The Enigma of Franceschi's Falso Scontro

Paolo Bonavoglia
Mathesis Venezia c/o Convitto Liceo "Marco Foscarini"
Cannaregio 4941 I 30121 Venezia
paolo.bonavoglia@mathesisvenezia.it

Abstract

Franceschi's recently discovered folder of writings sheds new light on his *Cifra delle Caselle*, and *Falso Scontro* ciphers; in fact he had in mind a *uera ziffra* (true cipher) a concept that, in a suggestive parallel, resembles the perfect Shannon cryptosystem, while the *Falso Scontro* (fake key) cipher closely resembles Vernam cipher.

1 Introduction

Hieronimo di Franceschi(1540-1600), his *Cifra delle Caselle* and his *Falso Scontro* ciphers are mentioned by several authors in the cryptographic literature, but both the man and the ciphers were almost unknown until the recovery of the *caselle* [1]. And now a recently found folder of papers[2] , entitled "*Scritture del sec.^{o} Franceschi* Writings by sec. Franceschi", sheds new light on Franceschi's cryptographic philosophy. First of all in several letters to the Council of Ten[3] he boasted his cipher was a *ziffra uera*, a true cipher, as opposed to old ciphers. Franceschi argues that these old ciphers, also known as nomenclators and used all over Europe, are no true ciphers since every sign of them can be deciphered in one and only one letter or syllable or word, the one reported by the *scontro* (the key sheet) so it id possible for a good professor of ciphers, to decrypt them.

But Franceschi had designed another remarkable cipher, the *Falso Scontro*. It is the main subject of this paper, using his newly found papers, to find the roots of Franceschi's invention, and in a reverse logic to link them to modern cryptography. So, first of all, let's start from the end, from the formal definition of a perfect cipher given by Claude Shannon in his paper of 1949[4], that looks very close to Franceschi's not so formal definition of true cipher, almost four centuries before. The reader already expert in this matter can safely continue to section 4.

2 Shannon's Definition of a Perfect Cipher

Claude Shannon in 1949 defined a perfect cryptosystem using the uncertainty function $H(_)$, equivalent to the information used in computer science, and to the entropy used in physics, that gives a measure of the uncertainty, here in particular of a given text[5].

Uncertainty should be zero when we are certain, here when we do know exactly the text; the maximum value should be when we know nothing about the text. A good measure is the number n of possible cases (texts) usually a huge number, so it is better to use the mathematical function of logarithm, the logarithm of the number of possible values; this is consistent with the case of certainty since $\log(1) = 0$, and for the case of n equally probable values $H = \log(n)$. The base of the logarithm is not important, it is just a change of the unity of measure. Here we will use base two, as it is in computer science. Using base 2 H can be interpreted as the number of binary devices necessary to store the information, for instance to store numbers in the range 0..15 one need $\log_2(16) = 4$ four bits, for example 4 lamps (on/off) ...

This definition is good only if all values are equivalent, have the same probability. In the general case, where we have different probabilities p_i,

[1] See for more details: (Bonavoglia, 2019a)

[2] They are in *ASVe, CX Cifre, chiavi e scontri di cifra ... busta 6*. Franceschi's papers are difficult to read, he is very verbose, obsessive and argumentative in describing his ciphers against his opponents; and he is reluctant to give technical details while listing the merits of his ciphers

[3] The *Consiglio di Dieci*, mostly spelled briefly as Cons^o di X, here also **CX**, was a powerful court and executive organ of the Republic, made of ten noblemen elected by the Major Council. six ducal councilors and the Doge himself, so the Ten were really Seventeen.

[4] See (Shannon, 1949) and also (Shannon, 1948)

[5] For more details see (Bauer, 2007) p. 491.

the definition requires a sort of weighted average: having n possible cases $i = 1..n$ with probability p_i the uncertainty is:

$$H = -\sum_{i=1}^{n} p_i \log_2 (p_i) \tag{1}$$

If the probabilities are all equal, $p_i = \frac{1}{n}$ then one can simplify this formula: $H = -\sum_{i=1}^{n} \frac{1}{n} \log_2 \frac{1}{n} = -n\frac{1}{n}(-\log_2 n) = \log_2(n)$, reducing to the first definition seen above, $H = \log_2(n)$:

The simplest case is the binary one, where only two equally probable events are possible, like an urn containing red and white balls in equal quantity, so $p(W) = p(R) = \frac{1}{2}$ and $H = \log_2 2 = 1$. This value has been taken as the unity of measure of H, uncertainty alias information, called bit.

The opposite case is when there is no uncertainty at all, for instance an urn containing only white balls. Then $p(White) = 1 \rightarrow H = \log_2(1) = 0$), here we have uncertainty zero, as expected.

Coming to letters of a text, the uncertainty of a single letter using a 26 letter alphabet depends on many things; first, if the letters are extracted at random from an urn containing 26 balls each of them labeled with one of the letters; then extracting a letter at random we have $p = \frac{1}{26}$ is : $H = \log_2(26) \approx 4.7 bit$

This result has an interesting meaning: to represent a letter of the alphabet one needs 5 bits of information, for instance five lamps that could be on or off, or five binary numbers 0 or 1 or five circles that can be holes or not. This is the case of Baudot code, a telegraphic code used around 1900, that used a paper tape having, for each row, five dots punched or not, that is 5 bits, codifying alphabet letters, numbers and various signs into a 5 bit string. So letter A is codified into 11000 a binary representation of number 24, B is codified into 10011 binary for 19 and so on[6]. Of course in a text written in a natural language, the letters have very different probability, for instance the probability of a letter **E** in an English text is $p(E) = 0.1144 = 11.44\%$, while $p(Z) = 0.0026 = 0.26\%$; this means that the uncertainty, alias information, alias entropy, is quite less than 4.7 and that a compression of data is possible.

According to Shannon, a cryptosystem is said to be perfect if the two following conditions are both satisfied, where P is the plaintext, and C is the ciphertext

$$\begin{aligned} H(P) &= H_C(P) \\ H(C) &= H_P(C) \end{aligned} \tag{2}$$

the first equation, translated in human readable language, sounds: the knowledge of the plaintext is the same either we know the cipher text, either we do not know it. In other words the knowledge of cipher text gives no information about the plain text. And vice versa in the second equation. After that Shannon defines a cryptosystem as "independent key if a similar condition is true for the plain text and the keytest:

From all this a pair of interesting consequences follows, for a perfect cryptosystem:

- If a given good plain text P is encrypted using key K producing the cipher text C one can always invent a fake key FK that translates C into any other required fake plain text FP. See below, section 6.
- If an enemy gets a couple of plain text P and the corresponding cryptogram C, he can easily recover the key used K, but this is useful only to decrypt C into P, already in his hands; in other words possession of the key is here completely useless.

The key used with such a perfect cipher, must be used once and only once, this is the reason these ciphers are called One Time Pad, shortly: **OTP**.

All this is wonderful in the theoretical world, but very difficult to fully implement into a real encrypting tool. Indeed a cipher of the like had been presented 30 years before Shannon, but lacked the most important piece to be really a perfect cipher.

3 Vernam Cipher

The Vernam cipher was first introduced by Gilbert Vernam in 1919 who patented a cryptosystem based on the XOR addition, symbol $\oplus$ and on the already mentioned Baudot code. Every letter or sign of the plain text P is converted into a sequence of 5 bits, so a text of 50 characters will require 250 bit. As a key you must use a random sequence K of 250 and make the XOR addition, bit by bit; the resulting sequence of bits is the cryptogram $C = P \oplus K$.

About the **XOR** addition, it is simply an addition modulo 2 with only two numbers 0 and 1; the possible cases are only 4: $0 \oplus 0 = 0$; $0 \oplus 1 = 1$; $1 \oplus 0 = 1$; $1 \oplus 1 = 0$. One can also interpret it in a geometrical way, as the concatenation

[6]The full Baudot code may be easily found on the web.

of only two possible rotations 0 as no rotation, 1 as a rotation of a flat angle, 180^o. So, it is intuitive that $1 \oplus 1 = 0$.

A XOR addition has a surprising and useful property: it is identical with its inverse, the subtraction modulo 2, as can be easily verified. So XOR is also the deciphering function $P = C \oplus K$.

Finally the Vernam cipher should use a key totally disordered and infinite[7]. This is necessary; using a finite key repeated periodically, statistical cryptanalysis is possible and the cipher is not perfect.

In conclusion the Vernam patent gives only a simple way to implement a polyalphabetic system into an electric device; but to be a perfect cipher it lacks the most important piece, a generator of a truly random sequence of bits.

Indeed many devices to generate random sequences were invented, particularly encrypting machines, like Lorenz and Siqaba, and nowadays software tools, algorithms, are used to produce sequences of random numbers, but these are always pseudo-random.

4 Franceschi's View: Old Ciphers vs True Ciphers

Now, let's do a 400 year leap backward, Venice in the 1500s, when Hieronimo di Franceschi was the top deputy of ciphers.

As stated above a folder of Franceschi's papers was recently found in the Venetian Archives *ASVe Consiglio di Dieci (CX), Cifre, chiavi e scontri di cifra busta 6.new*. It has many letters about the *Cifra delle Caselle* but also about the *cifra del Falso Scontro* mentioned in section 1.

In several letters to the **CX** Franceschi argues that the ciphers used in the present by the **CX**, basically nomenclators, were not true ciphers, and he calls them *ziffre uecchie* (old ciphers), because a ciphertext got with one of these ciphers had only one possible solution, indeed each cipher sign had one and only one meaning, the one found in the *scontro*(the key-sheet). This means it had inside all the information about the text, and there were already methods using frequency analysis, well known also to Venetian *cifristi*, to decrypt them without knowing the *scontro*.

Here is the original text[8]:

> Queste ziffre essendone alcune composte de simplici lettere et altre de lettere sillabe et alcune dittioni come è detto sono per necessità sottoposte all'obligo de simili caratteri per la qual simiglianza de caratteri quando fussero intercette non possendo esse riceuer mai altro senso differente, se non l'istesso che è formato sotto quel scontro, con che è stata scritta.possono esser sottoposte al pericolo di esser interpretate senza l'incontro più facilmente er più difficilmente secondo la diligentia et negligentia di chi le scriue.
> Onde per questa causa la ziffra da me ricordata fu accettata per esser quella impossibile d'esser mai cauata senza l'incontro, quando bene fusse intercetta, et capitasse in mano di professore che ne sapesse ancor formar di tal natura.

In contrast, he boasted the his cipher produced a ciphertext that had no information about the plaintext, because each sign of the encrypted text could stand for any letter, just changing the key. This aspect was underlined a few years before by Bellaso, [9], who in his first booklet of 1553[10] wrote also that the key length was not important and in fact he recommended a short word or a verse easy to remember.

Franceschi knew the ciphers of Bellaso[11] but was at least aware that a long and disordered key was better. And such is the key of the *caselle*.

5 The Cifra delle Caselle

The *Cifra delle Caselle*[12] is a superencrypted cipher invented by Franceschi about 1576[13].

[7] Indeed Vernam didn't require this. It was Joseph Mauborgne another well known American cryptographer to state that the cipher was much stronger using an infinite and disordered sequence of bits.

[8] English: These ciphers, some being composed of simple letters, others of letters, syllables, and a few words, as told, are necessarily under the obligation of correspondent characters, and for this obligation, were they intercepted, since they could not mean other different meaning than the one established by the key used to write it, they are under the danger to be interpreted without the key, more easily or more hardly according to the diligence and negligence of the writer.
Therefore for this reason the remembered cipher of mine was accepted, being the one impossible to be decrypted without the key, even if intercepted, and happened in the hands of a professor that knew how to write similar ciphers.

[9] It is a property of the polyalphabetic ciphers, Bellaso does not seem aware that this independence could be extended to a whole test only with an infinite *contrasegno*. Was Franceschi aware of this?

[10] (Bellaso, 1553)

[11] Bellaso's first booklet was presented and printed in Venice, Bellaso's book is listed among Zuan Francesco Marin's papers in the 1578 *post mortem* inventory, and Franceschi mentions several times Bellaso in his letters.

[12] See (Bonavoglia, 2019a) and (Bonavoglia, 2020)

[13] A recently found file of Franceschi's papers shows that *caselle* came after the first mode of *Falso Scontro*, probably as a simplification of it to meet the objections of Z.F. Marin, then main deputy to ciphers of the time: introduction of the grid with windows (the *caselle*) to facilitate arithmetic oper-

Cipher A16-36 alphabet

a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*z*
16	13	1	15	2	4	19	20	8	14	7	17	18	10	9	12	5	11	3	6
36	33	21	35	22	24	39	–	28	34	27	37	38	30	29	32	25	31	23	26

Figure 1: The A 16-36 cipher, used as first step of encryption. The 20 letters are encrypted with two homophones differing by 20: A with 16 36, ... equivalent to a modulo 20 arithmetic. Only H ha a single cipher 20. There was also a small dictionary of 60 words in the range 40..99.

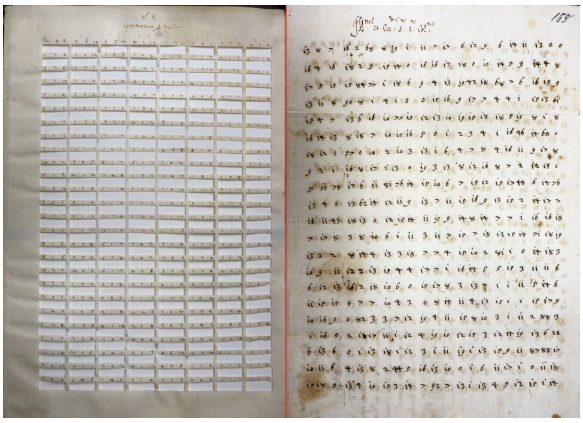

Figure 2: The *grata* Germania (Holy Roman Empire, Prague being the seat of Emperor Rudolf II); with 8 windows of 3 numbers, giving 24 columns and 26 lines, for a total of 624 numbers. On the right a message encrypted with this grid, a letter dated Jan 23, 1581, from Prague by Venetian ambassador A. Badoer. *ASVe CX Cifre, chiavi e scontri di cifra ... busta 4 - ASVe CCX Lettere degli Ambasciatori in Germania, b.12 c.155.*

1. A small cipher called A 16-36, having an alphabet of 20 letters with 2 homophones, and a 60 words dictionary. See figure 1
2. A polyalphabetic cipher using a paper grid with windows (*caselle*) for a key of 624 numbers. See figure 2.

So to encrypt you have to use the cipher A 16-36 to convert letters into a sequence of numbers p_i(i is the ordinal of the letter in the text); now you subtract the first number k_1 of the grid from p_1 the first of the plain text; calculate $c_1 = p_1 - k_1$ and write it inside the window under the number k_1; if $k_1 > p_1$ then use the highest homophone as p_1 or add 20. and so on $c_i = p_i - k_i$. All this is equivalent to a modular difference: $c_i = p_i - k_i \pmod{20}$[14]

To decrypt you put the encrypted sheet under the grid, and add every number of the grid with the number under it in the window; the resulting number is the cipher of the plain letter, given by the A 16-36 cipher; mathematically: $p_i = c_i + k_i$ or, calling $P = (p_0 \dots p_i \dots p_n)$ and in a similar way K and C you can write the encryption formula, using modern algebraic symbolism, in a very simple way:

$$\begin{array}{lll} C = P - K \pmod{20} & (toencrypt) \\ P = C + K \pmod{20} & (todecrypt) \end{array} \quad (3)$$

that is valid for alphabet letters, not for words that having a cipher in the range 40..99 do not requite modulo 20 arithmetic. Apparently Franceschi did not realize that these 60 words did not add strength to the cipher in an appreciable measure.

All this recalls Vernam cipher; the A 16-36 cipher vs the Baudot code to codify letters into numbers; the subtraction/addition modulo 20 vs the XOR modulo 2 operation.

5.1 Was the Cifra delle Caselle really Safe?

But was this cipher perfect, in Shannon's sense, or near to perfection?

The problem here is the key, the grid of 624 numbers, exactly one page; that is enough for short messages, for longer the page must be reused, worse it remained in use for years, so the key is disordered but finite and the cipher is not perfect. Theoretically methods used to break Vigenère could be used here also, knowing the size of a grid/page, well visible on the cipher sheet, one could simply divide the cryptogram into 624 (or fewer) cryptotexts, the first with all the first numbers of each page, the second with the second numbers of each page and so on, getting 624 MASC[15] cryptograms. But these messages were of course very short, not enough for a statistical cryptanalysis. One should collect tens of messages for that, not a light task. So the cipher is not perfect but very strong, surely much stronger than other polyalphabetic ciphers of the age like Bellaso and Vigenère that recommended the use of short keys, easy to remember[16]. That is better for ease of use, while *caselle* is much better for the safety of the cipher. Bellaso in his second book-

ations; two homophones equivalent to an arithmetic modulo 20 to keep numbers in the interval 1..19; swap roles of addition and subtraction; added a small nomenclator, while the fake key option was apparently absent.

[14] Only for letters; for words in the range 40..99 it is a normal difference.

[15] MASC is a very common acronym for Mono-Alphabetic Substitution Cipher.

[16] Of course, using Bellaso's of Vigenère's tables with an infinite and disordered key never to be reused, one has a perfect cipher.

let[17], apparently realized this problem and recommended also a poem or a verse as a long key easy to remember by heart. Such a key is clearly not disordered.

Trying to answer the question above: *caselle* was not perfect but on the right path to perfection.

6 The Idea of a Fake Key

As seen above in a perfect cipher the encrypting formula can be inverted, from any cryptogram C one can get any other plain-text FP just using the key $FK = FP - C \pmod{20}$.

This is the basic idea for a *Falso Scontro* cipher; if the fake key FK ends up in the hands of the enemy he will get the fake message FP.

But, what could be the practical use of this device? Could it be of interest in the real world? Indeed it was. On August 26, 1587[18] the CX approved Franceschi's *Falso Scontro* cipher to be used for communications with the embassies in Paris and Constantinople.[19] there are two huge grids with the indications, embassy in France and embassy in Constantinople. That day the CX wrote[20]

> [...]et essendo ancora grandemente à proposito che per ogni caso d'inquisitione, o di uiolenza che fussi fatta da' Turchi, per intender il contenuto delle Ziffre Nostre, ui sii celata sempre la uera intelligenza de gli auisi et cose Nostre, il fideliss^{o} sec^{o} del Senato Hier.mo di Franceschi[...] si è offerto di dare oltra quella delle caselle introdotta da lui, una nuova Ziffra di simili non più usata,

Franceschi had this new idea in mind for many years, and now had the opportunity to see his invention tested on the road, one key for Paris and one for Constantinople. But how did this cipher work? Long research inside the Venetian Archives finally resulted in the good luck to find papers, notes and examples about this cipher. More than detailed instructions Franceschi writes down the merits of his cipher and some examples; it was anyway more than enough to fill a good part of the puzzle, leaving a few pieces unsolved.

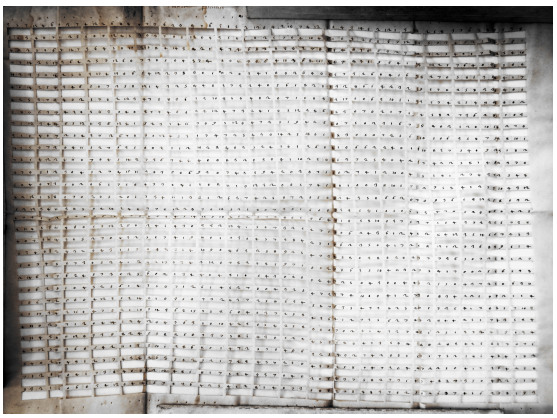

Figure 3: This huge *grata* in parchment has 20 columnns of 3 numbers each and 31 rows, for a grand total of 1869 numbers. It is likely the grid to be used with the *Falso Scontro* cipher, first mode. *ASVe CX Cifre, chiavi e scontri di cifra ... busta 6.3.*

7 Franceschi and the Falso Scontro

So, we now have a lot of pieces of the puzzle falling to their place, let us see a list of the main documents found[21] .

- Several loose sheets bearing a complete example of use in the first mode, see figure 5.
- A large *scontro*, a nomenclator labeled N. 11 in the Franceschi's book of cipher starting in August 1578. There is a signature of Franceschi, bottom right, asserting this n.11 cipher is the one approved by the CX on 1587, 31 August. See figure 7 and 9.1.
- The CX decree of August 26, 1587 approving the *Falso Scontro* with only a generic description of the basic idea.
- Two huge grids,ready for France and Constantinople. See figure 3
- A sheet signed by Franceschi describing two modes of use of this cipher, with a few details. See figure 4.
- A sheet signed by Franceschi having at its top an example of the second mode, using a square; the same example is found in many other sheets of *busta 7*.
- A memory dated January 1606, and a booklet, June 1606, by Pietro Partenio the archrival of Franceschi, saying this cipher could not be used because too slow,

[17](Bellaso, 1555).

[18]As stated above the idea was much older, a cipher of the like, most likely the first mode, was approved by CX in 1573, but never used for the opposition of Z. F. Marin.

[19]Indeed in busta 6.3 of the collection *ASve Cifre, Chiavi e Scontri di cifra ...*

[20]English: [...] and since it is still largely appropriate that in case of inquisition, or of violence that might be done by the Turks, to understand the content of our ciphers, the true intelligence of the notices and our affairs, the most faithful secretary of the Senate Hieronimo di Franceschi [...] offered to give in addition to the one of the *caselle* introduced by him, a new cipher of similar no longer used,

[21]The exact chronological order can not be determined, because most papers have the usual signature at the beginning: "... io Hier^{mo} di Franceschi ..." but no date. An approximate date was induced by mentions of persons or of events. For instance if Z. F. Marin is mentioned as a living person, we are before 1578; if the CX decree of August 1587 is mentioned we are after that date ...

being a letter by letter cipher, and dangerous because the fake key required a square.

Franceschi himself gave the following summary description[22] of the properties of his cipher, that could be used to implement a fake key cipher in two different modes.

8 Falso Scontro, 1st Mode

Here is the sheet signed by Franceschi listing the seven merits, called *condicioni*, of the first mode of the cipher[23]

Ha la ziffera mia queste condicioni
di grandissimo comodo e utile

1. *Leuar da questa palese si può un significato finto come si uuole, falso et uerisimile . Sopra l'istessi caracteri, poi si manifesta l'auiso uero securo et in tutto nascosto ad ognuno.*
2. *E facil a componer in qual ci uoglia lingua, et impossibile che s'intenda mai se non da colui che da me prima conoscenza la chiaue, o contrasegno con il quale s'apre l'interior mio rinchiuso.*
3. *Si mutano le chiaui o segni ad infinito, né scoprir si possono benché altre fiate alcuna di quelle insegnata s'hauesse.*
4. *Non u'entra alcun carattere inutile o uano, né scriue per sillaba, o dicione, ma ciascuna lettera scriui per una lettera sì nel senso bugiardo, come nel utile*[24]
5. *Intender si può la intencion secura senza l'uso del auiso finto ouer suo alfabeto alcun, o contrasegno, il che è assai di minor tempo e fatica.*
6. *Nel componer la ziffra predetta, hauer si può l'aiuto d'un scrittore, senza pericolo nè dubitacion alcuna d'esser conosciuto l'animo mio, finché co'l segno io reuelarò non lo habbia a chi farà bisogno.*
7. *Nella litera sigillata u'è quello che si ricerca ne accadi per ciò spedir altri messaggij se non per la replica, Inteso però che'l rispondente in alcun modo sia da me prima accennato.*

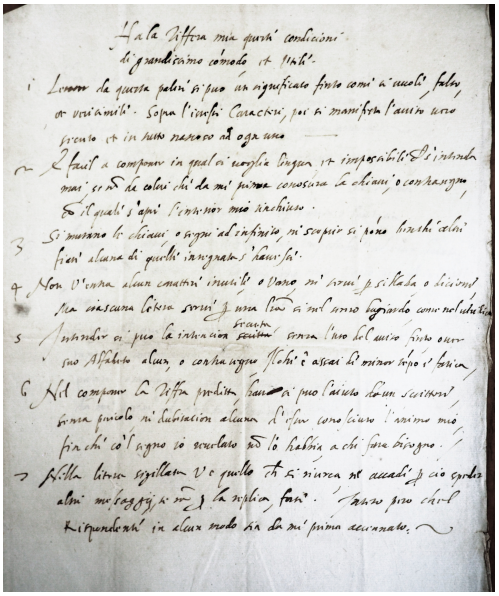

Figure 4: Franceschi's *condicioni* that make the cipher confortable and useful.*ASVe CX Cifre, chiavi e scontri di cifra ... busta 6, carte del sec. Franceschi.*

Point 4 indicates a letter by letter, monoalphabetic cipher, both for the true and fake text; this is in strong conflict with cipher N. 11, a nomenclator with hundreds of ciphers for syllables, words etc. A possible explanation is that N. 11 had to do with the second mode not with the first, another one is that N. 11 was simply abandoned.

8.1 An Example of the First Mode

Using the previous incomplete information, I tried to guess a possible implementation of the first mode; the encrypting procedure requires an addition of the plaintext, previously encoded into numbers and the key; the deciphering a subtraction[25]; finally, a set of four paper sheets with a complete example was found in *busta 7*[26] completing the

[22] This list of properties shows a strong resemblance to the 13 Bellaso's *Singolar qualità delle cifre* in his 1564 booklet, for instance Franceschi's 2nd is similar to Bellaso's 7th, Franceschi's 4th to Bellaso's 4th ... see (Bellaso, 1564). But Bellaso's ciphers had very little in common with Franceschi's, above all Bellaso never uses numbers and arithmetical operations.

[23] English:
My cipher has these conditions of great comfort and useful

1. One can extract from this plain-text a fake text as you like, false and plausible. Over the same characters thereafter the true notice safe and hidden from anyone.
2. Easy to compose in any language and impossible to be ever understood, except by the one that will know the key or *contrasegno* with which one opens the inside closed meaning.
3. One changes keys or signs ad infinitum, and they can not be discovered even if sometimes one had some of the used by them.
4. There are no useless or superfluous characters no syllables or words. But **every letter is written with a letter** both in the false sense than in the truthful one.
5. One can understand the intention written without the fake notice or the fake alphabet any *contrasegno* that is is of minor time or fatigue.
6. To write the before said cipher, one can have the assistance of a scribe without danger nor any dubious that my concepts could be known, until with the sign I will reveal to the one having need of it.
7. In the sealed letter there is all that is needed to send other messages if it isn't done for the reply. But it must be agreed that the respondent should not be informed before by me in any way.

[24] This property closely recalls Bellaso's 4th *singolar qualità* in his 1564 booklet, (Bellaso, 1564).

[25] Similar to Vernam, where the letters were converted into numbers by Baudot Code and then XOR additioned to random numbers.

[26] *ASVe CX Cifre, chiavi e scontri di cifra ... busta 7*

.

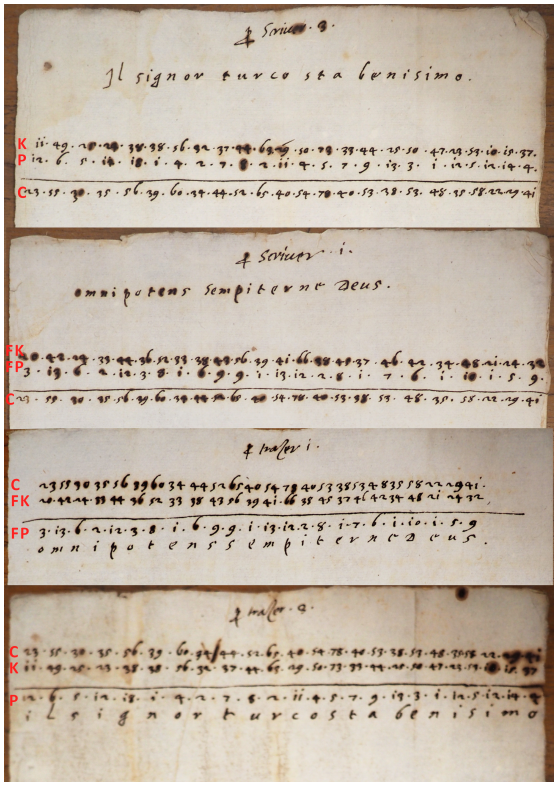

Figure 5: A complete example of the first mode. The red letters were added for a better link to the text. *ASVe CX Cifre, chiavi e scontri di cifra ... busta 7.*

puzzle.

The alphabet for the plaintext is a normal 1:1 scrambled alphabet (MASC) with numbers in the range 1..19[27], the fake alphabet is different but of the same type, MASC; the key is a random sequence of numbers in the range 10..79 so the sum (ciphertext) is alway two digits: 11..79; the example does not show it, but it is very likely the key can be easily written using a grid like those of the *caselle* maybe one of the huge, visible in figure 3, sufficient to cover a rather long message.

So the fake key included also a fake alphabet, different from the true, a superfluous device for secrecy? For this purpose Vernam used a public code or alphabet the Baudot.

Here is the procedure based on Franceschi's examples and seven conditions: I will use the conventional names Alice, Bob and Eva[28]

1. Alice and Bob exchange in some safe way the secret key K (here 23 55 30 35...) with instructions.
2. Alice uses the key K to encrypt the real message P (*Il Signor Turco sta benissimo*), into cryptogram $C = P + K$. By subtracting the fake message FP (*Omnipotens sempiterne deus*) from C you get the key $FK = C - FP$
3. Alice sends by courier the cryptogram C and, hidden in a sealed envelope, FK and the fake alphabet.
4. If the message C arrives undisturbed to Bob, he will decipher C with the good key K received earlier by Alice, retrieving the real message $P = C - K$.
5. Bob will use the FK safely received by Alice as the new good key K[29] to encrypt the next message to Alice, and generate a new random sequence of numbers FK for a new fake messageFP[30]. In this sense FK may stay also for *Future Key*.
6. If Eva captures the courier and under threat gets the cryptogram C and the key FK, she will decipher the fake message $FP = C - FK$.
7. It remains to be understood what happens if Eva opens the sealed envelope with FK. New keys to be generated and exchanged?
8. The play can go on back and forward ad infinitum always with a new key, and the key will always travel before being used for encrypting the message. Even if Eva understands that FK is a fake, FK is and will be of no use for her. Consistent with Franceschi's last condition.

It was possible to implement a software tool doing all the job, leaving also the option to reuse FK as the new K, or to generate a new random key (this would require a new exchange of key between Alice and Bob). The software tests confirm that the procedure works fine, but it is questionable if the successive fake keys could be considered really random, being formed by arithmetic operation with the true and false message, in a recursive formula $K_i = P + K_{i-1} - FP$. More, this formula is not stable, numbers can go out of the range $[0 \ldots 99]$; the fake key should be normalized inside the range $[21 \ldots 79]$ before using it as the

[27] In the examples not every letter appears, and 0 or 20 are not used, so it is not sure which of the two was used.

[28] For those who do not know: Alice is the sender, Bob the receiver of the message; Eva is the spy that intercepts the message and tries to decipher it

[29] One can argue that such a system may be classified as an autokey rather than an OTP; indeed the classical autokey uses only the original message, so it is a classification issue.

[30] This point is not documented by the example, like the previous; it seems the simplest way to fully implement point 3 of Franceschi's conditions: ¡i¿Si mutano le chiaui o segni ad infinito ...¡/i¿

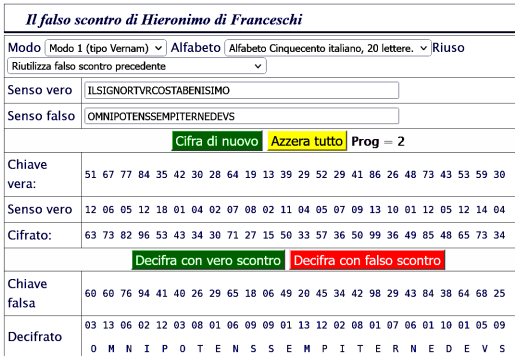

Figure 6: Software simulation of the *Falso Scontro* procedure. One can get the true message using the green button, the false message using the red button.

new key.

A possibility for Eva would be to seize the sealed envelope, open it with a tool leaving the envelocpe intact, copy the key, put it inside the envelope back in its place, leaving Alice and Bob unaware. Next time Eva will be able to read the message[31].

9 Falso Scontro, 2nd Mode

These are Franceschi's *condicioni* for the second mode[33]:

Nel modo secondo

1. Non da suspicion alcuna tal che in palese liberamente scriuer si puo con caratteri, sillabe et dicioni usate ogni aperto concetto latin o volgar et in quale altra si uoglia lingua ancora.
2. Il detto palese che si uede, non è conosciuto per enigma coperto neancho da chi lo porta. Benché iui sia la chiaue del secreto nascosto di qualunque imaginacion o fantasia.
3. È facil a componer et difficil anzi impossibile ad esser leuata se non con l'auiso del contrasegno mio vario però ad infinito.

Here the information is too scarce to arrive at a solid conjecture; it looks like Franceschi simply swapped the roles of plaintext and ciphertext.

[31] In his *Codebreakers* Kahn writes that such devices did exist in the 1700s in Vienna where the imperial secret services were able to open a letter, read it, and close it in a systematic way.[32]. Was a similar thing possible for the sealing wax in the 1500s?

[33] English:

1. It gives no suspicion at all for it can be written as a plaintext with letters, syllables and words used every day, in Latin or Vulgar or any other language.
2. The visible plain text is not recognized as an enigma, not even by the courier. Even if it is the key of any imaginable or phantastic secret.
3. It is easy to write and difficult, impossible to decrypt, except with the aid of my *contrasegno* key, but various to infinity.

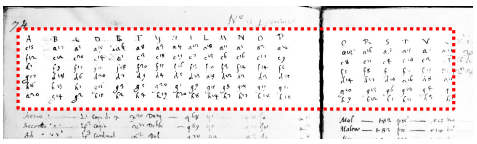

Figure 7: A cut of *Ziffra n.11* inside Franceschi's book, the alphabet is highlighted with a red dotted frame. *ASVe CX Cifre, chiavi e scontri di cifra ... b. 4 f. 16 c. 74.*

9.1 Ziffra N.11 and its Hidden Square

These conditions may have some link with this cipher N.11 found in 1578-87 Franceschi's book of ciphers, visible in figure 7. Another hint comes from the bottom right note of the second sheet, the deciphering list (*per trazer* that is to extract, to decipher):[34]

> *Ziffra N^{o} 11 Nouissima per trazer, fatta da me Hier^{mo} di Franceschi sec^{o} in essecution della deliberation dell'Eccelso Cons^{o} di X, sotto di 26 Agosto 1587 la qual è registrata in fine del presente libro.*

At first look it seems the usual XVI century Venetian nomenclator, but there is an unusual alphabet with six homophones for each letter: the numbers written as exponents, are in the range 1..20 and if the ciphers are rearranged and completed like in figure 8 a partial table of addition modulo 20 appears.

The other letters ***b, e .. z.*** have numbers mostly in the range 1..20, a few between 21 and 99, and represent syllables, numbers, and words.

The best fitting example[35] is present in many copies in the Archives and shown in table 4 and works fine using the square conjectured in figure 8. The first sign is L^{15} ; looking in row L for the number 15 one finds column q, the next sign d^{8} has in row d the number 8 at column u and so on getting a plain text: *Quanto io Hieronimo di Franceschi mi sono dim* written above in the example.

q	u	a	n	t	o	i	o	h	i	e	r	o	n	i	m	o	d
L^{15}	d^{8}	a^{20}	q^{8}	c^{10}	b^{5}	d^{13}	a^{2}	n^{3}	b^{15}	u^{19}	b^{19}	u^{15}	s^{12}	d^{13}	c^{5}	L^{4}	f^{11}
i	f	r	a	n	c	e	s	c	h	i	m	i	s	o	n	o	d	i	m
u^{5}	s^{19}	m^{5}	m^{9}	o^{19}	c^{20}	c^{1}	t^{14}	r^{9}	s^{15}	d^{15}	g^{8}	o^{10}	i^{17}	r^{6}	L^{3}	L^{4}	z^{9}	s^{3}	c^{6}

(4)

Another sheet found in *busta 7* has only the letters of this cryptogram:

L d a q c b d a n b u b u s d c L f
u s m m o c c t r s d g o i r L L z s c

[34] English: Figure N. 11 Very new for trazer, made by me Hieronimo di Franceschi secretary in execution of the resolution of the Most Excellent Council of X, under August 26, 1587 which is registered at the end of this book.

[35] Trying to decrypt the same cryptogram using *ziffra N.11*

Alfabeto

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	z
a^{20}	a^{17}	a^{5}	a^{19}	a^{6}	a^{8}	a^{3}	a^{4}	a^{12}	a^{18}	a^{11}	a^{1}	a^{2}	a^{14}	a^{13}	a^{16}	a^{9}	a^{15}	a^{7}	a^{10}
c^{15}	c^{12}	c^{20}	c^{14}	c^{1}	c^{3}	c^{18}	c^{19}	c^{7}	c^{6}	c^{13}	c^{16}	c^{17}	c^{9}	c^{8}	c^{11}	c^{4}	c^{10}	c^{2}	c^{5}
d^{1}	d^{18}	d^{6}	d^{20}	d^{7}	d^{9}	d^{4}	d^{5}	d^{13}	d^{19}	d^{17}	d^{2}	d^{3}	d^{15}	d^{14}	d^{17}	d^{10}	d^{16}	d^{8}	d^{11}
f^{12}	f^{9}	f^{17}	f^{11}	f^{18}	f^{20}	f^{15}	f^{16}	f^{4}	f^{10}	f^{3}	f^{14}	f^{6}	f^{5}	f^{8}	f^{1}	f^{7}	f^{19}	f^{2}	
g^{17}	g^{14}	g^{2}	g^{16}	g^{3}	g^{5}	g^{20}	g^{1}	g^{9}	g^{15}	g^{8}	g^{18}	g^{19}	g^{11}	g^{10}	g^{13}	g^{6}	g^{12}	g^{4}	g^{7}
h^{16}	h^{13}	h^{1}	h^{15}	h^{2}	h^{19}	h^{20}	h^{9}	h^{14}	h^{7}	h^{17}	h^{18}	h^{10}	h^{9}	h^{12}	h^{5}	h^{11}	h^{3}	h^{6}	

	a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	z
a	20	17	5	19	6	8	3	4	12	18	11	1	2	14	13	16	9	15	7	10
b	3	20	8	2	9	11	6	7	15	1	14	4	5	17	16	19	12	18	10	13
c	15	12	20	14	1	3	18	19	7	13	6	16	17	9	8	11	4	10	2	5
d	1	18	6	20	7	9	4	5	13	19	12	2	3	15	14	17	10	16	8	11
e	14	11	19	13	20	2	17	18	6	12	5	15	16	8	7	10	3	9	1	4
f	12	9	17	11	18	20	15	16	4	10	3	13	14	6	5	8	1	7	19	2
g	17	14	2	16	3	5	20	1	9	15	8	18	19	11	10	13	6	12	4	7
h	16	13	1	15	2	4	19	20	8	14	7	17	18	10	9	12	5	11	3	6
i	8	5	13	7	14	16	11	12	20	6	19	9	10	2	1	4	17	3	15	18
l	2	19	7	1	8	10	5	6	14	20	13	3	4	16	15	18	11	17	9	12
m	9	6	14	8	15	17	12	13	1	7	20	10	11	3	2	5	18	4	16	19
n	19	16	4	18	5	7	2	3	11	17	10	20	1	13	12	15	8	14	6	9
o	18	15	3	17	4	6	1	2	10	16	9	19	20	12	11	14	7	13	5	8
p	6	3	11	5	12	14	9	10	18	4	17	7	8	20	19	2	15	1	13	16
q	7	4	12	6	13	15	10	11	19	5	18	8	9	1	20	3	16	2	14	17
r	4	1	9	3	10	12	7	8	16	2	15	5	6	18	17	20	13	19	11	14
s	11	8	16	10	17	19	14	15	3	9	2	12	13	5	4	7	20	6	18	1
t	5	2	10	4	11	13	8	9	17	3	16	6	7	19	18	1	14	20	12	15
u	13	10	18	12	19	1	16	17	5	11	4	14	15	7	6	9	2	8	20	3
z	10	7	15	9	16	18	13	14	2	8	1	11	12	4	3	6	19	5	17	20

Figure 8: Alphabet of Franceschi's cipher N. 11, with six homophones, and below the same arranged and enlarged to a square, a table of subtraction modulo 20, with a diagonal of 20 instead of the 0 we would expect today. The rows in red are those corresponding to the homophones above. This square table fits perfectly Franceschi's example.

9.2 Partenio's own Falso Scontro

All this closely recalls the last cipher of Pietro Partenio (1538-1620), the archrival of Franceschi[36], in his booklet of June 1606[37] using a square very similar to Franceschi's one, shown in figure 9.

The example given by Partenio is: good message "*Vi sono in Brescia capi ribelli*", fake message "*Dalle sue parole io spero buona pace*". Alice transposes this good message using a key transposition:

i r c n i a v a b n c a i a i b p r s a i o e l o e i s l

and now uses the square in figure 9 so: take the first letter **I** of the transposed text and looks in the row **I** for the number under the first letter of the fake message **D**: she finds number 10, and writes this number above the letter *i* as an exponent and so on; she will get the cryptogram:

$$i^{10}r^{15}c^{8}n^{17}i^{18}a^{13}v^{11}a^{10}b^{15}n^{11}c^{18}a^{4}i^{14}a^{10}i^{3}b^{5}p^{6}r^{9}s^{6}a^{16}i^{12}o^{4}e^{17}l^{13}o^{13}e^{4}i^{2}s^{16}l^{12}$$

If Eva intercepts this cryptogram and uses the previous procedure, looking for the number inside the square, she will get the fake message. Indeed an experienced codebreaker may become suspicious by noting that the letters used as a basis have the frequency distribution of a natural language, and could understand that the numbers are just a diversion.

	S	P	I	R	T	Q	V	A	N	D	C	O	H	L	F	Z	G	E	M	B
I	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
L	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1
M	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2
N	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3
O	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4
P	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5
Q	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6
R	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7
S	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8
T	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9
V	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10
Z	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11
A	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12
B	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13
C	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14
D	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
E	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
F	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
G	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
H	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

Figure 9: The square used in Partenio's last cipher; booklet of 1606 last page.

If Eva intercepts this cryptogram and uses the previous procedure, looking for the number inside the square, she will get the fake message. Indeed an experienced codebreaker may become suspicious by noting that the letters used as a basis have the frequency distribution of a natural language, and could understand that the numbers are just a diversion.

9.3 A Plausible Conjecture about the Last Mode

The best interpretation I could guess by Franceschi's three conditions, example and Partenio's last cipher, assuming the square as a table of addition to avoid calculations, and a swap between plain-text and cipher-text, is the following:,

- Alice encrypts a message into a plain non suspicious text FP using the good square and the numbers used inside a sealed envelope, together with a fake square that produces a fake message;
- Bob receives FP and using the good square and the numbers in the sealed envelope translates it into the good text.
- If Eva intercepts the non suspicious message FP, she may not realize it is a cryptogram;

give inconsistent result, so that cipher may have been a first try later abandoned.

[36]The dispute between Franceschi and Partenio can now be seen in a new light, not only a clash of [bad] characters, but also as a clash between two different methods of cryptography; Franceschi was a supporter of polyalphabetic ciphers, such were his *ziffre uere*, and he despised nomenclators like *ziffre uechie*. Partenio defended nomenclators, syllabaries and dictionaries, possibly reinforced by a super-encryption and flaunted contempt for encrypting letter by letter. On the nomenclator-polyalphabetic question in the Renaissance, see (Kahn, 1996), chapter: "On the origin of a species".

[37](Partenio, 1606). A cipher almost surely derived from this second mode, that may help here.

A feew months before, Jan 30, 1606, talking of Franceschi's *Falso Scontro*, in a letter to the **CX**, Partenio wrote[38]

[...] perché se il .q. magnifico segretario Franceschi uoleua dar senso finto alla sua cifra la quale per lunghezza et difficoltà non si è potuto adoprare; bisognaua in occasione di leuarlo che si cauasse con il solo quadrato, che in tal senso diuentaua scontro, il quale portaua seco due mortali oppositioni; prima di lunghezza estrema scriuendosi a lettera per lettera, poi per mezo di esso quadrato hauerebbe dato sospetto del uero senso, sapendosi che lui adopraua una casella o grada.

Indeed a *quadrato* (square) is found in the mentioned cipher in the 1606 booklet of ciphers[39]

but even if she opens the envelope, and uses the numbers with the fake square she gets a fake message.

It is just a conjecture, and this second mode remains an enigma, many pieces of the puzzle are still missing and can only be guessed.

10 Conclusions

In addition to the almost complete reconstruction of the *Falso Scontro* cipher, a suggestive parallel emerges from this research: Franceschi's idea of a *uera ziffra* resembles Shannon's idea of a perfect cryptosystem[40], and the *Falso Scontro* first mode cipher resembles Vernam cipher[41].

If the procedure of the first mode was the one conjectured above, it had a disordered and infinite key, or at least a huge one, one of the first, maybe the first of this kind; possible previous candidates are Trithemius's *Orchema*[42], p. 567, but Trithemius dancing letters were not really disordered and a similar cipher of the *Codice Urbinate* dated 1501-1505 digitized and published by the Vatican Apostolic Library[43]; it is attributed to Federico da Montefeltro, but since he died in 1482, the attribution is likely wrong.

The *Falso Scontro* although officially adopted by the CX in 1586 as seen above, was, as far as we know, never used. As Partenio wrote, the cipher was seen as too long and difficult[44].

[40] One may argue that this statement is exaggerated: assuming that obviously "resembles" is not the same as "is equivalent", here I'm speaking only of the basic idea of a perfect cipher, not of the mathematical formulation, something well beyond the mathematics of the sixteenth century. Franceschi's statement that using a *uera ziffra*, given any desired fake-text one can always find a fake-key good to get it, hints that his basic idea was similar to Shannon's about the indipendence between plaintext and ciphertext, and between plaintext and key.

[41] Both use addition/subtraction to encrypt/decrypt; in the first mode Franceschi clearly is aware that to be unbreakable and to allow the fake key, the key must be long at least as the ciphertext; the *caselle* did not satisfy any more this requirement and the fake key was also dropped.

[42] See (Trithemius, 1613)

[43] *Biblioteca Apostolica Vaticana: Manoscritti digitalizzati - Urb.lat.948*

[44] Inside the draft of the final 1599/1600 relation of the five noblemen called to examine the Partenio vs Franceschi dispute, one reads that the day of the final test, Piero Amai, son of Agostino Amadi and the pupil of Franceschi, apologized for not wanting to participate in this contest using the *casella* ... not being very good at adding and subtracting, he did not feel suitable for that test. Franceschi died not long after, and his ciphers died with him.

Acknowledgments

Special thanks to the archivists of the State Archives of Venice, for the helpfulness shown, and to Richard Bosch, Portland, Oregon for reviewing the English language.

References

Bauer, F. L. (1991 - 2007). *Decrypted secrets: Methods and Maxims of Cryptology*. Springer, Berlin.

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

Bellaso, G. B. (1555). *Noui et singolari modi di cifrare de l'eccellente dottore di legge messer Giouan Battista Bellaso nobile bresciano, con le sue regole & essempi con somma & chiara breuità composti ..* L. Britannico, Brescia.

Bellaso, G. B. (1564). *Il vero modo di scrivere in cifra*. L. Britannico, Brescia.

Bonavoglia, P. (2019a). The cifra delle caselle a xvi century superencrypted cipher. *Cryptologia*.

Bonavoglia, P. (2019b). Hieronimo di franceschi and pietro partenio: two unknown venetian cryptologists. Uppsala. Linköping University Electronic Press.

Bonavoglia, P. (2020). A partenio's stegano-crypto cipher. Uppsala. Linköping University Electronic Press.

Kahn, D. (1967 - 1996). *The codebreakers*. Scribner, New York.

Partenio, P. (1606). *Cifre di Pietro Partenio*. Manoscritto, Archivio di Stato di Venezia, Venezia.

Shannon, C. E. (1948). A mathematical theory of communication. *The Bell System Technical Journal*.

Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell System Technical Journal*.

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