84}\) MNL OL G 15 Caps. C. Fase 36, fol. 13–15.
As this example shows, the danger was not that readers would figure out who the addressee was (which was known well in advance), but that the broken passage is a promising clue with which one can attack the remaining, more valuable and more private parts of the ciphered message.

The same danger threatens when one thoroughly compares letters from the rich correspondence of Rákóczi with his Polish partners. The two hundred and fourteen folios of the National Archives of Hungary G 15 Caps. C Fasc. 39 contain about a hundred coded and fifteen un-coded letters in French from the years 1704–1706. This was done by the same table that the prince used with the French envoys. Containing 450 codes, this encryption was the most elaborate table of the freedom fight. But the sophisticated method is useless, as forty of the letters start with the encoded form of the same phrase: “a Danzik, le 20 Février, Monsieur” (where, of course, the date varies). As the key is homophonic, the particular number sequences differ; however, the corpus is large enough for a skillful adverse agent to correctly identify the numbers corresponding to the same syllables and letters. Even nullities do not pose much difficulty, because the writer of the letters always inserted them at the end of the rows. With such recklessness neither the homophonic system, nor the use of pseudonyms (Nathanaël Sylver or Pompeo Cesoni), makes Rákóczi’s messages difficult to uncover.

6.6. Sand in the machine

When many different people use a technology for different purposes, often under difficult circumstances, hitches do happen.

The most frequent and practical problem is the absence of the key for the enciphered message. Such questions often arise: “Your letters written with clavis have arrived to my hands, my lord, but I could not proceed with them happily, as the clavis you used was not given or sent, thus I am blind in their many terms to this day.” “A letter came from Incédi in Canea. He writes he is close to the Turkish vizier, but his letter being written with a clavis it is still untranslated, because neither my lords János and Miklós Bethlen has the copy of the clavis. Now they have taken it to Baló, hoping that he has the clavis.”

85 MNL OL G 15 Caps. C. Fasc 44.
86 Teleki 6, 394–398.
87 Teleki 4, 278–279, 206.
it, as I do not know its clavis." Thököly wrote to Teleki: “Lord Ubrisi’s clavis being lost, God knows what 88 means, I do not.”

The problem of the absent clavis remained quite persistent in the case of Teleki’s letter, full of numbers, to Mária Széchy dated 6 July 1666. Széchy writes back three weeks later at the end of her letter, on a separate sheet, “My dear Lord Teleki, I could not answer your letter of numbers, you have not sent me its clavis, but I am asking you kindly, please send it.” The key has never been found, and the letter was published in ciphers.

Another woman having problems with Teleki’s claves, his sister, Kata Bornemissza asked him, “My dear Lord Brother, I was unable to read the whole letter which you have recently sent by post, since it is not written in that note which you have left here. These are the unknown words: 020, 550207, 4yo4, 9100, 1, I do not have these.”

In other cases the problem is not the absence of a clavis but that the sender or the addressee is unsure which one to use. Imre Thököly in 1679 was well aware of the problems of handling the ciphers in a secure way: “Regarding the question of the clavis I have no clue, my lord; for I have written using two different claves to You, and I do not know which one you understand.” The writer continues, explaining that the “clavis of mine which was with you I am going to tear up and destroy completely; I have written this letter with the clavis of Lord Fajgel. It would not be secure to send the ciphered letter together with the clavis. Please make a new one, let us use that from now on.”

And again: “My Lord Bocskai had sent the letter included here. Although I tried eight or nine different claves, I was unable to read it. Please send it back from my Lord Gyulafi, maybe you can decipher it, or perhaps it is written using that big old clavis of which I have no copy.”

In the letter of Gáspár Pápai sent to Rákóczi in 1706 it is really difficult to follow the path of some claves, “I have passed on Your Majesty's honorable letter to my Lord Vajovics, however, since the included ciphers did not harmonize, he could not read any of Your Majesty’s letter, and since the time he left Your Majesty he received two letters from Your Majesty, but he understands the meaning of none, for which reason he sent back the cipher

88 Teleki 8, 400, 376.
89 Teleki 8, 401–402, 378.
90 Teleki 3, 582–583, 432.
91 Teleki 3, 592–593, 441.
92 Teleki 1, 220–221, 191.
93 Teleki 8, 543–547, 526.
94 Teleki 4,176–178, 134.
and the letters, keeping a copy of the cipher, so that Your Majesty should use this cipher and it should not be changed as it happened now as a result of forgetfulness; now he has written his own letter to Your Majesty using my cipher.”95

Prince Rákóczi gets similarly lost occasionally when he does not find the proper key. He writes Pál Ráday: “Since your departure from Moldova we have not received more than one letter of yours which, however short it be, we could not translate, although we even tried with the clavis we had given to Pápai when he left to Nándorfehérvár. Therefore we had to use the clavis of Lord Károlyi, which you may even know memoriter, we have once given a similar one to Dániel Eszterház.”96 Ten days later Rákóczi brings up the case again, but now in possession of the solution, “Although recently, being in Munkács, we were unable to translate your letter dated 3 September despite trying numerous claves, and therefore we had to use Lord Károlyi's clavis, when we received your letter written two days ago, on the 21, translating it we laboriously found the clavis, that is why we are writing this letter using that one, and you can safely use it too from now on.”97

Even in the background of these complications, it must have been an exceptional case when Prince Rákóczi was unable to decide if some “suspicious” letters were written “with clavis or simply in Polish”.98

Occasionally, the addressee writes back to a letter – with some amount of reproach – that he is unable to read the ciphered message: “Lord Szepesi wrote the clavis full of mistakes; especially the part about Lord Szalai I was unable to make out, and the end of the parchment which you had written. The rest I could figure out.”99 Pál Szepesi himself, in a similar situation with Teleki, acts more proactively when he reports, “I cannot figure out that capital D, and the [graphic symbol] in your letter, although I can make a good explanation for them.”100

Such reproaches often do not lack humor: “What kind of gold did you write about in the postscript, with nice things about it, I could not penetrate your writing. At such times I wish that you were writing to me without clavis.”101 Correspondents of Teleki are less courteous: “Your witchlike writing caused us awful puzzlement. You wrote about so many things, as we

95 Benda Ráday Pál iratai, vol. 1, 728.
96 AR I. vol. 2. 582–583. 125.
99 Teleki 8, 310–312, 288.
100 Teleki 7, 158–159, 118.
101 Teleki 5, 126–127, 79.
spell out one, we forget the other. It has a start somehow, yet in the end it becomes like the bulls of Kővár let loose on the hillside.”

Miklós Bethlen also does not shy away from reproaching Teleki, “The Palatine’s wife could never read your letter, neither could I, and if you write to me more in this way, I will still not be able to, not even if I put twelve glasses on my nose. It was a cipher indeed – maybe you could not have read it yourself. Next time be sure to write more orderly, if you want anyone to make out a word of it.”

Sometimes it happens that the addressee has the clavis, but it is faulty, or had not been followed correctly. Dániel Absolon simply confuses the nomenclator numbers in a letter, and writes 241 (Polish king) instead of 240 (French king). Funnily, in another letter two weeks later he makes the same error the other way round, and writes French king instead of Polish, as if making some sort of compensation: “I wonder if now and in the future the Hungarian nation can live without the French and the French kings.”

We also find an example of a subtle sense of humor in the following, where Rákóczi asks his envoy János Pápai in a letter from Miskolc to refer to the Porte for permission to invade Szeged. However, the Prince’s chancellor must have made a mistake in ciphering the name of Szeged, as Pápai, in his coded answer, jokes about it. Despite the incorrect encoding he perfectly knows which city the message refers to, but he still writes: “Your Majesty commands that we petition the vizier to ... allow Your Majesty to invade Szrülavár. We were really curious to find this place on the map, but we have not found such fortification, we do not know anything similar under the Hungarian crown, so we cannot act accordingly. If, however, Your Majesty wishes to have permission to invade Szeged, since it is not yet under Your Majesty’s protection, we judged it to be unnecessary to ask permission from the Turks.

Sometimes it is not evident which party makes (more) mistakes. In such cases the correspondents can mutually blame one another. Here, Dénes Bánffy blames Teleki: “You are writing about the deficiencies in my usage of the clavis – perhaps there were a few, but in fact it is the blind laughing

102 Teleki 7, 140–142, 104.
103 Teleki 3, 594–596, 442.
104 Teleki 8, 188–191, 157.
105 Teleki 8, 195–198, 162.
106 Benda, Ráday Pál iratai, 502.
at the sightless. *Turpe est doctori.* It is through such examples that the difference between the theory of cryptology and its meticulous everyday application can be grasped.

### 6.7. Breaking the code

Cryptography users in early modern Hungary did not always take the necessary precautions to avoid the secret message coming to light. Did the enemy take advantage of their carelessness? What kind of code-breaking professionals and offices were formed in the past to break the cipher texts of the enemy, and what tools did they use? My book has thus far focused on the process of decryption by the intended reader, but attention should also be paid to the tools applied by the enemy, who does not have the key and wants to reconstruct it. What did the science of cryptanalysis and code-breaking look like in Hungary in the early modern period? This topic is inherently more discreet, so there are obviously fewer sources, data, or notes related to it than other areas of cryptography.

Code-breaking handbooks of the age available for average readers did not contain the most up-to-date decryption methods. The top-notch handbooks were only available by a privileged few among the political elite. It may sound odd today that J.P. Devos cryptography historian complained in 1967 about the fact that there was virtually no accessible information on the ciphers of WWII, but this in fact had been true for all ages.

A large part of the code-breaking methods available in the early modern handbooks could only have been used for analyzing monoalphabetic ciphers. The 1474 collection of rules *Regule ad extrahendum litteras ziferatas sine exemplo* of Cicco Simonetta is one such cryptological resource. Simonetta, as a statesman of Milan, worked with ciphered texts on an everyday basis for thirty years. Interestingly enough, his book was outdated even in his own time, because it exclusively dealt with cryptograms indicating word boundaries and having no homophones, nullities or nomenclatures,

---

108 Teleki 2, 244–247. 182.
109 Cryptanalysis is a modern word invented by William Friedman, codebreaker of the first half of the 20th century.
in a period when these had already been applied for decades in the diplomacy of the Italian cities.\textsuperscript{112}

Another handbook from 1641 was written by Antonio Maria Cospi, secretary of the prince of Tuscany. Cospi admits that his expertise is limited to decrypting simple monoalphabetic ciphers and he clearly stays away from dealing with homophonic systems that he calls complex ciphers (chiffres composés), declaring these to be basically impossible to decrypt.\textsuperscript{113} He then goes on to offer a detailed methodology on how to solve monoalphabetic ciphers, how to identify vowels, and he also presents frequency charts for syllables in French, Spanish and Latin.

Luckily, there were more adventurous codebreakers. The famous François Viète, a French lawyer and nonprofessional mathematician (1540–1603) who became known as “the father of algebra” after having used letters symbolizing mathematical quantities consistently for the first time in history. It is a little-known fact that he was also a genial codebreaker in service of the French King Henry IV, and he regularly assisted his king by cryptanalyzing messages of the hostile Spanish king. In a secret letter to the Prince of Sully, King Henry’s minister, Viète describes an infallible code-breaking method (infallible rule).\textsuperscript{114} This helps identify the place of vowels by analyzing the frequency of the combination of double and triple characters of the ciphertext. Since languages have fewer vowels than consonants, and since their places identify the structure of a word clearly, vowel-analysis is a necessary part of every codebreaking process. Viète’s analysis begins with the typical code signs of the Spanish court, the most significant rival of France. He points it out that the Spanish codes of his age usually used three or four symbols for each letter, one or two for each syllable, several series of characters for the most frequent words and proper names, and special signs for double letters. He discusses frequency analysis, not so much of a novelty at the time; and then analyzes the triads and diads, or trigrams and bigrams of a text, so the hidden vowels can be discovered.

This method is effective indeed in breaking monoalphabetic secret writings where every character stands for a given letter. Homophonic ciphers, nevertheless, are a great deal more complicated, particularly

\textsuperscript{112} Buonafalce, “Cicco Simonetta” 67–69.

\textsuperscript{113} Antonio Maria Cospi, \textit{L’interpretation des chiffres ou reigle pour bien entendre et expliquer facilement toutes sortes de chiffres simples} (Paris: Courbes, 1641), 3: “Or comme il y a deux sortes de chiffres, les uns simples, et les autres composez, laissant à part ces derniers comme presques impossibles à rencontrer et deschiffer, nous ne parlerons que des premiers quiue sont les simples.”

when they encode syllables as well. Despite what the author suggests, his method may only be applied for homophonic ciphers with any chance of success if the text is strongly formalized, with a well-identifiable addressing, greeting, signature, date and other parts. Applying the “infallible rule” will be especially complicated if nomenclatures are extensively used and they are not easily distinguishable from the symbols of letters and syllables. One may reasonably suppose that Viète, the talented mathematician and experienced codebreaker, could successfully find vowels in homophonic ciphertexts too, and thus break a given code. This public description of the infallible rule, however, does not lead the reader into the depths of his method and does not provide them with really useful tools. It would seem more interesting to see what this writing does not tell us than what it does.

The most detailed and most didactic cryptological handbook survived from the early modern period is by an anonymous (supposedly Spanish) author, *The Art of Deciphering* (*Art de deschiffrer*). This 136-page manuscript has come to us in seventeenth century French translation. Not offering “infallible” solutions, it does describe a number of observations, maxims, rules and recipes that can help identify the language of the plain text, identify which signs stand for letters and which for syllables, recognize nullities, analyze letter frequency, and so on. The author, of course, distinguishes between simple (monoalphabetic) and complex (homophonic) ciphers, gives a detailed analysis of both, and introduces a case study for each, where he breaks a ciphertext step by step, applying his own maxims and recipes. As for the theory, it does not provide more than Viète’s secret advices. What makes this handbook more helpful is that it is more detailed and practical, describing specific examples that illustrate the application of principles. Following the step-by-step analyses of the anonymous author and learning these skills one can successfully attack a cipher created in this period.

There is no indication in the early modern Hungarian sources that these four, or any other cryptanalytic handbooks were used. One can plausibly suppose, however, that practicing codebreakers had at most similar, if not more limited tools in solving the cipher messages of the enemy. Some sources imply a preference towards torturing the messenger or stealing the key instead of intellectually reconstructing it.

Many of the claves used in the anti-Habsburg Wesselényi movement, for example, were outdated monoalphabetic ciphers\textsuperscript{116} that the Habsburg court could easily have broken. Still, there is no source indicating that anyone bothered with code-breaking. It seems from the documents that they focused solely on intercepting the keys as the main method of mopping up the organization.\textsuperscript{117}

The physical and not so much the intellectual way seemed to have been more rewarding and more practical in other cases too. Messengers or spies were tormented, executed, their letters and keys confiscated. The 1709 diary of the Edirne legation of two Hungarian envoys tells how concerned they were about securing the lines of information during the negotiations with the pasha. They were wondering about what kind of information they can send enciphered, what they can send only via special secret envoys, and whether that messenger would be tortured.\textsuperscript{118}

The military regulations of Rákóczi are specifically keen on intercepting the enemy’s letters.\textsuperscript{119} “The punishment for knowing about the enemy’s correspondentia and not reporting it: Whoever may hear about such correspondentia and does not capture it, does not report it to the officers, does not send it or give it to the officers, or hears about spies and messengers and does not report it, does not capture them and does not bring them and all their belongings to us or our generalissi, is sentenced to death.” Moreover, “The enemy's letters should not be delivered: No one should deliver the letters of the enemy, but upon finding them, should hand them to us or the general nearby them, otherwise the person who knows about someone who has such letters or delivers them and does not report it is considered a traitor and will be punished as such.”

Attempts were made on both sides to intercept the enemy’s letters. István Ébeni mentions a systematic hunt for Hungarian letters twice in his messages to Mihály Teleki, the first time saying that the claves can be found out with the help of the captured letters.\textsuperscript{120} Teleki’s wife, Judit Véér attaches

\textsuperscript{116} ÖStA HHStA Ungarische Akten Specialia Verschwörerakten VII. Varia, Fasc. 327. Konv. D. Chiffres 1664–1668, fol. 1–61. See also MNL OL E 199.


\textsuperscript{118} Thaly Kálmán, ed., Gr. Teleki Mihály és Pápai János Nándorföjervári követségének diariuma (Diary of the embassy of Mihály Teleki és János Pápai) 1709. (Budapest, 1875), 240–241.

\textsuperscript{119} Regulamentum universale, inclytorum confoederati regni Hungariae statusum ac ordinum, tam militarium, quam et ex parte inclytorum comitatu, liberarum item ac regiarum civitatum, aliorumque quorumvis, observandum (Nagyszombat, 1707), quoted by Révay, II Rákóczi Ferenc, 14–15. See also Benda, Ráday Pál iratai, 415–6.

\textsuperscript{120} Teleki 2. 396–397, 293. and 436–437, 320.
a completely enciphered postscript to her undeciphered short letter mentioning a captured and hanged messenger, “If you had left this place earlier you would have been captured by the men with a rifle. The peasant from Szelnicze who was taking a letter to Szamosujvár (Gherla, Romania) was captured, taken to Apafi and the Turks had him hanged.”

Dénes Bánffy confesses to opening the letters of both the emperor and the bishop only in a ciphered part of the letter, here typeset in italics: “... and all of these things I have learned when I cut open the letter to the bishop, and took out from the envelope the letter to the emperor also, and forwarded these letters enciphered to Your Lordship.”

It seems that for these people the only possible way of reading an encrypted text was to get or own a copy of the key, the possibility of breaking a cipher by means of mathematical methods was hardly ever considered. János Kemény was writing to György Rákóczi I. in 1644, “I was brought some letters from Poland, I opened them, hoping to make sense of them, but since they are deciphered, I cannot read them. I am asking Your Majesty to let us know what they are writing.” In 1678, István Koháry reports to palatine Pál Esterházy the capturing of Thököli’s letters, but, again, he seemed to have lacked tools for breaking the ciphered letters, “I would like to humbly report to Your Majesty that my soldiers have intercepted a lot of letters and I have torn these open. (They were sent from the camp of Count Tököli to Kővár and from Kővár to Count Tököli.) Unfortunately, almost all of them are written in numeric ciphers so I could not learn anything from them. They must be really important. (...) Among these are letters of Teleki and some other important French people and these cannot be read without a clavis.”

There are only a few references that suggest that someone did not sit around idly until they get hold of the proper key, but the cipher itself was also investigated. In 1706, Rákóczi reports in his confessions that he had learnt about the emperor’s instructions to Rabutin through a ciphered letter that he had broken himself. He also mentions the capture of a secretary of the enemy in 1708, who happened to carry a cipher key to General Heister. Miklós Bercsényi, in his letters to the prince, mentions several intercepted ciphered letters during the years 1705 and 1706 that he was trying

121 Teleki 2, 294–295, 223.
122 Teleki 2, 309–311.
123 MTT III. 3. vol. 45–46, 5.
125 Révay, II. Rákóczi Ferenc, 14 and 98.
to break. And finally, there remained in the archives of the freedom fight at least ten German claves written in Gothic letters (including one from Rabutin to the emperor, and others to various captains and generals) that must have contained secret information from the Habsburg Court, and that were probably reconstructed by the prince’s secretaries through intercepted letters. Logical codebreaking practice had few followers in the area, Prince Rákóczi being the most famous among them.

6.8. Advanced or outdated?

The question arises: how sophisticated was Hungarian cipher use compared to the cryptologic technology of Europe at the given time? The first impression might be positive. Comparing the best tables of the Rákóczi freedom fight to those of the chancellery of the Habsburg court, for example, of the papal diplomacy, or the French court, one sees that they are not inferior in quantity (of numbers assigned to letters, syllables, and nomenclatures), nor in structure (since they were carefully designed homophonic systems complemented by nullities). It is also worth noting, however, that the most advanced practices of the prince’s diplomatic correspondence were influenced by the French. It was the tables sent by the French court that helped Rákóczi catch up with the rest of Europe in this respect. In the seventeenth century, Antoine Rossignol, mathematician-cryptographer of Richelieu and then of Louis XIV, developed an enormous homophonic system of 590 items that coded syllables. The “Grand Chiffre,” as it later became to be known, was a puzzle to everyone for the next two centuries, until Étienne Bazeries (1846–1931) came along and solved it. The ‘Sun King’ of course did not offer this unbeatable system to his Eastern ally, but he shared their second most advanced one, which was still considered one of the most sophisticated tables of the time.

126 AR I. vol. 4. 374–375, 61; and AR I. vol. 5. 100–104, 38; 120–122, 53.
In Rákóczi’s environment, many envoys received claves that were developed according to the French system, just like the table of Pápai discussed above, but the locally used codes of the freedom fight remained surprisingly primitive. The 1705 clavis of General Sándor Károlyi and general Miklós Bercsényi, for example, was not only monoalphabetic; it also used graphic signs. Using these obviously did not help fast and clear communication on the battlefield. It is wearisome to draw a square instead of the letter ‘a’, a triangle instead of a ‘b’, an ‘m’ sign with a cross at the end instead of the letter ‘e’, but one should also consider how much more difficult it is to look up those signs from a table that cannot be ordered logically in any way, as opposed to consecutive numbers.\footnote{War History Archives E. 1705/18.} Still, there are a number of letters proving that this very impractical table was indeed used.\footnote{War History Archives of Budapest E. 1705/5, 6, 03, 16, 17.} Similarly monoalphabetic and consisting of signs are the clavis of Rákóczi and Bercsényi from 1704,\footnote{The key reconstructed in AR I. Vol. 4. köt. Appendix. The letters: AR I. vol. 2. 163–167, 10, 13, 28, etc.} as well as the 1707 key of Mihály Hentér, Rákóczi’s ambassador in Constantinople.\footnote{MNL OL G 15 Caps. D. Fasc 80. fols. 38, 40, 46. MNL OL G 15 Caps. E. Fasc 109.} The enciphering practice of the prince’s diplomacy was not uniformly developed: higher-level ciphers were used internationally, less advanced ones internally.

Another feature of Hungarian cryptographic practice was that it advanced more slowly than in Western Europe, and even towards the middle and end of the seventeenth century, shockingly simple methods were used to cover information in life-and-death situations. In 1637, Prince György Rákóczi I was jovially writing to his envoy: “We would like to write more, but we cannot put it down in writing, so we are sending you a clavis that we are going to use in the future. Basically you only have to write down the above 12 letters with those of the bottom row, the bottom 12 letters with those of the top row.”\footnote{Beke and Barabás Samu I. Rákóczi György, 340–41.} In other words, the prince is offering a cipher that mutually assigns the second half of the alphabet to the first half. No nomenclatures, no nullities, no syllables, no homophones. And the prince of Transylvania actually used the system which could have been broken by a school-aged child.\footnote{Ötvös, Rejtelmes levelek, Révay, Titkosírások, 76–86.}

Staying in the Transylvanian area, a similarly odd case happened a few years later. Jónás Mednyánszky, in correspondence with the prince, György
Rákóczi II, used a decent homophonic system in his letters. In this system (the table of which is extant in several copies) three numbers are assigned to each letter, syllables have their distinct numbers, and all this is extended with a couple of nomenclators (191 – Rex Hung or King, 346 – Moldavia, 294 – Roman Catholic, 347 – Transalpina, 366 – Russia, 192 – Palatinus, 194 – Primas, 204 – Svecus, 193 – judex curiae). However, in 1658 they replaced this advanced homophonic clavis with a simpler, monoalphabetic key comprised of graphic symbols, letters and numbers. In this latter one, there are no codes for syllables, only six nomenclators stand at the end of the list (4 – Nádasdy, X – Archbishop, 10 – Porta ottomanica, Z – Rákóczy, W – Chancellor, 271 – King, N – Palatinus). What could have been the reason to drop the more advanced clavis in favor of a more primitive and laborious one? This is just as perplexing as those messages and tables of the mid-seventeenth century Wesselényi movement that were monoalphabetic.

Of course, it would be misleading to make the impression that in contrast with Hungary, Western Europe had a consistently high standard of ciphering. On the contrary, while the majority of the claves were certainly of a high standard, readers can find surprising exceptions. In 1621, Ferdinand II, Holy Roman Emperor, exchanged letters with Jacobus Curtis (Jakob Kurtz), his Polish trustee, using a monoalphabetic clavis. In 1628–1629, Johann Ludwig Kuefstein, ambassador at the Porte, wrote to Emperor Ferdinand III with a cipher of graphic symbols (and he did so using a weak homophonic, practically monoalphabetic system). Likewise, in 1632, the Emperor’s secret reporters, or spies, coded their Italian letters with a clavis of graphic symbols. Sixty years prior to this, it was a common method in the Imperial administration to use graphic symbols (see Carolus Rym’s letters from

138 MNL OL E 190, Arch Fam. Rakóczi, 43. 5. 794. 802. 816. 821. 872. 875. 886.
139 MNL OL P 497 Mednyánszky Family, fasc. 3. Keys for the correspondence of György Rákóczy II and Jónás Mednyánszky, fol. 13. 5. 2. 4.
140 MNL OL E 190, Arch Fam. Rakóczi, 44. 5. 891–893, 897–8, 901, 904, 909, 924, 926.
141 MNL OL P 497 Mednyánszky Family, fasc. 3. Keys for the correspondence of György Rákóczy II and Jónás Mednyánszky, fol. 11–12.
142 MNL OL E 199 fasc. 8, pallium 1.
144 HHStA, Ung Akt. Misc Fasc 422 Conv 1 fol. 72–79.
146 ÖStA HHStA Staatenabteilungen Türkei I. Kt. 112. Konv. 5. fol. 1–9 and fol. 17–28. I thank Dóra Kerekes for calling my attention to these sources.
Constantinople around 1571,\textsuperscript{147} but the seventeenth century is dominated by the use of the more comfortable numbers. One could make a long list of similar exceptions that prove that development was not linear (from simple monoalphabetic substitutions to the more complex homophonic methods) in the Court of the Habsburg Emperor either, and that historical figures had different meanings for the terms “improved” and “practical” when it comes to ciphering.

By the end of the early modern period, the usage of ciphers in Hungary had generally caught up with the Central and Western European standard. This, however, was mainly influenced by Western practice itself. The letters from the correspondence of Transylvanian princes reveal that by the middle of the seventeenth century, ciphering practices in the Principality of Transylvania were on a less complex level (using simple monoalphabetic ciphers) than those of the envoys of the Habsburg (who primarily employed homophonic methods); even Mihály Teleki had only a few tables of Western quality, many of his claves remained monoalphabetic ones.\textsuperscript{148} In addition, the fact that the Princes tended to do the coding themselves – something that György Rákóczi I, Imre Thököly and Ferenc Rákóczi II felt so natural – is not a practical usage of ciphering. Even a developed method can be used in an undeveloped way.

\textsuperscript{148} MNL OL P 1238 Mihály Teleki Collection, Miscellaneous documents, Cipher keys.