Colonnele Frank's Indecipherable Chiffre

Benedek Láng
ELTE, Hungary
benedeklang@gmail.com

Abstract

Colonnele Frank's 23-folio-long French-language description of what he calls a "chiffre indéchiffrable" survived in the cipher collection of Leopold, grand duke of Tuscany, and Holy Roman Emperor. The author lists the usual weaknesses of the ciphers and offers his technique to remedy them. It is a polyalphabetic method helped by a circular instrument, by no means a fundamental invention in the late 18th century. What makes it relevant is that it is a relatively early practical application of the polyalphabetic method, where not only letters of the alphabet, but even whole words are manipulated. Not much is known about the colonel author, but on the basis of the document, it becomes clear that he was a real user of military cryptography.

1 Context

Very little is known about Colonnelle Frank's undecipherable cipher. It is kept today in the Haus-, Hof- und Staatsarchiv in Vienna (Handarchiv, Kaiser Franz, Karton 21 07 f. 1-23, see in the Decode database: https://decrypt.ponens.org/decrypt-web/RecordsView/1910; Megyesi et al. 2019).

This archival collection famously collects the diplomatic documents (including the cipher keys) of the Austrian Habsburg monarchs (Láng, 2020); however, the documents of this specific folder seem to originate from a different source. The box groups the keys of Leopold (1747-1792), ninth son of Queen Maria Theresa (1740-1780), brother and successor of Emperor Joseph II (1780-1790), himself Holy Roman Emperor for a short period until his sudden death (1790-92). But Leopold is remembered not because of his brief two-year-long reign as emperor. From 1765 to 1790, he acted as the Grand Duke of Tuscany and became famous as one of the first enlightened absolutists, whose reforms have been modeled and copied by his many fellow sovereigns. His 25 years spent as the ruler of Tuscany marked a decisive modernizing period in the history of the Grand Duchy.

The 21st folder of the Kaiser Franz collection contains 17 different ciphers, most of them sophisticated homophonic tables and codebooks, including both the chiffrant and the déchiffrant parts. Only a few of them are dated, usually for the 1780s. The titles and names seem to indicate rather a North Italian than an Austrian origin; they rather belonged to Leopold's correspondence as a duke before 1790 than as an emperor after that date.

We have no clue who the lieutenant colonnele Baron de Francque – or as he is named elsewhere: Colonnele Frank – was. His name does not appear in the six-volume dissertation by Harald Hubatschke (1975) on the cryptography of Austria. We can plausibly suppose that he was part of Leopold's Tuscan past, and his cipher was transferred together with the whole collection by Leopold to Vienna, his city of birth and death.

2 The “Chiffre Indéchiffrable”

Colonnele Frank is keen to explain why his cipher outperforms all others! Most ciphers, he argues, are insecure and can be exposed easily by studying the ciphertext. Most of them are furthermore inconvenient because they encrypt few things in many lines. Finally, they are also inconvenient, because one needs a separate key for each correspondent, if one does not want any of them to read the letters sent to the others.

Colonnele Frank's cipher, however, is different. He was a practitioner of cryptography, and thus he could make precise observations about the practicability of ciphers. Even though his invention may not be that resistant to codebreakers as he believed it to be, he certainly had the talent to invent something practical. In his system – he writes – a lot of things can be written in a few lines, and it can serve for the correspondence of different people without enabling them to decipher the other's letters.

Finally, it is practical to use, one can look up the letters, numbers, and words with great ease. For the sake of easiness, not only the 26 letters of the French alphabet can be enciphered, but also those words, which are frequent in the given correspondence. These are typical military words in this very cipher, but any other set of words is possible.

The method consists of two concentrical circles, of which the middle one is movable (Figure 1). The outer circle (zone de l'alphabet) includes the alphabet and the common words arranged in alphabetical order (and the initials are indicated around the circle to help the user look up the given word). The inner circle (zone du chiffre) looks more complicated, but only for practical reasons. It is a simple circle including numbers from 1 to 99, scattered without any system (not arranged in a chronologic order – as the author stresses). The four inner circles within the "zone du chiffre" only serve to help the user to find where a given number can be found in the periphery, the first circle containing numbers from 1 to 20, the second up to 40, the third up to 60, and so on.

In the middle of the whole figure, we see the metacharacters of the system (signification des points, comas, et lignes). What is essential here is that by adding specific notations, the user can indicate whether a given number designates which cipher key is being used, serves as a cipher character standing for a letter, or as a character standing for a word. Cipher key starting, letter ending, and word ending notations are listed together with the proper punctuations (comma, colon, full stop), which can also be indicated in Colonnele Frank's system.

2.1 The Real Cipher and its Decryption

Colonnele Frank's text is highly instructional. He not only explains, but also demonstrates how his method works, using a longer military message as a sample. He puts forward two methods, both of which have two ways to use.

The first is what he calls the "chiffre reel" that is, the real cipher. Imagine, that you want to encrypt the following sentence: “Je ferai marcher le 9. armée par sa droite sur deux colonnes, les canons de 6.” First, you may choose 13 as the key of the cipher. You may choose any other number, this is just for the sake of an example, which is practical because this is precisely how the circles on Figure 1 are aligned. You write 13: because : is the notation that shows that 13 is not part of the ciphertext; it refers to the key. We turn the inner circles on the circular diagram so that 13 on the inner circle would be found directly below the letter A on the outer circle. This is precisely how we see it in the image. Now, you could decide to spell the first word, 'je', however as this word – being 'I', one of the most frequently used words in French – is part of the pre-set vocabulary of the machine, why not substitute the whole word with its equivalent: 18, that is directly under it. Then, you continue with the word faire (to do, another frequent word), the cipher equivalent of which is 69. However, it is not faire, that we should encrypt, but ferai (I will do), so we add an upper point to 69, showing that we are still within the same word and 13 (letter A) and 89 (letter I) to the word, and we close this with full stop '.' because this notation signifies the end of a word. We proceed with marcher, so we first add 39 (marche), upper point (we have not yet finished the word) and R (5.) the last point signifying the end of the word again. The following word, 'le' will be spelled out as 16 and 27. At this moment, it is time to turn the wheel to change the cipher alphabet: so we write 77:, and turn the inner wheel until 77 is below the letter A. Securing our method like this, we proceed the same way we have done so far changing the cipher alphabet (that is, the relative situation of the wheels) after 2-3 words. The first part of the encryption is this: 13:18.69˙13˙89.39˙5.16˙ 27.77: Colonnele Frank goes on with detailed explanations until he arrives at the end of the whole sentence.

Having understood the encryption, there is no reason to spend much time with the decryption process, even though Colonnele Frank, being a didactic teacher, devotes as much space to it as to the previous explanation. Imagine that you receive the above message, you are of course in possession of the wheel, so you turn the inner wheel until 13 is below A (as you recognize that 13: signifies the setting). Then you go step by step decoding the meaning of the numbers and the metacharacters. The method is unambiguous, there is no room for misunderstanding.

2.2 The Ideal Cipher and its Decryption

The second method offered by the lieutenant colonel is called ideal, a name indicating higher prestige and resistance than the real method. The main difference is twofold: the key is no longer

included in the message, and the wheel is turned after every new cipher character.

Imagine that you want to send the very same sentence as in the previous case. Imagine furthermore that you had previously agreed with the message's addressee upon the number 18, which will serve as the key (le reglé). What you do now is that you turn 18 in the inner wheel just below Je, the word you first want to encrypt. To easily follow this explanation, the wheels are again set for that value, as one can see in Figure 1. We do not write anything yet, instead we go to the letter A, and check the number below it, which is precisely 13. This is the regulating number (le reglant). So we write 13. Then we want to write ferai, so we turn 18, the key (le reglé) under faire, we check again the number under A, which is 6. Then, we go for A, which is easy because we turn 18 under A, and check the number under A, which is of course, 18. Then, we go for I following the same method. The beginning of our encryption will look like this: 13.6˙18˙12. Deciphering it is a simple mirroring of the procedure.

The colonel seems to be impressed by this method probably because there is a wheel movement after each cipher character. Still, it is easy to see that by moving the wheels according to this method, we get a simple monoalphabetic substitution cipher with a fairly limited nomenclature list.

He might have felt something because he proceeded to present a new method, which is basically the previous one, but using several keys (several reglé) changed according to specific pre-arranged rules (after every word, or after every 2nd, third, etc. words) in a way that after 18, they will be certain numbers which can be found in specific distances from 18 in the circular figure. The colonel gives an example, where 18 is the reglé for the first three words, 9 for the two second, 60 for the three following ones, 99 for two more, and then the cycle restarts, it is 18 again for three words. This modification renders the cipher indeed more resistant.

The author explains how to decipher such a ciphertext with different keys. And finally, he also explains how easily one can correspond with several addressees using the same wheels and agreeing upon a different set of key numbers (reglés) so that the various correspondents will not be able to read each other's messages.

On the last five pages, the author gives a long sample letter (starting with the well known "Je ferai marcher…" sentence); its encrypted version using the real cipher; the decipherment of this; its encryption with the ideal cipher using 18 as a key, then using 18, 9, 60, 99 as periodically changing keys; and finally he also provides the decryption of this last ciphertext.

An attentive reader of these 23 folios (basically 32 written pages) is provided with helpful step-by-step explanations and ample materials to understand the methods and practice them.

3 Merits and Historical Relevance

Was Colonnele Frank right when calling his method undecipherable? The quick answer is no. Since Charles Babbage polyalphabetic encryption can be broken making use of the fact that such ciphers are periodic. In defense of the colonel, one may object that Babbage's invention dates from seventy years after that of Colonnele Frank and that in Frank's method, the cipher alphabets do not change in a periodic way. Changes are after each word or randomly, making it harder to look for patterns in the ciphertext.

However, looking at the colonel's sample texts, which he provided amply, one cannot help recognizing lots of repetitions. Furthermore, when the user only applies three or four circle settings (both in the real and in the ideal ciphers), this polyalphabetic method basically turns into a small set of monoalphabetic ciphers. Consequently, the codebreaker does not need to wait seventy years until the polyalphabetic method is learned how to be broken. He can turn to the usual decrypting procedures, analyzing the different sets of monoalphabetic ciphers in the real cipher (where the key change can be recognized), or using the probable word method in the ideal cipher (where the key is not included, but where again, only four monoalphabetic methods are rotated).

However, to Colonnele Frank's merit, we should admit that his cipher machine *could* have been used with a larger number of settings avoiding periodicity. Only a sufficiently sophisticated method of changing settings should be agreed upon by the sender and the receiver using the ideal method (where the key is not included in the message), a practice that would render the technique a real polyalphabetic one. And his was

an easy encryption, not less practical than using any large homophonic table. Abundant sources from the 17th and 18th centuries (and even from the early 19th century) testify that the main reason polyalphabetic ciphers were not used was that they were seen as too complicated, tiresome, and tedious to apply (Kahn, 1996, 150).

The historical importance of Colonnele Frank's cipher does not lay in its combinatoric novelty because polyalphabetic method had been invented centuries earlier by the famous renaissance polymath, Leon Battista Alberti (1404-1472). It rather lays in its practicality. And since there was no decryption algorithm available to solve polyalphabetic ciphers at the end of the 18trh century, he was right calling it undecipherable. An achievement we would not expect from the battlefield.

Acknowledgments

The document under study has been found and copied in the Haus-, Hof- und Staatsarchiv in Vienna by Anna Lehofer. I am grateful to her for calling my attention to this unique source.

This work has been supported by the Swedish Research Council, grant 2018-06074, DECRYPT – Decryption of Historical Manuscripts. I am grateful to the members of the DECRYPT team, particularly to George Lasry, Bernhard Esslinger and Nils Kopal, and the team leader Beáta Megyesi. They – together with the anonym reviewers – gave me valuable feedback on an earlier version of this paper.

References

David Kahn. 1967. *The Codebreakers – The Story of Secret Writing*. Macmillan, New York; revised and updated edition: 1996. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet.* New York: Scribner.

Beáta Megyesi, Nils Blomqvist, and Eva Pettersson. 2019. The DECODE Database: Collection of Ciphers, and Keys. In *Proceedings of the 2nd International Conference on Historical Cryptology, Mons, Belgium.*

Harald Hubatschke. 1975. *Ferdinand Prantner, 1817-1871. Die Anfänge des politischen Romans sowie die Geschichte der Briefspionage und des geheimen Chiffrierdienstes in Österreich* (6 Bande, phil. Diss. Wien, 1975) Universität Wien, Universitätsbibliothek: D-20411/1-6.

Benedek Láng. Was it a Sudden Shift in Professionalization? Austrian Cryptology and a Description of the Staatskanzlei Key Collection in the Haus-, Hof- und Staatsarchiv of Vienna. 2020. Beáta Megyesi, ed. *Proceedings of the 3rd International Conference on Historical Cryptology HistoCrypt.* Linköping: Linköping University Electronic Press. 87-95.

Colonnele Frank. *Le chiffre indéchiffrable*, manuscript, Österreichisches Staatsarchiv, Haus-, Hof- und Staatsarchiv, Hausarchiv, Handarchiv, Kaiser Franz, Karton 21. 07 f. 1-23. In the Decode database: https://decrypt.ponens.org/decrypt-web/RecordsView/1910

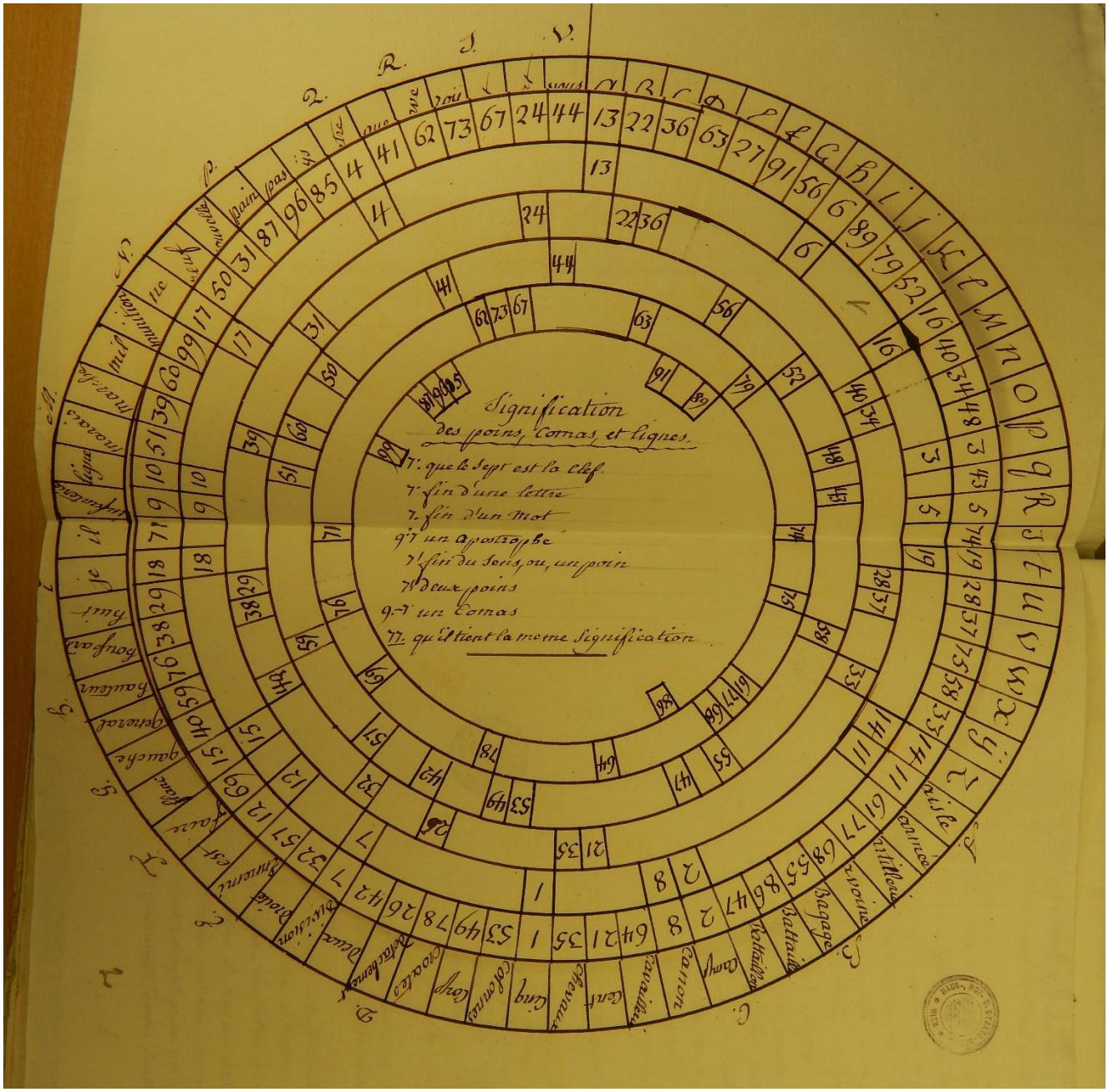

Figure 1. Colonnele Frank's encrypting machine
Österreichisches Staatsarchiv, Haus-, Hof- und Staatsarchiv, Hausarchiv, Handarchiv, Kaiser Franz, Karton 21. 07 f.2r.