A Florentine 'polyalphabetic' cipher in the 15th century

Marco Vito
marcovito001@gmail.com

Abstract

The 15th century in Italy was a period of revolution in cryptography. Leon Battista Alberti developed the first western polyalphabetic cipher, while the monoalphabetic system spread throughout the peninsula. The aim of this study is to present a never before published late medieval 15th-century Florentine polyalphabetic cipher, explain its functioning, and shed light on a system—specifically the polyalphabetic cipher—that, although seemingly unused during the 15th century, was in fact employed in Florentine diplomacy.

1 Introduction

The 15th century is the period in which traditional cryptography develops and is enriched by various forms of ciphering. The use of monoalphabetic substitution ciphers, homophones to reduce frequency, nulls to make decryption more difficult, as well as alchemical, astral, planetary and numerical signs, are all examples of a revolution in the field of cryptography. The most important of these innovations, although the least adopted by contemporaries in the 15th century, was the polyalphabetic system. The first Western inventor of this form of secret writing was Leon Battista Alberti in his *De Componendis Cyfris*. In his 1466 work, he devised a system that no longer relied on a single alphabet, but on multiple alphabets that could be used within a single encrypted message, thus giving birth to the Alberti cipher.

Alberti's work, which remained unpublished for some time, was followed a century later by Giovan Battista Della Porta in *De furtivis literarum notis vulgo de ziferis libri IIII*, who, following Alberti's model (but without mentioning it), described the use of cipher discs to write polyalphabetic ciphers[1].

Cipher disc systems were considered extremely useful and secure by Alberti himself:

> "Nunc de scribendi ratione a nobis inventa dicendum sequitur. Habet ea quidem has commoditates, nulla omnium qua qui suti possit cyfra expeditior, nulla scribitur commodius, nulla ubi ex instituto modum teneas, promptius apertiusque legitur, nulla (indices constitutos inter me atque alium, ad quem, scribo, si ignoraris) excogitari ptest obscurior"[2].

The importance of polyalphabetic cryptography (primarily in its theoretical formulation) had a greater impact in modern times, while in the late Middle Ages, apart from Alberti's treatise, there are no sources on the subject. With this in mind, it is interesting to note that among the Italian ciphers, there are mainly monoalphabetic substitution ciphers with homophones, followed in very small numbers by ciphers using only nomenclators and jargon ciphers. However, there is a cipher in the State Archives of Florence that could be considered as polyalphabetic, the only existing unpublished example currently known, demonstrating the intention to create a cipher with a mobile alphabet rather than a static one.

The cipher, located within a miscellany (miscellanea repubblicana),[3] appears in isolation and is not part of a homogeneous corpus. The file also separately includes a second, distinct cipher, this one written in jargon.

The difficulty in its identification stems from its archival placement, which is detached from

[1] See (Della Porta 1563).

[2] (Alberti 1994) P. 41. English translation: *We must now consider the method of writing which we have discovered. It has these advantages, each of which is more convenient for writing in cipher, Nothing is written more conveniently, nothing is written more easily and openly, where one sticks to the established manner, nothing (Indices established between myself and another, to whom I write, if you do not know) is more obscure to solve.* A revised and reprinted edition of the volume was issued in 1998 (Alberti 1998).

[3] Archivio di Stato di Firenze (ASFI). *Miscellanea Repubblicana 11*. fasc.292, I. All images are reproduced by permission of the Italian Ministry of Culture and the State Archives of Florence.

the original context in which the cipher was conceived and used. The author is unknown, most likely a chancellor for whom no certain information is available. The recipient, however, is known. Moreover, compared to many other ciphers currently under study, this cipher represents the only example of a 'polyalphabetic'[4] cipher.

This cipher allows us to see how Florence, even in the time of Lorenzo de' Medici, could have been at the forefront of cryptography and, above all, provides a point of comparison with other Italian contexts[5]. The Sforza case, for example, is one of the most analysed examples from the 15th century, showing that among the extensive series of ciphers, monoalphabetic ciphers with homophones were by far the most widely used, almost exclusively[6].

The Florentine testimony allows us to observe how, during the times of Lorenzo the Magnificent, there was a constant attempt to improve existing ciphers by experimenting with different and new ways of writing in code.

2 Context of the cipher

The fifteenth century in Italy was a turbulent period for all the forces involved. Lorenzo de' Medici, for his part, sought to be at the centre of these various forces, positioning himself as a mediator between competing territorial claims[7]. Especially in the 1480s, there were several destabilising factors, such as the War of Ferrara, which ended within two years with the Peace of Bagnolo (1482-1484), and the conspiracy of the Neapolitan barons (1485-1486), which took place at a time when Florence was allied to King Ferrante of Naples. There was also the internal front, with Florence concentrating on expanding and countering the Genoese in the Lunigiana[8].

The cipher provides no historical evidence of its use, other than the intended recipient of the cipher itself. Indeed, on the back of the sheet we can read 'Cifera di Livorno Conposta per la buona aromoria[9] di Piero Capponi'[10] (Cipher of Livorno, composed for the good harmony of Piero Capponi). Moreover, the word 'Ciffra' is written vertically on the verso.

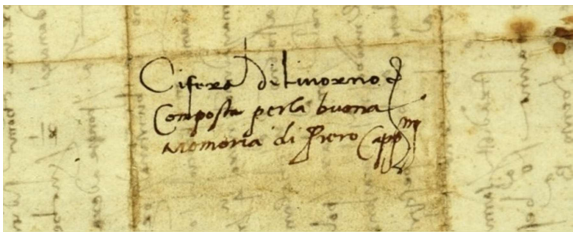

Figure 1. Detail of the back of the cipher, with reference to the holder

Piero Capponi was a loyal supporter and close associate of Lorenzo the Magnificent, serving as his ambassador and military commander on several occasions[11].

Capponi visited Livorno on two separate occasions. The first time was in December 1484, when he was appointed commissioner for the war against Genoa - a mission that ended in failure due to a storm during the expedition against the Republic.

In January 1486, Capponi was sent to Naples to support the Aragonese, who were then at war with the Papacy, allied with the mercenary captain Roberto Sanseverino. Capponi remained with the Aragonese allies until September of that year.

Following these events, Capponi returned to Livorno a second time in 1486-1487, this time as commissioner for the war against Sarzana.

Since Livorno and Piero Capponi are the only references given by the document, it is possible to date the cipher to the period between 1484-1485, corresponding to his mission against Genoa, and 1486-1487, corresponding to his mission against Sarzana.

Considering the events in Naples and likely his need to return to Livorno, it is reasonable to suggest that the cipher should be dated to 1487.

[4] The term is placed in quotation marks, as it was not employed by the cipher's creator or scribe, but came into scholarly use only at a later phase. Example (Sacco 1947) and (Zanotti 1928).

[5] The case of the Papal States, beginning in the Middle Ages, offers significant evidence of a sustained and systematic effort to refine and develop the secret writing practices in use, reflecting an evolving awareness of cryptographic needs within the administrative and diplomatic apparatus (Meister 1906).

[6] (Cerioni 1970).

[7] On Florentine diplomacy, see (Santini 1922) and (Lang 2014); for a general overview, see (Queller 1967).

[8] For further insights into the Italian context, with a specific focus on the Florentine setting, see (Fubini 1994).

[9] Uncertain transcription, as the text has an apparently incorrect spelling, most likely to be interpreted as 'armonia' for harmony.

[10] The italicised letters indicate the expansion of abbreviated words, in which one or more letters have been omitted through the use of abbreviation marks.

[11] (Mallet 1976).

3 The ‘polyalphabetic’ cipher

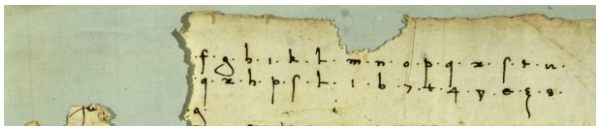

Figure 2. Cipher, detail of the alphabet (at the top the one in clear, at the bottom the one in figures)

The Florentine example makes it possible to analyse the cipher system and to understand it thanks to the work of the chancellor who composed it.

The document is part of the Miscellanea Repubblicana 11 fasc. 292 Cifra I and is in poor condition, with some tears around the cipher alphabet. However, it is still possible to understand how it works.

The cipher system in question consists of a single cipher alphabet which corresponds to the regular alphabet in a one-to-one relationship, meaning that for each letter of the alphabet there is a corresponding cipher symbol or letter, without the use of homophones. On this premise, it would appear to be a monoalphabetic substitution cipher with no distinguishing features. However, the writer provides a detailed explanation of how it works below the alphabet.

The writer offers an example word for coding: ‘*papa’* (pope)[12].

The first letter corresponding to the cipher to be used for encryption is taken (pigliasi i choxi che la prima lettera cum*que* a pro primo poi si ch*on*ta insino alla lettera che tu vuoi trovare). Since ‘*papa’* is the word to be encrypted, the corresponding cipher symbol for the letter ‘p’ is read from the cipher alphabet, which is ‘t’ (Chomincia alla prima lettera ad *esempio* a. b. c. *etc*. e troverrà che al p viene un t).

At this point the polyalphabetic factor comes into play, as the alphabet changes the cipher symbols for each letter, effectively creating a new cipher alphabet. This happens because once the single letter is ciphered, the next cipher symbol becomes the equivalent of the letter ‘a’ (the first letter of the alphabet). Specifically:

> ‘e poi rechomincia alla . a . che un 4. e poi rechomincia alla . a. un’altra volta de la ‘Ȳ’

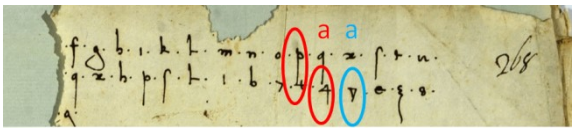

Figure 3. Cipher system: shift of the cipher sign and new alphabet. After ‘p’ the sign corresponding to ‘q’ becomes the sign to indicate ‘a’, the second letter being the second letter for papa, the next sign becomes the new sign to indicate the letter ‘a’

The cipher changes and the sign corresponding to the following letter becomes the new sign for ‘a’ so for the second letter of papa, ‘a’ now corresponds to ‘4’ and is the second letter in the cipher. For the third letter is repeated, the cipher following ‘4’ that is ‘ȳ’, now corresponds to ‘a.’ Scrolling through the letters, ‘p’ now corresponds to ‘l,’ which becomes the third letter of the word papa. Finally, the cipher symbol following ‘l’ is ‘i’ which now corresponds to ‘a’. Therefore, to write ‘*papa*’, one has to write ‘t4li’ (ntruovo a il p che .L. e poi ntruova e rechomincia a dare . a . al . i . adunque adire papa co*n* questa regola sia t4li).

Furthermore, the use of null letters is possible in order to complicate the cipher, although they must be added arbitrarily:

> “p*er* ischauvare il numero delle lettere vo messo . s. false *che*sono nel secondo merso a queste non rompano l’ordine ne se chontano chome s’elle no*n* vi fussino […] tu vuoi scrivere papa chomincia a una falsa . d. e poi per p. ti viene t. e poi una falsa . x . e poi seguente alla a. un 4. e poi Li e dirai papa. dt4xli ec*ho*si si *con*ti semp*er*e”[13]

Thus, following the cipher and its example, two letters are inserted: one before the word ‘*papa’* (which is ‘d’) and one in the middle, which is a ‘false,’ meaning a null ‘x.’ (queste non rompano l’ordine ne se chontano chome

[12] ‘tu vuoi scrivere papa’ in the text. English Translation: *you want to write pope.*

[13] English translation: *To hide the number of letters, I put fake letters between the real letters, which are used for encryption. The fake letters are not counted and do not follow the rule, as if they did not exist. If you want to write pope (papa) you start with a false ‘d’ and then, following the rule, for ‘p’ you write ‘t’ and then a false ‘x’ and then to write ‘a’ you use the sign ‘4’ and ‘li’ (as before) and you will write pope dt4xli and this is how it must always be done*. Note: Although the rule is written, the writer seems to have made a mistake, as he states that the ‘x’ should be placed after the first letter ‘p’, but still in the same period, he states that the letter null should be placed in the middle, as he then writes.

s'elle no*n* vi fussino). Following the same principle, the word '*papa*' can be ciphered by applying the principle of the null letters; thus the result is the word 'dt4xli'.

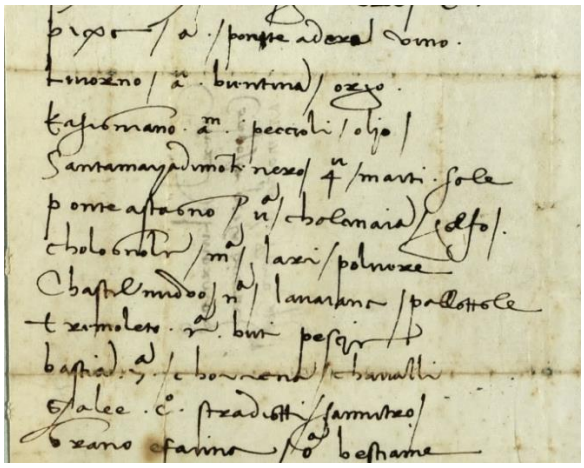

Figure 4. Nomenclator: on the left, the names to be encrypted; after the slash '/', the different possible substitutions

Finally, the cipher also includes a nomenclator to hide strategic words with substituted letters and words. It consists of thirteen words, each of which has three different possible substitutions, some of which concern places such as Livorno, Santamaria di Montenero in Liguria or Tremoleto in Tuscany.[14] Other elements of the nomenclator have to do with grain, provisions and galleys. The purpose of the second section of the cipher was twofold: to improve security by using a second encryption system, and to speed up and better conceal references to strategic information, such as locations and supplies.

4 Cipher utility and analysis

The cipher presented here is particularly effective for its time because, with the exception of Alberti's cipher discs, no other ciphers modified the cipher alphabet. The presence of a late medieval Florentine 'polyalphabetic' cipher is certainly an uncommon feature compared to other medieval Italian ciphers used on the peninsula and beyond. Furthermore, similarities with Alberti's work can be found in the substitution mechanism. Alberti, in explaining the functioning of his cipher discs, explains how one must change the alphabet:

> Cum autem tres quottuorve dictiones exscripsero mutabo nostra in formula situm indicis versione circuli[15].

The Florentine cipher operates in the same way for Piero Capponi, with the difference that the alphabet must be changed after each letter, rather than after every three or four words. The reason for this is the absence of cipher discs and the fact that there was no method for using the Florentine cipher outside the established rule. If this rule had not been followed, each letter in the cipher would no longer have corresponded to the plaintext. For this reason, the writer emphasizes the necessity of applying the rule only to the letters to be ciphered and using the nulls without following the rule, in order to avoid errors.

In fact, the error would have been irreparable: if one had made a mistake in writing a letter in cipher, the entire system would have shifted, changing the sign corresponding to each letter in the text and making it extremely difficult to decipher[16].

There was also the problem that if the rule for ciphering fell into the wrong hands, the entire cipher would become useless, a risk common to all existing ciphers.

The Florentine cipher, following the polyalphabetic system, decreases the frequency since, as seen for the word '*papa*' formed by only two repeated letters, it has formed four different signs to write in cipher, as if they were homophones, but with the characteristic that they can be used with several letters and not exclusively with one. The resulting frequency does not allow an intuitive association between a cipher symbol and a letter of the alphabet, as this association constantly changes. The result is a modified frequency in which the number of usable symbols matches the number of alphabetic letters, but they are used in a manner that appears confusing to one who needs to decrypt it, yet is extremely clear to the person using the cipher key.

Another defining feature of the cipher was the nomenclator, which enhanced the system by combining two ciphering methods.

[14] For the regions present in the cipher, see. (Repetti 2005).

[15] English Translation: *when I have written three or four words, I will change our formula by rotating the disk.*

[16] For example, if the character corresponding to the letter 'a' is used to write the character for 'b', the entire cipher would be incorrectly shifted by one position for each successive letter encrypted.

In this case, the nomenclator enabled the rapid insertion of keywords that, while not encrypted through the polyalphabetic system, introduced both an alternative method of encryption and a definition that, as with any nomenclator, conveyed a distinct and specific meaning.

As a result, in certain passages of text encoded with the polyalphabetic cipher, some words appeared that were not encrypted in the same way. Nevertheless, they still concealed meaning by employing the nomenclator, operating alongside the primary system.

5 Conclusions

The Florentine 'polyalphabetic' cipher is a very important example of how in the same century as Leon Battista Alberti and before Giovan Battista Della Porta, there was an example of a polyalphabetic cipher, used in diplomatic activity by a Florentine envoy closely linked to the figure of Lorenzo de' Medici.

The presence of this cipher makes it possible to analyse Italian secret diplomacy from a different critical perspective, showing how Florence tried to find better methods of ciphering that surpassed those of other Italian realities.

References

Alberti Leon Battista. 1994. *Dello Scrivere in cifra,* Galimberti, Torino.

Alberti Leon Battista. 1998. *De Componendis Cyfris,* Galimberti, Torino.

Archivio di Stato di Firenze (ASFI). *Miscellanea Repubblicana 11*. fasc.292, I.

Bullard Melissa Meriam. 1993. The Language of Diplomacy in the Renaissance. In *Lorenzo de'Medici, new perspectives: proceedings of the international conference held at Brooklyn College and the Graduate Center of the City University of New York, April 30-May 2, 1992*. Toscani B. (a cura di), San Francisco, Berna ed altri, Peter Lang, New York: 263-278.

Cerioni Lydia. 1970. *La diplomazia sforzesca nella seconda metà del Quattrocento e i suoi cifrari segreti*. Vol. I (di II), Fonti e studi del Corpus membranarum italicarum VII, Centro di Ricerca, Roma.

Della Porta Giovan Battista. 1563. *De furtivis literarum notis vulgo de ziferis libri IIII*. Vol. I-IV, Napoli.

Fubini Riccardo. 1994. *Italia quattrocentesca. Politica e diplomazia nell'età di Lorenzo il Magnifico*. Franco Angeli, Milano.

Lang Heinrich. 2014. Power in Letters. Political Communication and Writing in the Medici Letters. In *Medien der Macht und des Entscheidens. Schrift und Druck im politischen Raum der europäischen Vormoderne (14.-17. Jahrhundert)*, Wehrhahn, Hannover: 83-102.

Mallett Michael. 1976. Capponi, Piero. In *Dizionario Biografico degli Italiani (DBI)*, 19. Url: https://www.treccani.it/enciclopedia/piero-capponi_(Dizionario-Biografico)/ (Link active to the 30/01/2025).

Meister Aloys. 1906. *Die Geheimschrift im Dienste der päpstlichen Kurie*. Druck und Verlag von Ferdinand Schöningh, Paderborn.

Queller Donald Edward. 1967. *The Office of Ambassador in the Middle Ages*. Princeton University Press, New Jersey.

Repetti Emanuele. 2005. *Dizionario geografico, fisico, storico della Toscana*. Firenzelibri, vol. 5, Reggello.

Sacco Luigi. 1947. *Manuale di Crittografia*. Ist. Poligr. Dello Stato, Roma.

Santini Emilio. 1922. *Firenze ei suoi "Oratori" nel Quattrocento*. R. Sandron, Milano.

Zanotti Mario. 1928. *Crittografia, le scritture segrete*. Hoepli, Milano.

Appendix A Miscellanea Repubblicana 11 fasc.292 Cifra I Text.

Legend: [ ] The square brackets identify additions not present in the original text, provided for a clearer understanding of the content.

[…] Square brackets with ellipsis indicate a portion of the text that is illegible due to a tear in the paper, resulting in the loss of the written content.

"." The dots between the letters, as well as those evidently placed by the writer, have been preserved to maintain consistency with the original text.

Italics indicate abbreviations used by the writer of the 15th century document.

-Recto

[…] f g h I k L m n o p q r s t u
[…] q r h p s L I b 7 t 4 Ȳ e z 8
[…] g.
Con q[torn, perhaps questo] […] enna resta e pigliasi i choxi che la prima lettera cum*que* a pro primo poi si ch*on*ta[17] insino alla lettera che tu vuoi trovare e quella relieva quella lettera. Verbi *gratia*[18]*,* tu vuoi scrivere papa. Chomincia alla prima lettera ad *esempio* a. b. c. *etc*. e troverrà che al p viene un t e poi rechomincia alla . a . che [è] un 4. e poi rechomincia alla . a. un'altra volta de la Ȳ e vo ntruovo a il p che [è] .L. e poi ntruova e rechomincia a dare . a . al . i . adunque adire papa co*n* questa regola sia t4li e p*er* ischauvare il numero delle lettere vo messo . s. false *che*sono nel secondo merso a queste non[19] rompano l'ordine ne se chontano chome s'elle no*n* vi fussino, verbi gratia, tu vuoi scrivere papa chomincia a una falsa . d. e poi per p. ti viene t. e poi una falsa . x . e poi seguente alla a. un 4. e poi Li e dirai papa. dt4xli ec*ho*si si *con*ti semp*er*e.
Ce lego ogni chosa a . *et*. lo ze certi annota che cierti[20] no*n* rompano l'ordine chome se dice alle false.
[pixe][21] danare 1/r | suchero | e^{a}
Pixe[22] / a/ ponete adara vino
Livorno / a^{n} . bientina / orzo
Kasigriano a^{m} . peccioli / olio /
Santamarhia di Mo*n*tenero / 4^{n} / marti, sale
Ponte astagno / u^{a} / cholonaia / zolfo /
Cholognole / m^{a} / lari / polvere
Chastel Nuovo / n^{a} / Ianaiane / pallottole
Tremolete[23] r^{a} . buti peseri
Bastia 7^{a} chorrende chavalli
Zalee . c^{o} . stradiotti / Sarnitro[24]
Grano e farina / o^{a} bestiame
Vettovaglie / vento . B^{a} .

-Verso
Cifera di Livorno[25]
Composta per la buona aromoria di Piero Cappo^{ni}
Ciffra[26]

[17] 'ta' overwrite su sich*on*ta.
[18] As *exempli gratia,* that means for example.
[19] Added on line spacing.
[20] Uncertain transcription.
[21] deleted.
[22] Pisa.
[23] Tremoleto, (Repetti 2005).
[24] Salnitro, *saltpetre.*
[25] followed by an interruption sign.
[26] written vertically.

Appendix B. Cipher key recto-verso

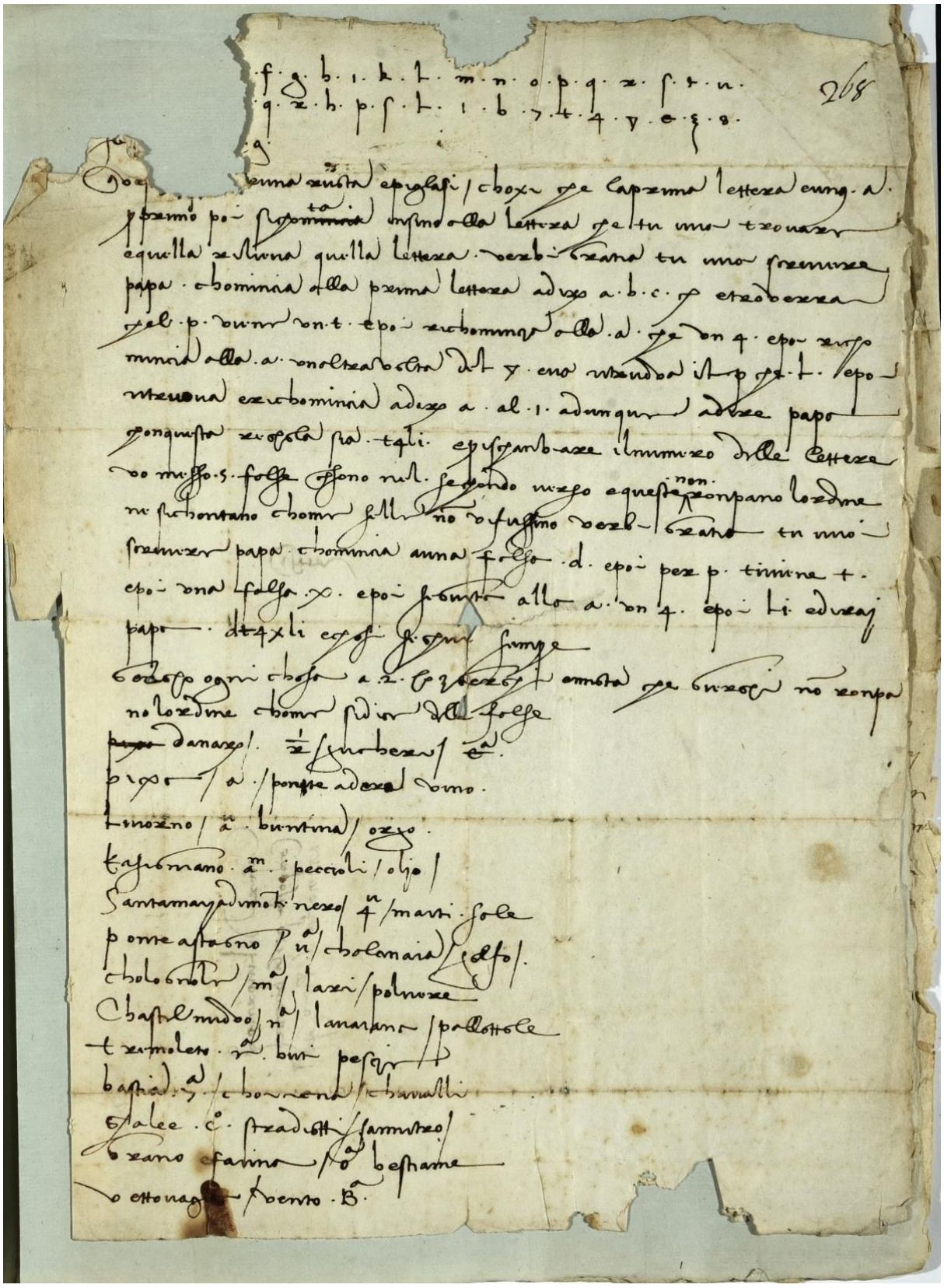

Figure 5. Polyalphabetic cipher of Piero Capponi, recto

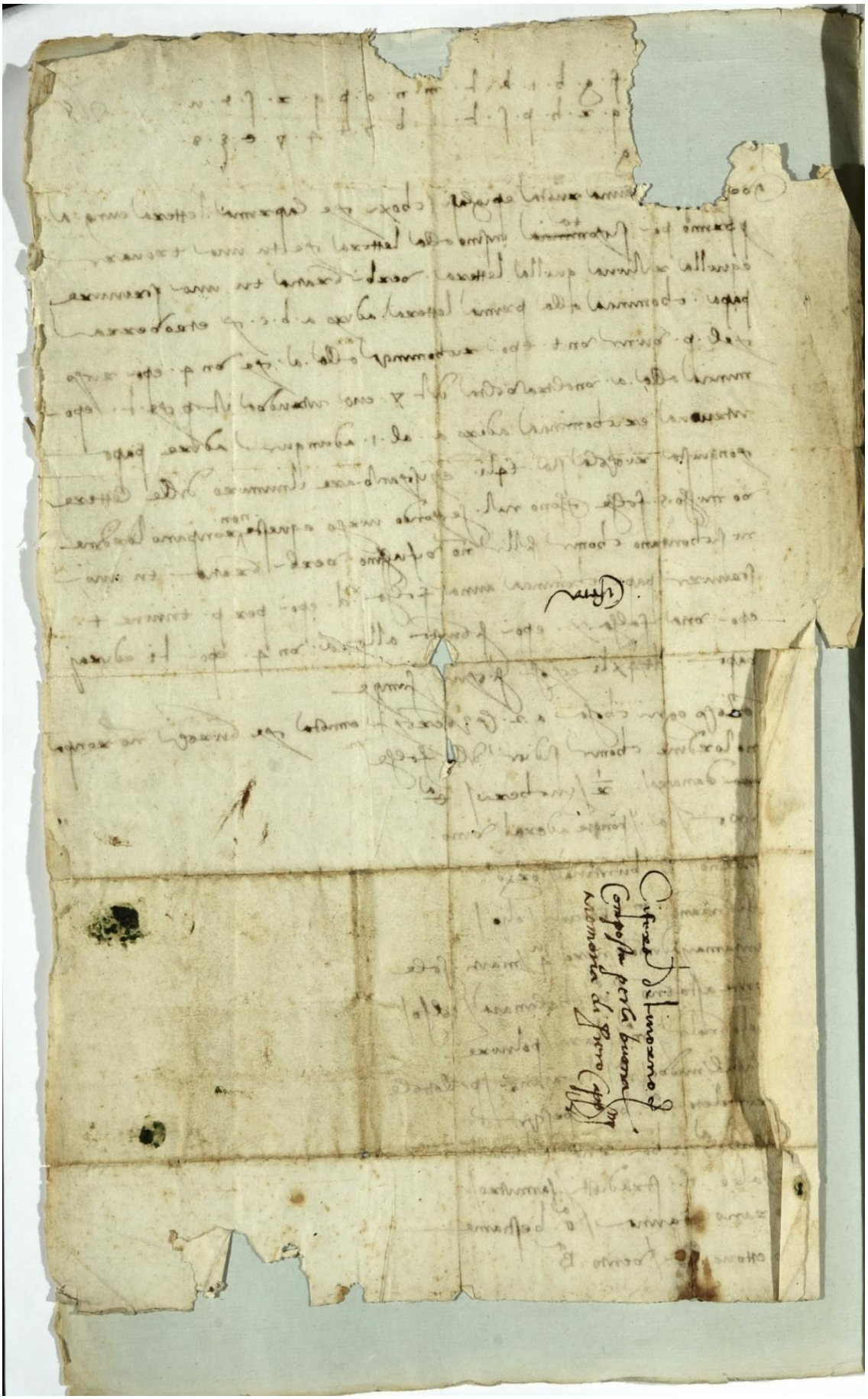

Figure 6. Polyalphabetic cipher of Piero Capponi, verso