# Ottavian Medici and the decline of Venetian cryptography

**Paolo Bonavoglia**
Mathesis Venezia c/o Liceo Foscarini Cannaregio 4942 I 30121 Venezia
paolo.bonavoglia@mathesisvenezia.it

## Abstract

The recent discovery, in the State Archives of Venice, of a 1621 final account from a committee of three noblemen charged to evaluate cipher services, sheds new light on the decline of cryptography in Venice in the subsequent centuries. The committee produced not only its evaluation, but also a new, interesting cipher, by the young Ottauian Medici. But, after Medici, stagnation and decline set in, until the final collapse of the Republic of Venice in 1797.

## 1 Introduction

The literature about cryptography in the 17th and 18th centuries in Venice is rather poor; Pasini in his booklet[1] does provide some limited insights, but his main subject is a set of cryptograms from around 1550; Meister in his chapter about Venice,[2] covers a limited period of research up to 1550, because his main goal was to study the various roots of modern cryptography; with only limited time to stay in Venice, he did not go beyond 1550. Other authors such as Preto[3] and Iordanou,[4] also wrote about cryptography in Venice, but their main interest was for its application for espionage and secret services, and less for technical considerations.

Four years of research at the State Archives of Venice, among other things, shed a little more light on this period.

In the 16th century Venice boasted a formidable team of cryptanalysts working under the control of the Council of Ten, henceforth abbreviated to CX:[5] Giacomo Soro, Alvise Borghi, Giambattista Ludovici, and Gianfrancesco Marin, who boasted to be able to break [almost] any cipher; Marin, eventually found himself in tears that he was the last one capable of decrypting foreign ciphers. The CX, also concerned about this situation, requested him to instruct his son, Ferigo in the art of cryptanalysis; and, then, when Gianfrancesco died unexpectedly in 1578, the CX ordered the requisition of all his books in the hope that these would be enough for Ferigo to learn alone the art of *leuar le ziffre senza scontro*.[6]

It was an unfullfilled hopes; before 1578 one finds many references from the CX praising the great cryptanalytic accomplishments of Soro, Borghi, Ludovici and Marin. After 1578, in spite of extensive research, I found no further mention of any successes in decrypting foreign dispatches. Obviously, this lack of evidence is not conclusive, after all, cryptanalysis is perhaps the only science where it is best not to boast or to publicize one's successes—in fact, it is often recommended (and done) to destroy any data about successful decryptions.

In a different consideration, that of designing ciphers, the 16th century in Venice had seen an evolution of ciphers, from those using fancy symbols, letters from exotic alphabets, geometric figures, etc., to ciphers consisting of letters followed by one or two numbers, usually written raised up, as an exponent. These were

[1] (Pasini, 1872 2019)
[2] (Meister, 1902)
[3] (Preto, 1994 1999)
[4] (Iordanou, 2019)

[5] The Council of Ten, often abbreviated to Cons$^o$ of X, or even shorter CX, was a powerful, perhaps the most powerful body of the Venetian Republic, and was also in charge of the secret services, among which was also the cryptographic service, entrusted to the so-called deputies of ciphers

[6] English: deciphering the cryptograms without the cipher sheet

usually nomenclators, consisting of an alphabet almost always with homophones, a certain number of nulls, and a dictionary of words encrypted with a single sign; increasingly the use of syllabaries (groups of letters formed by one or more consonants followed by a vowel), became widespread. Nothing out of the ordinary, the nomenclator was the most widely-used cipher in Europe for professional users, namely by the military, and especially for diplomatic purposes.

During the same century several polyalphabetic ciphers were invented by ingenious amateurs,[7] in particular the polyalphabetic ciphers of: Leon Battista Alberti,[8] one of the foremost architects of the Italian Renaissance; Johannes Trithemius,[9] an abbot; Giovan Battista Porta,[10] a playwright; and Blaise de Vigenère,[11] a diplomat; not to mention, Giambattista Bellaso, a secretary to various cardinals, who was in charge of their ciphers and published some very ingenious ciphers.

As early as the second half of the 16th century, a trend had begun to make ciphering and deciphering nomenclators easier to use and faster, which raised concerns about the safety of nomenclators, primarily by the two most brilliant designers of ciphers in the final decades of the 16th century, Hieronimo di Franceschi,[12] secretary of the Senate and deputy of ciphers for the Council of Ten from 1576 to 1600, and Pietro Partenio[13] a private notary from 1563 to 1610, with a great skill for ciphers. They all shared a common concern: other rulers would have their own skilled cryptanalysts, therefore the Venetian ciphers were no longer as secure as believed; the proposed remedy, however, was radically different, as we will see.

Franceschi considered nomenclators unreliable and proposed instead adopting the *uere ziffre* true ciphers, as he called the polyalphabetic ciphers—such was the *cifra delle caselle*, a polyalphabetic cipher based on arithmetic, subtraction and addition.[14] While Partenio despised letter-by-letter ciphering, as in mono- and polyalphabetic ciphers, and aimed rather at strengthening the nomenclators by increasing the size of the dictionary and syllabary, but above all by super-encrypting the nomenclator to keep it safe, even in case of theft of the cipher sheet. Such was his *cifra n. 5*, the only one that was used in 1595 by the Paris embassy, albeit for a very short time.

The polyalphabetic ciphers were presented as ciphers that were absolutely indecipherable unless one knew the key, for individual letters were not always encrypted with the same sign or at most with a choice of equivalent signs as in nomenclators, but the same letter could be encrypted with different letters, making frequency analysis, a statistical tool useful for of forcing monoalphabetic ciphers, useless. Indeed this is true only with a random and non-reusable key.

Nevertheless, the nomenclator continued to reign supreme for centuries, as David Kahn proposes in Codebreakers,[15] wondering why the cipher offices were so hostile to the polyalphabetic ciphers.[16] Franceschi's cipher was, to my knowledge, the only case of a polyalphabetic cipher that was actually used in the real world for diplomatic messages.

## 2 1600, year of the turning point

In 1596 the CX had resolved to elect a committee of five nobles to find a solution to the dispute between Franceschi and Partenio, specifically between the previously mentioned, Franceschi's *cifra delle caselle*, and Partenio's *cifra 5*.

Around 1599 or 1600 the dispute came to an inglorious end, with a final contest between the two ciphers and their inventors their

[7] Naturally I mean *amateurs* in the cryptographic field, people whose main profession was not in the cryptographic field

[8] (Alberti, 1511)

[9] His best known work is (Trithemius, 1507 1613).

[10] Author of a huge review of ciphers in (Porta, 1606)

[11] (de Vigenère, 1587)

[12] 1540 - 1600 . The name was spelled Hieronimo up to the end of the century, thereafter Girolamo.

[13] 1538 - 1620; the surname is also spelled Parthenio, and in Latin, Parthenius

[14] (Bonavoglia, 2019)

[15] (Kahn, 1967 1996)

[16] Agostino Amadi wrote in his treatise of ciphers, about the polyalphabetic ciphers of Bellaso: *[…] le quali tutte sono nobilissime inuentioni, ma non da da Principi che uogliono il sodo, il uero et saper ancora loro che quella zifra [sie li?] per quella forma and not another one.* English: […] all of them are very noble inventions, but not [used] by Princes (rulers) that want the practical, the true, and to know that one cipher has that meaning (word or letter) and not another one

adversaries, along with their respective assistants; it was held despite the decision by Pietro Amai, Franceschi's assistant, to excuse himself, because he did not feel skilled enough in adding and subtracting, a basic skill with the *caselle*! The five noblemen wrote a draft report[17] that ended with a verdict of parity between the two ciphers, with both rated as very strong, although with a slight preference for Franceschi's *caselle*; in the end they recommended using both ciphers, by alternating the two.

As it turns out, the final report does not appear to have ever been delivered to the CX, since only the draft could be found, more than likely because Franceschi had died in the first half of 1600. Therefore the above recommendations were completely ignored

## 3 Pietro Amai takes over from Franceschi

When Franceschi died, the role of chief deputy for ciphers passed into the hands of Pietro Amai, Franceschi's main collaborator, who was for some time joined by Ferigo Marin son of Zuan Francesco.

Although the son of the more-celebrated Agostino Amadi, author of the latest treatise on ciphers produced by Venetian cryptography, Pietro, like Ferigo Marin, comes across as a rather weak and lazy character, as was already evident from his inglorious withdrawal from the final round of the Franceschi—Partenio dispute, cited above.

Amai was careful not to reintroduce the *caselle*, much less Partenio's superencrypted systems. The current cipher, since 1599, has been the A = Z10,[18] a simplified nomenclator without homophones and nulls and with a total of 300 cipher signs. This is almost certainly the cipher that Partenio claimed to have easily decrypted in his 1606 letter, in which he

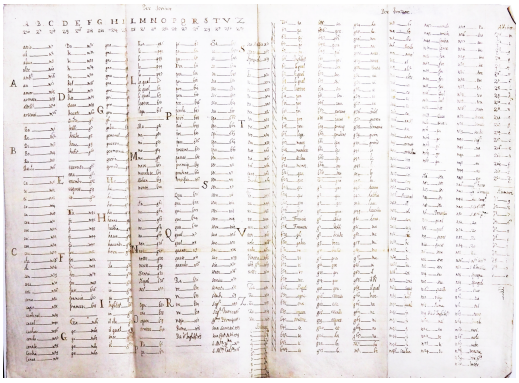


Figure 1: The Z10 cipher. Original cipher sheet. *ASVe Cifre, chiavi e scontri di cifra …busta 1, f. 3*

denounced the weakness of the ciphers being used during that period.

Indeed, the cipher has several weaknesses: 1) there are no homophones and nulls, but only one cipher sign for each letter; 2) there is a large syllabary, and although that should have been a strength, instead, there is a weakness, clearly visible in figure 2, the syllable ciphers are ordered by vowels: A = 1, E = 2, I = 3, O = 4, U = 5, following a medieval scheme, e.g.: the 1226 Liber Plegiorum.[19]

| letter | a | e | i | o | u |
|---|---|---|---|---|---|
| cipher | 1 | 2 | 3 | 4 | 5 |

Obviously, the cryptanalyst trying to crack this cipher, upon realizing that the syllables are ordered, would be greatly aided in reconstructing the syllabary, which is the backbone of the cipher, and would have had little difficulty finding the solution.

The CX was well aware of this situation and sent reprimands to the cipher deputies, complaining about the serious disorder in the ciphers office and the fact that for years and years the current cipher, the Z10, was never changed.

## 4 A committee of three noblemen is elected

Finally, in 1619, the CX approved the election of a committee of three noblemen charged with reforming the ciphers and to find a new cipher to replace the old Z10, which after twenty

[17] This long sought report, was found in 2022 as two almost identical minutes in poor condition due to oozing inks in an envelope in the State Archives of Venice, henceforth abbreviated to *ASVe. ASVe Cifre, chiavi e scontri di cifra …busta 6.*

[18] The classification of ciphers using the encryption of the letter **A** is due to Luigi Pasini (1835 1885) an archivist of the Archives of Venice, who reordered the cryptographic papers and wrote a booklet about the ciphers of the Republic of Venice, focusing on some encrypted letters around 1550 (Pasini, 1872 2019).

[19] A medieval register of chancery records digitized in *ASVe Collegio Minor Consiglio Liber Plegiorum, Reg-12231229, c. 48r, 84-v, 117r*

Figure 2: The Z10 cipher syllabary.

years had passed through too many hands to be considered safe.

Procurator Girolamo Giustinian, and noblemen Francesco Morosini and Ottaviano Valiero were elected. In the meantime, two young men Ottavian[20] Medici and Giambattista Lionello had passed the exams required to become deputies of ciphers, and therefore were able to collaborate with the newly-elected committee.

One of the committee's first acts was to consult the octogenarian Pietro Partenio, although these were no longer the years when the CX enthusiastically praised his ciphers. Here is an excerpt from the committee's final report of 1621:[21]

> Several times we had meetings with a diligent examination of a great variety of ciphers, by the *ziffristi* secretaries and by the late Pietro Parthenio very skilled in that profession; of this person we could tell Your Serenity, with our usual sincerity, that we saw, while he was in life, very witty inventions, of equal safety, and worthy of commendation, but balanced these requirements with some difficulty in the use and slowness in deciphering and enciphering, when a multiplicity of tasks are presented almost instantly every day on all sides, we have judged, for these causes alone, that we cannot recommend their use.

Ultimately an elegant way to dismiss Partenio, and generally an epitaph for overly-complicated and slow ciphers; indeed, finding the balance between security and speed of use is an age-old problem in cryptography.

As the text suggests, Partenio had since died in 1620, according to Tassini,[22] and there are no wives or children reported. He therefore had no direct heirs, but in his letter of January 1606 (1605 m.v.)[23] he designated one with these words:

> [...] so that we may instruct Ottauiano Medici, extraordinary of the Cancellaria, which is to me like a son, as everyone knows, of excellent hope.

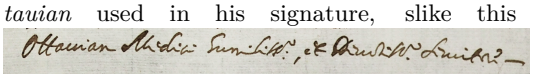
Partenio was right, as we shall see, the already-mentioned Medici would prove to be the dominant figure in Venetian cryptography in the first half of the 17th century; and in any case the last cipher deputy of any depth in the history of the Republic of Venice.

## 5 The cipher of the three noblemen, by Medici and Lionello

It took the committee more than two years to arrive at a consensual proposal, a report which, after rejecting Partenio's ciphers as too difficult and slow, proposed the adoption of a new cipher that assimilated some important innovations from the past.

The report attributes the design of this cipher to the deputies of ciphers in service at that time. Attached to the report are the enciphered and deciphered text of several pages, such as were typically used by ambassadors, and, in this case, used as an exam; on April

[20] The name is variously spelled as *Ottauio, Ottauian, Ottauiano.* I prefer the form *Ottauian* used in his signature, slike this one:



[21] 17th century Italian original text: *Più uolte siamo stati insieme con essaminatione dili[gentissi]ma sopra una gran uarietà de scontri, che ci sono stati presentati et dalli secretari ziffristi e dal già Pietro Parthenio peritissimo in tal professione; di questo soggetto potemo con la [nostra?] solita sincerità a dire a Vostra Serenità di hauer ueduto, mentre egli uiueua inuentioni molto spiritose, di pari sicurtà, et degne di comendatione ma bilanciati questi requisiti con qualche difficoltà nel uso et tardità nel trazer et scriuer, quando alla giornata occorre che che quasi a tempi presenti risorge la multiplicità da ogni parte habbiamo giudicato per queste sole cause di non poter determinare la loro essercitatione*

[22] citeTasCit88

[23] m.v. stays for *more veneto*. the Venetian style of the calendar: the first day of the year was March 1, following the ancient Roman Republic style; that's why September begins with *septem* Latin for seven, October with *octo* = eight ...so January and February 1606, are still 1605 m.v.

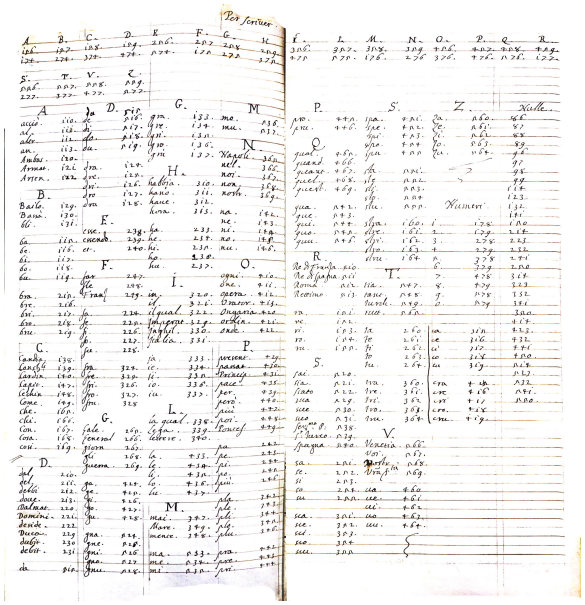


Figure 3: The 1621 cipher, original cipher sheet.*ASVe Cifre, chiavi e scontri di cifra …busta 2, f. 15*

28, 1622 it took Medici four hours to encipher the message; two days later it took Lionello three hours to decipher it—a confirmation that Medici and Lionello[24] were now the two main cipher deputies.

The cipher presents some interesting changes from the Z10 cipher and from those of the last half century.

- The cipher is now, and henceforth, formed of numbers only, each letter or group of letters being encrypted with a number of three digits. The numbers are to be written continuously without separator spaces so that one cannot tell where the single cipher begins and ends, nor how many digits they consist of, two? three? four?

- Homophones reappear, each letter has two cipher signs; put another way, it is a cipher of the double alphabet.

- There is a large number of nulls; secretaries are advised to insert many nulls here and there between the actual ciphers; particularly at the beginning and end of the line, between the double …

[24]For some reason Lionello disappears thereafter, a plausible conjecture is that he was among the victims of the 1630 devastating plague.

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ba | be | bi | bo | bu | bra | bre | bri | bro | bru | ca | ce | ci | co | cu | cra | cre | cri | cro | cru | da | de | di | do | du | dra | dre | dri | dro | dru |
| 115 | 116 | 117 | 118 | 119 | 215 | 216 | 217 | 218 | 219 | 315 | 316 | 317 | 318 | 319 | 415 | 416 | 417 | 418 | 419 | 515 | 516 | 517 | 518 | 519 | 124 | 125 | 126 | 127 | 128 | |
| fa | fe | fi | fo | fu | fra | fre | fri | fro | fru | ga | ge | gi | go | gu | gna | gne | gni | gno | gnu | gra | gre | gri | gro | gru | ha | he | hi | ho | hu | |
| 224 | 225 | 226 | 227 | 228 | 324 | 325 | 326 | 327 | 328 | 424 | 425 | 426 | 427 | 428 | 524 | 525 | 526 | 527 | 528 | 133 | 134 | 135 | 136 | 137 | 233 | 234 | 235 | 236 | 237 | |
| ia | ie | ii | io | iu | la | le | li | lo | lu | ma | me | mi | mo | mu | na | ne | ni | no | nu | pa | pe | pi | po | pu | pla | ple | pli | plo | plu | |
| 333 | 334 | 335 | 336 | 337 | 433 | 434 | 435 | 436 | 437 | 533 | 534 | 535 | 536 | 537 | 142 | 143 | 144 | 145 | 146 | 242 | 243 | 244 | 245 | 246 | 342 | 343 | 344 | 345 | 346 | |
| pra | pre | pri | pro | pru | qua | que | qui | quo | quu | ra | re | ri | ro | ru | sa | se | si | so | su | sca | sce | sci | sco | scu | spa | spe | spi | spo | spu | |
| 442 | 443 | 444 | 445 | 446 | 542 | 543 | 544 | 545 | 546 | 151 | 152 | 153 | 154 | 155 | 251 | 252 | 253 | 254 | 255 | 351 | 352 | 353 | 354 | 355 | 451 | 452 | 453 | 454 | 455 | |
| sta | ste | sti | sto | stu | stra | stre | stri | stro | stru | ta | te | ti | to | tu | tra | tre | tri | tro | tru | ua | ue | ui | uo | uu | za | ze | zi | zo | zu | |
| 551 | 552 | 553 | 554 | 555 | 160 | 161 | 162 | 163 | 164 | 260 | 261 | 262 | 263 | 264 | 360 | 361 | 362 | 363 | 364 | 460 | 461 | 462 | 463 | 464 | 560 | 561 | 562 | 563 | 564 | |

Figure 4: The syllabary of the 1621 cipher.

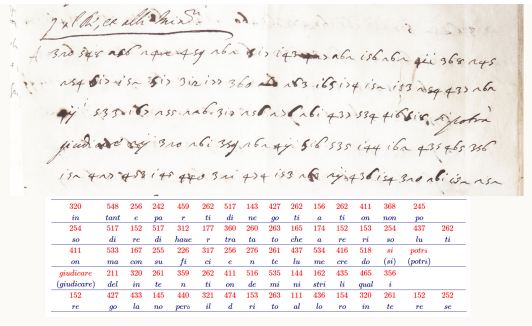


Figure 5: 1st dispatch using the new cipher, Paris July 3, 1623. *ASVe, Senate, dispacci degli ambasciatori, Francia, f.59, c.550*

- The syllabaries are partially ordered, in the sense that they are ordered by vowel as in Z10 starting from a to u, but without necessarily starting from 1, for instance.

The most significant feature is the large number of nulls, which are essential if the length of single ciphers has to be kept hidden.

The cipher is supposed to have come into use in 1622, but the earliest dispatch I have found that uses this cipher is a 23-page document dated July 3, 1623 from the Venetian ambassador to Paris, Giovanni Pesaro, encrypted only in part. In figure 5 two things are noticeable: 1) there is not even a single null; and 2) the spaces between the cipher marks are clearly visible. The previous recommendations were totally disregarded; the first dispatch using this cipher, from the ambassador to London, Alvise Vallaresso, dated August 23, 1623, also has the same problems, no nulls, spaces mostly visible, although the effort to write continuously is somewhat discernible. There is a strange difference from the cipher used in Paris; the syllables *da de di do du* are encrypted with the numbers *215 216 217 218 219*, which in Paris and in the version preserved in the Venetian archives stood instead for: bra bre bri bro bru. I did not find a sat-

isfactory explanation for this discrepancy.

Without nulls and with spaces left visible the cipher looks no safer than Z10, there remains only the fact of having a somewhat less-orderly syllabary. In later years things improved with regard to continuous writing, which ultimately became a habit for all secretaries, who, conversely, never became accustomed to using nulls.

## 6 The 1624 variable-size cipher

Then, in 1624, as a result of the embassy secretary in London being robbed of many documents, including cipher sheets, the CX ordered the cipher to be changed, and therefore Medici designed a new, and a very interesting one, at that.

It is a variable-size cipher: some letters or syllables or words were encrypted with numbers of two-decimal digits, others with three, and others with four. The idea was not new; it had been proposed in his treatise by Matteo Argenti,[25] secretary to the Papal ciphers in the late 16th century. Argenti used numbers of one or two digits, relying on the acumen of the cipher secretaries for a correct deciphering; for usually, the question as to whether the next number is of two or three digits is resolved by context—usually, but not always—only one combination will produce sensible texts.

We do not know if Medici knew of Argenti's treatise—at least I have found no trace of it in the archives; he clearly prefers another solution that leaves no doubt; numerals 5 and 6 are used exclusively as the first number of a group. An original idea, yes, but one has to wonder to what extent one can fool the enemy with this trick; those 5s and 6s are already at a glance distributed in a somewhat too-regular manner that might arouse suspicion in the eye of the enemy. Not to mention that many secretaries did not understand the instructions well and kept leaving a space between one cipher group and the next, as can be seen in figure 6.

## 7 Cipher A 105-115 the return of the fixed-size cipher, three digits

The 1624 cipher also had to be abandoned due to theft; Medici designed another one in collaboration with the now-elderly Pietro Amai and Antonio Marin, which was approved by the CX on March 23, 1630; there is a return to fixed-size cipher signs of three digits. There is a dual alphabet and that is two homophones per letter beginning with the A encrypted with 105 and 115. There is a syllabary sorted according to vowel by a criterion very similar to that of the deprecated Z10 cipher, only beginning with zero instead of 1: for example ba be bi bo bu are encrypted with 100 101 102 103 104, another step in the direction of simplification, at the expense of security. There is a large number of nulls; in short, it is a remake of the three-nobles cipher with different numbers. The cipher A 105–115 was used for many years even after the adoption of a new one in 1645.

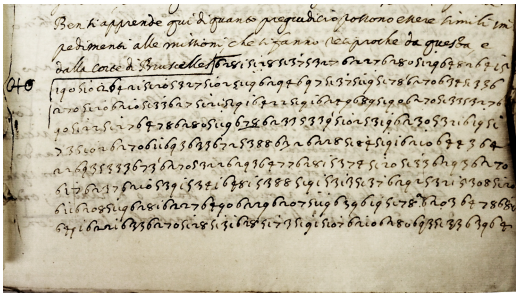


Figure 6: Good use of the Medici cipher. *ASVe, Senato, Dispacci degli ambasciatori in Francia, filza 74, no. 216, 3 ott 1630.*

## 8 1647, 28 February an encrypted message by the Capitano Generale da Mar

Here is an interesting example of use of the previous Medici cipher: a message encrypted only in its most delicate matter (see figure 7). It is an example of use by an admiral, the Capitano da Mar,[26] Giambattista[27] Grimani, from a galley (galera) in Porto di Scandia,[28] dur-

[25] (Argenti, 1906) p. 152, inside (Meister, 1906)

[26] *Capitano Generale da Mar* was the title of the commander in chief of the Venetian fleet. Grimani remained in office from 1646 to 1648, when he drowned with his ship in a violent sea storm while attempting to establish a Dardanelles blockade.

[27] At first reading I had interpreted the name in the signature, difficult-to-read handwriting, as *Ernesto*, but recently it clearly turned out to be *Giambattista*, in agreement with the very little historical information found on this character.

[28] It is the ancient name of a port of the island of Kythira between the Peloponnese peninsula and the

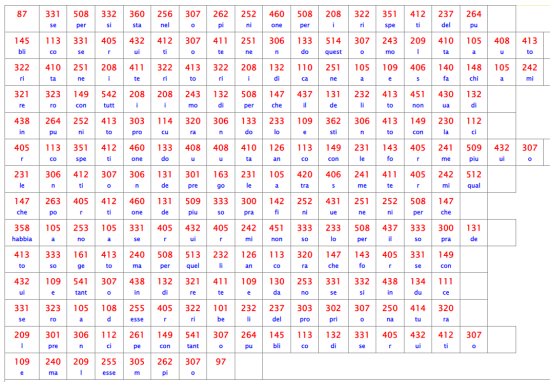



Figure 7: Grimani's cryptogram, decrypted.

ing the Siege of Candia, the long war with the Ottoman Empire over the possession of that island.

The first part of the message is in plain text and recounts that Michiel Caliergi, commander of the Canea,[29] while Grimani was visiting the nearby islands, had made himself all too familiar with the Vizier who treated him very well as a confidant. Grimani argues this behavior is treasonous (clearly, consorting with the enemy) and that it was essential to eliminate him…but in a discreet manner; he is more to-the-point in the encrypted part, presented here deciphered in English[30]

> If you confirm the opinion, for the respect of the public service, of holding so much authority in the territories of Canea and Sfachia, I will, by all means, manage it so that the offense does not go unpunished, procuring him extinguished, so with due circumspection, send me some portions of the most superfine poisons, so that I can use them not only for this subject, but for anyone in the future who may, in such an indirect and harmful way, be induced to be a rebel of his own natural prince, with such public bad service and bad example.

The State Inquisitors responded in April approving Grimani's request and loyalty; they enclosed a paper recommending three poisons: *scamonea*, poisonous if administered continuously; *cantarella*, which blocks urination; and the well-known *arsenic*. But they added that they could not procure and send them because they would have to confide the matter to many people, risking raising questions, objections and ill feelings, and Grimani certainly knew the right people to procure the poisons in Candia.

We do not know if Grimani got the poisons in Candia and if Caliergi was actually poisoned to disguise his death as natural. But, anyway, this provides a good example of when to encrypt a message.

From the cryptographic point of view, Grimani (or his secretary) does not deserve much praise; the A 105-115 cipher has a double alphabet, but here only 105 is used for A, 115 not a single time. The same for E 109 119, and other letters. In other words homophones are simply disabled. The dictionary as evident from figure 7 was never used, and so for the nulls. The rule of writing in a continuous way is well executed, but ends of lines are respected, so it is not difficult, having observed that every line has a number of digits in a multiple of 3, that the single ciphers have 3 digits. A confirmation that the military officer was less skilled than the diplomat, when writing in cipher. The reason is obviously the availability of time: the military can not spend much time encrypting messages, while the diplomat can work at a calmer pace.

## 9 1645 The scontro novissimo

On March 22, 1645 a new cipher with three-digit signs, was approved by the Council of Ten, under the name of scontro nouissimo (newest cipher). It was signed by Ottavian Medici and Marc'Antonio Padauin, the last to be signed by Medici. The alphabet is triplicate, so letter A is encrypted with three homophones 100, 300, 504. Despite its name, it has nothing really new.

Crete island.

[29] A port in the eastern part of the Crete island.

[30] Original 16th century Italian: *Se persista nel opinione per i rispeti del publico seruitio tenendo questo molta autorita nei teritorii di Canea e Sfachia mirerò con tutti i modi perché il delito non uadi inpunito procurandolo estinto con la circospetione douuta anco con le forme piu uiolente onde pregole a trasmetermi qualche portione de piu soprafini ueneni perche habbiaano a seruirmi non solo per il sopradeto sogeto ma per quelli ancora che forse con uie tanto indirete e danose si inducesero ad esser ribeli del proprio natural prencipe con tanto publico diseruitio e mal essempio.*

Medici retired about 1650, and in 1653 was made a nobleman, in recognition of his long-time service, and for a few years Marcantonio Padauin was at the helm of Venetian cryptography; when he died in 1653 two young men Lunardo Formenti and Ottavian Valier acquired the roles of deputy of ciphers. But one has to wait 22 years before seeing a new cipher, in 1675.

## 10 1675 The ghost cipher of Lunardo Formenti

In November 1674 the CX noted that 25 years had elapsed since the last change of the current cipher; they demanded that the State Inquisitors make contact with the deputies for ciphers to design a new one. Lunardo Formenti, Medici's successor, presented a new one on April 4, 1675, with an attached description in which we read:

> in several ways varied to the sign that to form a word, as for example *Bailo* may be explicated in the following four forms, that each of them in several ways referred to that same word of *Bailo*:[31]

The forms are:

700513966 600601501802902703500 866514607839 808908607507706

Is it possible to recover the cipher sheet? Theoretically it is impossible, if you allow for all possible enciphering of single letters, syllables, etc. But knowing the model used during those years, one can assume, with great certainty, three-digit ciphers:

| 700 | 513 | 966 |
|---|---|---|
| | BAILO | |

| 600 | 601 | 501 | 802 | 902 | 703 | 500 |
|---|---|---|---|---|---|---|
| | B | A | I | L | O | |

| 866 | 514 | 607 | 839 |
|---|---|---|---|
| | BA | I | LO |

| 808 | 908 | 607 | 507 | 706 |
|---|---|---|---|---|
| B | A | I | L | O |

And then, assuming that 500 600 700 866 966 are nulls and rather ordered alphabet and syllabaries, I found this possible, and plausible, conjecture for the alphabet:

[31] 16th century Italian: *in più modi uariate à segno che à formar una parola, come per esempio Bailo si può esplicarle nelle seguenti quattro forme, che ogn'una di esse in più modi riferisse quella stessa parola di Bailo, ciò è:*

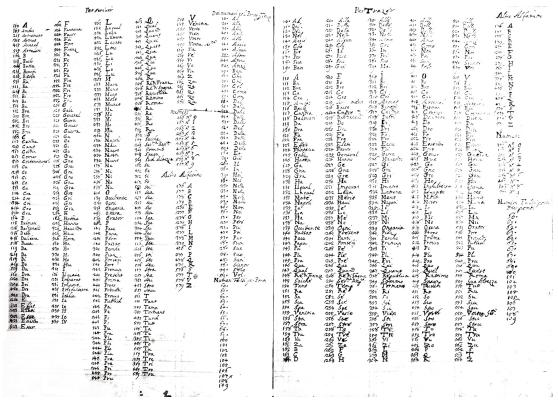


Figure 8: The 1691 cipher by Vettor Pozzo. *ASVe Cifre, chiavi e scontri di cifra …busta 1 f.7*

| A | B | C | D | E | F | G | H | I | L |
|---|---|---|---|---|---|---|---|---|---|
| 501 | 601 | 701 | 801 | 901 | 502 | 602 | 702 | 802 | 902 |
| 908 | 808 | 708 | 608 | 508 | 907 | 807 | 707 | 697 | 597 |

| M | N | O | P | Q | R | S | T | V | Z |
|---|---|---|---|---|---|---|---|---|---|
| 503 | 603 | 703 | 803 | 903 | 504 | 604 | 704 | 804 | 904 |
| 906 | 806 | 706 | 606 | 506 | 905 | 805 | 705 | 605 | 505 |

a single cipher 513 for the word Bailo and these possible syllables.

| BA | BE | BI | BO | BU | LA | LE | LI | LO | LU |
|---|---|---|---|---|---|---|---|---|---|
| 514 | 614 | 714 | 814 | 914 | 539 | 639 | 739 | 839 | 939 |

But, surprisingly, I have not found a single diplomatic or military letter encrypted this way, and no cipher sheet in the huge collection of ciphers kept in the archives. And another surprise is that most dispatches by the ambassadors were encrypted using the 1621 cipher of the three noblemen!

Thus, the strange case of a ghost cipher, a new cipher rejected, and a 60 year-old cipher recycled, mark the beginning of the definitive decline of Venetian cryptography.

## 11 1691 Cipher No. 11 Vettor Pozzo

On January 16, 1691 (1690 m.v.[32] the CX adopted a new cipher by Vettor Pozzo and Constantin Nicolosi, who were the main deputies for ciphers.

The cipher is very similar to the previous one in use since 1621; only an odd variation was introduced, the use of a dot as the eleventh cipher sign after the ten digits. The dot is used only as the third sign, like **10**. for *all*,

[32] See note 4

*Ottavian Medici 1630*

Alfabeto

| a | b | c | d | e | f | g | h | i | l | m | n | o | p | q | r | s | t | u | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 105 | 106 | 107 | 108 | 109 | 205 | 206 | 207 | 208 | 209 | 305 | 306 | 307 | 308 | 309 | 405 | 406 | 407 | 408 | 409 |
| 115 | 116 | 117 | 118 | 119 | 215 | 216 | 217 | 218 | 219 | 315 | 316 | 317 | 318 | 319 | 415 | 416 | 417 | 418 | 419 |

Numeri

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| 564 | 517 | 527 | 537 | 547 | 557 | 559 | 560 | 562 | 563 |

Sillabario

| ba | be | bi | bo | bu | ca | ce | ci | co | cu | cra | cre | cri | cro | cru | da | de | di | do | du |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 100 | 101 | 102 | 103 | 104 | 110 | 111 | 112 | 113 | 114 | 120 | 121 | 122 | 123 | 124 | 130 | 131 | 132 | 133 | 134 |
| fa | fe | fi | fo | fu | fra | fre | fri | fro | fru | ga | ge | gi | go | gu | gna | gne | gni | gno | gnu |
| 140 | 141 | 142 | 143 | 144 | 150 | 151 | 152 | 153 | 154 | 160 | 161 | 162 | 163 | 164 | 200 | 201 | 202 | 203 | 204 |
| gra | gre | gri | gro | gru | ha | he | hi | ho | hu | la | le | li | lo | lu | ma | me | mi | mo | mu |
| 210 | 211 | 212 | 213 | 214 | 220 | 221 | 222 | 223 | 224 | 230 | 231 | 232 | 233 | 234 | 240 | 241 | 242 | 243 | 244 |
| na | ne | ni | no | nu | pa | pe | pi | po | pu | pra | pre | pri | pro | pru | qua | que | qui | quo | quu |
| 250 | 251 | 252 | 253 | 254 | 260 | 261 | 262 | 263 | 264 | 300 | 301 | 302 | 303 | 304 | 310 | 311 | 312 | 313 | 314 |
| ra | re | ri | ro | ru | sa | se | si | so | su | sca | sce | sci | sco | scu | spa | spe | spi | spo | spu |
| 320 | 321 | 322 | 323 | 324 | 330 | 331 | 332 | 333 | 334 | 340 | 341 | 342 | 343 | 344 | 350 | 351 | 352 | 353 | 354 |
| sta | ste | sti | sto | stu | stra | stre | stri | stro | stru | ta | te | ti | to | tu | tra | tre | tri | tro | tru |
| 360 | 361 | 362 | 363 | 364 | 400 | 401 | 402 | 403 | 404 | 410 | 411 | 412 | 413 | 414 | 420 | 421 | 422 | 423 | 424 |
| ua | ue | ui | uo | uu | za | ze | zi | zo | zu | | | | | | | | | | |
| 430 | 431 | 432 | 433 | 434 | 440 | 441 | 442 | 443 | 444 | | | | | | | | | | |

*Vettor Pozzo 1714*

Alfabeto

| a | b | c | d | e | f | g | h | i | l | m | n | o | p | q | r | s | t | u | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 105 | 106 | 107 | 108 | 109 | 205 | 206 | 207 | 208 | 209 | 305 | 306 | 307 | 308 | 309 | 405 | 406 | 407 | 408 | 409 |
| 115 | 116 | 117 | 118 | 119 | 215 | 216 | 217 | 218 | 219 | 315 | 316 | 317 | 318 | 319 | 415 | 416 | 417 | 418 | 419 |

Numeri

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| 564 | 517 | 527 | 537 | 547 | 557 | 559 | 560 | 562 | 563 |

24 Nulle

| 0 | 6 | 7 | 8 | 9 | 66 | 67 | 76 | 77 | 78 | 79 | 86 | 87 | 88 | 89 | 96 | 97 | 98 | 99 | 551 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 552 | 553 | 554 | 555 | | | | | | | | | | | | | | | | |

| ra | re | ri | ro | ru | sa | se | si | so | su | sca | sce | sci | sco | scu | spa | spe | spi | spo | spu |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 330 | 331 | 332 | 333 | 334 | 340 | 341 | 342 | 343 | 344 | 350 | 351 | 352 | 353 | 354 | 360 | 361 | 362 | 363 | 364 |
| sta | ste | sti | sto | stu | stra | stre | stri | stro | stru | ta | te | ti | to | tu | tra | tre | tri | tro | tru |
| 370 | 371 | 372 | 373 | 374 | 410 | 411 | 412 | 413 | 414 | 420 | 421 | 422 | 423 | 424 | 430 | 431 | 432 | 433 | 434 |
| ua | ue | ui | uo | uu | za | ze | zi | zo | zu | | | | | | | | | | |
| 440 | 441 | 442 | 443 | 444 | 450 | 451 | 452 | 453 | 454 | | | | | | | | | | |

Figure 9: Part of the cipher sheet of the 1714 cipher, and of the 1630 cipher.

**20**. for *alla*. It is hard to imagine how this dot could have improved the security of the cipher; maybe one hoped to confuse the enemy? Ironically, this may have actually helped the codebreakers!

## 12 1714 Cipher No. 12 Vettor Pozzo

If the 1691 Pozzo cipher was very very similar to the 1622 cipher, 23 years later he did even better: cipher no. 12, approved on March 7, 1714, had been presented by the same Vettor Pozzo, purportedly as a new cipher. But a close scrutiny of the cipher unveils a simple clone of Medici's 1630 cipher, simply modified by adding 10 to every cipher, see figure 9.

## 13 1733-1787 Last ciphers of the Republic

A new cipher was approved as the replacement cipher in 1733, no. 13; the *primo cifrista* then was Agostino Bianchi, who designed not only no. 13, but also no. 14, to be kept by the State Inquisitors as a reserve in case something could happen to compromise no. 13. In fact, such an incident did occur 49 years later! In the meantime Agostino Bianchi had died leaving

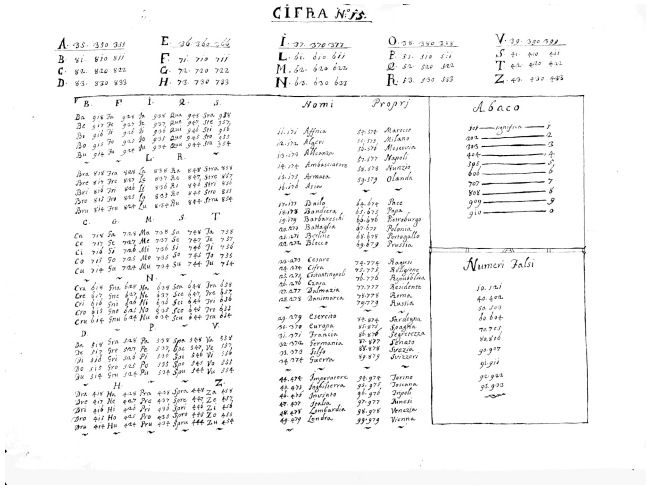



Figure 10: Cipher n.15, February 21 1787. *ASVe Cifre, chiavi e scontri di cifra ...Busta 3, f.78.*

the task of ciphers to his sons Francesco and Maffio, and then to Marcantonio Buseniello. No. 14 was, already in no. 13, a cipher simplified as much as possible, reduced to a double alphabet and a syllabary, all according to very regular, and therefore, cryptographically-weak patterns.

The last cipher found in the archives, no.15, is dated 1787 and has a note on the back indicating the cipher sheet was received to be copied to a book on February 21, 1787, by Buseniello, and returned on February 28. It is similar to the previous, but an appreciable improvement is the reintroduction of a dictionary, although simplified, and with something new: the words of the dictionary had two homophones each, although very similar, just a dot in the place of a 7, for instance *Affrica* has two ciphers: 11., and 171, *Algeri* has 12., 172 ...see figure 10.

## 14 Conclusions

The 1600s mark a watershed between the golden age of Venetian cryptography and the unstoppable decline that paralleled that of the last two centuries of the Republic of Venice.

Paradoxically, as hinted above, Ottavian Medici can be rated as the most successful Venetian *cifrista*: his ciphers were easier and less safe than Franceschi's or Partenio's, but met no opposition and furthermore, even after

his death were still used until the end of the Republic, used in the sense of emulated as a model, imitated and sometimes simply copied and simplified and reduced.

To his credit, he attempted to reinforce the nomenclators with other expedients, such as writing ciphers in a continuous form, and an opportune use of the nulls; but after him there is only a succession of epigones.

The decline of Venetian cryptography ran parallel with the political decline of the Republic, which in the 16th century was still recognized as a major power at the European level, although that was essentially the power of its naval fleet. After the Treaties of Utrecht (1713—1714), Venice had been downsized to little more than what it is today, a destination for world tourism.

An unanswered question remains: to what extent had a similar decline occurred in other European states, from the Papacy to the Habsburg empire, from France to England and Spain? The answer is probably: it varies. As far as Papal ciphers are concerned, the recent decryption of a dispatch from the apostolic nuncio in Brussels in 1721[33] reveals a cipher described by Matteo Argenti in his treatise;[34] apparently the Papal cipher office had also experienced a period of stagnation.

But in the field of cryptanalysis, according to what F. L. Bauer in his *Decrypted Secrets*[35] and David Kahn in his *Codebreakers*[36] the great European powers had developed their own cipher bureaus known as black chambers (*cabinets noirs*), which were increasingly efficient; in Paris the Rossignol became famous, but according to Kahn the best cipher bureau in Europe was the imperial one in Vienna, the *Geheime Kabinettskanzlei*.[37]

Now, it would be of great interest a research in the Vienna archives to see if Venetian ciphers were also systematically decrypted.

[33](Lasry and Bonavoglia, 2022)

[34](Argenti, 1906)

[35](Bauer, 1991 2007) p. 71.

[36](Kahn, 1967 1996)

[37](Kahn, 1967 1996) p.163. They were able to open sealed parcels with a steam system, extract the letter, decrypt it, reinsert it into the envelope, seal it and forward it to the addressee, unaware of being intercepted and decrypted.


## Acknowledgments

Special thanks to the whole staff of the State Archives of Venice, for the help and assistance given in these years of research.

A special thanks to Richard Bosch Architect for reviewing the English text.


## References


Leon Battista Alberti. 1511. De cyfris. In *ASVe, Chiavi di cifra b.41*. Manoscritto, Venezia.

Matteo Argenti. 1906. Trattatto che insegna a formar cifre di varie sorti ... In *Die Geheimschrift Im Dienste Der Papstlichen Kurie Von Ihren Anfängen Bis Zum Ende Des XVI. Jahrhunderts*. Ferdinand Schöningh, Paderborn.

Friedrich Ludwig Bauer. 1991 - 2007. *Decrypted secrets: Methods and Maxims of Cryptology*. Springer, Berlin.

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

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

Ioanna Iordanou. 2019. *Venice's secret service*. Oxford University Press, Oxford.

David Kahn. 1967 - 1996. *The codebreakers*. Scribner, New York.

George Lasry and Paolo Bonavoglia. 2022. Deciphering a short papal cipher from 1721. Uppsala. Linköping University Electronic Press.

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

Aloys Meister. 1906. *Die Geheimschrift Im Dienste Der Papstlichen Kurie Von Ihren Anfängen Bis Zum Ende Des XVI. Jahrhunderts*. Ferdinand Schöningh, Paderborn.

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

Giambattista [Della] Porta. 1606. *De Furtivis Literarum Notis, Vulgo de Ziferis ...* G. B. Sottile, Napoli.

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

Johannes Trithemius. 1507 - 1613. *Libri Polygraphiae*. Lazari Zetzneri, Argentorati (Strasbourg).