Deciphering Charles Quint (A diplomatic letter from 1547)

Cécile Pierrot, Camille Desenclos, Pierrick Gaudry, Paul Zimmermann

Deciphering Charles Quint
(A diplomatic letter from 1547)

Cécile Pierrot
Université de Lorraine
CNRS, Inria, LORIA
F-54000 Nancy, France
cecile.pierrot@inria.fr

Camille Desenclos
Université de Picardie Jules-Verne
Centre d'histoire des sociétés,
des sciences et des conflits
F-80025 Amiens Cedex 1
camille.desenclos@u-picardie.fr

Pierrick Gaudry
Université de Lorraine
CNRS, Inria, LORIA
F-54000 Nancy, France
pierrick.gaudry@loria.fr

Paul Zimmermann
Université de Lorraine
CNRS, Inria, LORIA
F-54000 Nancy, France
paul.zimmermann@inria.fr

Abstract

An unknown and almost fully encrypted letter written in 1547 by Emperor Charles V to his ambassador at the French Court, Jean de Saint-Mauris, was identified in a public library, the *Bibliothèque Stanislas* (Nancy, France). As no decryption of this letter was previously published or even known, a team of cryptographers and historians gathered together to study the letter and its encryption system. First, multiple approaches and methods were tested in order to decipher the letter without any other specimen. Then, the letter has now been inserted within the whole correspondence between Charles and Saint-Mauris, and the key has been consolidated thanks to previous key reconstructions. Finally, the decryption effort enabled us to uncover the content of the letter and investigate more deeply both cryptanalysis challenges and encryption methods.

1 Introduction

What is required to decipher an encrypted letter which was composed five centuries ago? Modern cryptographic knowledge would normally be more than sufficient to decipher a 3-page letter. That was the first guess while discovering, in a public library, the *Bibliothèque Stanislas* (Nancy, France), an isolated encrypted letter that was written on 22nd February 1547 by Emperor Charles V to Jean de Saint-Mauris, his ambassador at the French Court. But, due to too many symbols, brute force attacks were hopeless and cleverer methods were unsuccessful. This initial failure reveals the mutual benefits for cryptographers and historians to work together in order to uncover the content of an almost fully encrypted letter and, above all, to better understand the encryption methods, first by working from scratch, then by comparing with other deciphered letters and finally by merging with former partially recovered keys.

2 General context

2.1 The story of the project

The existence of an encrypted letter of Charles V, which had not yet been deciphered, was known in literary and cultural circles in the city of Nancy, but this letter was neither properly identified nor yet digitized. Two years passed between the first mention of this letter by some acquaintances of C. Pierrot, and the moment when she was able to see it and start working on it, thanks to a word-of-mouth game to find the letter that eventually worked. A mixed team of experts, first cryptographic researchers and then historians, was formed.

Now openly available online, the letter consists of two folios: three pages of text and an address on the last page. The first lines and the last two paragraphs on the first page as well as the last lines of the third page (date and signatures) are cleartext. As for many letters produced at that time by the Imperial chancellery or by the Imperial cabinet (Stix, 1934-1936), the letter was written in French. The bulk of the document (two and a half pages) is ciphertext. We counted 1767 symbols taken

from a set of 125 different ones[1] of various types: Latin characters, mathematical symbols and so on. Cleartext allowed a quick identification of the letter, written by Emperor Charles V to his ambassador at the French Court, Jean de Saint-Mauris. Sent to Francis I in 1544 as permanent ambassador, Saint-Mauris was related, by his wife, to Antoine Perrenot de Granvelle, Charles' state secretary and main counsellor in the Holy Roman Empire, and both were from Franche-Comté. This provided a substantial leverage for the decipherment process.

2.2 An isolated letter in a French public library

Although the letter meets the usual patterns of encrypted letters from the mid-16th century (diplomatic context, cleartext and ciphertext on the same page, alphabetical and numerical symbols, etc), its preservation history led us to adapt and question the traditional approach to such letters. This letter wasn't hitherto properly identified, although Saint-Mauris is well known to early modern historians, in particular because of his broad and extensive correspondence in which he reported on the complex relationship with Francis I (Cassan, 1878; Potter, 2013), either to Charles and Granvelle, to Maria of Austria (governor of the Lower Countries and Charles' sister), or to Infante Philip (Charles' son) and the state secretary for Spain, Francisco de Los Cobos y Molina. Not only was it misidentified (the date especially was wrong in the library catalog[2]) but it had no reason to be kept in Nancy. Indeed, despite first attempts of channeling the preservation of state papers in Simancas (Spain) from 1540, Saint-Mauris' letters, as many other diplomatic ones, match two common preservation patterns, depending on whether the correspondence is active (the ambassador is the one sending a letter) or passive (the ambassador is the recipient).

The active correspondence of Saint-Mauris[3] has mainly been preserved in the state archives that match the main location of the recipients [4]. It can thus be found in Vienna for the letters to Charles and Granvelle (OeStA-HHStA, Fr 10-16)[5], in Brussels for the letters to Maria of Austria (AGR Audience 420; AGR Audience 1672) and in Simancas for the letters to Infante Philip and Los Cobos[6]. Within this active correspondence, the two previous letters of Saint-Mauris to Charles have been identified: 11th February 1547 (copy) (BM Besançon, Granvelle 40)[7] and 6th February 1547 (Archives nationales, K1487)[8].

On the other hand, the passive correspondence was often kept by the ambassador with his private papers. Saint-Mauris' passive correspondence is no exception. One part is preserved at the public library in Besançon (BM Besançon, Granvelle 40; BM Besançon, Granvelle 70) but it concerns mainly the year 1545. Further letters, especially from Charles, are probably lost or scattered across Europe without global identification[9]. But if the preservation of some letters in Besançon makes sense (Saint-Mauris' correspondence is preserved along with the Granvelle collection), the existence of a single letter in Nancy is much more surprising. After some research, the letter would belong

[1] All the symbol counts are approximate since some symbols aren't always well formed and thus look very similar, see Appendix, Fig. 3.

[2] "1546" is written at the end of the letter. However, at that time, several dating systems could be used and the year could begin at Easter and not on January 1st. According to today's dating system, the letter was written in 1547.

[3] Unfortunately it hasn't yet been possible to check every part of this correspondence; it may thus have some deficiencies in the following presentation. Only the letters (or their copies) that are kept in Paris, Besançon and Madrid have been studied for now either directly or thanks to their digitization (Besançon, Madrid).

[4] Recipients do not always match the expected archival collections. Some letters to Maria of Austria are for instance preserved in Vienna.

[5] Seven letters to Charles and Granvelle, and especially a copy of a letter written in February 1547 can be found in Besançon (France) with Granvelle's papers (BM Besançon, Granvelle 40, fol.139, letter to Charles V, 11th February 1547). Another isolated encrypted letter from Saint-Mauris to Granvelle (1548) has been identified in the National library of Spain (Madrid) (BNE, 7913).

[6] Part of Simancas archives are accessible as microfilms at the French National archives (Paris) (AN, K1485-1488). One can found Saint-Mauris' active correspondence to Spain, some minutes from Infante Philip as well as some copies of letters from Saint-Mauris to Charles.

[7] Due to the long transmission delays, Charles hadn't yet received this last letter on 22nd February 1547. He acknowledged the reception of two letters only: 26th January and 6th February 1547.

[8] The letter in Simancas / Paris is however a copy made by the Spanish state secretary. Only plaintext and cleartext are hence transcribed

[9] Maxim Hoffman, PhD student in Ghent University, pointed us to Charles' minutes which would be kept in Brussels. Thus, a minute of the 22nd February letter would still exist. Unfortunately if a verification couldn't be carried out for this contribution, the authors will conduct some researches in the Archives générales du royaume in May 2023 in order both to compare their decipherment with the minute (if still existing) (AGR Misc 95-96) and to expand their corpus of encrypted letters from and to Saint-Mauris (AGR Audience 420; AGR Audience 1672).

to the collections since the 19th century. The library archives unfortunately do not keep tracks of the date or terms of its acquisition. One hypothesis can be formulated: part of the passive correspondence would have been scattered early, one letter bought by an erudite and then given to or bought by the library. That is consistent with the incomplete preservation of the passive correspondence for years 1546-1547[10] but confirming this hypothesis (and the loss of the other letters) will require further enquiries about Saint-Mauris' succession.

2.3 Historical context

When Charles wrote his letter on 22nd February 1547, the main European sovereigns were supposed to be at peace, while Emperor Charles V was dealing with a political and religious conflict within the Empire, the Schmalkaldic War[11]. Nevertheless, between Francis and Charles, and despite the peace treaty of Crépy (1544), war and mistrusts were not really over. The treaty provided the dispositions of former peaces and planned a marriage between Francis' first son (Francis, duke of Orléans) and Charles's daughter, Maria (or Ferdinand's daughter, Anna) while Francis committed to support Charles against the Schmalkaldic League. But one year later, Francis had not yet fulfilled his obligations and his armies were still in Piedmont and Savoy (Babel, 2013). Moreover, after Charles claimed the restitution of Hesdin or at last Thérouanne (North of France) that Francis denied, both sovereigns armed again in Italy (Milanese and Piedmont) (Nawrocki, 2015). Furthermore, in June 1546 Francis concluded the peace of Ardres with Henry VIII (England would keep Boulogne (North of France) until France paid the amount of 2 millions *écus*) (Potter, 2011) and two months later, Francis, duke of Orleans, died. Although the process was obviously more complex and non-linear, Francis' intentions moved back to war, at least against Charles: he secretly reconnected with the Schmalkaldic League (Potter, 1977) and did not push back the offer of a defensive alliance against the Emperor, which Henry VIII was also supposed to join. At the same time, the French King did some military preparations.

At the end of 1546 and beginning of 1547, uncertainties were numerous on both sides and the Imperial presence in Milan and the French one in Piedmont still fed tensions. Charles' situation in the Empire certainly became better: in January 1547, Ülrich von Württemberg came to an agreement with him and the cities of Ulm and Frankfurt submitted themselves (Potter, 2011). However, Francis' intentions were still alarming Charles, who suspected them as either resuming war in Italy or supporting Charles' opponents (League of Schmalkalde, Ottoman Empire). Indeed, undercover but separate negotiations took place between France, England and the Schmalkaldic League in order to conclude an alliance, even though tensions remained between England and France, because of Boulogne but most of all because of Scotland. In January 1547, an agreement between Henry VIII and the League was almost concluded while the negotiations about the conditions of the French financial loans (towards the League) were still ongoing (Pariset, 1981).

However, on 28th January, Henry VIII died: Edward VI, his only legitimate (but very young) son, ascended the throne. The negotiations seemed jeopardized as the new King and his ministers expressed their unwillingness to support the Schmalkaldic League (Nawrocki, 2015). French military preparations on the other hand were continuing, and after being presented in late 1546 as a defensive preparation either against the Emperor (when talking with English ministers) or against the King of England (when talking with Imperial ministers), they were by then a defensive preparation for a new war that Charles V would declare in Italy as soon as he had brought back the Empire under his authority (Potter, 2011). Francis' motives remained ambiguous for foreign informants and ambassadors like Saint-Mauris who suspected either preparations against the Emperor or preparations against the new King of England, with whom negotiations about Boulogne were still

[10] At this stage, apart from the copies of letters which are preserved in Brussels, only one other letter from Charles to Saint-Mauris has been identified for the first months of 1547 (until Francis' death in late March): David Potter (Potter, 1977) refers to a letter from 19th January 1547 which has been edited from a Viennese copy (von Druffel, 1878, p.39-45).

[11] Since 1542, several German Lutheran cities and princes whose religion was prohibited had been revolting against Charles and gathering in a League (the Schmalkaldic League) conducted by John Frederick, elector of Saxony, and Philip I, landgrave of Hesse. Thanks to the treaty of Crépy which momentarily interrupted the Italian Wars, Charles launched a military and political campaign against the League. He used the invasion of the duchy of Brunswick-Wolfenbüttel in 1542 by John Frederick and Philip as an excuse; he banished them and convinced Maurice, duke of Saxony and John Frederick's cousin, to join him in exchange of his cousin's lands and electoral dignity.

ongoing in order to obtain a confirmation of the treaty of Ardres and an early return of the city.

3 Decryption methods

3.1 Names and statistics

As no other letter from Charles or Saint-Mauris was preserved in Nancy, it was first decided to work on it as a single letter in order to test the cipher and its strength. The first step was to name each of the 125 different symbols (see Fig. 1). These names were useful to identify several occurrences of a particular symbol, distinguish families of similar ones, and record our observations (statistics, patterns...). Later, it was also necessary for a computer treatment of the ciphertext. Our

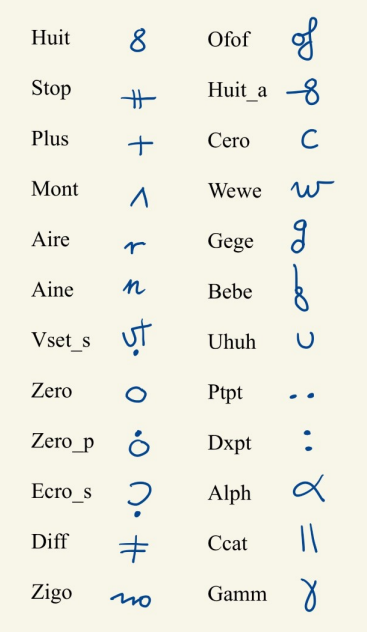

Figure 1: A sample of symbols and their names. The symbols `stop`, `plus` and `mont` are simple symbols, whereas `vset_s`, `zero`, and `zero_p` are complex symbols.

first observation was that among those 125 symbols, 50 were "simple" ones, and 75 were "complex" ones, i.e., there is at least one occurrence in the ciphertext of this symbol with a dot or a hyphen around it (examples are shown in Fig. 1). Among the 75 complex symbols, there were only 17 "root" symbols (without any dot or hyphen), for example `aire`. Among the 50 simple symbols, we noticed that 8 symbols appeared only once.

After re-encoding the ciphertext as a list of strings in the Python computer language, we ran small programs to get quick and reliable confirmations of our observations and intuitions. First we analyzed the frequency of each symbol, and sequences of two or three symbols. The most frequent symbols are[12] `huit` (8.3%), `plus` (7.8%), and `stop` (6.2%). The most frequent bigrams are `huit stop` (2.2%), `mont huit` (1.7%), and `huit plus` (1.3%). The most frequent trigrams are `plus stop aire` (0.39%), `huit stop dxpt` (0.39%), and `gege mont huit` (0.39%). Since we have 125 symbols and only 24 letters in the French alphabet[13] it is clear that a plaintext letter can be encrypted by different symbols. This is a classical trick in Renaissance cryptography to avoid easy frequency analysis. We thus tried to find sets of symbols whose cumulative frequency would match the frequency of a given letter in *Moyen Français* (Fig. 2). For instance, given that `dxpt` has a frequency of 3.1%, we could have the set `plus, stop, dxpt` representing the letter 'e', with a cumulative frequency of $7.8+6.2+3.1=17.1$, which is near the frequency 17.2 of 'e'. Alas this led to a dead end, and likewise for bigrams and trigrams.

e	s	u/v	n	a	t	i	r
17.2	8.1	8.1	7.4	7.2	7.2	6.6	6.2
o	l	c	d	m	p	q	g
5.7	5.5	3.3	3.3	2.9	2.6	1.6	1.4

Figure 2: Frequency of letters in *Moyen Français* (in percent). These statistics come from an analysis of Rabelais' novel, *Pantagruel*, published in 1532.

3.2 Looking for words and patterns

We then searched for repetitions: the same sequence of symbols appearing at least twice in different parts of the ciphertext. We found such a repetition of 11 consecutive symbols (`vset_s huit stop uhuh bebe zero_p mont aire aine huit stop`), another one of 10 symbols, one of 8 symbols, one of 7 symbols and other shorter ones. With the hope that these repetitions of ciphertext symbols correspond to full words in the plaintext, we tried to make them match with words in *Moyen Français*. We efficiently restricted the search with the following remark. For the above repetition of 11 symbols, since the frequency of say `huit` is 8.3% in the ciphertext,

[12] We used our names here.

[13] The characters 'i' and 'j' are the same, as for 'u' and 'v'.

it may be an 'e' , 's', 'u/v', or 'n' in the plaintext according to Fig. 2 (a small margin of error is allowed, but, for instance if it corresponds to 'c', then the frequency of 'c' exceeds the expected 3.3%). At one point we thought that the 8-symbol repetition could correspond to *royaumes* (Kingdoms in English) and the 7-symbol one to *écuries* (stables in English), but this promising idea also led to a dead end. Yet, looking at our repetitions and thinking they were likely to be words, we noted that `plus` was very often at the end of words that existed also without it. We concluded that `plus` was likely to be a symbol for the letter 's'.

Not only did we search for exact repetitions but we kept in mind that one letter in the plaintext probably had several symbols to encipher it. For this reason we looked at near repetitions, that are repetitions of sequences of symbols that are exactly equal except for one inner position where they are allowed to have different symbols. For instance, we found the sequence of 10 symbols (`ecro_s, ofof, huit_a, uhuh, plus, aire, cero, wewe, mont, plus`) and later (`ecro_s, ofof, huit_a, uhuh, plus, aire, cero, wewe, ptpt, plus`). We conclude that `mont` and `ptpt` were likely to represent the same letter.

Moreover we noted that the symbol `zede_p` was always followed by the same symbol, namely `gamm`. We thought that `zede_p` could encode 'q' (their frequencies are 0.6% and 1.6%) and `gamm` could encode 'u' (frequencies 2.3% and 6.5%), since in French the letter 'q' is almost always followed by 'u'. A similar search for the letter 'x' was indecisive.

Another interesting idea was to try to split the 120 symbols between vowels and consonants. With 125 symbols, there can theoretically be 2^{125} possible partitions between vowels and consonants. However, assuming a word has at most 3 consecutive vowels (as in *oiseau*) and 3 consecutive consonants (as in *prendre*), it is possible to restrict the number of possible partitions. In the 11-symbol repetition above, assuming `huit`, `stop`, and `uhuh` are vowels, the next symbol `bebe` is necessarily a consonant. If we only consider the 14 most frequent symbols, yielding $2^{14} = 16384$ subpartitions, we find only two possible partitions of the full 125 symbols. Unfortunately, this also led to a dead end.

At the end we had several hypotheses that appeared to be right. Basic statistics led us very quickly to decide that no symbol (or even pair or triplet of symbols) was there to represent a space, which was correct. Basic statistics again gave possible values for the most common symbols, for instance we thought that `huit` was either 'e', 'u', 's' or 'n' (which was correct, `huit` is an 'n'). Looking at words told us that `plus` encoded 's'; and nearly repetitions combined to statistics led us to conclude that `diff, zigv, zigo` were the same letter and encoded one of 'e', 's', 'u', 'n', 'a', 't', 'i', 'r', 'o', or 'l' (which was correct, they are 'u'). Similarly we thought that `alph` and `ccat` encoded the same letter (which was correct, they both encode 'i'), and that `ptpt` and `mont` encoded the same letter (which was correct, they are both 'e').

Other hypotheses were wrong and led to a dead end. As we will see later, the main trick of Saint-Mauris' cipher consists in hiding vowels, and for this reason our guesses concerning vowels were hazardous, while it would have worked for other ciphers from that time which equally encrypted vowels and consonants. For instance, we thought that `stop`, `bebe`, `dxpt` and `ptpt` encoded a vowel, which was partially wrong, since the first two are respectively 't' and 'r' but the last two are respectively 'a' and 'e'. Similarly, hidden vowels and almost systematic bigrams were the reason why we were misled about `zede_p`, thinking is was a 'q' instead of 'qu'. Finally we looked for repetitions of several symbols with an extra symbol interspersed in order to identify nulls, but this was unsuccessful because nulls were not frequent enough in the ciphertext, and we were not aware of it with a single document. For instance we thought that `aire` might be a null but this was wrong.

3.3 Increasing the amount of data

We were puzzled with several unexplained observations: why did families of symbols that were graphically rotations to each other exhibit similar behaviour? How could we see repetitions of 11 symbols when the writer surely had two or more choices for each letter to be encrypted? At this point, the study of other encrypted letters from and/or to Saint-Mauris was needed to corroborate hypotheses. For practical convenience (the letters were digitized), the choice was made to work on the letters which were preserved in Besançon (BM Besançon, Granvelle 70). Some of them, espe-

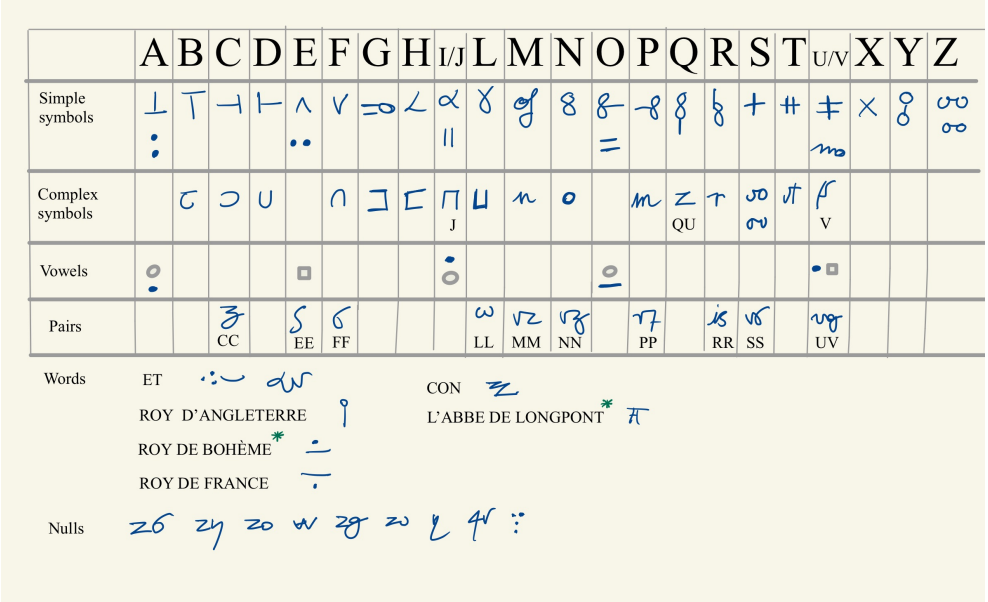

Figure 3: The reconstructed cipher key. Some symbols in the nomenclator can only be guessed from the historical context: they are indicated by a green asterisk in the table.

cially the ones written by Charles and Granvelle (even though two years earlier) were encrypted with almost the same cipher and deciphered in the margin. This was sufficient to start the reconstruction of the cipher key (Fig. 3) and decipher the main part of the letter.

Saint-Mauris' cipher perfectly matches the Renaissance cryptographic practices, especially for European diplomacies. It relies on homophonic substitution and a nomenclator. As for every homophonic substitution, each plaintext letter can be represented by one (consonant) or two (vowel) ciphertext symbols. However, it goes further. Each consonant, if followed by a vowel, can also be encrypted by an extra complex symbol. In this case, the complex symbol is associated with a diacritical mark: dot at the bottom for 'a'; dot on top for 'i'; hyphen at the bottom for 'o'; dot on the left for 'u'. If there is no diacritical mark, it means that the symbol should be deciphered as consonant followed by 'e'. In addition, a ciphertext symbol exists for each repeated consonant (for instance a '3' for 'cc').

The letters in Besançon helped a lot for the value of the usual ciphertext symbols, much less for the nomenclator. Some ciphertext symbols remained a mystery. Four symbols did not appear in the letters in Besançon, but were crucial for understanding the letter in Nancy[14]. Surprisingly, the reconstruction of the nomenclator was quite easy and questions the complementary security that it is supposed to grant. The context of the letter, as well as the similarity between two symbols which encrypted kings, enabled us to identify two kings (in addition to the French King who was several times mentioned): the English King was associated to a recent death, and the Bohemian King to the Empire and to Charles' family. The last symbol, which encrypted Gabriel de Guzman, abbot of Longpont, was harder to uncover. Its decryption was made possible by Saint-Mauris' letter on 6th February, in which he mentioned his negotiation[15]. For this case, it would save little in case of an interception but reminds the main purpose of encryption: delaying the reading of the letter (if it was intercepted) and not fully preventing it.

[14]Three historians or cryptographers had previously reconstructed the key but not the nomenclator (Stix, 1934-1936; Tomokiyo, 2022) or they have not made it accessible (Potter, 2013). As we primarily worked on the 22nd February letter and used other letters only to pursue the global understanding of the core key, the nomenclator in this paper is incomplete and presents only the part of it which is used in the letter in Nancy.

[15]We have been able to consult the copy of this letter (AN, K1485-1488) only. The original encrypted letter, which we have not yet identified, and/or the minute of the 22nd February letter would confirm the attribution of this symbol to Longpont.

3.4 A very structured key.

Deciphering[16] the letter revealed both some patterns in the creation of the key itself and specific rules to use it. This structure is double-edged for the cryptanalyst. On the one hand, hidden vowels make usual statistics and methods fail, but on the other hand, any attack becomes easier as soon as the adversary is familiar with the Imperial cryptographic patterns. Although Charles' ciphers are nowadays little known, contemporary enemy cryptographers knew much better their common patterns and, several years later, Philip II himself acknowledged their low security and recurring decryptions.

Hidden vowels. Saint-Mauris' key uses a clever trick that explains both the failure of our first hypotheses and the unexplained observations we made: when they are following a consonant and form thus a bigram, the vowels are somehow hidden as diacritics. To encrypt a message the rules are the following. If you have to write a consonant followed by a vowel then use the complex symbol for the consonant and add around it the corresponding hyphen or dot for the following vowel. If you write a consonant not followed by a vowel or a vowel not following a consonant, just use one of its simple symbols. Always use the corresponding symbol for a pair of identical letters, and often the nomenclator if it exists. Nulls are not very frequent, except to hide important words and names, at least in this letter. Because of these rules, bigrams always consisted of a pair consonant-vowel but no symbol existed for (even frequent) bigrams of the form vowel-consonant (as 'un' or 'en' in French).

Rotation of symbols. With the reconstructed key in hand, we see a startling structure that betrays how the table was created. Symbols have been assigned in alphabetical order, and rotations were done to create new symbols, without mixing up these symbols. For example, the simple symbols for 'a', 'b', 'c', and 'd' are identical up to rotation, as are those for 'e' and 'f'; 'i' and 'l'; 't' and 'u' ; 'y' and 'z'. The symbols for 'n', 'o', 'p', 'q' and 'r' form another family. The observations we made about similar behaviours (':' and '..'), ('=' and '||') or the complex symbol family representing 'b', 'c', 'd', and 'f' are well explained by this structure. That tempers the cryptographic abilities of those who conceived the ciphers. Certainly the global patterns (homophonic substitution, vowel indicators, etc) were suggested and designed by cryptographers. The daily conception of ciphers however was the work of a secretary who was less concerned by the strength of the cipher (finding various symbols without any consistency between them) than by the need to quickly conceive multiple ciphers. The pattern relies here on rotation (as in some Hungarian ciphers (Lang, 2018)) as it relies, in some other ciphers, on alphabetical or numerical order. Indeed, Saint-Mauris' cipher presents also a numerical pattern for pairs ('5' for 'ee', '6' for 'ff' and so on). That truly questions its strength.

3.5 Merging keys

Finally, we compared the key to previous reconstructions we were able to access. The first one (Stix, 1934-1936) was conducted by Franz Stix within a general study of Charles' cryptographic practices from the Vienna archives (OeStA-HHStA, Fr 10-16). The second one (Tomokiyo, 2022) relied on a single letter which Satoshi Tomokiyo found in Madrid (BNE, 7913). Results were convergent but the comparison allowed us to understand better some aspects of the ciphering process and question once again the security that the cipher granted to the letter. Stix reproduced the main part of the key: symbols for letters, bigrams (all the bigrams are developed and not presented, as in our reconstructed key, as complex symbols and vowel indicators), and repeated consonants[17] but neither the null symbols, the ciphertext symbol for 'com/con', nor the nomenclator. On the other hand, the first key reconstructed by S. Tomokiyo presented only a subset of simple and complex symbols. The null symbols were also reconstructed but not the ciphertext symbols for 'et' and 'com/con' nor the nomenclator. All the identified symbols in the three tables were very similar, even though the writing frequently differed. In fact, it was only when comparing with the other reconstructions that we were able to con-

[16] In order to facilitate the understanding of the encryption processes, we have separated simple symbols, complex symbols and vowel indicators for the presentation of the reconstructed cipher key. Nevertheless, according to the usual presentation of Renaissance ciphers, one can assume that the plaintext bigrams were developed (ba, be, bi, bo, bu, ca, ce, ci, ...). The key might thus be structured in 3 parts: the simple symbols (with the nulls), the bigrams and the nomenclator.

[17] For the repeated consonants, the key reconstructed by Stix revealed the symbol for 'pp' and 'rr' for instance, but not for 'ee'.

firm that the repeated consonants symbols were numbers, even in increasing order. For instance 'll', 'mm' and 'nn' are encrypted with 10, 12 and 13 while 'rr' and 'ss' correspond to 15 and 16. Finally, at first sight the nulls that Tomokiyo identified are quite different from ours, but most of them are digit numbers too. There could even be a rule that any number larger than or equal to 20 is a null. For instance the first three symbols of Fig. 3 might be particular spelling for $26, 24$ and 20. In our case, another null symbol is formed from 4 dots. This is consistent with what we found in Besançon, where more than one dot around a symbol automatically cancels it out.

The comparison with the works of Stix and Tomokiyo highlighted differences and developments in some symbols, such as the complex symbol for 's'. In the reconstruction of F. Stix it looked like a letter 's' with a small circle attached on the top right part. In S. Tomokiyo's table, this structure was still visible, but one might not interpret it this way if not aware of the other table. In this letter, however, the complex symbol for 's' sometimes became almost flat and was hard to distinguish with the symbol for 'z'. These variants of 's' are shown in Fig. 4, and we chose to let the ambiguity between 's' and 'z' be visible in Fig. 3. This example however highlights one of the issues of deciphering early modern letters: characters can be written in different ways even when they are the same (bad writing, different secretaries, cipher evolution and so on).

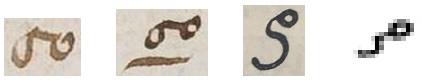

Figure 4: Variants of the complex symbol for 's'. From left to right: Symbols for 'se' and 'so' in the 22nd February letter; symbol for 'se' in Stix' key; symbol for 'se' in Tomokiyo's key.

Finally, there are several ways to interpret the various writing styles for the ciphertext symbols that occurred in the letters, and which have consequently been passed on to the three reconstructed keys. It could be that the writer was requested to cipher quickly or because he was not mastering the process well. In both cases, that underlines the difficulties of manual ciphering. In fact, in addition to the bad writing of some symbols, many ciphering errors can be pointed out in the letter. They never prevent the complete understanding but are comparatively more frequent than in the other correspondences we have worked on. Further research could help to determine whether these ciphering errors are specific to that letter or if they were common in Charles' encrypted correspondence, but also to define the type of errors (writings, cross-contamination from other keys and so on). This investigation as well as the reconstruction of the whole nomenclator should help to question the quality of the Imperial ciphers as well as the ciphering mastering of its secretaries.

4 Results

The deciphering enabled us to uncover the content of the letter (mainly about Charles' concerns towards Francis) and also Charles' encryption methods in the mid-16th century.

4.1 Content of the letter

In a first part, Charles reaffirmed his concern about Francis' intentions while he was gathering his military forces in the Empire against the Schmalkaldic League. These concerns were earlier made public by Saint-Mauris at the French Court while Charles had several times expressed, during audiences with Jacques Mesnage, the French ambassador at the Imperial Court, his good will towards Francis and had exhorted him to peace but without clearing away the French doubts[18]. Saint-Mauris was thus encouraged not to openly express Charles' mistrust or relaunch the negotiations (probably about Hesdin and/or "demilitarisation" of Northern Italy). On the contrary, Charles ordered him to discover the French intentions towards England following Henry VIII's death. Saint-Mauris however seemed to remain in the dark about the French intentions towards both Boulogne and a general alliance with England, the Schmalkaldic League, and even Venice (Potter, 2013). As this letter shows, Saint-Mauris was still fishing. This concern about maintaining peace is finally expressed one more time at the end of the first page: Charles immediately accepted the proposal of Claude d'Annebault, Francis' main counsellor and previous governor of Piedmont, to keep running the cooperation and mutual surveillance of the Milano-Piedmontese border. By countering the French diplomatic and military maneuvers, the

[18]Two letters from Mesnage to Francis, written on 16th January and 20th January 1547 testified those speeches (Ribier, 1666, p. 591-593 and p. 595-600).

letter reveals part of Charles' foreign policy. It is hardly surprising that his concerns were encrypted while his public demonstration of goodwill by accepting Annebault's proposal was written in cleartext.

In a second part, Charles reported a disturbing rumor: Piero Strozzi, who belonged to an Italian banker family and served Francis both with his financial and military abilities, was planning to assassinate him. Strozzi was indeed sent to the Schmalkaldic League to bring them the French financial subsidies and was suspected of taking advantage of his journey for much more dangerous matters. However, Charles acknowledged that the French King would have refused to support such an assassination project. The fear may originate from the dubious status of Strozzi's missions in the Empire. They were mostly managed directly in the Empire by Jean Sturm, and Strozzi made frequent journeys back and forth, including in Italy, in order to elaborate the French loans (Potter, 1977; Pariset, 1981). When replying on 6th March 1547 (OeStA-HHStA, Fr 10-16; Potter, 2013), Saint-Mauris confirmed that it was only a rumor.

The last part of the letter outlines the state of the Schmalkaldic war. Charles mentioned his upcoming journey to Frankfurt in order to confer with his brother Ferdinand, King of Bohemia and King of Romans, about the operation led by Maurice, duke of Saxony, against John Frederick, elector of Saxony and one of the leaders of the Schmalkaldic League. Nevertheless, if the military situation was improving for Charles, there arose in Prague a revolt which was immediately reported by Jacques Mesnage[19]. In response, Charles encouraged Saint-Mauris to minimize the scale of the revolt as well as the night flight of Ferdinand of Tyrol, Charles' nephew, by transforming it into a simple hasty departure to join his father, Ferdinand, King of Bohemia, and the fight against the Elector of Saxony. In fact, on 22nd February 1547, the revolt was not yet over: Ferdinand, King of Bohemia, was still negotiating with the States of Bohemia, and also with those of Moravia and Silesia, who had joined the first ones.

[19]His diplomatic papers can be found at the French national library (Paris) (BnF, 17889-17890). For preservation motives, the letters are not accessible anymore. Some of his letters have been edited but not the one to which Saint-Mauris referred (Ribier, 1666).

4.2 Cryptography under Charles V's reign

Imperial cryptographic practices have suffered from a bad reputation, because of both insufficient historical knowledge [20] and the comparison with Philip II's ciphers. Nevertheless, Saint-Mauris' cipher isn't less complex than other European ciphers at the same time. French diplomacy for example already used in the 1530's two or three ciphertext symbols for each plaintext letter (Desenclos, 2021). In the 1540's, Charles' brother Ferdinand, as King of Hungary, used ciphers with two or three ciphertext symbols with his ambassadors (Lang, 2018). In Saint-Mauris' key, the complex symbols act as a second set for plaintext letters as do the vowel indicators. It thus presents two ciphertext symbols for consonants and three for vowels. Moreover, as for many other European ciphers, Saint-Mauris' cipher offers complementary encryption processes: null ciphertext symbols, ciphertext characters for each repeated plaintext consonant, nomenclator.

The diacritical marks for vowels seem to be specific to Imperial ciphers, to the authors' current knowledge. Those vowel indicators could offer the encrypted letter extra strength. As our deciphering attempts show, vowel indicators prevent (or at least slow) any cryptanalysis by frequency analysis. But Charles' encrypted letters were regularly deciphered by enemies who discovered this main pattern of his ciphers. On this basis, Charles' ciphers lost their strength: unlike bigrams (using a different ciphertext symbol each time), using the same diacritical mark for each vowel again made possible frequency analysis. On that perspective, Saint-Mauris' cipher could be considered as less strong than other European ciphers, but it reminds us also of the value of the Imperial ciphers in the history of cryptography, especially for the understanding of Spanish cryptography under the reign of Philip II.

This use both of bigrams and diacritical marks indeed was not new. Since 1527, it can be observed within several ciphers such as the one used between Iñigo Mendoza, ambassador at the French Court, and Charles V. Since then, those diacrit-

[20]The correspondences both from Charles V and from Granvelle have been broadly studied and, sometimes, edited. But the cryptographic practices are only quickly mentioned: their existence are acknowledged, sometimes the kind of cryptographic symbols described (see for instance (Berthomeu Masia, 2006)) but the keys are rarely transcribed or even studied.

ical marks were regularly used by Imperial ciphers (Tomokiyo, 2019). They can be observed until 1555 (Tomokiyo, 2022). This vowel encryption process can be considered at the ancestor of encrypted bigrams and trigrams under Philip II's reign. Indeed, Spanish ciphers after 1556 still used diacritical marks for vowels in the exact same way (the same diacritical mark for each vowel whatever the consonant is) (Devos, 1950), but they progressively moved from vowel indicators to proper bigrams and trigrams (two consonants and one vowel such as 'cha', 'che', etc): each bigram and trigram was now encrypted by a different ciphertext character. Certainly, they often matched to increasing numbers (e.g. 10 for "ba", 11 for "be", ...) but vowels could no longer be spotted easily.

5 Conclusion and perspectives

Deciphering this letter may have taught little about the relationship between Charles and Francis. As a large part of Saint-Mauris' correspondence had already been studied, the uncovered content only confirms current historical knowledge. The main value of this work lies in understanding the cryptographical approach of the letter. When deciphering, how to deal with an isolated letter, encryption patterns which aren't well known or documented, and with inconsistent writings? This work led us to question both the ciphering and deciphering process. By working only on one specimen, then by reinserting it in a larger sample, and finally by merging with other similar keys, cryptographic patterns have been highlighted. The decryption of this letter nevertheless is the beginning and not the end of a general study of Charles' cryptographical practices. In the future, thanks to the corpus enlargement (Vienna and Bruxelles mainly), the authors aim to investigate both the cryptographic adaptations to Charles's diplomacy network (Saint-Mauris wrote with the same cipher to Charles, Granvelle, Maria of Austria, Infante Philip and Los Cobos, but they may have adaptations, especially in the nulls and nomenclator) and the exact process of manual ciphering (misuse of complex symbols, ciphering errors, bad writings, nomenclator evolutions and so on). Thereby, the authors hope to consolidate the cipher key from Fig. 3 and contribute to a better knowledge of Renaissance cryptographic practices.

Acknowledgements. The authors thank Sophie Toulouze, Anne Canteaut, Olivier Canteaut, and Lana Martysheva who were involved in making this collaboration possible, the three anonymous referees, and Richard Brent who helped to improve our written English.

References

[AGR Audience 420] Archives générales du royaume. Audience 420. Correspondence between the Imperial agents at the French Court and the Holy Roman Empire, 1535-1563.

[AGR Audience 1672] Archives générales du royaume. Audience 1672/2/E. Correspondence between the Imperial agents in France and the Low Countries, 16th century.

[AGR Misc 95-96] Archives générales du royaume. Manuscrits divers 95-96. Correspondence from Charles V and Maria of Hongria to Jean de Saint-Mauris, copies.

[AN, K1485-1488] Archives nationales, "Fonds de Simancas". K1485 to K1488. Correspondence between the Imperial agents in France and Spain, 1544-1548.

[Babel, 2013] Rainer Babel. 2013. *La France et l'Allemagne à l'époque de la monarchie universelle des Habsbourg, 1500-1648*. Presses Universitaires du Septentrion, Villeneuve d'Ascq.

[Berthomeu Masia, 2006] Maria José Bertomeu Masia. 2006. *Cartas de un espia de Carlos V. La correspondancia de Jeronima Bucchia con Antonio Perrenot de Granvela*. M. Rieger, Munich.

[BM Besançon, Granvelle 40] Bibliothèque municipale de Besançon. Granvelle 40. fol. 139, Letter from Jean de Saint-Mauris to Charles V, 6th February 1547. `https://memoirevive.besancon.fr/ark:/48565/th72lvsb095f/6dc4e84d-9393-4e5c-9172-e1360a268aaf`.

[BM Besançon, Granvelle 70] Bibliothèque municipale de Besançon. Granvelle 70. Lettres et papiers de l'ambassade de Jean de Saint-Mauris, 1544-1576. `https://memoirevive.besancon.fr/ark:/48565/t43hg0sk92jl/72919b8a-dacd-44a5-a220-a6987a0378d9`.

[BM Nancy, letter] Bibliothèque Stanislas de Nancy. Letter from Charles Quint to Jean de Saint-Mauris, 22nd February 1547. `https://galeries.limedia.fr/ark:/31124/dct0sbwx8vmhspk0`.

[BNE, 7913] Biblioteca nacional de España. MSS/7913/127. Letter from Jean de Saint Mauris to Granvelle, 5th July 1548.

[BnF, 17889-17890] Bibliothèque nationale de France. Manuscrits français 17889 to 17890. Ambassade de Jacques Mesnage auprès de Charles Quint, 1544-1546.

[Cassan, 1878] Auguste Cassan. 1878. La mort de François I^er et l'avènement de Henri II d'après les dépêches secrètes de l'ambassadeur impérial Jean de Saint-Mauris. *Mémoires de la société d'émulation du Doubs*, pages 422–454.

[Desenclos, 2021] Camille Desenclos. 2021. Écrire le secret quotidien. Pratiques de la cryptographie au sein de la diplomatie française (XVI^e-premier XVII^e siècle). In G. Braun and S. Lachenicht, editors, *Spies, espionnage and secret diplomacy in the early modern period*, pages 85–103. Kohlhammer.

[Devos, 1950] Jean-Pierre Devos. 1950. *Les chiffres de Philippe II (1555-1598) et du despacho universal durant le XVII^e siècle*. Palais des Académies, Bruxelles.

[von Druffel, 1878] August von Druffel. 1878. *Briefe und Acten zur Geschichte des sechszehnten Jahrhunderts*. M. Rieger, Munich.

[Kopal and Waldispühl, 2022] Nils Kopal and Michelle Waldispühl. 2022. Deciphering three diplomatic letters sent by Maximilian II in 1575. *Cryptologia*, 46/2:103/127.

[Lang, 2018] Benedek Lang. 2018. *Real Life Cryptology. Ciphers and Secrets in Early Modern Hungary*. Amsterdam University Press B.V., Amsterdam.

[Nawrocki, 2015] François Nawrocki. 2015. *L'amiral Claude d'Annebault, conseiller favori de François I^er*. Classiques Garnier, Paris.

[OeStA-HHStA, Fr 10-16] Österreichisches Staatsarchiv / Haus Hof und Staatsarchiv. Frankreich, Berichte 10 to 16. Imperial diplomatic correspondence to France, 1542-1548.

[Pariset, 1981] Jean-Daniel Pariset. 1981. *Les relations entre la France et l'Allemagne au milieu du XVI^e siècle*. Librairie Istra, Strasbourg.

[Pariset, 1982] Jean-Daniel Pariset. 1982. La France et les princes allemands. Documents et commentaires (1545-1557). *Francia*, 10:229–301.

[Potter, 1977] David Potter. 1977. Foreign Policy in the Age of the Reformation: French Involvement in the Schmalkaldic War, 1544-1547. *The Historical Journal*, 20/3:525/544.

[Potter, 2011] David Potter. 2011. *Henry VIII and Francis I. The Final Conflict, 1540-1547*. Brill, Leiden.

[Potter, 2013] David Potter. 2013. La fin du règne de François I^er et l'avènement d'Henri II d'après les dépêches de Jean de Saint-Mauris. `https://cour-de-france.fr/article2749.html`.

[Ribier, 1666] Guillaume Ribier. 1666. *Lettres et mémoires d'Estat des roys, princes, ambassadeurs et autres ministres sous les regnes de François premier, Henry III et François II, tome premier*. François Clouzier, Paris.

[Stix, 1934-1936] Franz Stix. 1934/1936. Die Geheimschriftenschlüssel der Kabinettskanzlei des Kaisers. *Nachrichten aus der Mittleren und Neueren Geschichte*, 1/2:207–226/61–70.

[Tomokiyo, 2019] Satoshi Tomokiyo. 2019. Tracing the origin of vowel indicators in Spanish ciphers. `http://cryptiana.web.fc2.com/code/vowel.htm`, retrieved 2023-04-19.

[Tomokiyo, 2022] Satoshi Tomokiyo. 2022. Ciphers during the reign of emperor Charles V. `http://cryptiana.web.fc2.com/code/spanish2.htm#SEC14B`, retrieved 2023-04-19.

Appendix: The Decrypted Letter

(We put the decrypted part in italics.)

L'empereur et roy
Chier et feal

Nous avons receu voz deux lettres des XXVI[e] du passé et VI[e] du present et par icelles entendu bien amplement tous occourans en ce coustel là et mesmes la responce que vous a fait le roy sur ce que luy avyons fait remonstrer par vous *par vous [sic] et puisque luy ny ses ministres ne se sont extendus davantaige quant à la plus estroicte amyté et moyens d'icelle, sinon qu'il seroit bon remectre la negociation à l'abbé de Longpont, il sera bien laisser la chose ainsi sans en faire plus de mention jusques l'on voye s'ilz retourneront à en parler et en feront plus d'instance, et proposeront aucuns moyens où l'on puisse prendre quelque fondement dont nous advertirez. Et nostre dicte seur vous tenant tousjours cependant ès mesmes termes qu'avez jusques à maintenant sans en riens vous eslargir davantaige en sunvant [sic] ce que vous avons tousjours escript. Et sera bien que nous advertissez de ce qu'aurez pu assentir de leu[r] intention depuii qu'ils auront sceu le trespas [du] roy d'Angleterre et z'ilz n'etendent rien s[e] mouvoir en ce coustel là et si soubz ceste couleur ils se font plus grant amas de gens ensemble de toutes aultres particularitez.* Et quant à ce que l'admiral vous a dit que pour entretenir bonne voisinance et eviter tous scrupules, il seroit bon que l'on observa du coustel de Piedmont ce que faisoient le feu marquis del Gasto et luy d'advertir l'ung l'aultre quant aucunes garnisons se augmentoient ou changeoient d'ung lieu à aultre, vous luy pourrez dire que le trouvons bon et ferons escrire au sieur Don Fernande que à l'advenir il en use ainsi et que de leur coustel ilz facent de semblable à leur gouverneur audit Piedmont. Ledit Don Fernande nous a envoyé le memoire cy joinct dont pourrez parler comme aurrez l'opportunité.

Au surplus l'on nous a adverty que estant dernierement le roy ou coustel de Bresse, aulcuns gentilz hommes ytaliens suyvans le sieur Oracio, eulx monstrans affectionnez à nous, auroyent dit qu'ilz se covoyent certainement que Pierre Strossy en partant dernierement de France et lors qu'il vint au camp des rebelles dit entre aultres choses au roy que s'il vouloit qu'il entreprendroit de nous tuer et qu'il n'en demandoit aulcune recompense ny se soucioyt d'estre apres prins, car il estoit content de mourir moyennant que aussi [nous] mourissions, et que le dit sieur roy luy auroit respondu qu'il ne s'estoit jamais meslé de telles praticques, et qu'encores ne le vouldroit y faire et que ledit Strossy fit ce qu'il vouldroit. Lequel auroit depuis encores dit aillieurs qu'il s'en iroit audit camp des rebelles et trouveroit moyen d'entrer au nostre soubz quelque couleur que ce fut et mectroit sa volonté à execution quoiqu'il en deust advenir. Et pour ce que vouldrions bien que cecy se puist en aucune manière veriffier pour avoir occasion de faire apprehender ledit Strossy et nous en pouvoir justifier en ce coustel là, sera bien que regardez tous moyen possibles pour si faire se peult scavoir si ledit Strossy auroit tenu audit roy les susdictz propoz ou encores aillieurs. Et cecy vous recommandons nous affectueuzement.

En oultre nous sumes deliberé partir d'icy dans cincq ou six jours et tirer contre Francfort pour estre là à propos de tous affaires et pouvoir tinir meillieur correspondence avec le roy de Boheme en l'emprinse de Saxe de laquelle somes actendant nouvelles du succes. Et pour ce que l'ambassadeur Mesnaige auroit par adventure escript par delà et fait grant cas de l'emotion de Praghe. Et aussi que Monsieur l'Archiduc nostre nepveu s'estoit une nuict party secretement vous advisons que quant à ladicte emotion elle est cessee et a esté seulement une assemblee de peuple sans qu'il en soit ensuy aultre chose. Et quant à nostre dit nepveu ayant entendu que son pere delaberoit soy trouver en la dicte emprise contre le jadis electeur, et doubtant que ne luy eussions voulsu permectre d'y aller s'estoit desrobé pour soy y trouver mais il rev[i]ent le mesme jour et ainsi en pourrez respondre si vous en es[t] parlé. À tous chiers et feal Dieu vous ait en sa saincte garde. De Ulme le XXII[e] de fevrier 1546.

Charles
Bave