The enigma of Lorenzo Ventura's cipher

Paolo Bonavoglia
paolo.bonavoglia@liceofoscarini.it
Former teacher, webmaster
at the "Convitto-Liceo Marco Foscarini"
I 30121 Venice / Cannaregio 4942

Abstract

The aim of this research was to find the algorithm used in the ciphers mentioned by Blaise de Vigenère in his treatise, where he states that in 1569, while in Venice, he learned about a steganographic cipher by a certain Lorenzo Ventura, similar to Tritemio's *Ave Maria*. It had been used by the bailo in Constantinople after Sultan Selim II prohibited him from writing his dispatches in cipher. Now that a collection of letters, notes, and handwriting examples belonging to Ventura has been found in the State Archives of Venice, initial findings emerge that confirm, at least in part, Vigenère's claims.

.

1 Introduction. Vigenère wrote ...

In 1569 Blaise de Vigenère was in Venice as an officer of the French embassy, and in his *Traicté des chiffres*[1] wrote[2]:

> In the year 1569, I was in Venice, the Turk Selim father of Amurath who reigns today, secretly making his preparations to invade the kingdom of Chippre; for fear that the Bayle of the Venetians residing in Constantinople, should not inform them of what could be foreseen, forbade that they no longer had to write by any sort of cipher, as well as in all patent and open packages, & in intelligible letter: while some people found themselves in difficulty, a doctor named Lorenzo Ventura introduced himself, who presented them with the following secret; to write whatever they wanted, especially all kinds of remarks, and in common writing, which had another meaning hidden underneath, as they pleased, subject to certain very advantageous conditions which he paid for his salary. What I wanted to allege to show what esteem and importance it is is artifice.

It is clear that Vigenère is describing a steganographic cipher, citing Trithemius Polygraphiae[3] and the Ave Maria cipher[4]. as the source for the *Ave Maria* cipher. However, a search of the Venetian archives reveals that soon after the sultan banned ciphers in 1567, the baylo Giacomo Soranzo wrote very brief dispatches with a long postscript in red ink[5]. Soranzo, in fact, used lemon

[1] (de Vigenère, 1587) p. 183.

[2] Ibidem, p.183; translated from the French original, 1587: *L'An 1569. que i'estois à Venise, le Turc Selim pere d'Amurath qui regne auiourd'huy, faisant sourdement ses apprests pour enuahir le royaume de Chippre; de peur que le Bayle des Venitiens residant à Constantinople, ne les aduertist de ce qu'il en pouuoit pressentir, defendit qu'ils n'eussent plus à fentr'escrire par aucune sorte de chiffre, ains à pacquets tous patents & ouuerts, & en lettre intelligible : de eproyeux se trouuans en peine, se presenta vn medecin nommé Lorenzo Ventura, qui leur presenta le secret cy dessus; d'escrire tout ce qu'ils voudroienr, surtoutes sortes de propos, & en escriture commune,qui eust autre sens caché audessous, tel leur plairroit, moyennant certaines conditions bien aduantageuses qu'il demâdoit pour son salaire. Ce que i'ay bien voulu alleguericy pour monstrer de quelle estime & importance est cest artifice*

[3] (Trithemius, 1613). Polygraphiae VI is the main work of Abbot Tritemio, also known as Johannes Trithemius (1462-1516), considered one of the founding fathers of modern cryptography. His first work, titled Steganographia, was the first cryptography book published in print, but accused of witchcraft, it was condemned by the Church and placed on the index of prohibited books, where it remained until 1900. Tritemio's most well-known ciphers are the Ave Maria and the Recta Tabula, of which something will be said in this article.

[4] Trithemius did not use the name *Ave Maria* for his cipher, a nickname that was introduced much later.

[5] *ASVe CCX Dispacci degli ambasciatori a f.2 3-6-1567* In the following these archive abbreviations are used: *ASVe*

juice as invisible ink, a method for which he was severely reprimanded by the Council of Ten[6] because the method was known even to the Turks. Among the archive papers, one finds a draft letter by the Council addressed to Selim, rejecting his ban using subtle arguments. It is not certain whether the letter was actually sent; however, Soranzo's dispatches reverted to being encrypted as before.

Perhaps Vigenère had misunderstood? It remained doubtful whether one of Ventura's ciphers had been employed at any time. It is obvious that a steganographic text, by its very nature, can be very difficult to detect, if used correctly, and Vigenère provides no details about this cipher.

2 Ventura's papers

A necessary premise: Ventura calls *manifesto* or *palese* the text that is visible and meaningful but hides a secret message. The real message is called "secreto" (secret). *Scontro* is a cipher sheet, *contrasegno* is a keyword or key-phrase.

These papers were found in *busta* 6 of the State Archives of Venice collection named *Cifre, chiavi e scontri di cifra* . . . , in a fascicle named *Lorenzo Ventura fisico*[7].

At the beginning of this file, we find a letter in which Ventura presents to the Council of Ten a new method of writing in code that is articulated in various ways, as we will see later on. He boasts that his ciphers cannot be decrypted without the most profound artifice of the various *scontri* (key sheets) and *contrasegni* (keywords or keyphrases) of his.

We will now see three examples of different modes, without instructions.

3 Example n.1

Among the sheets of this file we find one with this introduction[8]:

> A very easy and convenient method, which requires no keyword or keyphrase, but only the first and second letter of one's own name, or of the one who writes, or to whom it is written, and thus the first or last characters of the plaintext, and the entire complete phrase if desired. Indeed, the composition is somewhat forced because it is formed like that of the *caselle*. But what is of greater importance is that no perforated paper is required; everything necessary is provided . . .

The word *caselle* brings to mind Hieronimo di Franceschi's *cifra delle caselle*[9], a cipher that utilized small windows for arithmetic encryption and decryption operations. However, Ventura's method, mentioned in 1567, appears to differ significantly. It is more likely referring to Cardan's grid, also known as Richelieu's grid[10]. Both systems employed small windows cut out of cardboard to write the message inside. After removing the cardboard, the remaining space was filled with additional text to make the message appear plausible, and even misleading.

Indeed, at first glance, the first example looks like a Cardan's grid without a grid; the words of the true and secret text are hidden between the words of the *manifesto* i.e., the false text, as seen in Figure 4.

The first segment of the secret text *L'armata nemica è già ritornata* is hidden in the manifest in the middle, the following segments of the secret

= *Archivio di Stato di Venezia, CX = Consiglio dei Dieci; CCX = Capi del Consiglio dei Dieci*The *Consiglio di Dieci* = Council of Ten was a powerful organ of the Republic of Venice, responsible for state security, intelligence and also for cryptography.

[6]The letter is in *ASVe CX Parti Secrete filza 12 3-4-1567*

[7]Here *fisico* should be understood as physician, not physicist. Lorenzo Ventura is mentioned in Paolo Preto's book (Preto, 1994) on page 272. Preto's book, *I servizi segreti di Venezia*, focused on secret services and intelligence, with only a chapter dedicated to cryptography. It is rich in citations and references to the Venice Archives collections, but provides fewer details on cryptographic technicalities. There are few works specifically dedicated to Venetian cryptography, including essays by Predelli (Predelli, 1869) and Cecchetti (Cecchetti, 1869), Pasini's booklet (Pasini, 2019), which was republished in 2019 under my editorship, and Meister's chapter on Venetian ciphers (Meister, 1902), which is undoubtedly valuable from a cryptographic perspective. It is unfortunate that Meister's research only reaches up to the year 1550 and does not mention Ventura.

[8]English translation; here is the original 16th century Italian: *Modo facilissimo, et comodo, che non ha bisogno alcuno di scontro, ouer contrasegno, ma è basteuole la prima et seconda litera solamente del proprio nome di coluj che scriue, ouer a chj vien scritto, et così li primj , o ultimj caratterj del palese, et tutta la integra dicione se si vuole. Ben è uero che la composicion è alquanto forzata perciò che è formata come quella delle caselle. Ma quello che è di maggior importanza non ui si ricerca carta sbusata, ma qui u'è tutto quel che fa di mestierj nell'occorrenze sue.*

[9]For more information about this cipher, see (Bonavoglia, 2019) and (Bonavoglia, 2023), p. 166.

[10]See (Kahn, 1996) p.144-145. Original is in (Cardanus, 1553)

text are also confused, apparently in random order.

What is yet to be understood is how the sender could let the recipient know how and where to find the right windows. To locate them, a number could be used for the location of each window. How can the recipient know the location of the words or letters in the secret text? Clearly, this information should be present in the keyword, which in this case is the last word of the overt message, *satisfacione*. So, this word should contain information about the location of the virtual windows, but how?

4 Example n.2

As a second example, we see, in Figure 5, a very short message and a corresponding ciphertext (above, Manifesto).

It is immediately noticeable that there is no trace of the words of the secret text in the manifest message. So it must be a system that uses single letters instead of words.

Indeed, looking in the *manifesto* for the letters of the secret message we find them in good order, marked bold in the figure, until the letter ***m***; now after ***m*** we expected a ***p*** like in *tempo* but the only ***p*** in the manifesto is in the first line in *per*. Of course this is not the way.

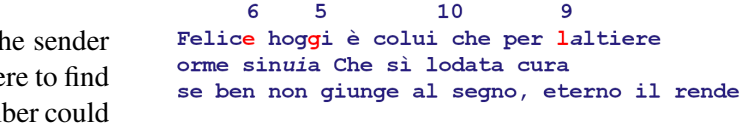
And how was the sender supposed to communicate the position of the first letter of the secret, and the one of the next letter and so on?. The keyword (contrasegno) here *FELICE* should contain this information in some way.

The first simple conjecture is that a letter of the key means a number, the ordinal inside the alphabet, so:

F	E	L	I	C	E
6	5	10	9	3	5

where 6 could mean sixth letter from the beginning, 5 mean the fifth letter from here, and so on.

Now, this rule initially works fine: the sixth letter is **E**, the following fifth is **G**, the following tenth is a space, and the following ninth is **L**. So far, we have **EGL**. By counting spaces as well as letters, this forms the beginning of the secret message, although the spaces should be ignored when completing the plaintext. However, in the subsequent part of the cryptogram, this rule no longer applies. Therefore, there seems to be something wrong; it's likely just a coincidence, and the general rule remains unknown



5 Example n.3

This example, visible in Figure 6, was the most puzzling of the three. Ventura boasted that he could reduce the secret message to a much shorter one, which is the opposite of what usually happens in steganography, where the ciphertext is often longer, sometimes much longer, than the original message. In this case, an Italian text of 977 characters is compressed into a Latin text of 32[11] words, totaling 206 characters, with a compression ratio of 4.7. While a Latin text is typically shorter than its Italian equivalent, it's rarely to such an extent. Modern compression algorithms can achieve similar ratios, but the resulting compressed file is usually a sequence of bits rather than a text readable in any known language.

And so the suspicion arises that Ventura invented a method or algorithm specifically tailored for this message. In other words, a method that does not apply to just any text, which is a prerequisite for any form of communication.

One of the most efficient compression algorithms used today involves converting the sequence of bits into a single number using a base much greater than 2. For example, the decimal number 10000, in base 2, is represented as 0010 0111 0001 0000, which is much bulkier; in hexadecimal, it's represented as 2710, which is more compact. With larger bases, the representation becomes increasingly compact. Of course, for this method to work, both correspondents must know the number N used as the base, as well as all the N signs used.

These considerations reminded me that algorithms of this type were well known and used since the 15th century: syllabaries and dictionaries, used by most nomenclators, were useful also to shorten the length of a message and the time necessary to write it, using an enlarged alphabet, one that had also tens of syllables and hundreds of words. They were naive compression algorithms after all.

On the contrary, Trithemius' *Ave Maria*[12] de-

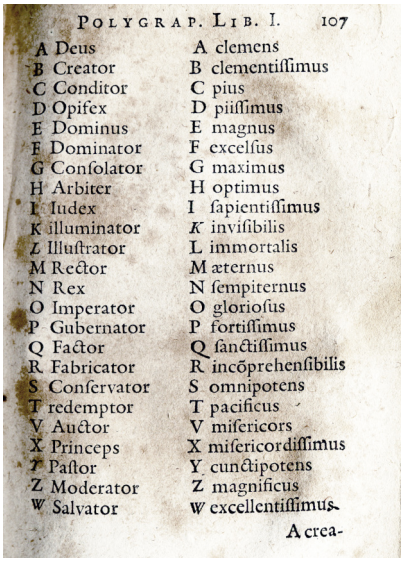
[11] Indeed, there are 31 clearly visible words and a closing sign barely readable; in the following, I assume 32.

[12] See (Trithemius, 1613) p. 107. The name *Ave Maria* is

scribed in the next paragraph, was well known and often ridiculed as a waste of paper and time. However, if used in reverse, could it significantly reduce the size of the message?

Is it possible that Ventura employed a reverse *Ave Maria*?

This idea may seem absurd for many reasons, yet it aligns remarkably well with this example, not to mention what Vigenère wrote in his treatise


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-

Figure 1: The first page of the *Ave Maria* with two alphabets.

Firstly, for readers unfamiliar with this cipher, let's provide a brief explanation starting from Figure 1, where the first two alphabets of 24 letters appear[13]. In Trithemius' book, there are hundreds of such alphabets to cover messages of equivalent lengths. Each character is encrypted with a word chosen sequentially from the corresponding alphabet[14]. For instance, if the first character is **T**, the next word in the sequence is *Redemptor*, which becomes its cipher. Similarly, if the second character is **R**, the next word is *Redemptor*, resulting in a ciphertext beginning like this: *Redemptor excelsus*. Eventually, the ciphertext resembles a sermon or prayer[15], appearing unsuspected to any potential intercepting spy. Each alphabet provides roughly 24 interchangeable words, ensuring the creation of plausible texts such as sermons and prayers.

After examining the three components of the example—the fake Latin text, the key, and the true text in Italian—the broad outline method attributed to Ventura emerges as follows[16]:

1. Encrypt each word (or group of words) of the secret plaintext into letters of the alphabet, using a reverse *Ave Maria* in Italian.

2. Encrypt each single letter and the corresponding letter of the keyword into another letter, using a polyalphabetic cipher like Bellaso's or Recta Tabula with a *Bellaso contrasegno*[17].

3. Encrypt each letter obtained in the previous step into a word, using a cipher like *Ave Maria* in Latin.

A first way to synthesize this method is to use mathematical symbolism: let A be an *Ave Maria* enciphering function to substitute an Italian word (or group of words) x with a single letter a, and A^{-1} its inverse; let P be the polyalphabetic cipher that transforms a letter of the alphabet into another from the same alphabet; let B be another *Ave Maria* cipher in Latin. Finally, we have the formula:

$$y = B(P(A^{-1}(x)))$$

A second way is to use a flow-chart like diagram like the following:

never used by Trithemius but was introduced much later.

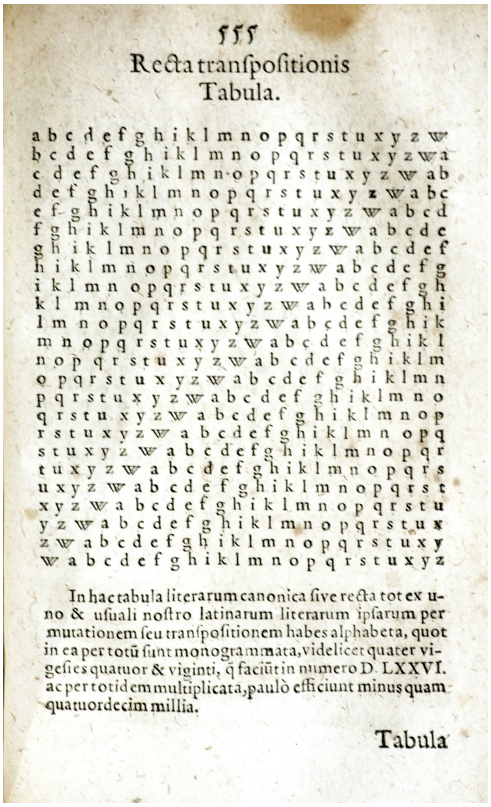
[13]This alphabet was used at the time for the German language: ABCDEFGHIKLMNOPQRS TVXYZW. Note that **W** is the last letter after Z, presumably added recently.

[14]It's important to emphasize that *Ave Maria* corresponds to a polyalphabetic cipher, meaning it's a one-to-one relation, not a one-to-many relation as sometimes misconceived. In fact, the encryption function takes as input not only the letter or word to be encrypted but also, essentially, the ordinal number n of the alphabet used, and outputs the encrypted letter or word, as well as the ordinal number of the alphabet to be used in the next step, which here is simply $n+1$ but could also be interpreted differently. Thus, both the procedure for encrypting and that for decrypting are unambiguous.

[15]Hence the name *Ave Maria*, as mentioned earlier.

[16]A very similar outline is found in one of the *Falso Scontro* cipher variants by Hieronimo di Franceschi, see (Bonavoglia, 2022), the most prominent secretary of ciphers in the late 1500s. Did Franceschi, who was about 30 years old, know Ventura or read his papers?

[17]I did not refer to it as Vigenère's tableau (see the original in French (de Vigenère, 1587) p. 50, and (Kahn, 1996) p. 149) because Vigenère published it in 1586-87, two decades later!.



fff

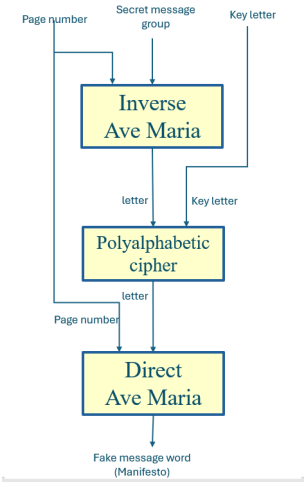
Recta tranſpoſitionis Tabula.

a b c d e f g h i k l m n o p q r s t u x y z w
b c d e f g h i k l m n o p q r s t u x y z w a
c d e f g h i k l m n o p q r s t u x y z w a b
d e f g h i k l m n o p q r s t u x y z w a b c
e f g h i k l m n o p q r s t u x y z w a b c d
f g h i k l m n o p q r s t u x y z w a b c d e
g h i k l m n o p q r s t u x y z w a b c d e f
h i k l m n o p q r s t u x y z w a b c d e f g
i k l m n o p q r s t u x y z w a b c d e f g h
k l m n o p q r s t u x y z w a b c d e f g h i
l m n o p q r s t u x y z w a b c d e f g h i k
m n o p q r s t u x y z w a b c d e f g h i k l
n o p q r s t u x y z w a b c d e f g h i k l m
o p q r s t u x y z w a b c d e f g h i k l m n
p q r s t u x y z w a b c d e f g h i k l m n o
q r s t u x y z w a b c d e f g h i k l m n o p
r s t u x y z w a b c d e f g h i k l m n o p q
s t u x y z w a b c d e f g h i k l m n o p q r
t u x y z w a b c d e f g h i k l m n o p q r s
u x y z w a b c d e f g h i k l m n o p q r s t
x y z w a b c d e f g h i k l m n o p q r s t u
y z w a b c d e f g h i k l m n o p q r s t u x
z w a b c d e f g h i k l m n o p q r s t u x y
w a b c d e f g h i k l m n o p q r s t u x y z

In hac tabula literarum canonica ſive recta tot ex uno & uſuali noſtro latinarum literarum ipſarum permutationem ſeu tranſpoſitionem habes alphabeta, quot in ea per totũ ſunt monogrammata, videlicet quater vigeſies quatuor & viginti, q̃ faciũt in numero D. LXXVI. ac per totidem multiplicata, paulò efficiunt minus quam quatuordecim millia.

Tabula

Figure 2: Trithemius recta tabula.



Now let's see if it is possible, consistently with the example provided, to reconstruct the method in detail, how the *Ave Maria* cipher type should be structured, how many pages, how many alphabets, and how to use them.

Let's examine two possible implementations:

5.1 Implementation 1

The first implementation assumes that the secret text is arranged in a single line of 32 groups. The cipher should consist, as in the *Ave Maria*, of as many rows as there are letters of the alphabet (24 in German or 20 in Latin and Italian). For simplicity, let's assume that the text in the example is all placed on the line identified by the letter **T**:

	A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X
A	A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X
B	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X	A
C	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X	A	B
D	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X	A	B	C
E	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X	A	B	C	D
F	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	X	A	B	C	D	E
G	G	H	I	L	M	N	O	P	Q	R	S	T	V	X	A	B	C	D	E	F
H	H	I	L	M	N	O	P	Q	R	S	T	V	X	A	B	C	D	E	F	G
I	I	L	M	N	O	P	Q	R	S	T	V	X	A	B	C	D	E	F	G	H
L	L	M	N	O	P	Q	R	S	T	V	X	A	B	C	D	E	F	G	H	I
M	M	N	O	P	Q	R	S	T	V	X	A	B	C	D	E	F	G	H	I	L
N	N	O	P	Q	R	S	T	V	X	A	B	C	D	E	F	G	H	I	L	M
O	O	P	Q	R	S	T	V	X	A	B	C	D	E	F	G	H	I	L	M	N
P	P	Q	R	S	T	V	X	A	B	C	D	E	F	G	H	I	L	M	N	O
Q	Q	R	S	T	V	X	A	B	C	D	E	F	G	H	I	L	M	N	O	P
R	R	S	T	V	X	A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q
S	S	T	V	X	A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R
T	T	V	X	A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S
V	V	X	A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T
X	X	A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V

Figure 3: The original Vigenère table using the 20 letters Latin alphabet; given key letter E and text letter Q, the cipher letter is V at the intersection of row E and column Q (Or vice versa).

The cipher should consist, as in the *Ave Maria*, of as many rows as there are letters of the alphabet (24 in German or 20 in Latin and Italian), and assuming for simplicity that the text in the example is all placed on the line identified by the letter **T**:

S	…	S	…	S	…	S	…	T	…
T	Tenetevi	T	a tutta forza	T	et non ui rendete	T	à patto alcuno	T	hauerete subito
V	…	V	…	V	…	V	…	V	…

and the resulting ciphertext from this first step would now be **TTTTTT**.

The next step involves encrypting each of the letters obtained with another, using the keyword or *contrasegno*, which here is *SANCTVSMARCVSVENETVS*. For this purpose, one of the many polyalphabetic ciphers invented in the sixteenth century is required. Ventura uses the unusual *contrasegno*, which is the one used by Bellaso in his ciphers[18]. It is likely that he uses one of these. To simplify matters, I have used the well-known Vigenère table with an alphabet of 20 letters (see Figure 3), despite it being an anachronism as it was only published in 1586.

Secret	T	Tenetevi	T	a tutta forza	T	et non ui rendete	T	à patto alcuno	T	hauerete subito …
Key	S		A		N		C		T	…
Fake	P	Nunc	T	dimittis	I	seruum	Z	tuum	Q	Domine …

The ciphertext is now: **PSTIZQR …**, which in the next step must give Ventura's solution: *Nunc dimittis seruum tuum …*; this requires assigning

[18] See (Bauer, 2007) and the original (Bellaso, 1553).

the first resulting letter **P** to *Nunc*, the second **S** to *dimittis*, and so on.

5.2 Implementation 2

The second implementation hypothesis is suggested by the fact that the secret text is a sequence of eight sentences of similar structure, an imperative followed by an object complement or similar, a conjunction, and a subordinate sentence: it could thus be a cipher of only eight lines of four groups; each line is identified by a letter of the *contrasegno* (keyword) **SANCTVSMARCVSVENETVS** as follows:

A	Teneteui	a tutta forza	et	non ui rendete …
C	Hauerete	subito soccorso	di	vittouaglia dinari soldati et altre monicjoni
E	Non innouate	cosa alcuna	fin che non	hauete altre nostre per salute comune.
M	Defendeteui	alla muraglia	quanto podete et non	uscite fin che altro auisamo
R	Viuete	sicuri	che senza fallo alcuno	s'hauera Vittoria immortalissima
S	Scriuete	quanto più presto	per più strade se	ui occorrera cosa che ui sia di importanza …et bisogno Accioche subito proueder si possa
T	Sappiate	che si tenira sempre buon conto	de	la fede et sincerita che …hauete sempre uerso noi dimostrato
V	Perseuerate	donque al simile	che non	si mancherà di giusta ricompensa

Indeed, several combinations produce plausible texts, such as the following two, while others sound really bad.

A	Teneteui	M	alla muraglia	E	fin che non	S	ui occorrera …
M	Defendeteui	A	a tutta forza	M	quanto podete et non	V	si mancherà …

This first step produces **AMESMAMV** as an intermediate ciphertext to be overwritten with the letters of the keyword. This can be implemented using an 8x8 Vigenère table identified by the eight letters of the keyword. Finally, as in the previous implementation, the individual letters will be replaced by words from the fake text *palese*.

Overall, this example method 3 is an ingenious steganographic cipher, producing short fake texts from a limited set of true secret messages. This makes it impractical for long diplomatic dispatches; it can be used for short conventional messages, such as the famous Radio London messages during World War II. However, for this purpose, there are lighter methods available.

6 Conclusions, open questions

In conclusion, Vigenère did not misunderstand; indeed, he was quite accurate in mentioning Trithemius ciphers as the source of Ventura's ciphers.

Still, there are open questions:

- How did Vigenère learn about these Ventura ciphers in 1569, two years after this episode? Did he have some knowledge among the secretaries of ciphers for the Council of Ten? In 1567, Zuan Francesco Marin (or Marino) was the most prominent secretary for ciphers, the last great Venetian cryptanalyst.
- Were these ciphers actually used by the Republic for diplomatic or military dispatches? No evidence of such use has been found, up to now.
- The first mode is a Cardan Grid without holes in the paper, only virtual holes; but how to find their location using the *contrasegno*?
- The second mode looks similar but works on single letters rather than words. Same question as above.
- The third mode uses a reverse and a normal *Ave Maria* cipher with a polyalphabetic system. The outline design is clear, a detailed implementation

7 Acknowledgements

A special thanks to the entire staff of the State Archives of Venice for their assistance during my research.

Thanks also to ChatGPT 3.5 for the revision of the English text, that was done by paragraph.

References

Friedrich Ludwig Bauer. 2007. *Decrypted secrets: Methods and Maxims of Cryptology*. Springer, Berlin.

Giovan Battista Bellaso. 1553. *La cifra del sig. Giouan Battista Bellaso, gentil'huomo bresciano ...* G.B. Bellaso, Venezia.

Paolo Bonavoglia. 2019. The cifra delle caselle a xvi century superencrypted cipher. *Cryptologia*.

Paolo Bonavoglia. 2022. The Enigma of Franceschi's Falso Scontro. In *Proceedings of the 5th International Conference on Historical Cryptology HistoCrypt 2022*, Uppsala. Linköping University Electronic Press.

Paolo Bonavoglia. 2023. *La crittografia della Repubblica di Venezia*. Aracne, Roma.

Hyeronimus Cardanus. 1553. *De subtilitate*. Sebastianum HenricPetri, Basilea.

Bartolomeo Cecchetti. 1869. Le scritture occulte della diplomazia veneziana. In *Atti del Regio Istituto Veneto Tomo XIV Serie III*, Venezia. Istituto Veneto.

Blaise de Vigenère. 1587. *Traicté des chiffres ou secrètes manières d'escrire*. Abel L'Angelier, Paris.

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

Aloys Meister. 1902. *Die Anfänge der modernen diplomatischen Geheimschrift*. Ferdinand Schöningh, Paderbord.

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

Riccardo Predelli. 1869. Saggio di scritture in cifra usate dalla repubblica veneta (sec xvi-xviii) estratte dagli archivi veneti. In *Atti del Regio Istituto Veneto Tomo XIV Serie III*, Venezia. Istituto Veneto.

Paolo Preto. 1994. *I servizi segreti di Venezia*. Il Saggiatore, Milano.

Johannes Trithemius. 1613. *Libri Polygraphiae*. Lazari Zetzneri, Argentorati (Strasbourg).

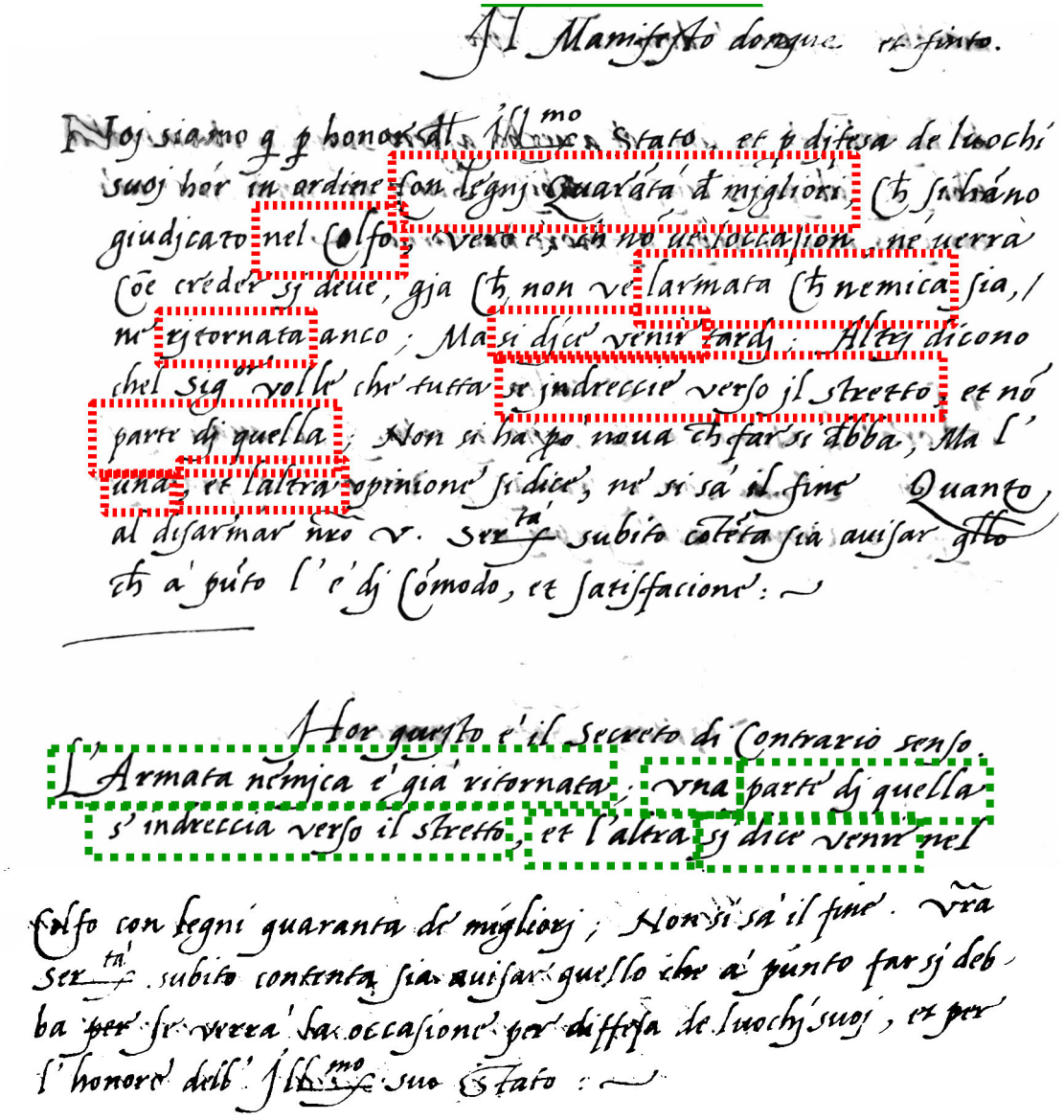


Figure 4: Example n.1. The red-border boxes show possible windows, but how was their position found? Note: Images are in HR and can be enlarged by zooming in with Acrobat or other pdf readers. *ASVe CX Cifre, chiavi e scontri di cifra b.6 misc.*

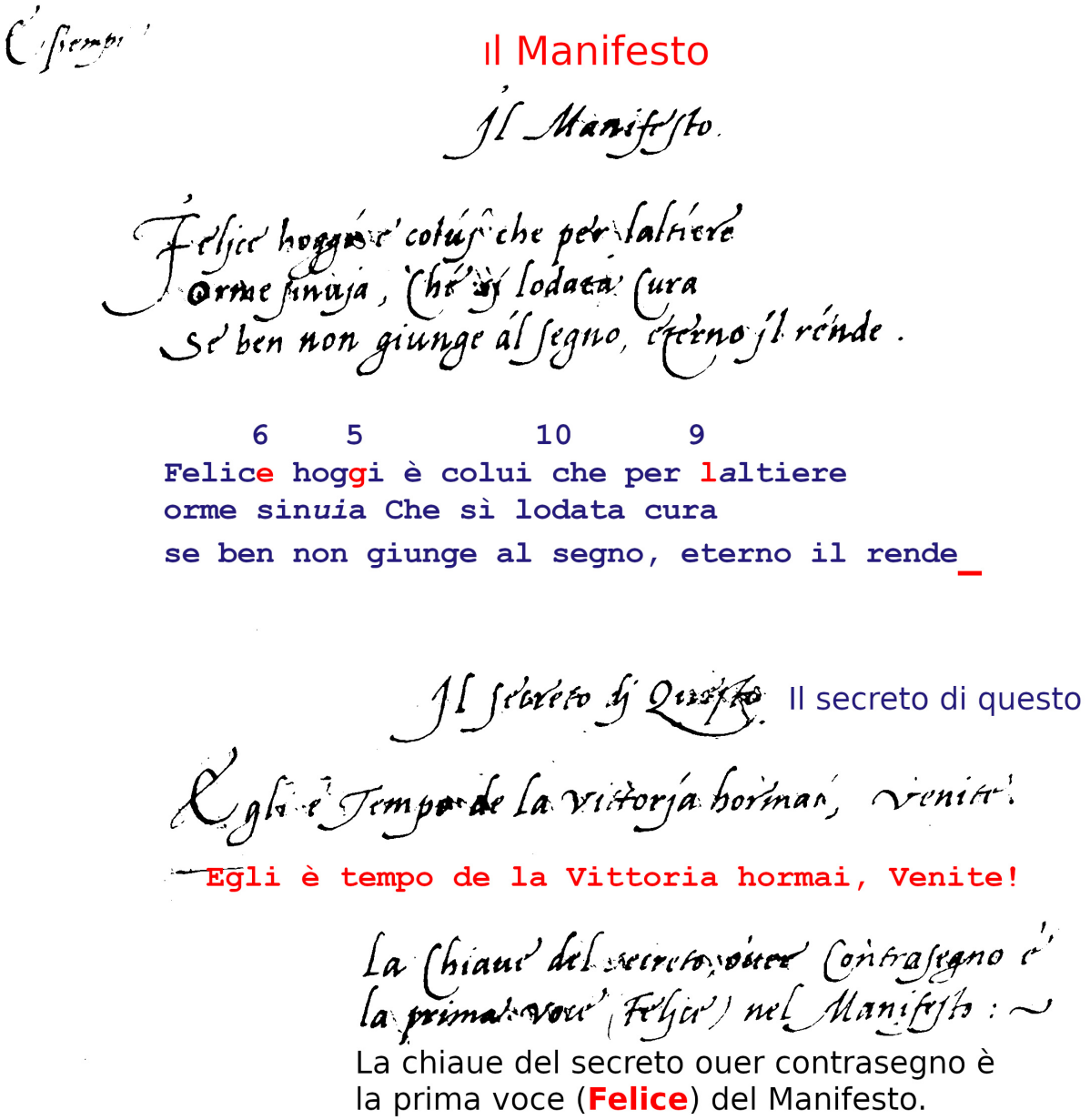


Figure 5: Example 2: The possible solution where letters of the key are interpreted as numbers of step forward. *Ibidem*

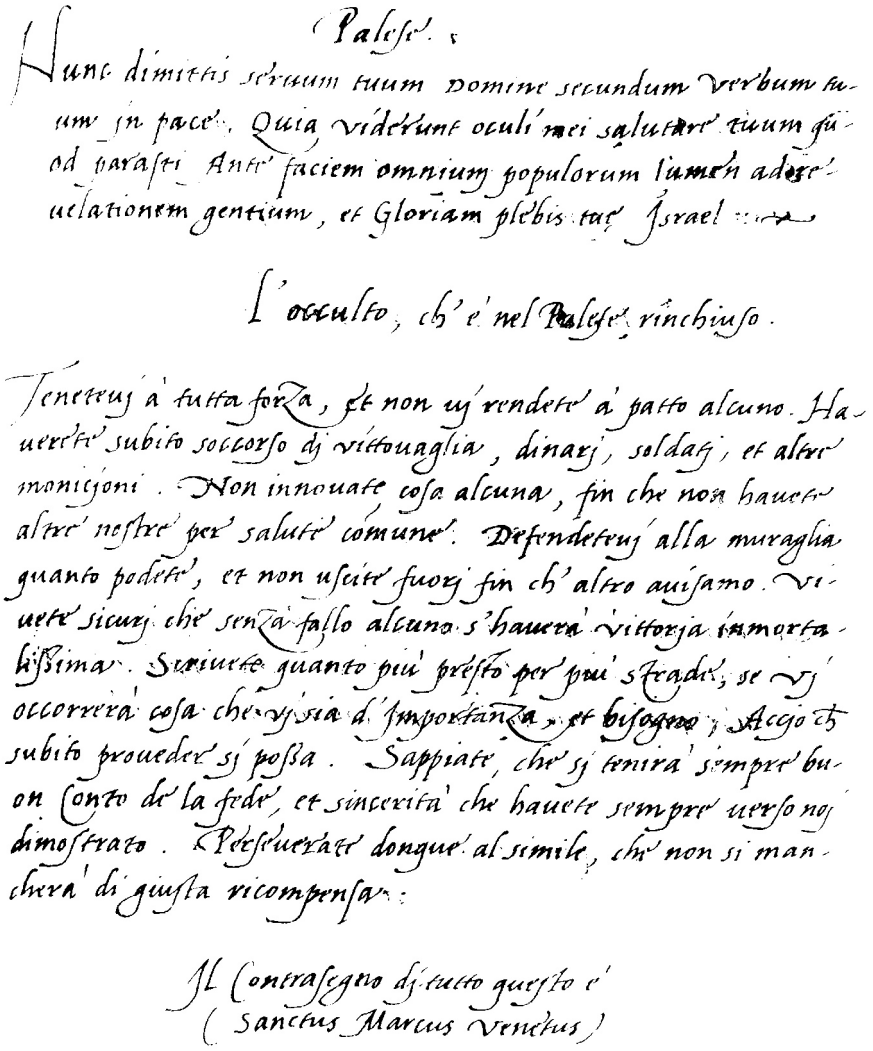


Figure 6: Example n.3, top, the *palese* fake text in Latin; middle: the true text in Italian; bottom: the keyword (*contrasegno*). *Ibidem*