A Partenio's Stegano-Crypto Cipher

Paolo Bonavoglia
Mathesis Venezia c/o Convitto-Liceo Marco Foscarini 4942 Venezia, Italy
paolo.bonavoglia@mathesisvenezia.it

Abstract

Pietro Partenio's second cipher in the CX[1] book of 1592-93 is an unusual mix of a *cifra sospetta* (suspicious cipher) and a *cifra non sospetta* (non suspicious cipher), that is cryptography and steganography. The cipher has some possible roots in Trithemius's Ave Maria, Vigenère's and Francis Bacon's ciphers.

1 Pietro Partenio

Pietro Partenio was one of the most brilliant Venetian cryptologists. He was born in 1538 or possibly in January 1539[2].

He was a notary whose deeds are stored in the State Archives of Venice, for the 1563-1610 period under his name, and from 1610 to 1628 in association with another name; so he probably died between 1618 and 1628, a very long life for the XVI century.

In his notary deeds the name of Hieronimo di Franceschi, the main CX deputy for ciphers in those years, is often present as a solicitor for other people. So Partenio and Franceschi knew each other, and the first mentions very often Franceschi in his cryptographic papers, comparing the well known *cifra delle caselle*[3] used by Venetian embassies in the 1577-1595 period with his ciphers and boasting the superiority of his ones. Apparently there was a mix of friendship and rivalry between the two.

[1]CX is the acronym for *Consiglio di Dieci* = Council of Ten, the powerful council of the Republic of Venice that had wide powers in matter of security and domestic and foreign policy, and was also in charge for choosing the deputies for ciphers, and approving the ciphers to be used. The ten members were elected by the *Maggior Consiglio*, the House of Lords of Venice; the Doge and his six advisers had the right to join the meetings of the CX, that could thus have up to 17 participants.

[2]The date can be inferred from the letter Partenio wrote to the CX, in January 1606, where he states to have reached the age of 67. *ASVe CX deliberazioni segrete, f. 28.* ASVe is an acronym for *Archivio di Stato di Venezia* (State Archives of Venice).

[3]See (Bonavoglia, 2020).

He started to design ciphers for the CX in the early 1590s when he was in his fifties; between 1592 and 1593 he gave seven ciphers to the CX.

Most of his ciphers are clearly derived from the two main ideas of Franceschi: superencryption of a nomenclator as in the already mentioned *cifra delle caselle*, and fake key ciphers; and Partenio repeatedly criticized Franceschi's ciphers claiming his own were more secure and easier to use.

From the Archives' papers quite a different story comes out; up to now only three diplomatic messages from Paris using one of Partenio's ciphers, in July-August 1595, have been found; apparently the secretaries found the cipher too complicated and cumbersome to use.

In spite of this failure, Partenio's ciphers are fascinating and unusual for those years. One among them is the cipher presented here, a classical nomenclator followed by a super-encryption generating a common language message, that is a kind of steganography.

Before looking at the cipher in detail, a few words about steganography.

2 Non Suspicious Ciphers, alias Steganography

Steganography, the art of concealing secret messages inside innocuous texts, is very old, indeed older than cryptography. Invisible inks, dissimulated writing using conventional words and phrases in most cases preceded classical cryptography; so was the case in Venice too, whose first encoded messages used conventional language. [4]

In the Italian cryptographic jargon of those times *cifre sospette* (suspicious ciphers) were normal encryption methods: the resulting cryptograms were easily recognized as encrypted texts, and that's why they were suspicious; *cifre non sospette* (non suspicious ciphers) were methods producing plausible text, apparently innocuous, while hiding a secret message.

[4]See (Pasini, 1872).

Steganography was largely neglected by the cipher offices after cryptography became the standard method used by ambassadors and military chiefs to communicate in a secret way. It remained viceversa very popular among amateurs.

In spite of this we find several interesting *cifre non sospette* both before and after Partenio. We will see a few that have something in common with this one.

3 Partenio's non Suspicious Ciphers

And now let's go to the Venetian Archives, where a fine handwritten parchment book[5] has a *cifra non sospetta* (non suspicious cipher), a curious mix of cryptography and steganography.

Partenio presented this cipher to the CX during a meeting held in 1592.

Later, in 1606, he wrote a booklet, to be used as a textbook for teaching ciphers and cryptography to a few young pupils. One of them was Ottaviano Medici, a future CX deputy for ciphers. In this booklet he presents again this non suspicious cipher, adding to it a fake key variant.

Let us now see in detail these two ciphers.

4 The 1592 Second Cipher

The basic idea of this cipher is to encrypt a message using a 3 digits nomenclator (see figure 1); the resulting cryptogram is super-encrypted substituting orderly every digit with a piece of a sentence to be chosen among ten variants as shown in figure 2.

The pieces of sentence are so conceived to give a plausible message as shown in the following example. Suppose the message to encrypt is:

> *È venuto noua che Re di Spagna è risentito con pericolo di uita*[6],

for a total of 51 letters.

The nomenclator has a cipher, 315, for the statement *È venuto noua che*, a cipher, 678, for *Re di Spagna* and cipher 312 for *È risentito con pericolo di uita*. So the first step gives the cryptogram 314 678 312.

The second encryption requires to encrypt every digit with a different piece of phrase; the first digit, 3, has to be looked in the first column of the phrasebook, where one finds "*Ser.^{mo} Principe*", the second digit 1 has to be looked for in column 2, and you get "*non si marauiglia*", and the job continues until column 9. Finally one gets this fake message:

> *Ser.^{mo} Principe non si marauiglia se non ha mie lettere che se uolessi dargli raguaglio con lettere suspette sarebbe tutto squarciato con disgusto suo*[7].

for a total of 125 letters, more than double the ones in the plain text; and the example is somewhat artificial, a best case, being composed of statements present in the nomenclator; if they were not, the message would have to be split into syllables and letters, 30 of which would generate 90 numbers of cipher text, and a thousand letters of fake text; in such case, one would need a much larger phrasebook, or limit himself to very short messages.

Indeed the method is practical only for very short, telegraphic messages. The clumsiness is anyway a problem common to most steganographic methods.

Another problem is that using always the same phrasebook will produce messages very similar, and the enemy intercepting them would be alerted; so the cipher will be no more *non sospetta*. For this reason one should change the key very often, or prepare and exchange a very long strip of hundreds of plausible words or phrases.[8]

Only in this last case the cipher could be considered very difficult to break, without the *scontro* (the phrasebook), even knowing the method.

5 The 1606 Remake

As anticipated above, in 1606 Partenio, wrote a book, signed *Pietro Partenio di sua mano*[9] that contains four ciphers, with some new ideas. The third of them is a cipher very similar to the 1592 one, but with an increased phrasebook (15 items instead of 9, see figure 4) allowing for longer messages, a different nomenclator (see figure 2) using more common short messages, and the following interesting variant.

[5] ASVe CCX Raccordi, Registri 1. CCX is an acronym for *Capi del Consiglio di Dieci*, the three chiefs of the Council of Ten; they were elected monthly and had final court enforcement powers.

[6] English: A news has come that the King of Spain is ill in danger of life.

[7] Most Serene Prince, do not be surprised if you do not receive my letters, because if I would give details with suspect letters, you would be torn with disgust.

[8] Something of the like was made by Abbot Trithemius for his *Ave Maria* cipher. See paragraph below.

[9] The manuscript is kept in the *ASVe, CX Cifre, chiavi e scontri di cifra ..., busta 2*.

5.1 The *Altro Senso* Variant

This remake has also something really new, the *altro senso* variant. Partenio proposes, as an alternative to the phrasebook, the following complex method to get a plausible text from the nomenclator numbers.

The basic idea is to hide the information in the ligature (binding) between consecutive letters; Partenio defines *unite* the letters united with a continuous writing (without raising the pen from the paper) and *disgiunte* if there is no binding.

The way to get a number in the range 0..9 from these continuities and discontinuities in the handwriting is not so simple and Partenio conceives a complicated set of rules that require a bit of arithmetic. The rules are:

1. Every number begins with two letters *disgiunte* and ends with two lettters *unite*. This rule defines the boundaries of the single numbers.
2. A letter *disgiunta* isolated on both sides get a score of 4.
3. A letter *disgiunta* on the left and *unita* on the right gets a score of 4 as well.
4. A letter *unita* with both adjacent letters get a score of 1.
5. A letter *unita* with its left letter, at the end of a number gets a score of 1
6. The resulting number is the sum of all scores from the beginning to the end, as defined above.
7. The first letter of a word inside a number is not computed.

Having this in mind you can use any phrase and write it using continuous or discontinuous writing in such a way as to get the numbers to hide. Using the first example given by Partenio, let's see how to get number 3 out of the word *amor*; one must write it so:

a m or

the first two letters **a, m** are *disgiunte* and by rule 2 score 4 each, while **o** and **r** are *unite*, but **o** is *disgiunta* on the left and by rule 3 has a score of 4, while the **r** is *unita* and by rule 5 scores 1. As a conclusion we have 4+4+4+1= 13. But being 13 out of the range 0..9, you have to subtract 10 and get 3. Here again, like in other ciphers, Partenio uses a modulo 10 arithmetic, to use the modern mathematical language.

But if one writes *il be* this way, at first look equivalent to the previous one:

i l be

The score is now 4+4+0+1 = 9 because **b** is initial of a word inside the number, while the **o** of *amor* wasn't!

A question arises; can one obtain any digit with these rules?

Partenio addresses this problem, giving the two extreme cases: a) one cannot get 1 with a single letter, which scores 4, so you have to reach at least 11, that is 1 modulo 10. For instance you can get 1 with this sentence:

i l ben fa.

Indeed this gives 4+4+0+1+1+0+1 = 11 that modulo 10 is 1 (the initial **b** and **f**are not computed, by rule 7).

Partenio at the end shows a complete example of his super-encryption; one has to write the message:

Le cose sono accomodate.[10]

Luckily the nomenclator has an entry for this, with cipher 393; now you can use the fake sentence *Illustrissi* to get 393, writing it as follows:

i llu s tr i s si

Indeed it is:

i l lu	4+4+4+1 = 13	3
s tr	4+4+1 = 9	9
i s si	4+4+4+1 = 13	3

In this case, 11 letters are needed for a 20 letters message, thus the fake message is shorter than the true message; using Bacon's cipher it would require 100 letters. But Partenio's example here is quite artificial, because the message uses a single cipher from the nomenclator, which is the best possible case. If one encrypts it using only letters and syllables, the worst case, he gets $10 \times 3 = 30$ numbers which would require about 150 letters.

To conclude let's get all 10 digits:

[10] English: Things are settled.

i l ben fa	4+4+0+1+1+0+1 = 11	1
i l ben far	4+4+0+1+1+0+1+1 = 12	2
e s so	4+4+4+1 = 13	3
i de al	4+4+1+4+1 = 14	4
i de ale	4+4+1+4+1+1 = 15	5
i dei	4+0+1+1 = 6	6
i divi	4+0+1+1+1 = 7	7
i dieci	4+0+1+1+1+1 = 8	8
l ui	4+4+1 = 9	9
l oro	4+4+1+1 = 10	0

The trick requires great care in writing, to avoid ambiguities while deciphering; at the same time a gap too large may become suspicious to an expert's eye.

5.2 Conclusion about the Cipher

This 1606 version of the second cipher of 1592 is an improvement both because the nomenclator has been enlarged with many common phrases, and the phrasebook has been enlarged from nine to fifteen pieces.

The *altro senso* variant is rather puzzling; it is really ingenious in itself, but a bit too demanding, and Partenio seems to be struggling to solve the problem of getting numbers in the 0..9 range. The advantage is that the fake message can be shorter.

The whole cipher looks more a cryptographic *divertissement* than a cipher usable in the real world. No message using this cipher was found up to date, but of course such a *without suspicion* message would be very difficult to find.

6 Origins of the Cipher: Trithemius? Vigenère? Bacon?

An interesting problem is to find the sources, if any, of this cipher, and of the calligraphic variant. Were these ideas born from scratch? Or did Partenio stand on the shoulders of the giants who preceded him?

I found a few possible links, the first almost certain, the others more problematic.

Let's start with the first, the cipher known as *Ave Maria* abbot Johannes Trithemius[11].

[11]Ioannes Tritemius (later spelled Johannes Trithemius, 1462-1516) was a German priest and abbot who wrote about cryptography and steganography but also astrology and occultism; his first book *Steganographia* was placed on the Index of prohibited books by the Catholic Church as heretical, the second *Polygraphia* containing the *Ave Maria* cipher and the *Recta Tabula*, was written in 1506-1508, and published in 1518 after his death.

6.1 Trithemius's *Ave Maria* Cipher

In his main cryptographic work *Libri Polygraphiae VI*[12] Trithemius presents two ciphers without suspicion (steganography) followed by four suspicious (cryptography).

Trithemius's best known cipher is the last one, the *Recta Tabula*, but here we are more interested to the cipher described in the first two books, *Liber I* and *Liber II*, best known as the *Ave Maria* cipher [13] cipher[14].

The basic idea is to encrypt every letter of the plain text with a word taken from a list of 384 alphabets of 24 letters, published from page 107 to 298 of the book, every page having two columns with two alphabets (see the first pages in figure 5). The words of each column are roughly interchangeable, and written in order produce a plausible text; Trithemius in the *explanatio* of Liber 1, gives a simple example[15] : in case a malicious man asks to be recommended to a friend of yours, and you want to alert the friend of the danger, you can give the rascal a message so encrypted:

> *Cave tibi ab isto viro, quia fur est, et nequam pessimus.*[16]

Using orderly the list of alphabets you substitute C with *Conditor*, A with *clemens*, V with *discernens*, E with *mundana*, T with *insinuet*, I with *expetentibus* ... and so on. At last you get a very long fake message, so beginning:

> *Conditor clemens discernens mundana, insinuet expetentibus amoenitatem seraphicam [...]*

The message has the look of an innocuous religious sermon, and the rascal will bring it, without suspicion of his real content.

The cipher is very bulky, in this example it generates a fake text of ten lines for a single line of plain text, and has the defect that whoever knows the book could easily decipher the fake text, while to write a new fake book is a huge task. Indeed Trithemius was well aware of this and recommended to rewrite the book shuffling the word

[12]Six books of polygraphy(Trithemius, 1508).

[13]I don't know when and why this cipher received the name of *Ave Maria*; Trithemius and Vigenère do not use it. In Liber II there is the sequence of words *Ave Maria gratia plena ...*, maybe it comes from here.

[14]See also (Kahn, 1996), pp. 133-135 and (Schmeh, 2017).

[15](Trithemius, 1508) p.55

[16]English: Beware of this man, because he is a thief, and the worst criminal

of every column. Not a light task, to rewrite and shuffle 384 pages!

Trithemius himself writes that one can get more comfortable ciphers renouncing the "without suspicion" condition; and the following ciphers do this up to the *Recta Tabula* that again proposes an ordered list of alphabets, this time encrypted with single alphabet letters shifted; *Polygraphia* ends with the simplest polyalphabetic cipher, opening the route to Vigenère's table.

Partenio's superencryption closely resembles this *Ave Maria* cipher of Trithemius. Indeed there are differences: Trithemius uses a 24 letter alphabet, Partenio reduces it to a 10 digits one; this should make things easier when trying to assemble plausible text binding together the single pieces. Trithemius has a 384 alphabets repertory, while Partenio has only 9 or 15, but of course it could be enlarged at will by the user.

Did Partenio know Trithemius's work? Among the papers kept in the Venetian Archives, Trithemius is repeatedly mentioned. Agostino Amadi in his treatise[17] ridicules this cipher writing:

> *Il Tritemio abbate che tra sinonimi [...] con tanta fatica, tanto perdimento di tempo, tanto logoramento di carta [...] nascondeua breue et minima cosa.* [18].

Surely Partenio knew Amadi's treatise and maybe his goal was to improve Trithemius's idea, with less effort and less waste of time and paper; besides he was a notary used to write deeds in Latin, so he could read the book without any difficulty. So it is very likely that the first idea came to him from Trithemius.

6.2 The Cipher of Francis Bacon

The second possible link is with Bacon's cipher; Francis Bacon is best known as a philosopher and statesman but he gained a place in the history of cryptology also, because of this cipher.

In his book *De dignitate et augmentis scientiarum*[19] he presented this curious cipher[20] producing common language message, a message "without suspicion". He wrote to have conceived the cipher when he was young (*adoluscentuli*) in Paris, during his tour in Europe between 1576 and 1579.

The first step was a MASC cipher where single letters were encrypted with a five letter group using only two letters, **a** and **b**; the 24 letters of the XVII century English alphabet are so encrypted:

A	aaaaa	B	aaaab	C	aaaba	D	aaabb
E	aabaa	F	aabab	G	aabba	H	aabbb
I	abaaa	K	abaab	L	ababa	M	ababb
N	abbaa	O	abbab	P	abbba	Q	abbbb
R	baaaa	S	baaab	T	baaba	V	baabb
W	babaa	X	babab	Y	babba	Z	babbb

Nowadays we can say that using 0 and 1 instead of a and b, these are the binary numbers from 0 to 23. By the way, the binary notation was introduced by Leibniz in 1703.

Once a message is encoded this way you get a sequence of **a** and **b**. Bacon's idea is to print a generic text using two distinguishable fonts, e.g. serif and sans serif, the first for each **a**, the second for each **b**. If the two fonts are not very different in size and look, you get an innocuous message, and one can not guess it hides another secret message.

Of course an expert eye could notice the diverse fonts distributed in such a strange way, and suspect something ... and the cipher is no more without suspicion.

And, again, the message will be much longer than the plain text, here five times longer.

Partenio's *altro senso* variant closely resembles Bacon's cipher; instead of two different fonts, it uses the ligature vs. non ligature difference to encode the message; in either case, it is a font matter. Is it a mere coincidence? Here the relationship is much more unlikely than for the Trithemius's case. Indeed the English version of Bacon's book[21] was published in 1605, but had only a short chapter about ciphers, and no mention of this cipher, which was added to the Latin translation of 1624[22], 18 years after Partenio's hand-

[17]This 700 handwritten pages treatise (Amadi, 1588) was recovered by the CX after Amadi's death in 1588, and is still kept in the Venetian Archives; the book in ten volumes was his textbook for teaching cryptography and cryptanalysis to the future deputies for ciphers.

[18]English: "Abbot Trithemius among synonymous [...] with so much effort, so much waste of time, so much wear of paper [...] was hiding a short and minimum thing"

[19]The book was first published in English in 1605, with the title "Of Proficience and Advancement of Learning Divine and Human" and later translated into Latin with the cited title; the English text had only a short chapter about ciphers, while in the Latin version he presented this cipher in detail.

[20]See first of all (Bacon, 1624) as the primary source and other books dealing with this cipher:(Fouche, 1939) p. 6, (Kahn, 1996), p. 882 or (Schmeh, 2017), p. 62.

[21](Bacon, 1605).

[22](Bacon, 1624).

book; so a link between Partenio and Bacon looks problematic. Maybe there was a common origin.

6.3 Vigenère

A possible common root is Vigenère and his treatise. There he proposed a 3 letters substitution cipher, where a letter say A can be substituted by a group of three letters *a b c*[23], while Bacon used only two letters. A few pages after, Vigenère writes that one can use a single letter in different fonts, without producing non suspicious texts, for example a very suspicious sequence of **o** and *o*[24]. Vigenère does not use a second step (superencryption) here.

Vigenère in his treatise was rather skeptical about Trithemius and similar ciphers, writing[25]:

> Mais cela est trop laborieux et bien rarement se peuuent rencontrer des mots, nompas seulement des syllabes bien propres, pour remplir la suitte & le contexte de l'oraison, qu'on ne s'appercuie de l'artifice [...][26]

A few lines after, to show that anyway this artifice can be actually used, Vigenère reports that when he was in Venice in 1569, he learned that a similar cipher was proposed to the Venetian Baylo[27] by the physician Lorenzo Ventura to get around the bans by Sultan Selim II to write encrypted messages.

Indeed in the Venetian archives the dispatches of the Baylo in the years from 1566 and 1569 were mostly encrypted with a classical nomenclator, as usual, while one finds several dispatches having parts written using invisible inks [28]. Was this the way to evade Selim's prohibitions, as proposed by Ventura, who wrote a book on medicine and chemistry, not on cryptography? Did Vigenère misunderstand the whole affair? The question remains open, a letter written with steganographic methods is difficult to locate.

[23]See (Vigenere, 1586), ff. 200-201

[24]See (Vigenere, 1586) f. 243r

[25](Vigenere, 1586), p. 182.

[26]English: But this is too demanding and very rarely can words be found, not only fitting syllables, to fit the text and the context of the prayer, without revealing the artifice.

[27]Baylo or Bailo was the name traditionally given to the Venetian ambassador in Constantinople.

[28]The Baylo, Giacomo Soranzo had a severe reproach from the CX for using lemon juice as an invisible ink, which was a very dangerous practice, since the expedient was also known to the Turks. But more sophisticated invisible inks were used by the Venetians. See (Preto, 1994), p. 281.

More interesting: did Vigenère have contact with Venetian cipher deputies that year? And did Bacon meet Vigenère in Paris during his journey a few years after? Again we are in the realm of conjectures.

7 Conclusion about the Origins

This cipher of Partenio is in no way revolutionary, and looks at the same time ingenious and problematic to use. Indeed it is the result of joining a classical nomenclator and a *Ave Maria* like superencryption, while the *altro senso* ligature vs. non ligature method was maybe his own invention with some possible some root in Vigenère's treatise or, much less likely, from Bacon.

What Partenio and Bacon have in common is a two step encryption, producing common language text, the first step being a substitution (cryptography), the second a kind of steganography.

So, we can call this cipher a crypto-steganographic one.

8 Can such a Cipher be used Today?

This cipher has many limits: slow and clumsy like other steganographic methods, it would require a much larger phrasebook (well more than 9 or 15 pieces of phrases), and a fastest way to encode the text.

As already stated above, for this reason steganography was largely neglected and left to amateurs. In 1939 Helen Fouché Gaines wrote at the end of her short chapter about steganography:[29]:

> Concealment cipher has, of course, the unique virtue of being able to convey message under circumstances which make it seem that no communication has passed [...] But we rather suspect that, for the end desired, invisible inks are more convenient and practical.

As we have seen above, invisible inks were used by Venetians, and apparently several messages went unnoticed.

But nowadays in the computer era, the above mentioned problems can be easily overcome. And steganography is again used, in upgraded forms. Secret messages or, worse, secret malicious software can be hidden in a graphic image using a

[29](Fouche, 1939) p. 6

few pixel, very difficult to spot among millions, or even the Exif data of the jpeg format or other tricks. There are so many bits in an image!

So, why not to implement a Partenio like steganography software producing fake text hiding, without suspicion, secret messages?

Of course this is possible and rather easy to do, as it is the case for many others historical ciphers. Figure 6 and 7 show the output of a software designed for this purpose[30]. Moreover, it is possible to do much better, have a much larger phrasebook, even a Trithemius phrasebook can be stored in a few kilobytes, encrypt and decipher in a matter of seconds what in the past required hours.

Problem number one is to find a safe way to exchange the keys. In this case the nomenclator and the phrasebook are clumsy, huge if you make a Trithemius like phrasebook, but a modern database has room for much larger keys, and modern cryptographic methods like RSA may be used to exchange the key.

Problem number two is more serious; is it possible to implement a software that will produce absolutely plausible, enough long and non suspect texts?

Problem number three: does such a thing make sense, when we have already powerful tools to transmit message in a secret and safe way?

As for the *altro senso* variant, it seems madness, but of course it is possible using fonts making ligature possible, like the *Calligra* used for the above examples. And problem number three remains unchanged.

9 Acknowledgments

A special thank goes to Giovanni Caniato and all the other archivists of the *Archivio di Stato di Venezia* for assistance and help in recovering Partenio's papers, and to Antonio Giovanni Colombo for reviewing the English text.

References

Agostino Amadi. 1588. *Trattato delle cifre*. Digitized manuscript in ASVe, Inquisitori di Stato, Codice Amadi, Venezia.

Francis Bacon. 1605-1901. *Of Proficience and Advancement of Learning Divine and Human*. London.

Francis Bacon. 1624. *De dignitate et augmentis scientiarum*. London

Paolo Bonavoglia. 2020. *The cifra delle caselle a super-encrypted XVI century cipher*. Cryptologia, Vol.44-1.

Paolo Bonavoglia. 2019. *Hieronimo di Franceschi and Pietro Partenio, two unknown Venetian cryptologists*. Proceedings of the HistoCrypt 2019 Linkoping University Electronic Press, Sweden.

Helen Fouché Gaines. 1939, 1956. *Cryptanalysis a study of ciphers and their solution*. American Photographic Publishing Co. Dover, New York.

David Kahn. 1996. *The Codebreakers*. Scribner, New York.

Pietro Partenio. 1592, 1593. *Seven cipher offered to the Council of Ten*. Manuscript in ASVe, CX Raccordi 1.

Pietro Partenio. 1606. *Handwritten booklet*. Manuscript in ASVe, CX chiavi e scontri di cifra, b.2, f.14.

Luigi Pasini 1872, 2019. *Delle scritture in cifra usate nella Repubblica di Venezia*. Aracne, Roma, 2019.

Paolo Preto 1994-1999. *I servizi segreti di Venezia*. EST, Milano, 1999.

Klaus Schmeh. 2017. *Versteckte Botschaften*. Scribner, New York.

Joannes Trithemius. 1508. *Libri Polygraphiae VI*. Argentorati (Strasbourg), 1613.

Blaise de Vigenère. 1586. *Traictè des chiffres, ou Secrètes manières d'escrire*. Abel L'Angelier, Paris.

[30] The software written in PhP/MySQL was useful also to test the cipher. It works fine, within the size limits mentioned above.

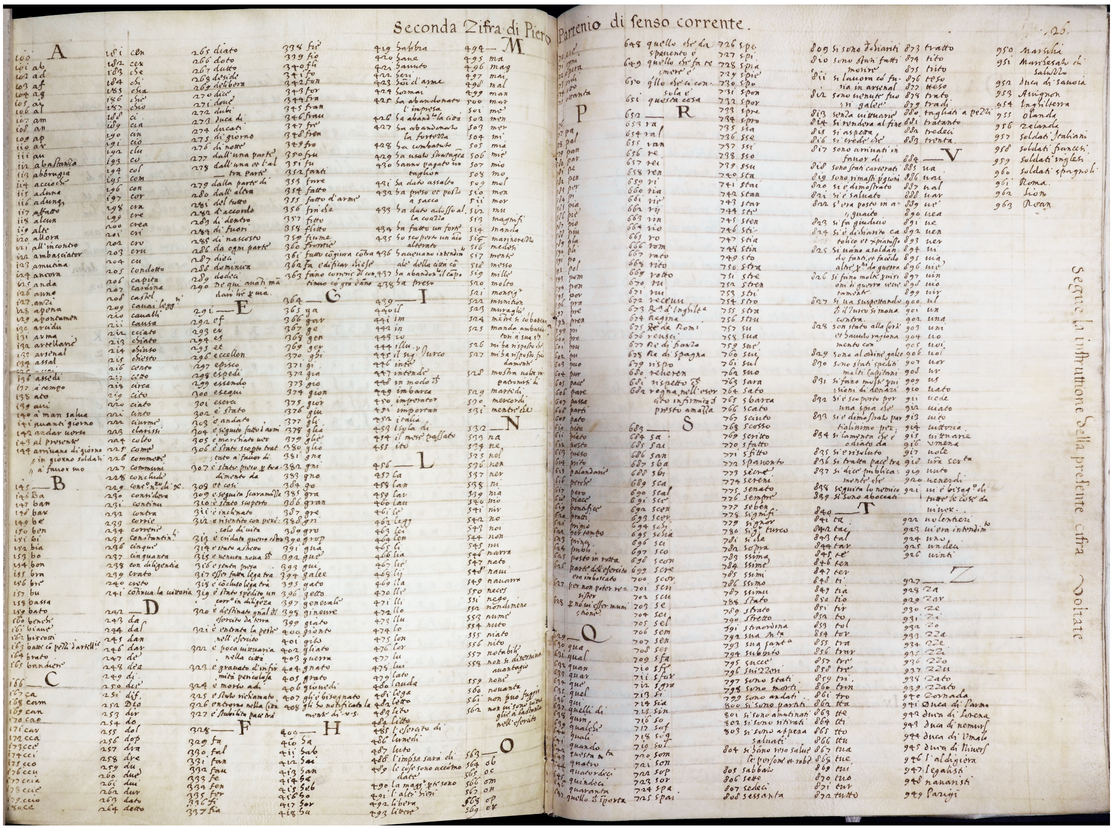


Figure 1: Partenio's 1592 three digits nomenclator. *ASVe CCX Raccordi 1*

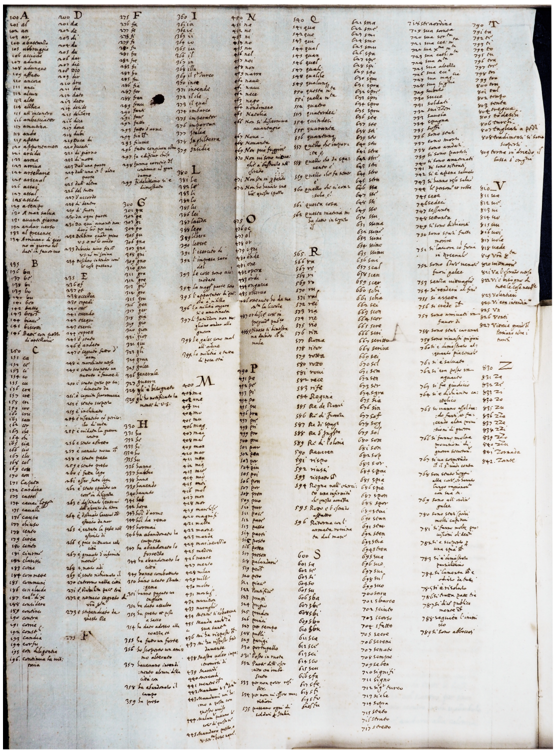
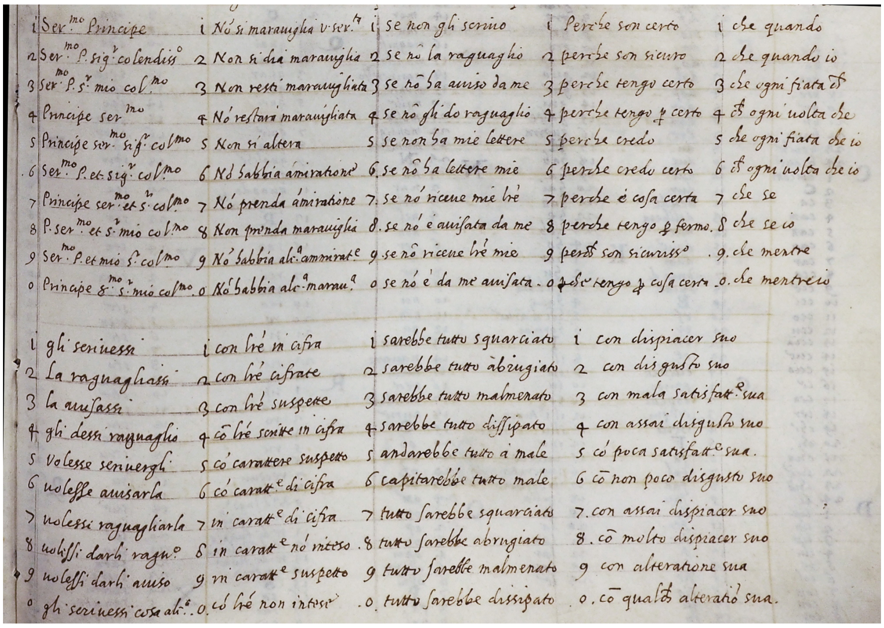


Figure 2: Partenio's 1606 three digits nomenclator. *ASVe CX Cifre, chiavi e scontri di cifra con studi successivi, busta 2 fasc. 14*.



1 Ser.mo Principe	1 Nó si marauiglia V. Ser.tà	1 se non gli scriuo	1 Perche son certo	1 che quando
2 Ser.mo P. sig.r colendiss.o	2 Non si dia marauiglia	2 se nó la raguaglio	2 perche son sicuro	2 che quando io
3 Ser.mo P. S.r mio col.mo	3 Non resti marauigliata	3 se nó ha auiso da me	3 perche tengo certo	3 che ogni fiata che
4 Principe ser.mo	4 Nó restarà marauigliata	4 se nó gli do raguaglio	4 perche tengo per certo	4 che ogni uolta che
5 Principe ser.mo sig.r col.mo	5 Non si altera	5 se non ha mie lettere	5 perche credo	5 che ogni fiata che io
6 Ser.mo P. et sig.r col.mo	6 Nó habbia amiratione	6 se nó ha lettere mie	6 perche credo certo	6 che ogni uolta che io
7 Principe ser.mo et s.r col.mo	7 Nó prenda amiratione	7 se nó riceue mie lre	7 perche è cosa certa	7 che se
8 P. ser.mo et s.r mio col.mo	8 Non prenda marauiglia	8 se nó è auisata da me	8 perche tengo per fermo	8 che se io
9 Ser.mo P. et mio S.r col.mo	9 Nó habbia alc.a ammirat.e	9 se nó riceue lre mie	9 perche son sicuriss.o	9 che mentre
0 Principe & s.mo S.r mio col.mo	0 Nó habbia alc.a maraui.a	0 se nó è da me auisata	0 perche tengo per cosa certa	0 che mentre io
1 gli scriuessi	1 con lre in cifra	1 sarebbe tutto squarciato	1 con dispiacer suo	
2 la raguagliassi	2 con lre cifrate	2 sarebbe tutto abrugiato	2 con disgusto suo	
3 la auisassi	3 con lre suspette	3 sarebbe tutto malmenato	3 con mala satisfatt.e sua	
4 gli dessi raguaglio	4 cō lre scritte in cifra	4 sarebbe tutto dissipato	4 con assai disgusto suo	
5 volesse scriuergli	5 cō carattere suspetto	5 andarebbe tutto à male	5 cō poca satisfatt.e sua	
6 uolesse auisarla	6 cō caratt.e di cifra	6 capitarebbe tutto male	6 cō non poco disgusto suo	
7 uolessi raguagliarla	7 in caratt.e di cifra	7 tutto sarebbe squarciato	7 con assai dispiacer suo	
8 uolessi darli ragu.e	8 in caratt.e nó inteso	8 tutto sarebbe abrugiato	8 cō molto dispiacer suo	
9 uolessi darli auiso	9 in caratt.e suspetto	9 tutto sarebbe malmenato	9 con alteratione sua	
0 gli scriuessi cosa alc.a	0 cō lre non intese	0 tutto sarebbe dissipato	0 cō qualche alteratiō sua	

Figure 3: The phrasebook of the 1592 CCX cipher, *ASVe CCX Raccordi 1*

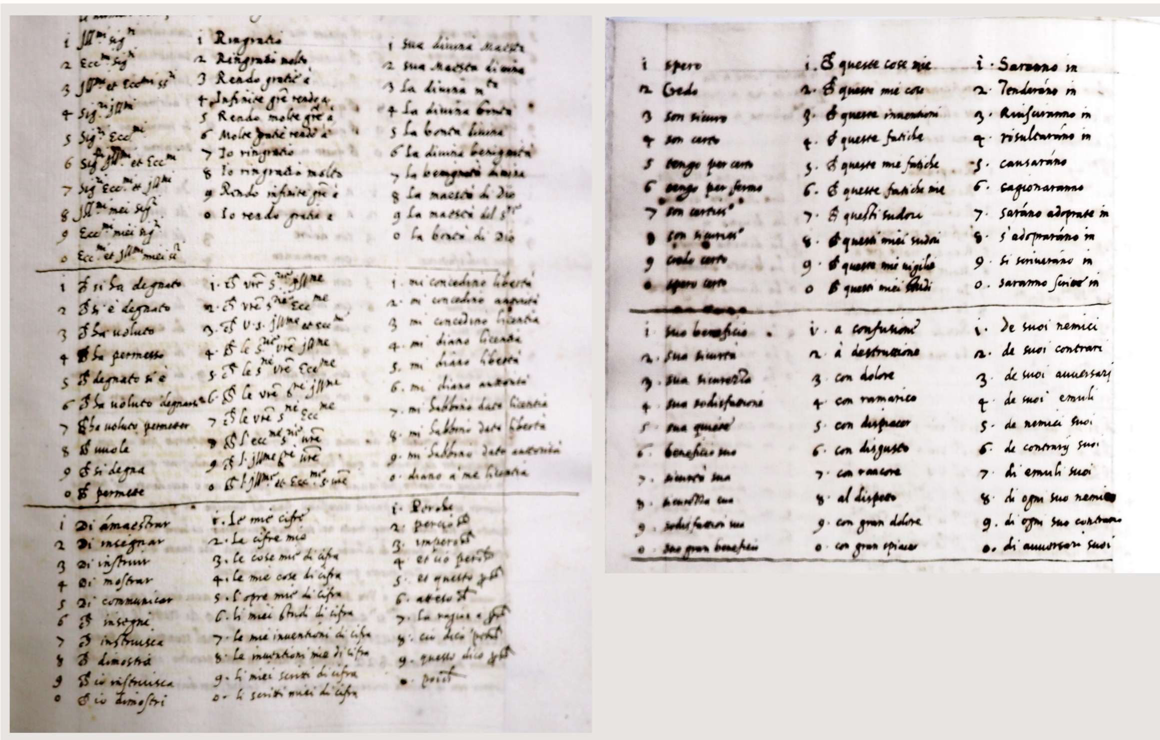
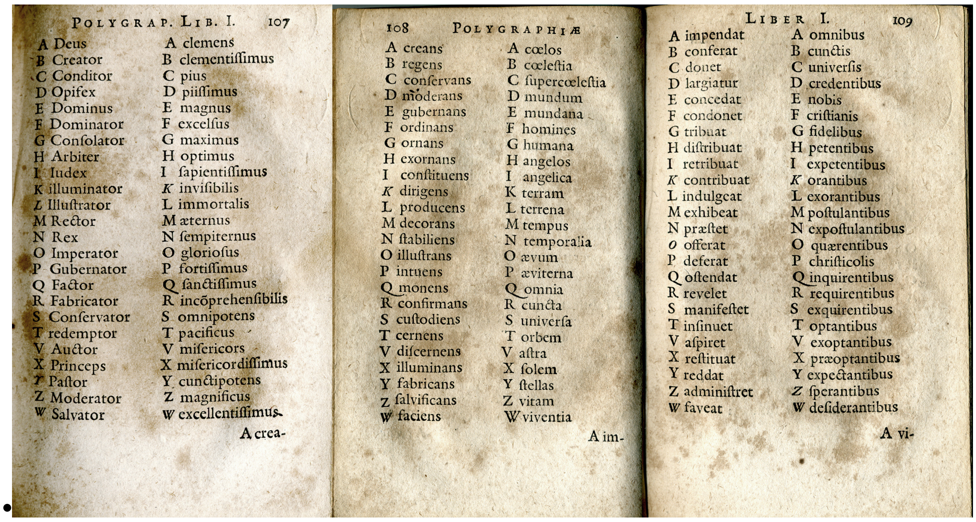


Figure 4: The phrasebook of the 1606 booklet cipher. *ASVe CX Cifre, chiavi e scontri di cifra con studi successivi, busta 2 fasc. 14.*



POLYGRAP. LIB. I. 107

A Deus	A clemens
B Creator	B clementiſſimus
C Conditor	C pius
D Opifex	D piiſſimus
E Dominus	E magnus
F Dominator	F excelſus
G Conſolator	G maximus
H Arbiter	H optimus
I Iudex	I ſapientiſſimus
K illuminator	K inviſibilis
L Illuſtrator	L immortalis
M Rector	M æternus
N Rex	N ſempiternus
O Imperator	O glorioſus
P Gubernator	P fortiſſimus
Q Factor	Q ſanctiſſimus
R Fabricator	R incõprehenſibilis
S Conſervator	S omnipotens
T redemptor	T pacificus
V Auctor	V miſericors
X Princeps	X miſericordiſſimus
Y Paſtor	Y cunctipotens
Z Moderator	Z magnificus
W Salvator	W excellentiſſimus.

A crea-

108 POLYGRAPHIÆ

A creans	A cœlos
B regens	B cœleſtia
C conſervans	C ſupercœleſtia
D mõderans	D mundum
E gubernans	E mundana
F ordinans	F homines
G ornans	G humana
H exornans	H angelos
I conſtituens	I angelica
K dirigens	K terram
L producens	L terrena
M decorans	M tempus
N ſtabiliens	N temporalia
O illuſtrans	O ævum
P intuens	P æviterna
Q monens	Q omnia
R confirmans	R cuncta
S cuſtodiens	S univerſa
T cernens	T orbem
V diſcernens	V aſtra
X illuminans	X ſolem
Y fabricans	Y ſtellas
Z ſalvificans	Z vitam
W faciens	W viventia

A im-

LIBER I. 109

A impendat	A omnibus
B conferat	B cunctis
C donet	C univerſis
D largiatur	D credentibus
E concedat	E nobis
F condonet	F criſtianis
G tribuat	G fidelibus
H diſtribuat	H petentibus
I retribuat	I expetentibus
K contribuat	K orantibus
L indulgeat	L exorantibus
M exhibeat	M poſtulantibus
N præſtet	N expoſtulantibus
O offerat	O quærentibus
P deferat	P chriſticolis
Q oſtendat	Q inquirentibus
R revelet	R requirentibus
S manifeſtet	S exquirentibus
T inſinuet	T optantibus
V aſpiret	V exoptantibus
X reſtituat	X præoptantibus
Y reddat	Y expectantibus
Z adminiſtret	Z ſperantibus
W faveat	W deſiderantibus

A vi-

Figure 5: The first three pages of Trithemius's *Ave Maria* cipher.

è uenuta noua che 315	Re di Spagna 678	è risentito con pericolo di uita 312
Ser.mo P. S.r mio col.mo non si marauiglia se non ha mie lettere	perché credo certo che se gli dessi raguaglio	con lettere suspette sarebbe tutto squarciato con disgusto suo

Figure 6: Partenio's example, encrypted by a software

<table>
<tr><td>Ser.mo P. S.r mio col.mo
3</td><td>non si marauiglia
1</td><td>se non ha mie lettere
5</td><td>perché credo certo
6</td><td>che se
7</td><td>gli dessi raguaglio
8</td><td>con lettere suspette
3</td><td>sarebbe tutto squarciato
1</td><td>con disgusto suo
2</td></tr>
<tr><td colspan="3">315
è uenuta noua che</td><td colspan="3">678
Re di Spagna</td><td colspan="3">312
è risentito con pericolo di uita</td></tr>
</table>

Figure 7: The same example deciphered by software