Antonio Elio "Cipher" and his Polyphonic-Syllabic Cipher

George Lasry
The DECRYPT Project
george.lasry@gmail.com

Marcello Simonetta
The Medici Archive Project
marcello.simonetta@gmail.com

Norbert Biermann
Universität der Künste Berlin
mail@norbertbiermann.de

Abstract

Antonio Elio (Helius) (1506–1576) was a Roman Catholic prelate who served as Bishop of Capodistria and Pola and Titular Patriarch of Jerusalem. Also a prolific cryptographer in the service of Pope Paul III, he is credited for the invention of polyphonic ciphers. In this article, we provide an overview of his career and work in cryptography and describe an ingenious polyphonic-syllabic cipher he designed. Although several matching plaintext-ciphertext segments were available, reconstructing the cipher key required a significant and unusual amount of time, underscoring the cipher's high level of security. Ciphertext-only cryptanalysis for such a cipher would be extremely difficult and nearly impossible, even with modern computing, without prior knowledge of the principles of its complex design.

1. Biography

In April 1535, Bernardo Boccarini, the secretary to the papal nuncio in France, Rodolfo Pio da Carpi, wrote to a colleague a facetious letter in which he complained about the fatigue of his own profession and, while sketching the portrait of the "perfect secretary," he asked him to send nice words to "Antonio" so that he would not perceive all the curses ("cancari") he had in store against him for having created his own set of ciphers that made him sweat so much.[1] By then, this nearly twenty-year-old man had already created a reputation for himself so that he was universally known as "Antonio delle Zifre."

Antonio was born in Capodistria[2] in the first decade of the 16th century in a noble family.[3] He gave early signs of his brilliance and was recommended to his compatriot Aurelio Vergerio, the resident cryptographer ("a secretis") in Clement VII's curia. After Aurelio's tragic death in 1532, Antonio took over his job and started his own career as a prelate and diplomat. His first known letter of May 1535 was addressed to Aurelio's brother, Pier Paolo Vergerio, then a papal nuncio in Vienna at the court of Ferdinand I Habsburg, and by 1536, bishop of Capodistria. Over the next few years, the relationship between the two competing curial officers became sour over some unpaid debts, and eventually, their breakup became very public and violent.

By 1549, Vergerio left Italy and his bishopric, turning on the Protestant side, while Elio became bishop of Pola[4] in 1548. This shift reflected the trust that he had earned working loyally for the Farnese family under Pope Paul III. After the pope's death, for a few months, Antonio entertained the idea of moving to Florence at the service of Duke Cosimo I de' Medici, but he decided to stay loyal to the Farnese, even when the new pope, Julius III del Monte, waged war against Parma. Elio remained in the papal curia also under Paul IV Carafa and the following pontiffs, who always highly valued his special services.

One particularly appreciated aspect of Elio's skills was his ability to break enemies' codes. For instance, we learn from Medici correspondence that the Carafas systematically intercepted all outgoing diplomatic dispatches and submitted the ciphered samples to Elio. Bongianni Gianfigliazzi, the Florentine ambassador in Rome, wrote to his duke in June 1558 that one informant told him that "*the aforementioned monsignor had deciphered many letters of*

[1] Bernardo Boccarini to Trifon Benci, Rouen, 4 April 1535 (*Lettere facete*, D. Atanagi ed., 1561, I, 349).
[2] Koper, in today's Slovenia.
[3] For an introductory biography, see L. Byatt, https://www.treccani.it/enciclopedia/antonio-elio_(Dizionario-Biografico)/
[4] Pula, Croatia.

Proceedings of the 8th International Conference on Historical Cryptology, pages 80-89
Poznań, Poland, 16-18 June, 2025

ambassadors, and in this genre it is an awesome thing that he does, since he saw him sometimes be handed a cipher, shut himself in a room alone, and in a short time break it. This achievement appears miraculous."[5]

However, it is unclear whether anyone managed to break Elio's ciphers. Antonio invented a new kind of encoding that, even when known, still requires a high degree of concentration and imagination to be fully decoded.

Antonio Elio, during his long service in the papal curia (1532-1572), laid the ground for the establishment of a professional cipher service, and his work significantly influenced further generations of cipher secretaries. He trained Giovanni Battista Argenti before he became the pope's cipher secretary (Meister 1906, p.55), and in his treatise on cryptography, Matteo Argenti, Giovanni's nephew and successor, recognizes Elio's contribution (Meister 1906, p.50, p.161).

2. Antonio Elio's innovative cipher - the Challenge

We found a document partially in cipher that exemplifies Antonio Elio's innovative contributions to cryptography. This is a batch of letters sent by Filiberto Ferrerio, Bishop of Ivrea and Apostolic Nuncio in France, between 1537 and 1540. The letters we consider were written from Paris in late October 1540, and they all bear the unmistakable cryptographic marks of Elio's work for the Farnese chancery.

This document from the Vatican Archives (AA.Arm. XVIII. 6532) contains several segments of interlinear deciphered text. As part of the analysis of this letter and the cipher employed to encode it, we needed to reconstruct the original key. As shown in Figure 1, the enciphered parts consist of a mix of graphical cipher symbols with Latin letters. Our initial assumption was that the cipher was homophonic, with each alphabet letter represented by one or more cipher symbols and other cipher symbols representing elements of a nomenclature, such as words or proper names. We identified approximately 40 distinct cipher symbols, which usually hints at a simple cipher with a small number of homophones per letter of the alphabet. Some symbols have dots on top, and we also needed to determine their role in the enciphering and deciphering process.

Based on our experience extracting a cipher key from matching ciphertext-plaintext symbols, we expected that this analysis would take no more than an hour or two. However, it took two full days of intensive work to make initial inroads into the cipher and begin to understand its principles. Numerous additional hours were required to identify most of the elements of the cipher key. Before proceeding to our detailed analysis of the cipher and its principles in Section 4, we invite the curious reader to experiment and attempt to recover the key from the samples in Figures 1, 2, and 3 below. The ciphered passages are underlined.

[5] "*detto monsignor di quelle delli Imbasciatori ne ha deciferate assai*, et che in questo genere è cosa grande quello che fa che l'ha visto qualche volta havere una cifra, et riserarsi in camera da per sè, et in poco tempo ritrovarla et la par' cosa miracolosa." (Bongianni Gianfigliazzi to duke Cosimo, Rome, 10 June 1558 (Archivio di Stato di Firenze, Mediceo del Principato, f. 3278, 90)

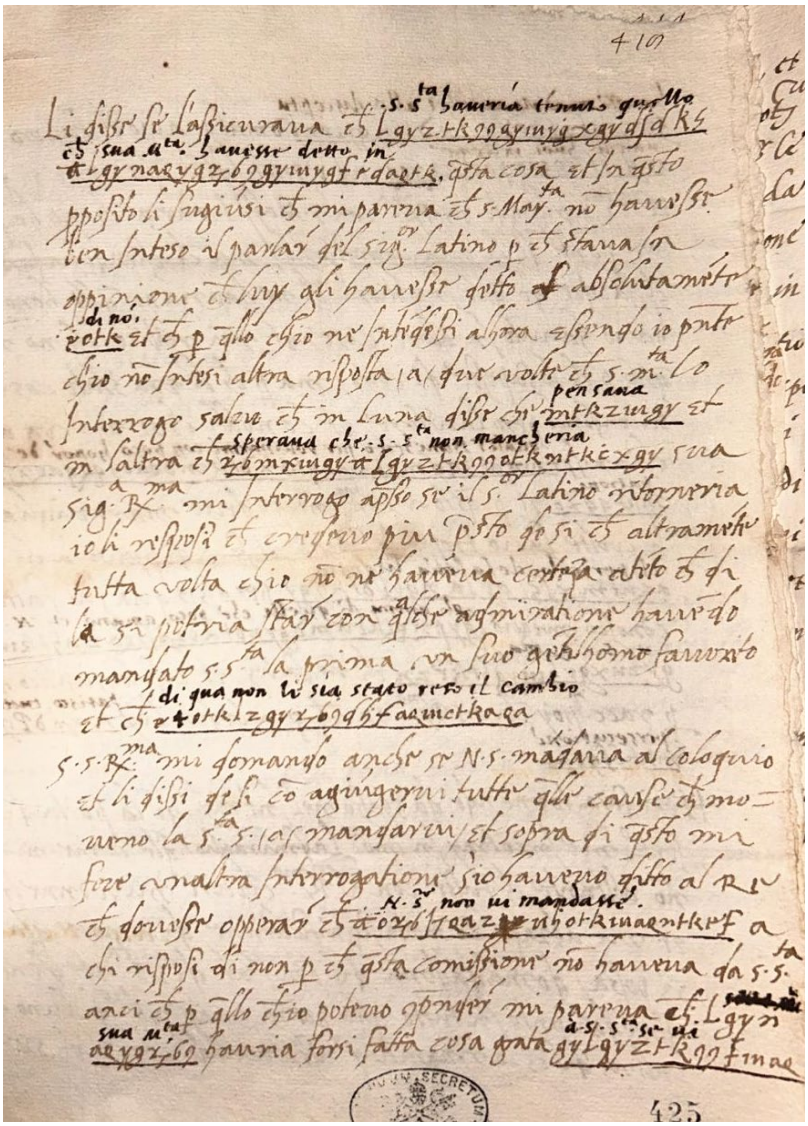


Figure 1 - First part

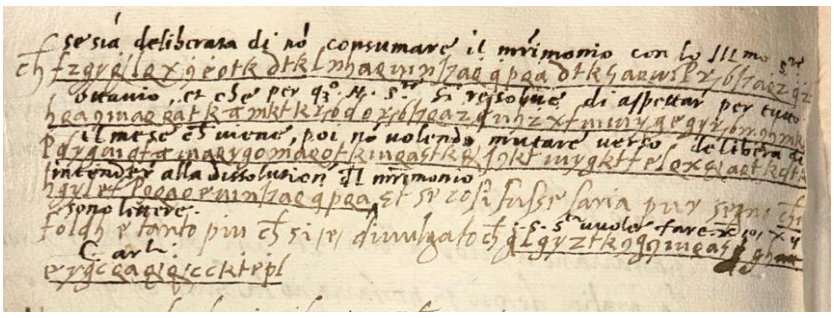


Figure 2 - Second part

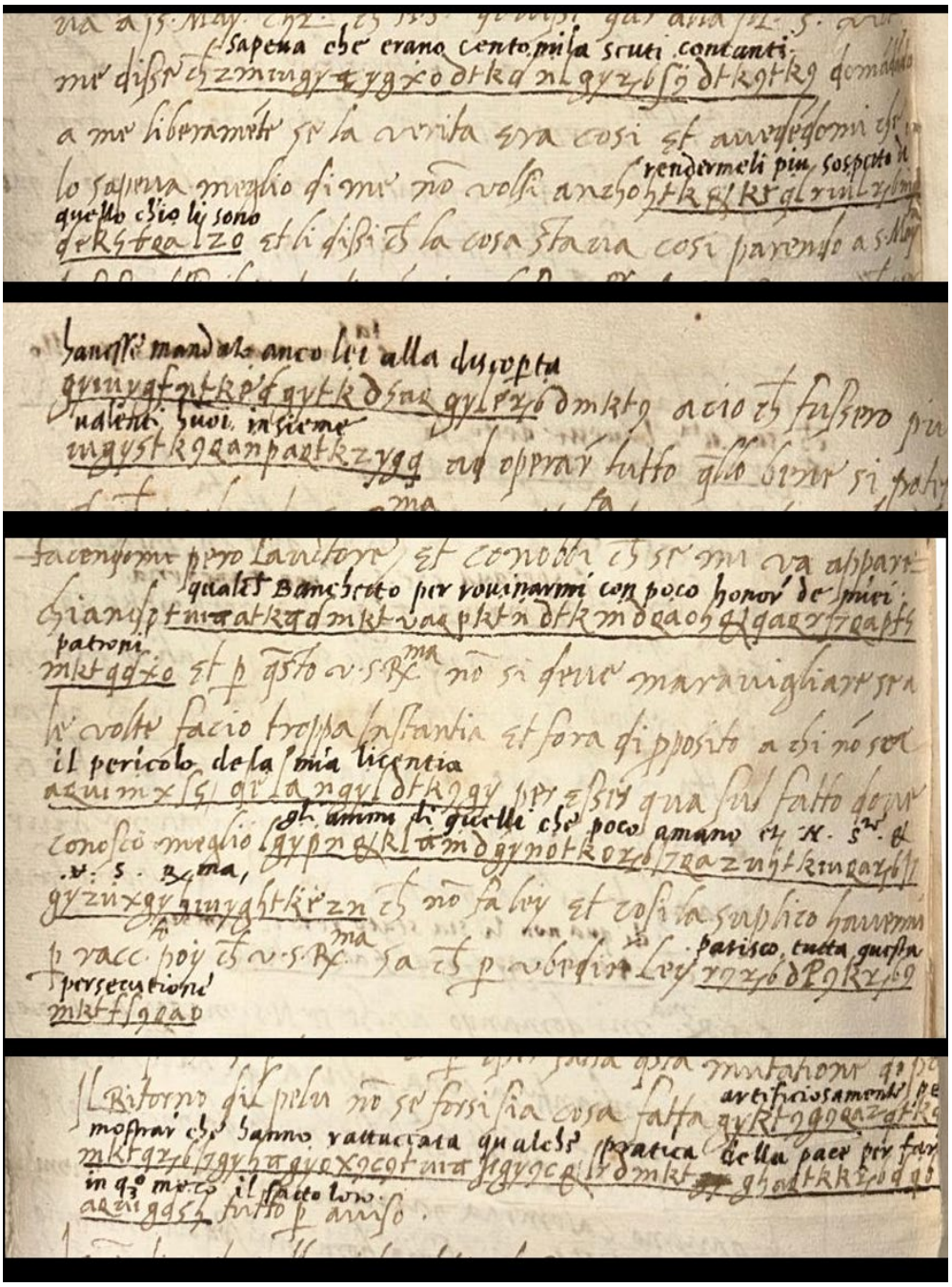


Figure 3 - Third part

We provide here a transcription of the interlinear decrypted text:[6]

First part:
Sua Santità averia tenuto quello / che Sua Maiestà havesse ditto in / di non / pensava / sperava che Sua Santità non mancaria / di qua non li sia stato reso il canbio / Nostro Signore non vi mandasse/ Sua Maiestà … a Sua Santità se vi

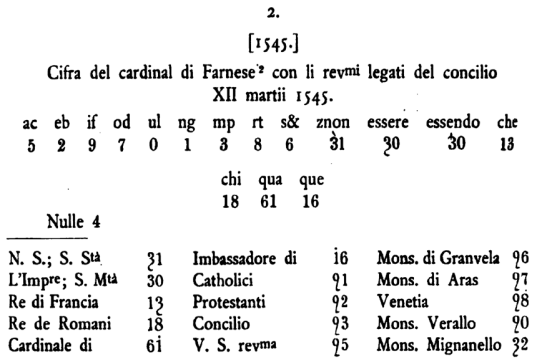
Second part:
se sia deliberata di non consumare il matrimonio con lo illustrissimo signore /
Ottavio, et che per questo Nostro Signore si risolve di aspettare per tutto / el mese che viene, poi non volendo mutar verso, delibera de /
intendere alla dissolutione del matrimonio / sono lettere … Sua Santità vuole fare dieci o dodeci / cardinali

Third part:
sapeva che erano centomilia scuti contanti / rendermeli più suspetto di / quello ch'io li sono
…
havesse mandato anco lei alla discoperta /
valenti homini insieme
…
qualche banchetto per ruinarmi con poco honore de miei / patroni [se lo permetteranno] / il periculo de la mia licentia / li animi de quelli che poco amano et Nostro Signore et / Vostra Signoria reverendissima / patisco tutta questa / persecutione
…
artifitiosamente per / mostrare che hanno rattuccata qualche pratica della pace per fare /
in questo mezo il fatto loro

3. Antonio Elio's Work on Cryptography

The invention of polyphonic ciphers has been attributed to Antonio Elio (Sacco, 1958, p. 15). In the 16th Century, papal cipher secretaries widely used those ciphers (Meister, 1906; Lasry et al., 2020). Those were employed sporadically elsewhere (Lasry, 2023). In Figure 4, we show the earliest known published polyphonic cipher, used by Cardinal Farnese. It is highly likely that Antonio Elio, his cipher secretary, was behind the design of this cipher. Dozens of similar polyphonic papal ciphers from 1545 to 1583 are documented in (Meister, 1906). Other examples of Elio's ciphers are illustrated in (Lestocquoy 1966, pp. 42-45).

With polyphonic ciphers, a cipher symbol (e.g., a certain digit) may have multiple meanings, usually two possible meanings. First, some letters of the Latin alphabet (typically h and z) are removed and ignored, and only the remaining 17 or 18 letters of the alphabet must be encoded. For that purpose, only 9 of the 10 digits are often used, and the 10th is assigned to be a null.



2.

[1545.]

Cifra del cardinal di Farnese[2] con li revmi legati del concilio XII martii 1545.

ac	eb	if	od	ul	ng	mp	rt	s&	znon	essere	essendo	che
5	2	9	7	0	1	3	8	6	31	30	30	18

chi qua que
18 61 16

Nulle 4

N. S.; S. Stà	31	Imbassadore di	16	Mons. di Granvela	96
L'Impre; S. Mtà	30	Catholici	91	Mons. di Aras	97
Re di Francia	13	Protestanti	92	Venetia	98
Re de Romani	18	Concilio	93	Mons. Verallo	90
Cardinale di	61	V. S. revma	95	Mons. Mignanello	32

Figure 4 – Example of polyphonic cipher used by Cardinal Farnese – 1545 (Meister, 1906, p. 222)

In the example shown in Figure 4, only the letters a,b,c,d,e,f,g,i,l,m,n,o,p,r,s,t, and u can be encoded. For example, the digit 5 is used to encode both the letters "a" and "c," and the digit 2 is used for the letters "e" and "b." The digit 4 represents a null. Note that "et" ("and," in Italian, shorthanded with "&") is encoded with the digit 6, which also encodes the letter "s." Additional words or proper names are encoded using two-digit numbers (e.g., 18 = "chi"). In this cipher example, one of these numbers may also

[6] Note that in this transcript, we have made some adjustments to the interlinear decryption to match the actual encrypted text better and that the line breaks do not necessarily correspond to those of the ciphertext.

represent a special symbol or a digit with a dot above it.

As a result, the key of a polyphonic cipher is usually shorter and more compact than the key of a homophonic cipher. The polyphonic key can be memorized easily if it does not include a large nomenclature for words or names. Furthermore, as most entities are encoded with a single digit, ciphertexts tend to be shorter than ciphertexts with a homophonic digit cipher, where most entries are encoded with two-digit or three-digit codes.

While innovative, with more compact keys and ciphertexts of shorter lengths, polyphonic ciphers have several drawbacks. Firstly, polyphonic ciphers, such as the example above, are not difficult to break. For more details on a modern technique for the cryptanalysis of polyphonic ciphers, see (Lasry et al., 2020). Secondly, the work of the decipherer, even of a secretary who knows the key, may not be trivial. Because there is ambiguity in deciphering most digits, multiple options exist to decipher a segment of ciphertext, some of which may be plausible, and decipherment, even if the key is known, is not deterministic. Cipher secretaries in the 16th Century were expected to determine which decipherment options were correct based on context and their experience. To remove ambiguity in deciphering, diacritics such as dots were sometimes added (above or below the current digit or the preceding one) to indicate to the decipherer which of the two options should be chosen. Examples of deterministic and non-deterministic polyphonic ciphers are given in (Meister, 1906) and (Lasry et al., 2020).

4. Antonio Elio's Innovative Cipher - our Analysis

In this section, we present our analysis of the cipher introduced in Section 2. Following days of intensive teamwork testing numerous hypotheses, we were able to understand how the cipher works, recover most of the key, and decipher those parts for which there was no matching plaintext. The cipher features several characteristics that make it unique, innovative, and hard, if not impossible, to break.

- **Syllabic**: Most of the enciphered text consists of symbols that encode consonant-vowel syllables, such as "ca" or "ni." A few other symbols encode other types of syllables or letter combinations, or short words, such as "gno", "nd", or "che".

- **Polyphonic**: Each symbol used to encode a syllable has a dual meaning. For example, the symbol  used to encode "de" also encodes the syllable "do". The second choice ("do") is indicated by adding a dot above the previous cipher symbol. Without the dot on the previous cipher symbol,  represents "de". Similarly,  represents "di" if a dot is above the previous symbol and "da" if there is no such dot. In theory, decipherment is deterministic. However, those dots are not consistently inserted; in other cases, they might not be visible. As a result, deciphering those symbols is often non-deterministic.

- **Compound symbols**: Using two digits or more (e.g., 23, 123) to encode a specific alphabet letter was customary with digit ciphers. Such compound cipher symbols were rare with non-digit ciphers, which employ graphical symbols or letters to encode plaintext entities. In the present cipher, compound symbols (pairs of graphical or letter symbols) encode some plaintext elements, making cryptanalysis significantly more challenging, as any symbol may be either a stand-alone symbol or part of a pair of symbols used in conjunction. For example,  represents "r" and  represents both "n" and "&", while  and alone represent "qua" and "que". As a result, deciphering segments with such dual-use symbols may not be deterministic.

Each attribute adds to the cipher's complexity, but their combination is unique and unseen in other contemporary ciphers. Generally, consonant-vowel syllables and short words are encoded using single symbols. Compound symbols (using pairs of letters of the Latin alphabet) are used to encode individual letters of the alphabet (e.g., "a", "r") or pairs of consonants such as "nt" or "cr". As with most contemporary Italian ciphers, the letter "h", and any doubled letter are omitted before encryption. For example, "hoggi" is first reduced to "ogi" before being encrypted.

In Figure 5, we show the reconstructed key, where a dot (if present) indicates that the previous symbol had a dot on top. In Figure 6, we show a decipherment example, highlighting the correspondence between the cipher symbols and the elements of the deciphered plaintext. Note: In the colored boxes, a dot on the left indicated that the previous symbol had a dot on top (or was supposed to have one).

At the time we were about to finalize the paper, we discovered another ciphered document sent by the apostolic nuncio in Spain, Giovanni Guidiccioni, to Pope Paul III and the Farnese Curia, from 1535 to 1537, held in the Institute of History in Petersburg. Interestingly, recovering the key, based on matching plaintext sequences, of the cipher employed to encode this document was also quite challenging. The recovered key for this cipher is shown in Figure 7. This cipher has several features in common with the cipher from 1540, such as encoding syllables and using polyphonic symbols and compound symbols. It is also more complex than the cipher from 1540, as it is also a homophonic cipher, unlike the 1540 cipher, which has only one symbol per letter of the alphabet. Furthermore, the 1535-1537 cipher does not employ diacritics to disambiguate polyphones. This cipher further exemplifies the sophistication of cryptographic techniques employed during Elio's service at the papal curia.

5. Conclusion

The present work illustrates Antonio Elio's creative and original approach as a cryptographer. His work also exemplifies the advantage of expertise in both code-making and codebreaking, as only a deep understanding of potential weaknesses in codes can lead to the design of secure ciphers that would withstand cryptanalysis even today.

Funding

The work of one of the authors has been supported by the Swedish Research Council, grant 2018-06074, DECRYPT – Decryption of Historical Manuscripts.

References

Byatt, L., 1993. "Antonio Elio", in *Dizionario Biografico degli Italiani*, vol. 42, Rome, Instituto dell'Enciclopedia Italiana.

Meister, A., 1906. *Die Geheimschrift im Dienste der Päpstlichen Kurie von Ihren Anfängen bis zum Ende des XVI. Jahrhunderts*, vol. 11. Paderborn: F. Schoningh.

Lasry, G., B. Megyesi, and N. Kopal, 2020. "*Deciphering Papal Ciphers from the 16th to the 18th Century*," Cryptologia, 2020, pp. 479–540.

Lasry, G., 2023. "*Armand de Bourbon's Poly-Homophonic Cipher – 1649*," in Proceedings of the 6th International Conference on Historical Cryptology, 2023, pp. 105–112.

Lestocquoy, J., 1966. *Correspondance des nonces en France. Dandino, Della Torre et Trivultio (1546-1551)*, Roma-Paris, Gregoriana- Boccard.

Sacco, L., 1958. *Un primato italiano: la crittografia nei secoli XV e XVI*. Instituto storico e di cultura dell'arma del Genio.

Figure 5 - Reconstructed key - 1540 cipher

Figure 6 - Sample decipherment

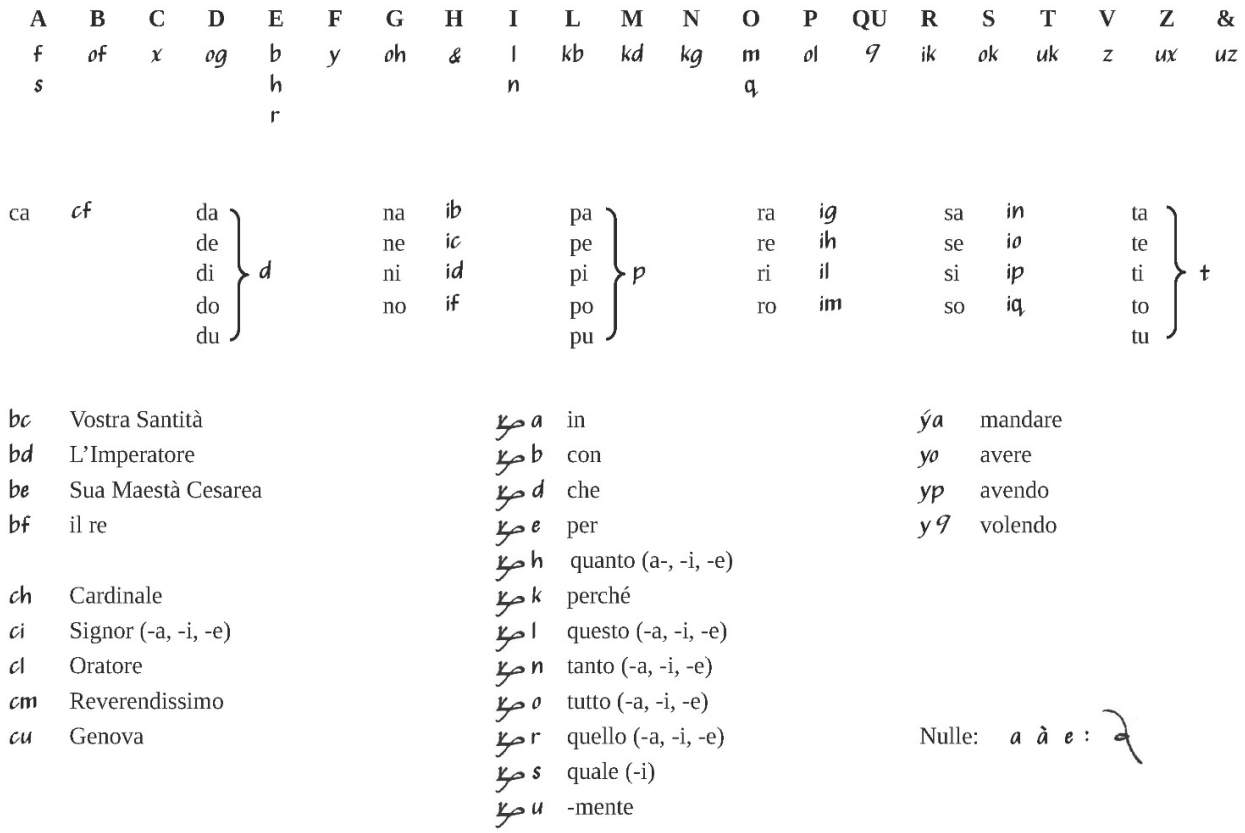


Figure 7 – Reconstructed key for a similar cipher from 1535-1537