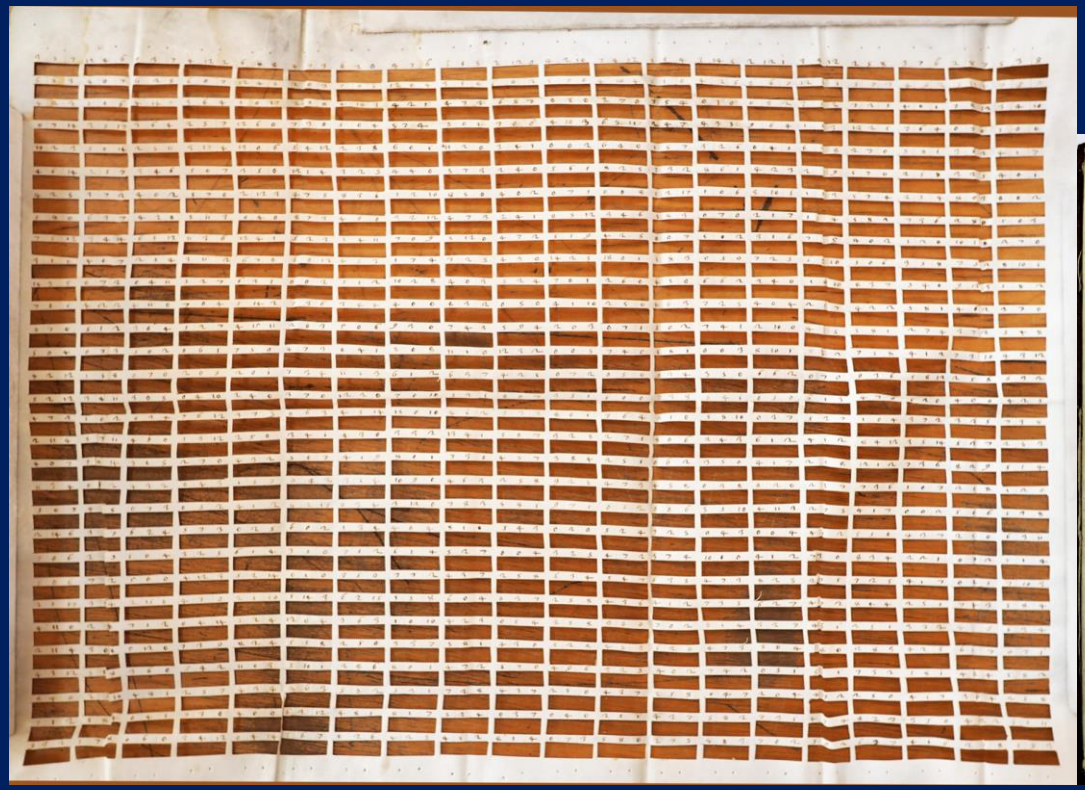
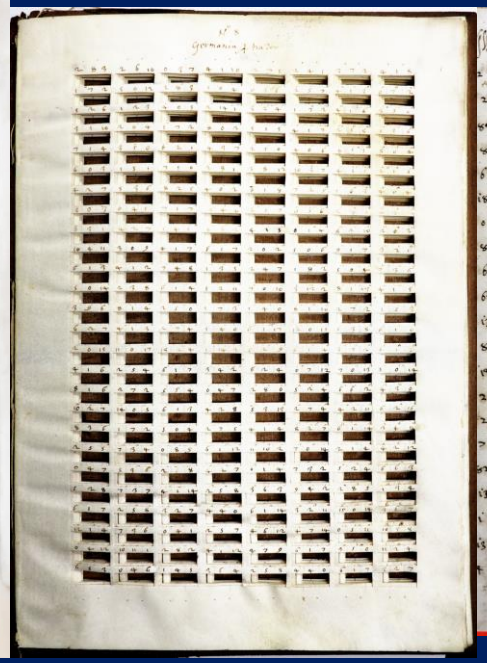
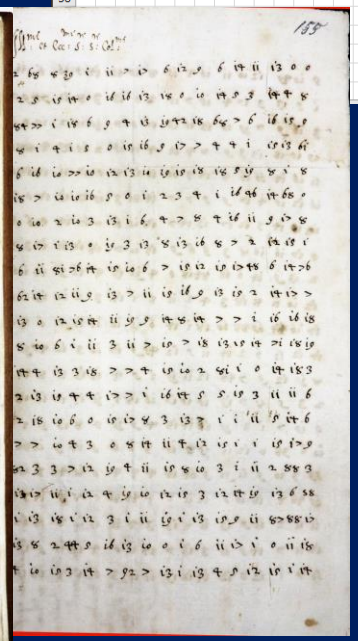
The Enigma of Franceschi's *Falso Scontro*

An unknown battle between polyalphabetic and nomenclator







	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ	AK	AL	AM	AN	AO	AP	AQ	AR
1		a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	z			a	n	o	g	h	c	e	u	f	s	z	m	i	q	p	t	r	b	l	d
2	a	20	17	5	19	6	8	3	4	12	18	11	1	2	14	13	16	9	15	7	10			a	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
3	b	3	20	8	2	9	11	6	7	15	1	14	4	5	17	16	19	12	18	10	13			b	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2
4	c	15	12	20	14	1	3	18	19	7	13	6	16	17	9	8	11	4	10	2	5			c	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14
5	d	1	18	6	20	7	9	4	5	13	19	12	2	3	15	14	17	10	16	8	11			d	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
6	e	14	11	19	13	20	2	17	18	6	12	5	15	16	8	7	10	3	9	1	4			e	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13
7	f	12	9	17	11	18	20	15	16	4	10	3	13	14	6	5	8	1	7	19	2			f	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11
8	g	17	14	2	16	3	5	20	1	9	15	8	18	19	11	10	13	6	12	4	7			g	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
9	h	16	13	1	15	2	4	19	20	8	14	7	17	18	10	9	12	5	11	3	6			h	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
10	i	8	5	13	7	14	16	11	12	20	6	19	9	10	2	1	4	17	3	15	18			i	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7
11	l	2	19	7	1	8	10	5	6	14	20	13	3	4	16	15	18	11	17	9	12			l	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1
12	m	9	6	14	8	15	17	12	13	1	7	20	10	11	3	2	5	18	4	16	19			m	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8
13	n	19	16	4	18	5	7	2	3	11	17	10	20	1	13	12	15	8	14	6	9			n	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
14	o	18	15	3	17	4	6	1	2	10	16	9	19	20	12	11	14	7	13	5	8			o	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
15	p	6	3	11	5	12	14	9	10	18	4	17	7	8	20	19	2	15	1	13	16			p	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5
16	q	7	4	12	6	13	15	10	11	19	5	18	8	9	1	20	3	16	2	14	17			q	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6
17	r	4	1	9	3	10	12	7	8	16	2	15	5	6	18	17	20	13	19	11	14			r	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3
18	s	11	8	16	10	17	19	14	15	3	9	2	12	13	5	4	7	20	6	18	1			s	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10
19	t	5	2	10	4	11	13	8	9	17	3	16	6	7	19	18	1	14	20	12	15			t	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4
20	u	13	10	18	12	19	1	16	17	5	11	4	14	15	7	6	9	2	8	20	3			u	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12
21	z	10	7	15	9	16	18	13	14	2	8	1	11	12	4	3	6	19	5	17	20			z	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9
22																																													
23																								a	n	o	g	h	c	e	u	f	s	z	m	i	q	p	t	r	b	l	d
24																								a	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
25																								n	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
26																								o	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
27																								g	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
28																								h	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
29																								c	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14
30																								e	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13
31																								u	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12
32																								f	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11
33																								s	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10
34																								z	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9
35																								m	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8
36																								i	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7
37																								q	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6
38																								p	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5
																								t	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4
																								r	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3
																								b	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2
																								l	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1
																								d	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

HistoCrypt 2022 Amsterdam

Foreword

A premise: this presentation is a bit different from the proceedings, for the following reasons:

1. The mathematical exposition of Shannon's theorem, and Vernam cipher will be only hinted, time is limited and the matter is nothing new, most mathematicians know it already, others can read the proceedings if interested;
2. The chronological order had to be changed, because of new findings in the archives, above all the examination of lot of papers. Apparently *Caselle* approved in 1577 came before *Falso Scontro*, now there are documents proving the idea of *Falso Scontro* dates 1572/73

An unsolved question

Two years ago, beginning of 2020, after two years of research in the State Archives of Venice, I thought there was little left to discover and it was time to close the research and the book I was writing.

One of the few unsolved questions was the ***Falso Scontro*** of Franceschi a mysterious cipher approved by the Council of Ten in August 1587.

Shortly after, the Coronavirus crisis caused lock down and disruptions of service, only at the end of 2021 service came back to normal.

And a surprising discover, a box full of papers, among them a folder entitled "*Scritture del segretario Franceschi*" opened the door to the solution

The characters

Consiglio di Dieci *(Council of Ten)*: the powerful organ of the Republic in charge for security, espionage and cryptography: named a few secretaries as deputies of ciphers, in charge for encrypting, decrypting diplomatic and military dispatches, and everything about ciphers,

Zuan Francesco Marin (or **Marino**, about 1510- 1578): was the top deputy of ciphers until 1578, the last great Venetian cryptanalist, he boasted to be the only one left, able to decrypt foreign ciphers. Author of a treatise «*De l'arte de estrazer le ziffre senza scontro*»

Hieronimo di Franceschi (1540-1600): his family was a distinguished in Venice since the XI cent. His uncle Andrea was *Cancellier Grande* of the Republic, many others were secretaries in the Ducal Chancellery and the Senate. He was the main deputy of ciphers for the CX from 1578 to 1600, best known for the invention of the *Cifra delle Caselle*

Pietro Partenio (1538-1620): came to Venice from Spilimbergo (Friuli), He was the owner of a renowned notary's office from 1563 to 1610, and was many times member of the notary council of Venice. About 1590 he became interested in ciphers and donated to the CX a few ciphers

Piero Amai, the son of **Agostino Amadi** author of a monumental treatise of ciphers. He asked to be trained as a deputy of ciphers in 1590, was the main aid of Franceschi in the dispute with Parrtenio, and succeeded him as top deputy of ciphers

Polyalphabetic vs Nomenclator

[…] This explains Matteo's paean: “The key cipher is the noblest and the greatest in the world, the most secure and faithful that never was there man who could find it out.”

Why, then, did the nomenclator reign supreme for 300 years after Porta?

Why did cryptographers not use this “noblest” and “most secure” cipher instead?

Apparently because they disliked its slowness and distrusted its accuracy. Encipherment in a polyalphabetic system, with its need to keep track of which alphabet was in use at every point and to make sure that the ciphertext letter was taken from that alphabet, could not compare in speed with a nomenclator encipherment.

- David Kahn *Codebreakers,* «On the Origin of a Species», 1967-1996

Franceschi vs Partenio
A case with reversed roles

[…] The case we are going to examine is the one of Venice where there was such a debate, but with reversed roles: they were

1. a citizen, secretary of the Ducal Chancellery and of the Senate, **Hieronimo di Franceschi**, an advocate of the polyalphabetic cipher and a fierce adversary of *old ciphers*, where every sign has a unique deciphering.
2. a private notary, **Pietro Partenio** to act as the advocate of nomenclators, who despised coding letter by letter as in the 90-year-old ciphers of the Tritemius, as obsolete methods .

Both agreed in considering the ciphers used in those years as not safe and promoting new ones.

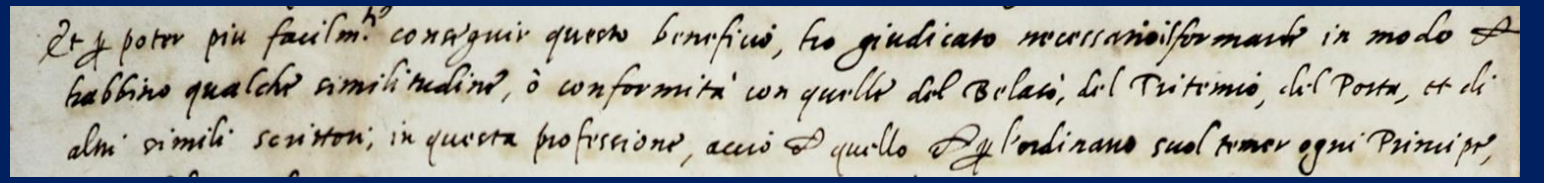
Franceschi's *uere ziffre* (true ciphers) as opposed to *ziffre uecchie* (old ciphers)

- Franceschi burst onto the scene in 1572-1573, proposing a new cipher, and his theory about ciphers.
- A *uera ziffra = true cipher* is **a cipher that it is absolutely impossible to be deciphered without the key**. That can be said in another way: a text encrypted with a true cipher should be independent from the plain text and therefore can decrypted in ***any plain text*** of the same length, simply using an appropriate key; hence the idea of a fake key, in XVI century Italian un ***falso scontro***.
- In contrast in a *ziffra uecchia* = old cipher, every cipher sign **can be deciphered in one and only one letter or word**, if one has ten identical signs in a cryptogram, it is sure these mean always the same plain text letter or syllable or word. Decrypting such a cipher can be difficult, but it is always possible. Such ciphers should rather be called «dark ways of writing».

What had Franceschi in mind for *uera ziffra*?

- Nothing else than a polyalphabetic cipher? Possibly, but the cipher proposed using addition, subtraction and keys long as the message, like a Vernam, goes a step forward.
- Shannon's *perfect cryptosystem*? Of course not, Franceschi did not give a rigorous definition, indeed he did not have the mathematical tools and the formalism to do so. Things like logarithms, modular arithmetic, formal logic … were yet to come. But the basic idea and the cipher proposed hints something similar.
- Just another absolutely unbreakable cipher, like those proposed by so many people in the XVI century? Maybe something more as we will see.

Franceschi and Bellaso

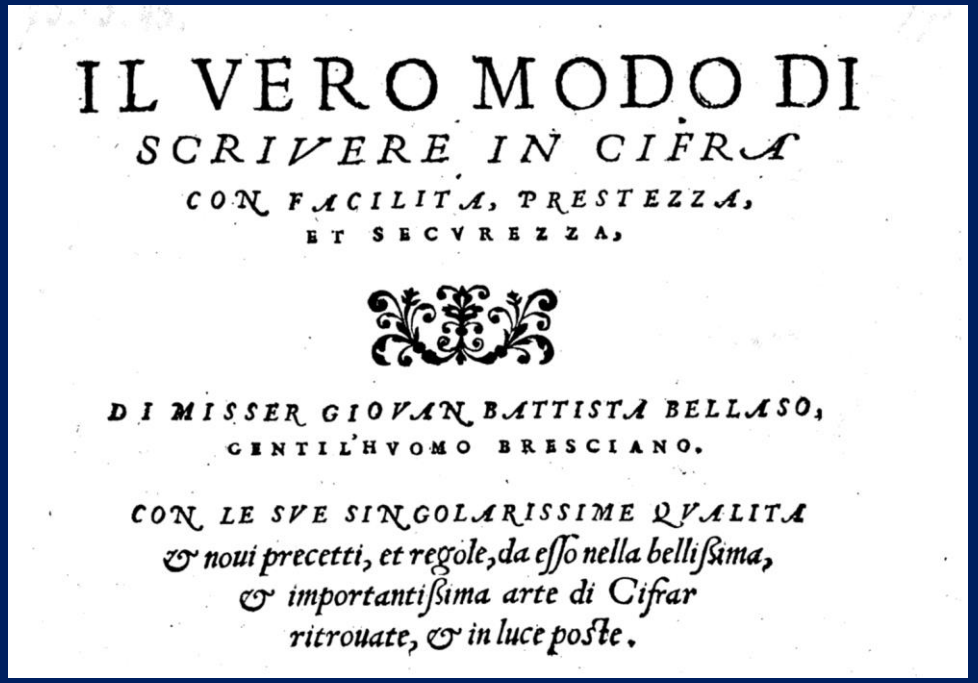


Was there a source for this idea of *uera ziffra*?

The plausible conjecture that Franceschi knew Bellaso's works and was influenced by them, has been fully confirmed. In his letters he names Bellaso, Trithemius and Porta as a reference for his true ciphers.

The *uera ziffra* of Franceschi clearly resembles this *Vero modo di scriuere in cifra*.

And many merits of his cipher resembel the *singular qualità* listed by Bellaso in his 1564 booklet.



IL VERO MODO DI
SCRIVERE IN CIFRA
CON FACILITA, PRESTEZZA,
ET SECVREZZA,

DI MISSER GIOVAN BATTISTA BELLASO,
GENTIL'HVOMO BRESCIANO.

CON LE SVE SINGOLARISSIME QVALITA
& noui precetti, et regole, da esso nella bellissima,
& importantissima arte di Cifrar
ritrouate, & in luce poste.

LE SINGOLAR QVALITA
DELLE CIFRE, SONO QVESTE,

LA prima è, che se tutto il mondo sapesse le regole sue, niuno intendera (seruando li precetti insegnati) la lettera dun'altro, come se fusse carta bianca.

La seconda è, che sono di tal prestezza da cifrare, & decifrare, atteſa la loro ſecurezza, che non ui si trouerà pari, esseudo in esse esercitati.

La terza è, che col primo, terzo, quarto, & quinto modo di cifrare, si può cifrar senza far le minute delle lettere, il che importa assai, & se pure à principianti il cifrare sarà di qualche incommodo, alli esercitati sarà di piacere & spasso.

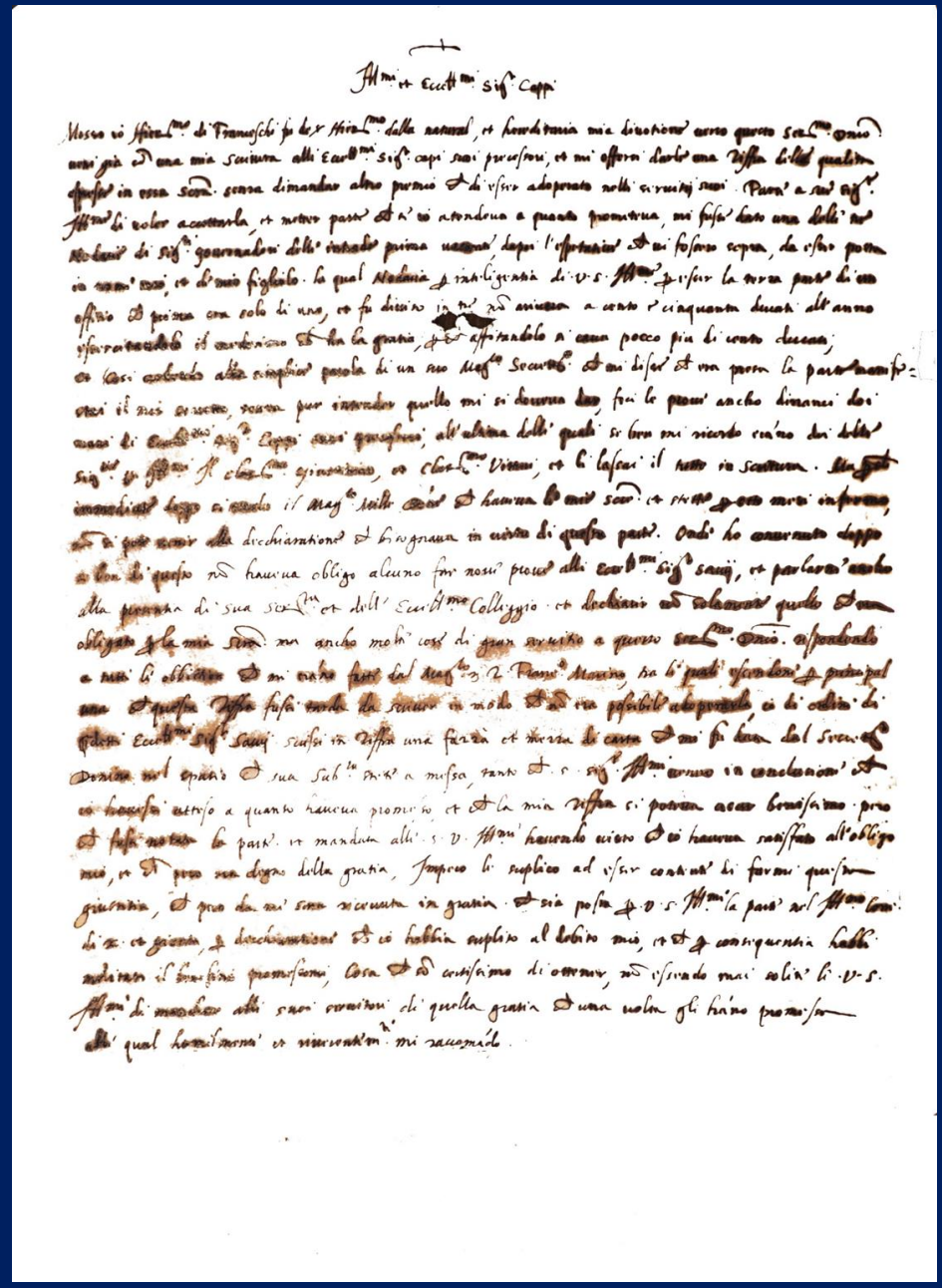
La quarta è, che son compoſti solo di lettere dell'alfabeto, & non ui sono nulle, nè titoli, nè tratti, nè ponti, nè lettere per parte, nè duplicate.

La quinta è, che se le prime quattro cifre, per qualche accidente si perdono, si possono subito riformare con la dittione, con laquale son compoſti gli alfabeti, come stauan prima.

La sesta è, che le cifre si mutano, mutando la dittione, con laquale son compoſti gli alfabeti, senza mutar punto la forma della cifra, imperò che si muta la sostanza, & non la forma.

Franceschi's first cipher, 1573

- Let us now see the indecipherable cipher that Franceschi proposed in 1572-1573.
- On the right Franceschi's letter to the CCX (The three Chiefs of the Council of X) attached to the deed of the Council of 1573, Sep 28. Here Franceschi list the merits of his cipher, but gives no technical detail.
- More details can be found in the following sheet found among Franceschi's papers.



Condicioni of this cipher, first mode

•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.

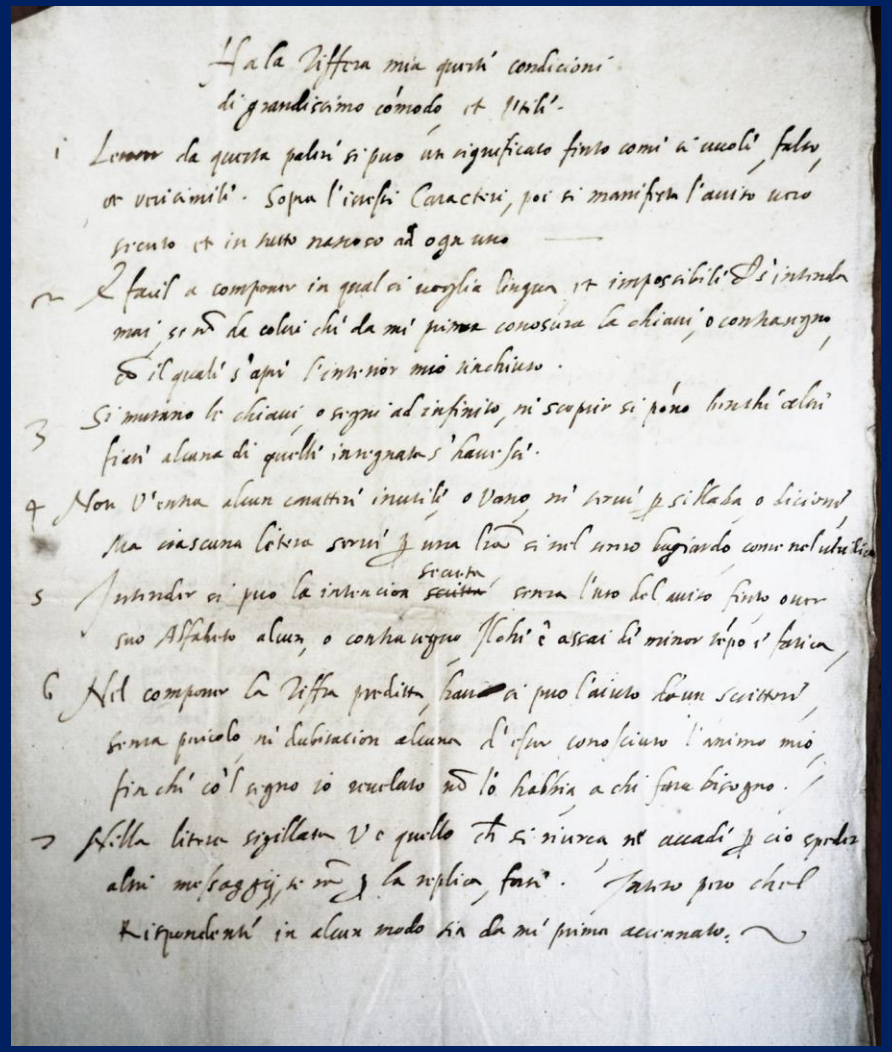
3.One changes keys or signs ad infinitum, and they can not be discovered even if sometimes one had some of the used by them.

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 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.



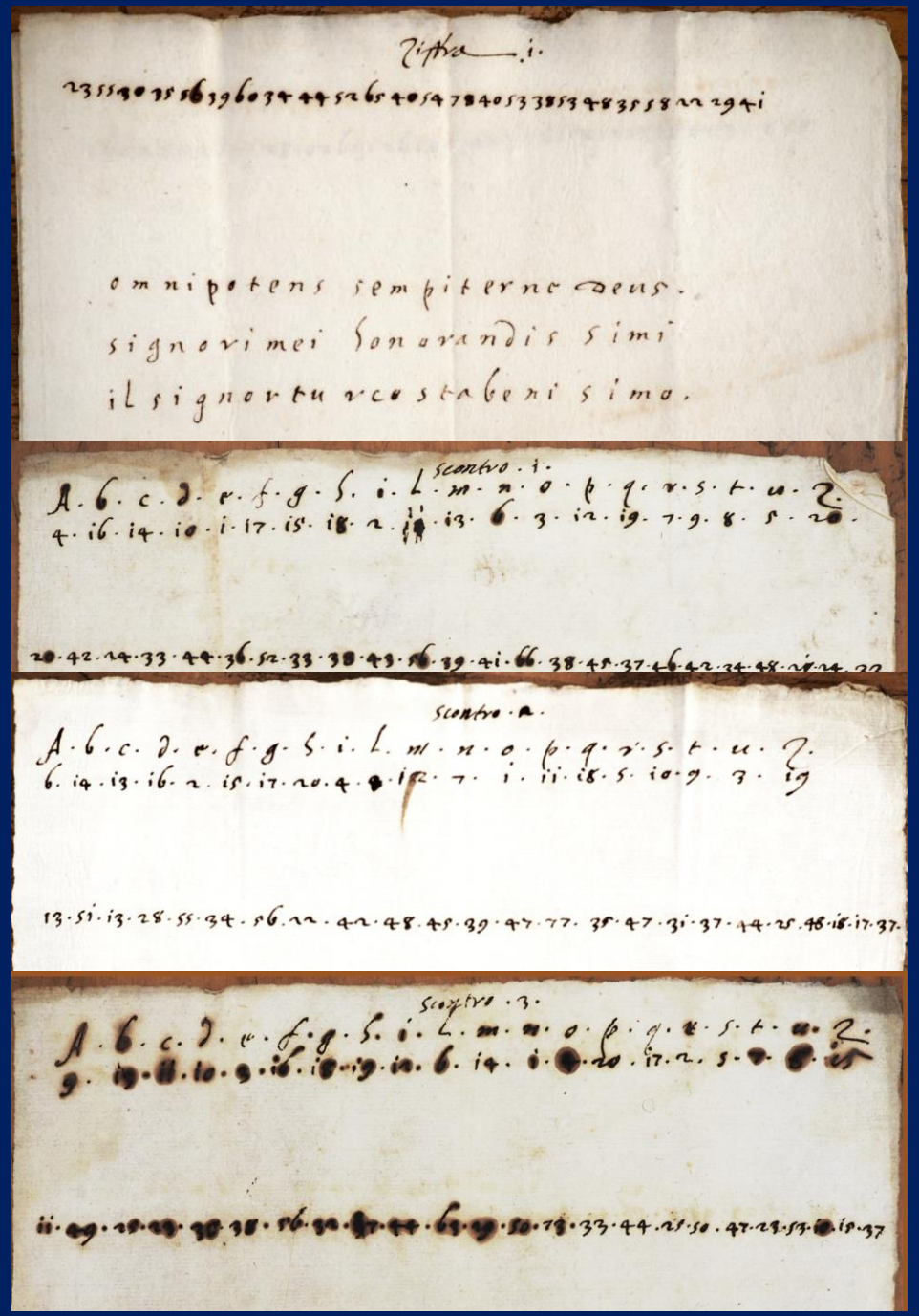
Franceschi's first mode, 1) converting letters to numbers

Decisive was the finding of a set of sheets, apparently as an example of a cipher that can be decrypted into any possible text, just using the appropriate key.

There are three possible messages, each of 24 letters:

Omnipotenssempiternedeus
Signorimeihonorandissimi
Ilsignorturcostabenisimo

And three different *scontri* having a monoalphabetic cipher useful to convert letters into numbers, and a key consisting of 24 random numbers.

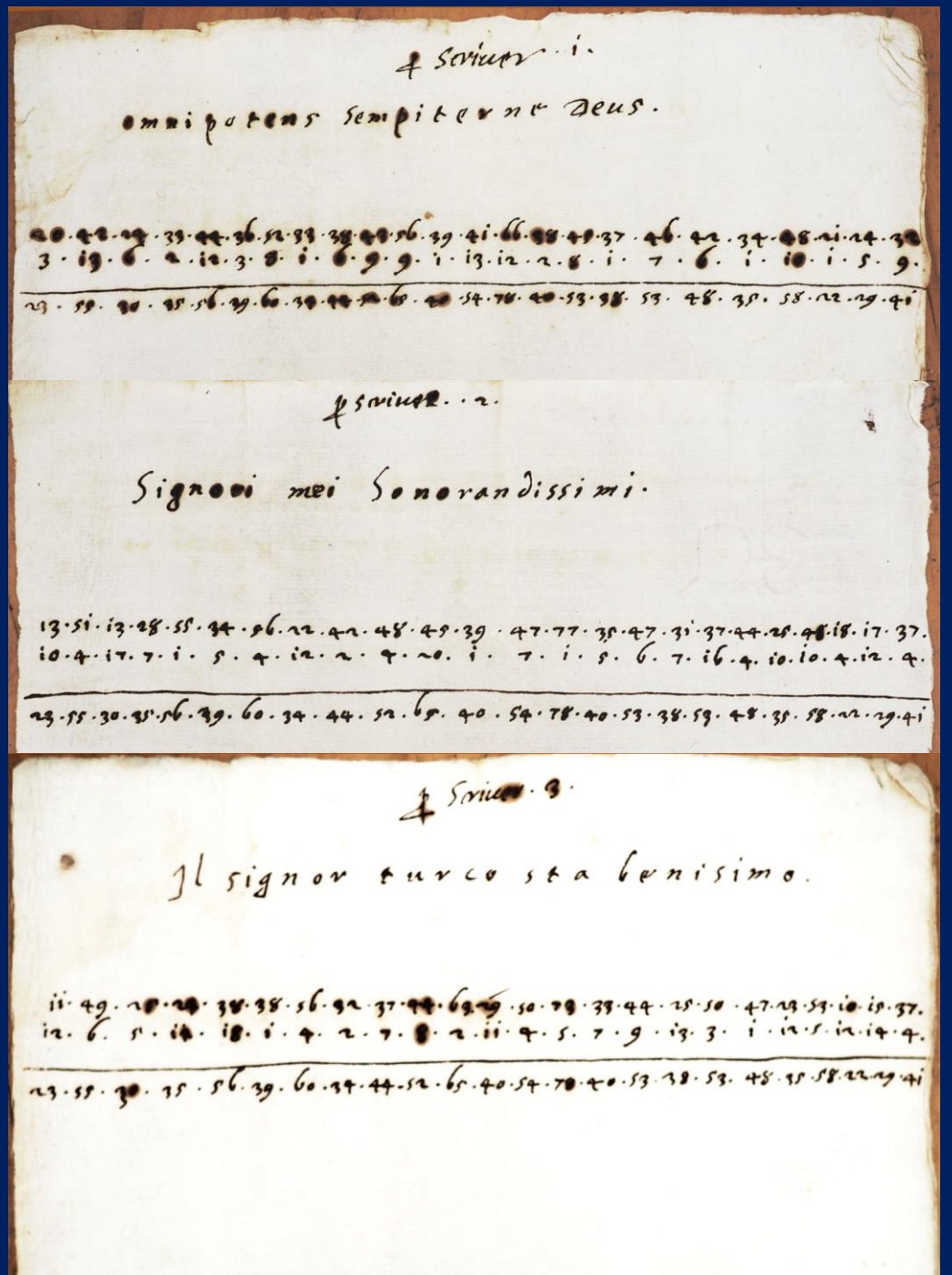


Franceschi's first mode, 2) Encrypting

If one has to write (*scriuer*), first substitutes each letter with the number given by the scontro, then adds this number with the corresponding one of the key.

That's all, just a simple addition.

But … was it really an elementary job for a secretary? Doing it speedy and without errors?



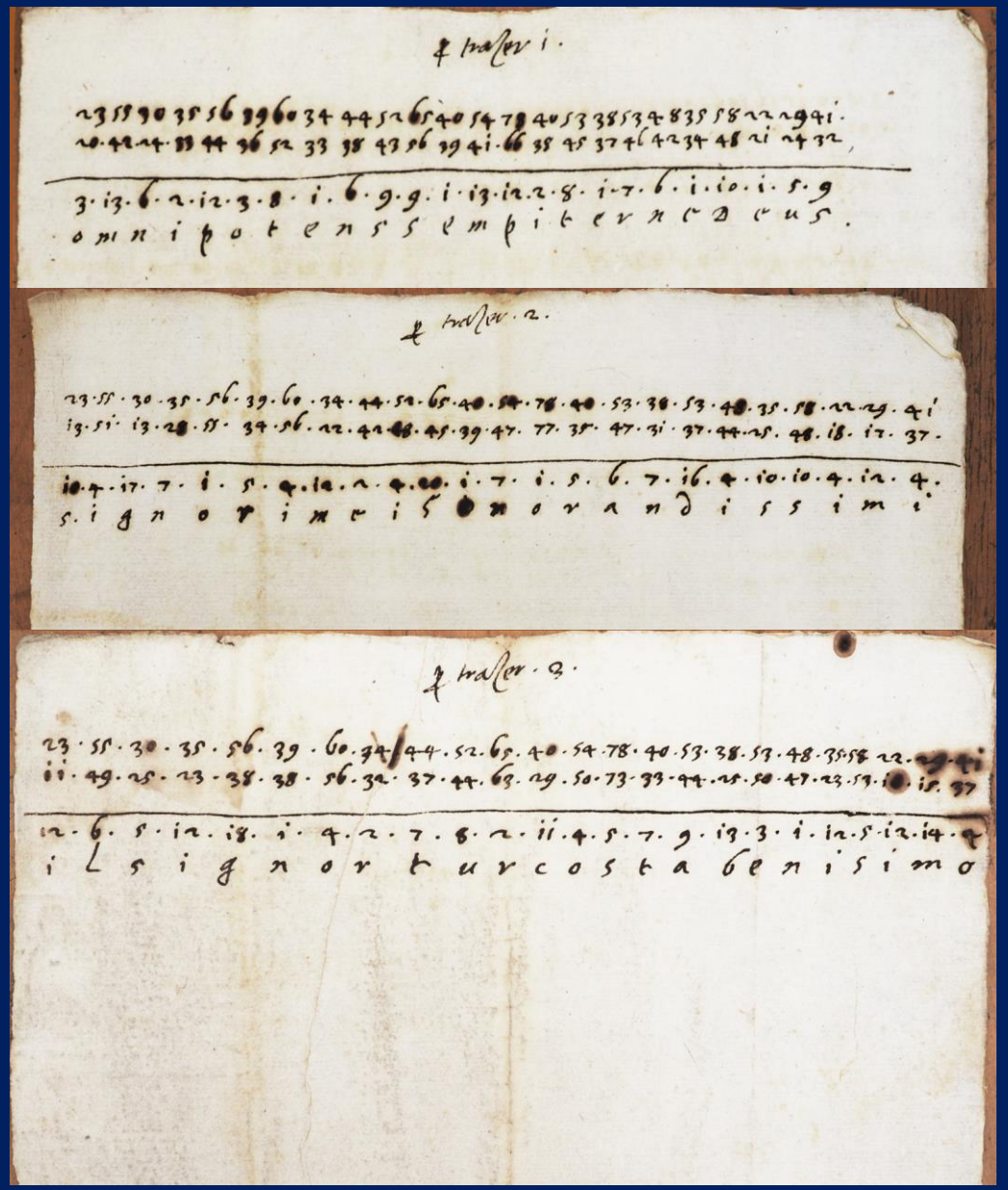
Franceschi's first mode, 3) decrypting

Finally, the procedure for deciphering (*trazer*) the received message.

It is just the inverse fo the previous: subtract the single number of the cryptogram from the one of key, then substitute the result with the letter of the *scontro*.

That's all, just a simple subtraction.

But … to subtract is a bit more difficult than to sum …



A conjecture about the procedure

Demo Franceschi's fake key.

One changes keys or signs ad infinitum, and they can not be discovered even if sometimes one had some of the used by them

Encrypted message brought by the courier →

Inside the sealed envelope ▼ →

In the sealed letter there is all that is needed to send other messages if it isn't done for the reply

Encrypt newly	Empty and restart																									
Good key:	60	33	51	29	64	59	60	77	54	74	68	55	78	36	40	53	60	46	68	51	62	50	77	32		
Good message	I	L	S	I	G	N	O	R	T	V	R	C	O	S	T	A	B	E	N	I	S	I	M	O		
	12	06	05	12	18	01	04	02	07	08	02	11	04	05	07	09	13	10	01	12	05	12	14	04		
Cryptogram:	72	39	56	41	82	60	64	79	61	82	70	66	82	41	47	62	73	56	69	63	67	62	91	36		
Decrypt using true key	Decrypt using fake key	S	T																							
Fake key	63	37	41	35	79	53	62	66	60	80	52	63	76	38	40	58	67	46	67	54	58	60	78	34		
Decrypted text	09	02	15	06	03	07	02	13	01	02	18	03	06	03	07	04	06	10	02	09	09	02	13	02		
	S	I	G	N	O	R	I	M	E	I	H	O	N	O	R	A	N	D	I	S	S	I	M	I		

To answer the secretary uses the received fake key as the good key for the answer →

Encrypt newly	Empty and restart																									
Good key:	63	37	41	35	79	53	62	66	60	80	52	63	76	38	40	58	67	46	67	54	58	60	78	34		
Good message	I	L	S	I	G	N	O	R	T	V	R	C	O	S	T	A	B	E	N	I	S	I	M	O		
	12	06	05	12	18	01	04	02	07	08	02	11	04	05	07	09	13	10	01	12	05	12	14	04		
Cryptogram:	75	43	46	47	97	54	66	68	67	88	54	74	80	43	47	67	80	56	68	66	63	72	92	38		
Decrypt using true key	Decrypt using fake key	S	T																							
Fake key	66	41	31	41	94	47	64	55	66	86	36	71	74	40	40	63	74	46	66	57	54	70	79	36		
Decrypted text	09	02	15	06	03	07	02	13	01	02	18	03	06	03	07	04	06	10	02	09	09	02	13	02		
	S	I	G	N	O	R	I	M	E	I	H	O	N	O	R	A	N	D	I	S	S	I	M	I		

Inside the sealed envelope a new fake key. →

Zuan Francesco Marin does not like

Zuan Francesco Marin,, the main deputy of ciphers of those years, strongly opposed Franceschi's cipher, arguing that it was too slow, too difficult and prone to errors.

Franceschi at last came to a compromise and revised the cipher, the result was the *Cifra delle Caselle*, the cipher of the windows, from the main innovation, the use of a grid to facilitate the job.

This cipher was approved and used by Venetian embassies starting in 1577.

Cifra delle Caselle - Esempio interattivo

Grid fot the bailo in Constantinople.
ASVe CX Cifre, chiavi … b. 6.3

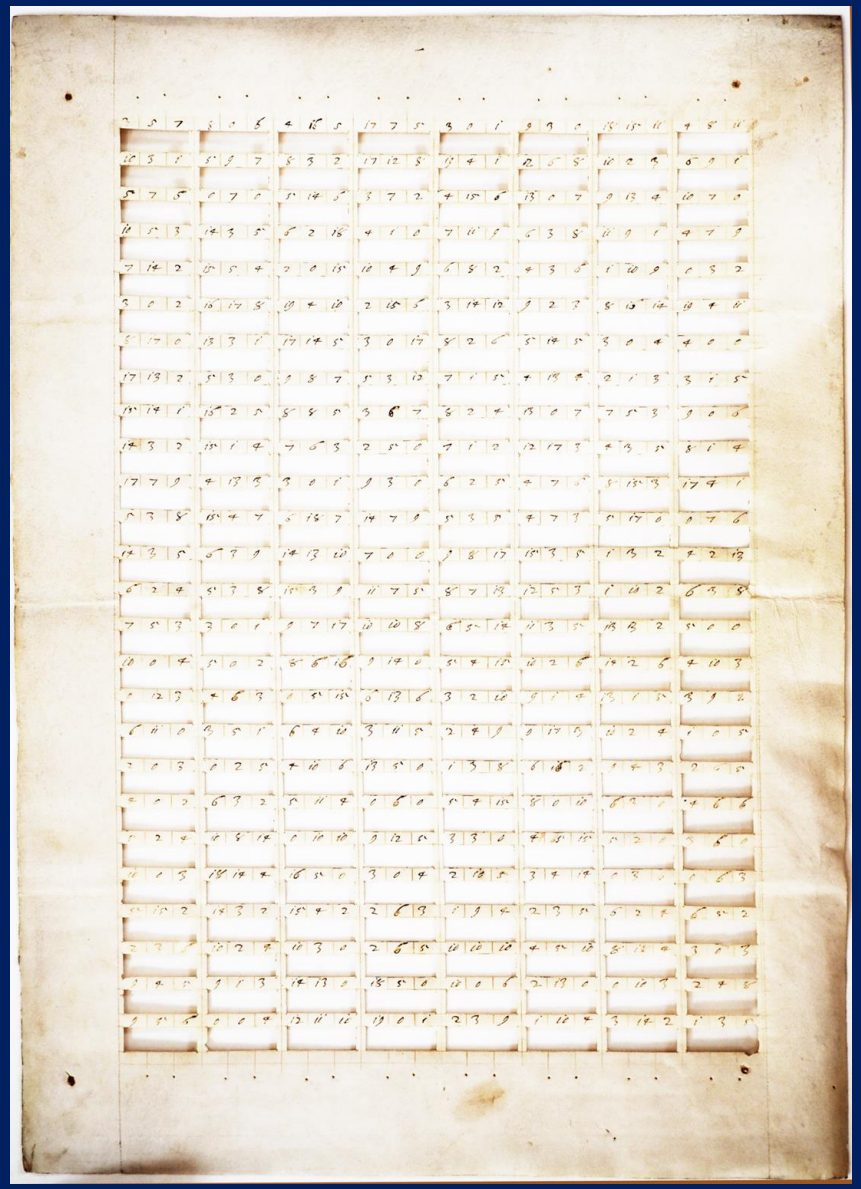
The Cifra delle *Caselle*

Zuan Francesco Marin, the main deputy of ciphers of those years, strongly opposed Franceschi's cipher, arguing that it was too slow, too difficult and prone to errors.

Franceschi at last came to a compromise and revised the cipher, the result was the *Cifra delle Caselle*, the cipher of the windows, from the main innovation, the use of a grid to facilitate the job.

This cipher was approved and used by Venetian embassies starting in 1577.

Cifra delle Caselle - Esempio interattivo

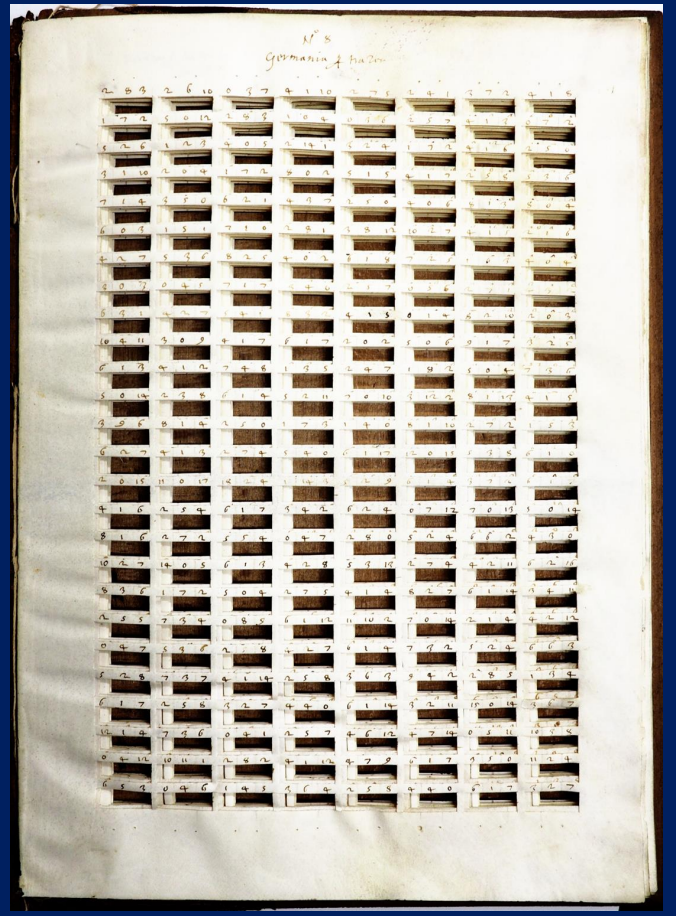


Grid fot the bailo in Constantinople.
ASVe CX Cifre, chiavi … b. 6.3

What's new?

What was new in this new cipher?

1. The key is written on a paperboard or parchment grid, with many small windows (the *caselle* that gave the name of the cipher). The secretary will put a blank sheet under the grid do the subtraction and write the resulting number inside the window, under the corresponding number of the key), so it is impossible to lose the alignment.
2. The key can be of 26x24 = 624 numbers of 2 ciphers, for 8 column grids, less for smaller grids of 7 column. If a text has more than 624 letters, put a new sheet under the same grid. So, the key long as the message principle and fake key were abandoned, at least for long messages.
3. The alphabetic cipher has now two homophones for every letter A has 16 36 realizing a raw modulo 20 arithmetic; numbers in the range 1..40
4. The remaining 60 numbers in the range 40..99 are used for a small dictionary, with minimal or null advantage and contradicting the single letter principle. A compromise?



Cifra delle Caselle - Esempio interattivo

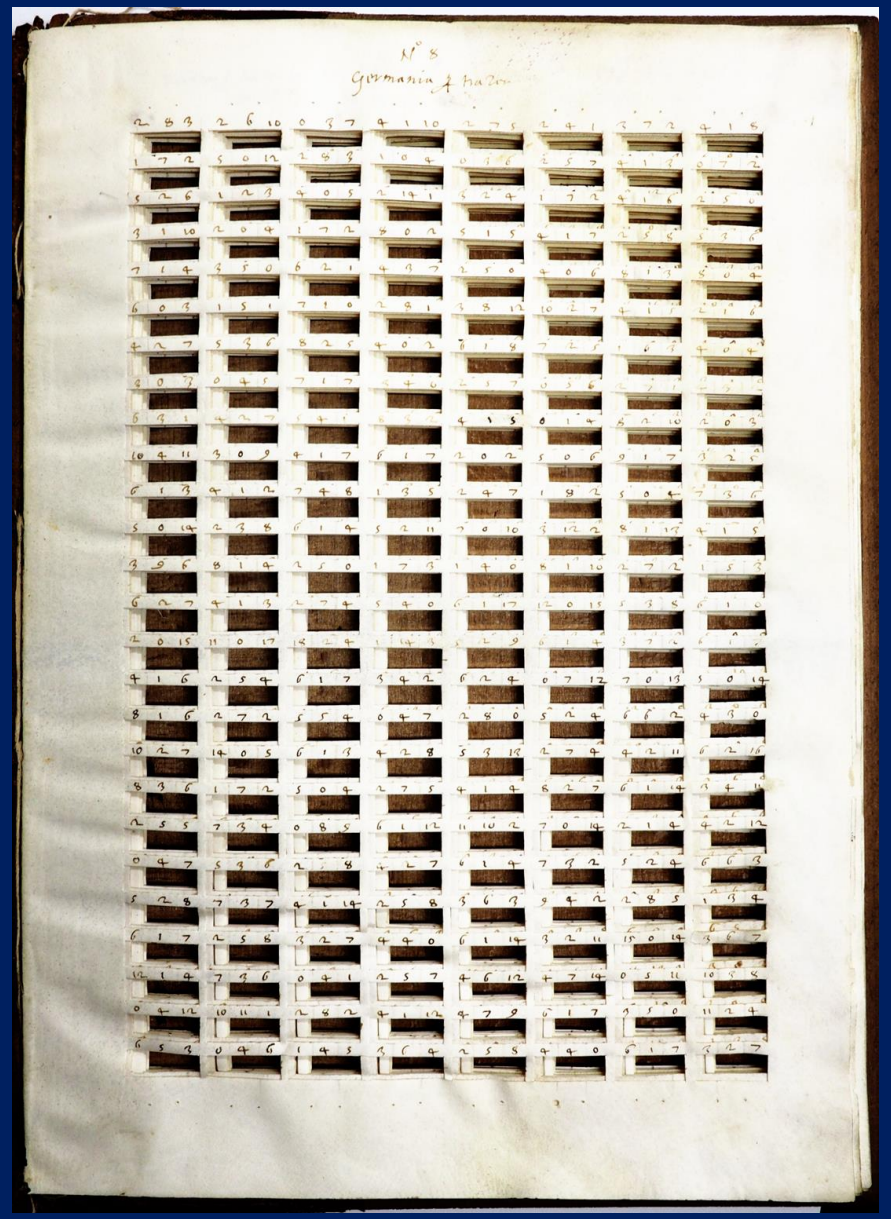
The *Caselle* cipher

Grata → 8 A → 16 16 − 8 = 8 La cifra di A è 8

Grata → 19 A → 36 36 − 19 = 17 La cifra di A è 17

Grata → 19 A → 16 16 − 19 = 17 (*mod* 20) La cifra di A è 17

Cifra delle Caselle - Esempio interattivo



Let’s encrypt using Caselle

To be, or not to be, that is the question,
Whether 'tis nobler in the mind to suffer

To be, or not to be, that is the question,
Whether 'tis nobler in the mind to suffer

Clic qui per cifrare con le caselle

Sovracifra con grata Germania (Sacro Romano Impero)

t	o	b	e	o	r	n	o	t	t	o	b	e	t	h	a	t	i	s	t	h	e	q	u
11 – 2	18 – 8	13 – 3	2 – 2	18 – 6	12 – 10	17 – 0	18 – 3	11 – 7	11 – 4	18 – 1	13 – 10	2 – 2	11 – 7	20 – 5	16 – 2	11 – 4	8 – 1	5 – 3	11 – 7	20 – 2	2 – 4	9 – 1	3 – 8
9	10	10	0	12	2	17	15	4	7	17	3	0	4	15	14	7	7	2	4	18	18	8	15
e	s	t	i	o	n	h	e	t	h	e	r	t	i	s	n	o	b	l	e	r	i	n	t
2 – 1	5 – 7	11 – 2	8 – 5	18 – 0	17 – 12	20 – 2	2 – 8	11 – 3	20 – 1	2 – 0	12 – 4	11 – 0	8 – 3	5 – 6	17 – 2	18 – 5	13 – 7	14 – 4	2 – 1	12 – 3	8 – 0	17 – 7	11 – 2
1	18	9	3	18	5	18	14	8	19	2	8	11	5	19	15	13	6	10	1	9	8	10	9
h	e	m	i	n	d	t	o	s	u	f	f	e	r										
20 – 5	2 – 2	7 – 6	8 – 1	17 – 2	15 – 3	11 – 4	18 – 0	5 – 5	3 – 2	4 – 14	4 – 1	2 – 3	12 – 2										
15	0	1	7	15	12	7	18	0	1	10	3	19	10										

Cifrato da trasmettere:

```
 9 10 10  0 12  2 17 15  4  7 17  3  0  4 15 14  7  7  2  4 18 18  8 15
 1 18  9  3 18  5 18 14  8 19  2  8 11  5 19 15 13  6 10  1  9  8 10  9
15  0  1  7 15 12  7 18  0  1 10  3 19 10
```

Cifra delle Caselle - Esempio interattivo

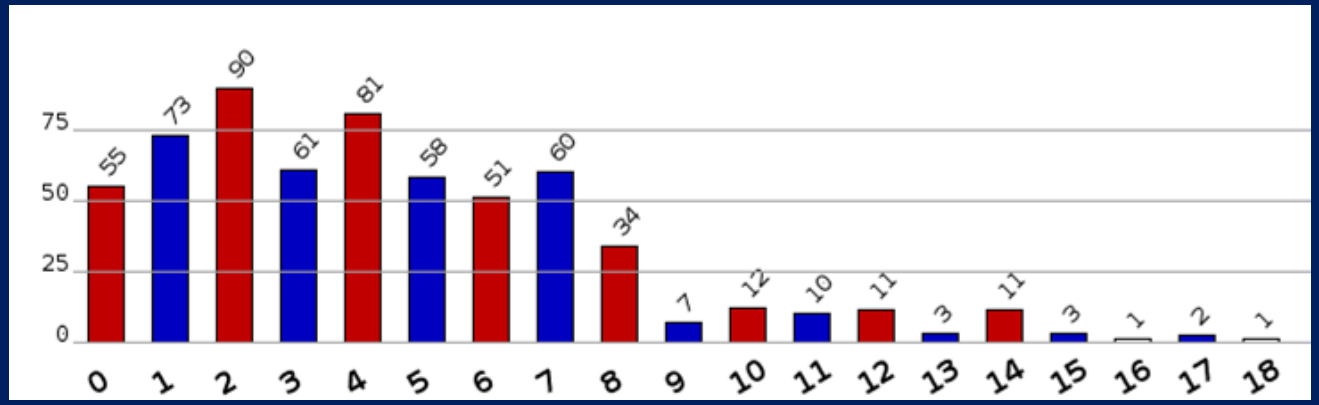
Plain text
Cifra A16-36
Grata Germania

Cifra caselle

2	8	3	2	6	10	0	3	7	4	1	10	2	7	5	2	4	1	3	7	2	4	1	8
1	7	2	5	0	12	2	8	3	1	0	4	0	3	6	2	5	7	4	1	3	0	7	2
5	2	6	1	2	3	4	0	5	2	14	1	3	2	4	1	7	2	4	1	6	2	5	0
3	1	10	2	0	4	1	7	2	8	0	2	5	1	5	4	1	7	2	5	8	5	3	6
7	1	4	3	5	0	6	2	1	4	3	7	2	5	0	4	0	6	8	1	3	8	0	4
6	0	3	1	5	1	7	1	0	2	8	1	3	8	12	10	2	7	4	1	5	2	1	6
4	2	7	5	3	6	8	2	5	4	0	2	6	1	8	7	2	5	1	6	3	4	0	4
3	0	3	0	4	5	7	1	7	3	4	0	2	5	7	0	5	6	2	7	1	4	3	2
6	3	1	4	2	7	5	4	1	8	3	2	4	1	5	0	1	4	8	2	10	2	0	3
10	4	11	3	0	9	4	1	7	6	1	7	2	0	2	5	0	6	9	1	7	3	2	5
6	1	3	4	1	2	7	4	8	1	3	5	2	4	7	1	8	2	5	0	4	7	3	6
5	0	14	2	3	8	6	1	4	5	2	11	7	0	10	3	12	2	8	1	13	4	1	5
3	9	6	8	1	4	2	5	0	1	7	3	1	4	0	8	1	10	2	7	2	1	5	3
6	2	7	4	1	3	2	7	4	5	4	0	6	1	17	12	0	15	5	3	8	6	1	0
2	0	15	11	0	17	18	2	4	1	14	3	5	2	9	6	1	4	3	7	2	6	1	7
4	1	6	2	5	4	6	1	7	3	4	2	6	2	4	0	7	12	7	0	13	5	0	14
8	1	6	2	7	2	5	5	4	0	4	7	2	8	0	5	2	4	6	6	2	4	3	0
10	2	7	14	0	5	6	1	3	4	2	8	5	3	13	2	7	4	4	2	11	6	2	16
8	3	6	1	7	2	5	0	4	2	7	5	4	1	4	8	2	7	6	1	14	3	4	11
2	5	5	7	3	4	0	8	9	6	1	12	11	10	2	7	0	14	2	1	4	4	2	12
0	4	7	5	3	6	2	5	8	4	2	7	6	1	4	7	3	2	5	2	4	6	6	3
5	2	8	7	3	7	4	1	14	2	5	8	3	6	3	9	4	2	2	8	5	1	3	4
6	1	7	2	5	8	3	2	7	4	4	0	6	1	14	3	2	11	15	0	14	3	6	7
12	1	4	7	3	6	0	4	1	2	5	7	4	6	12	4	7	14	0	5	11	10	3	8
0	4	12	10	11	1	2	8	2	4	1	12	4	7	9	6	1	7	3	5	0	11	2	4
6	5	3	0	4	6	1	4	5	3	6	4	2	5	8	4	4	0	6	1	7	3	2	7

Grata Germania
(Holy Roman Empire, Prag, Vienna)

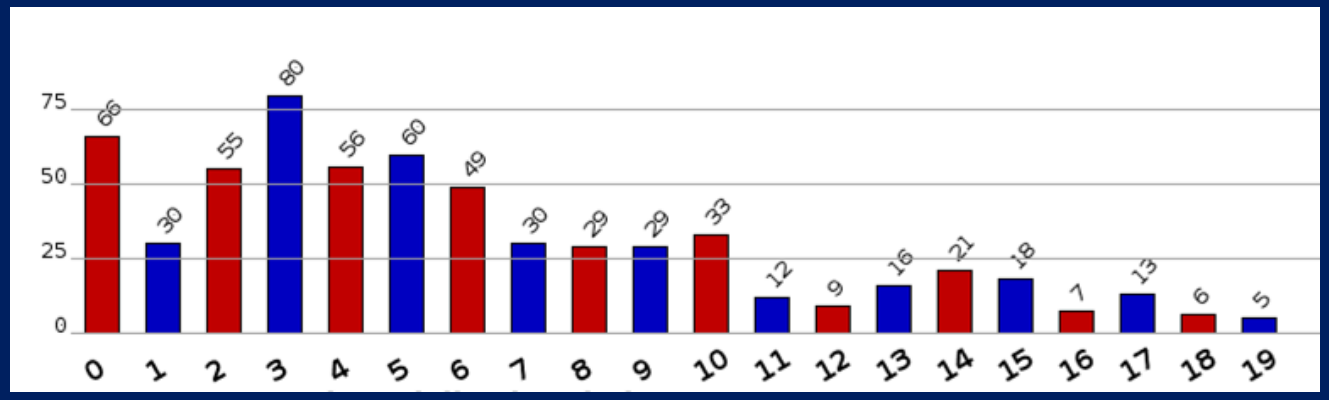
Is it really disordered?



2	8	3	2	6	10	0	3	7	4	1	10	2	7	5	2	4	1	3	7	2	4	1	8
1	7	2	5	0	12	2	8	3	1	0	4	0	3	6	2	5	7	4	1	3	0	7	2
5	2	6	1	2	3	4	0	5	2	14	1	3	2	4	1	7	2	4	1	6	2	5	0
3	1	10	2	0	4	1	7	2	8	0	2	5	1	5	4	1	7	2	5	8	5	3	6
7	1	4	3	5	0	6	2	1	4	3	7	2	5	0	4	0	6	8	1	3	8	0	4
6	0	3	1	5	1	7	1	0	2	8	1	3	8	12	10	2	7	4	1	5	2	1	6
4	2	7	5	3	6	8	2	5	4	0	2	6	1	8	7	2	5	1	6	3	4	0	4
3	0	3	0	4	5	7	1	7	3	4	0	2	5	7	0	5	6	2	7	1	4	3	2
6	3	1	4	2	7	5	4	1	8	3	2	4	1	5	0	1	4	8	2	10	2	0	3
10	4	11	3	0	9	4	1	7	6	1	7	2	0	2	5	0	6	9	1	7	3	2	5
6	1	3	4	1	2	7	4	8	1	3	5	2	4	7	1	8	2	5	0	4	7	3	6
5	0	14	2	3	8	6	1	4	5	2	11	7	0	10	3	12	2	8	1	13	4	1	5
3	9	6	8	1	4	2	5	0	1	7	3	1	4	0	8	1	10	2	7	2	1	5	3
6	2	7	4	1	3	2	7	4	5	4	0	6	1	17	12	0	15	5	3	8	6	1	0
2	0	15	11	0	17	18	2	4	1	14	3	5	2	9	6	1	4	3	7	2	6	1	7
4	1	6	2	5	4	6	1	7	3	4	2	6	2	4	0	7	12	7	0	13	5	0	14
8	1	6	2	7	2	5	5	4	0	4	7	2	8	0	5	2	4	6	6	2	4	3	0
10	2	7	14	0	5	6	1	3	4	2	8	5	3	13	2	7	4	4	2	11	6	2	16
8	3	6	1	7	2	5	0	4	2	7	5	4	1	4	8	2	7	6	1	14	3	4	11
2	5	5	7	3	4	0	8	9	6	1	12	11	10	2	7	0	14	2	1	4	4	2	12
0	4	7	5	3	6	2	5	8	4	2	7	6	1	4	7	3	2	5	2	4	6	6	3
5	2	8	7	3	7	4	1	14	2	5	8	3	6	3	9	4	2	2	8	5	1	3	4
6	1	7	2	5	8	3	2	7	4	4	0	6	1	14	3	2	11	15	0	14	3	6	7
12	1	4	7	3	6	0	4	1	2	5	7	4	6	12	4	7	14	0	5	11	10	3	8
0	4	12	10	11	1	2	8	2	4	1	12	4	7	9	6	1	7	3	5	0	11	2	4
6	5	3	0	4	6	1	4	5	3	6	4	2	5	8	4	4	0	6	1	7	3	2	7

Grata Constantinople
(Ottoman Empire)

Is it really disordered?

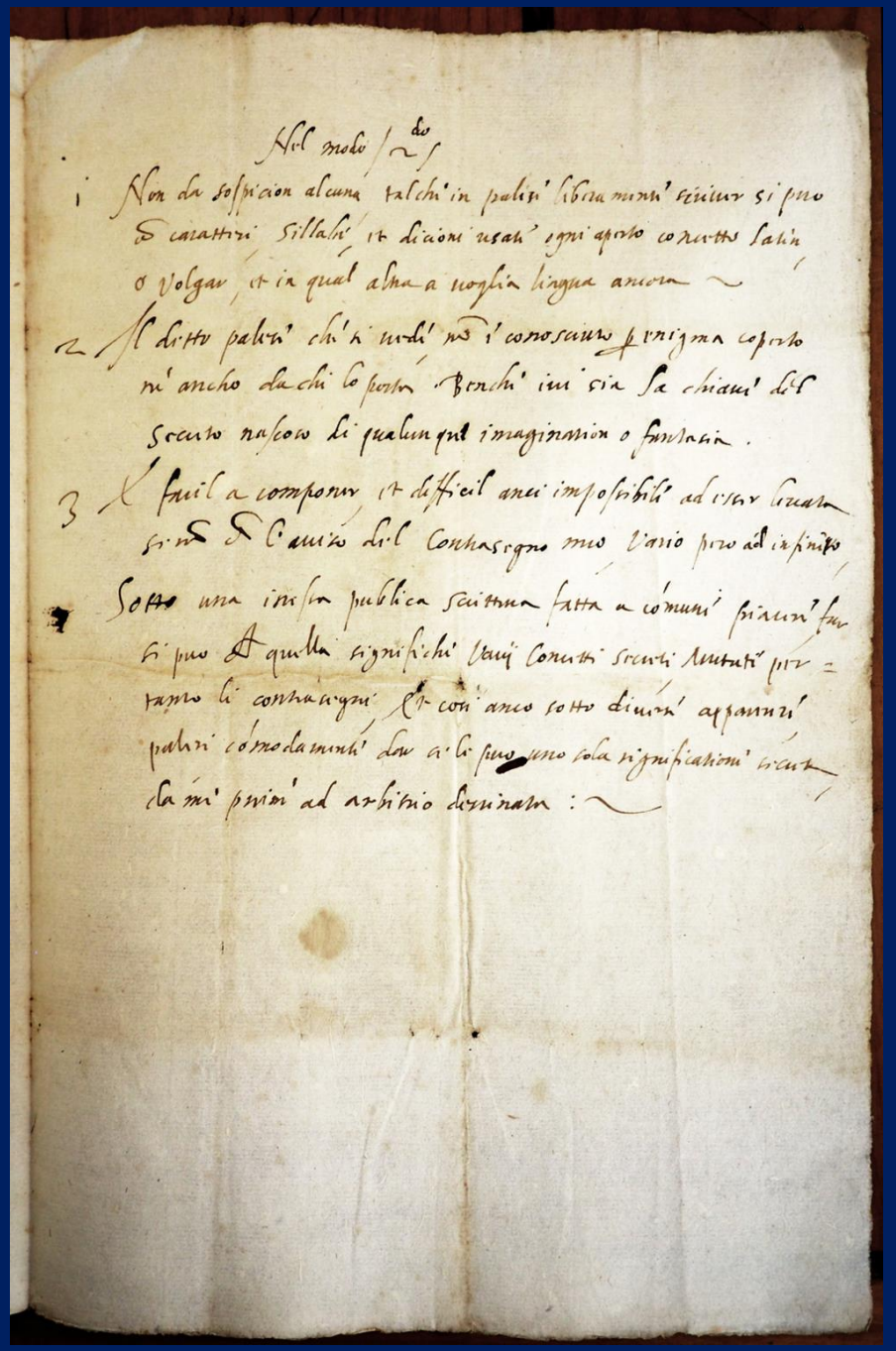


3	5	7	8	0	6	4	16	5	17	7	5	3	0	1	9	3	0	18	15	11	4	8	11
10	3	1	5	9	7	8	3	2	17	12	8	19	4	1	2	6	8	10	2	3	6	9	1
5	7	6	0	7	0	5	14	6	3	7	2	4	15	6	13	0	7	9	13	4	10	7	0
19	5	3	14	3	5	6	2	18	4	1	0	7	11	9	6	3	8	11	9	1	4	7	9
7	14	2	15	5	4	2	0	15	10	4	9	6	8	2	4	3	6	1	10	9	0	3	2
3	0	2	16	17	8	19	4	10	2	15	6	3	14	12	9	2	3	8	16	14	19	4	11
8	17	0	13	3	1	17	14	5	3	0	17	8	2	6	5	14	5	3	0	4	4	0	0
17	13	2	5	3	0	9	8	7	5	3	12	7	1	5	4	13	4	2	1	3	3	1	5
15	14	1	16	2	5	8	8	5	3	6	7	8	2	4	13	0	7	7	5	3	9	0	6
14	3	2	15	0	4	7	6	3	2	5	0	7	1	2	12	17	3	4	3	5	8	1	4
11	7	9	4	13	3	3	0	1	9	3	0	6	2	5	4	7	6	8	15	3	17	4	1
5	3	8	15	4	7	6	18	7	14	7	9	5	3	5	4	7	3	5	17	0	0	7	6
14	3	5	6	3	9	14	13	10	7	0	0	9	8	17	15	3	5	1	3	2	4	2	13
6	2	4	5	3	8	15	3	9	11	7	5	8	7	13	12	5	3	1	10	2	6	3	8
7	5	3	3	0	1	9	7	17	10	10	8	6	5	14	11	3	5	13	3	2	5	0	0
10	0	4	5	0	2	8	6	16	9	14	0	5	4	15	10	2	6	14	2	6	4	10	3
0	12	3	4	6	3	0	5	15	6	13	6	3	2	10	9	1	4	13	1	5	3	9	2
6	11	0	3	5	1	6	4	10	3	11	5	2	4	9	0	17	3	10	2	4	1	0	5
2	0	3	0	2	5	4	10	6	13	5	0	1	3	8	6	16	2	9	4	3	2	6	5
4	0	2	6	3	2	5	11	4	0	6	0	5	4	15	8	0	10	6	3	0	4	6	6
15	2	4	10	8	14	0	10	10	9	12	5	3	3	0	4	5	15	5	2	0	3	6	0
10	0	3	18	14	4	16	1	0	3	0	4	2	10	5	3	4	14	0	3	6	0	6	3
5	15	12	14	3	2	15	4	2	2	6	3	1	9	4	2	3	5	6	2	4	6	5	2
2	3	6	10	2	4	10	3	0	2	6	5	10	10	10	4	5	10	8	18	4	3	0	3
9	4	5	9	1	3	14	13	0	18	5	0	10	0	6	2	13	0	0	10	3	2	4	8
9	5	6	0	0	4	12	11	10	19	0	1	2	3	0	1	10	4	3	14	2	1	3	5

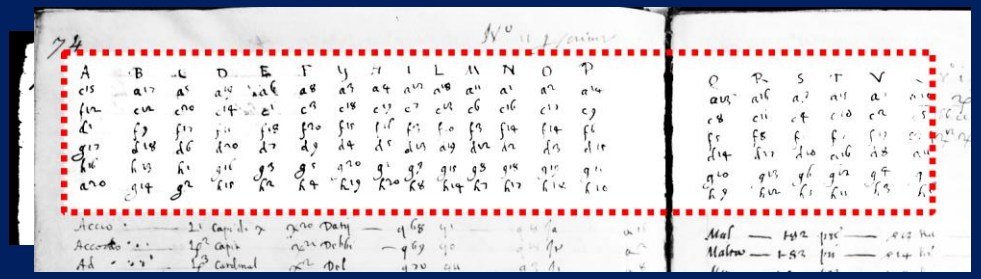
Condicioni of this cipher, second mode

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.

This is really too little to assemble a plausible conjecture.



N.11 a strange cipher



In the register of ciphers kept by secretaries Franceschi and Milledonne between 1578 and 1587. this cipher N.11 apparently a nomenclator like so many others, has a strange note signed by Franceschi stating that this cipher has been done in execution of the 1587 CX decree. So it should have something to do with the Falso Scontro. But what?

No instruction has been found, so we can only try.

Looking at the alphabet with six homophones for letter, it is noteworthy that the homophones has a letter among a, c, d ,f, g, h. followed by a number in the range 1..20, and the number 20 acts as a sort of neutral element, e.g a20 = a, d20 = d, f20 = f, g20=20, h20 =h.

Finally, it appears that this 6 rows are part of a 20x20 square shown here on the right.

Pietro Partenio the archrival of Franceschi, wrote in 1605 that the late secretary Franceschi used a square for his Falso Scontro cipher. Was this that square?

Two confirmations emerged from the archivial papers.

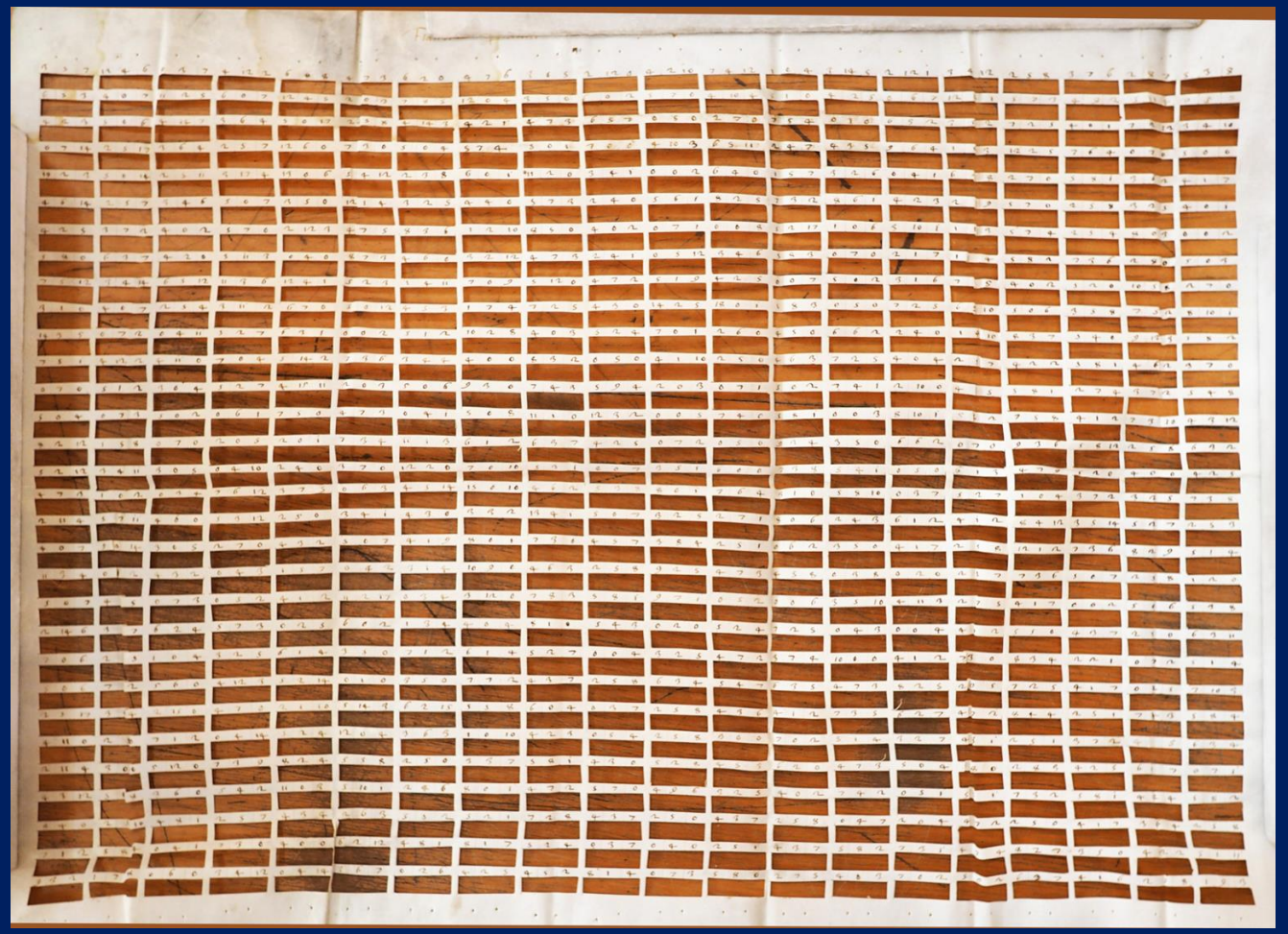
Alfabeto

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^{13}	c^{6}	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^{12}	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^{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^{4}	h^{19}	h^{20}	h^{8}	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

Two huge grids

Inside busta 6.3 of the CX cipher collection one finds a couple of huge grids, same structure as the Caselle grids, but 31 rows and 20 columns with 3 places, so 31x20x3 = 1860 numbers, a very long key.



How could it be used?

1. Maybe like an easier to use first mode (addition/subtraction) of the *Falso Scontro*?
2. Or just as a reinforced *cifra delle caselle?*
3. Or rather for the second mode?
4. Or something else, a third mode?

Unanswered questions

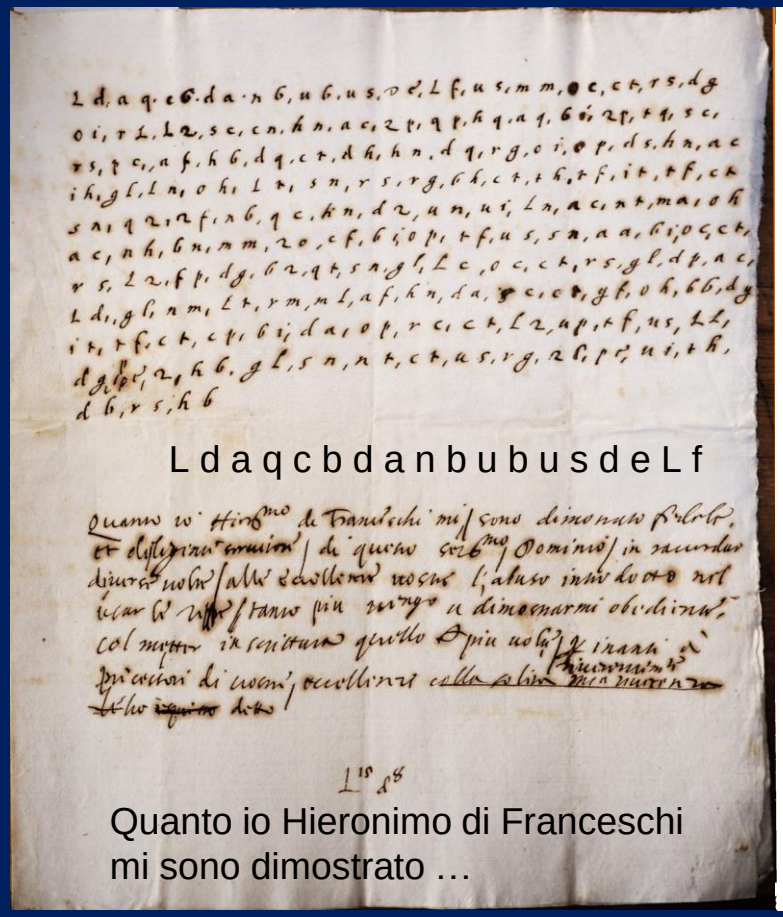
Many questions remain without an answer:

1. Was the latter a cipher or rather part of a cipher?
2. Had something to do with the huge grids?

	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

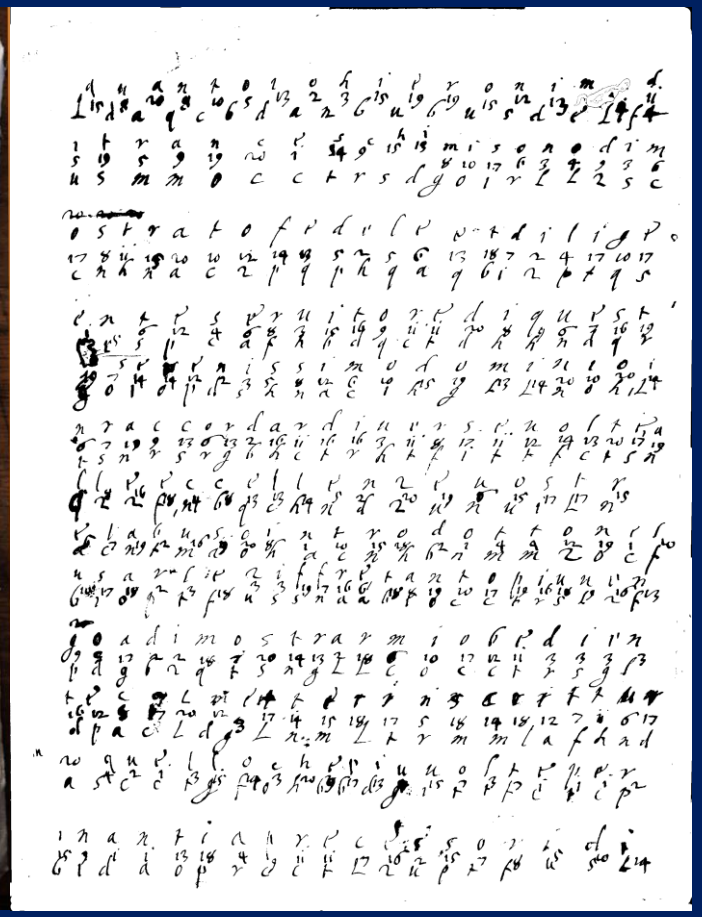
An example

This way, one can encipher a plain text
Into any other plain or fake text; the key is the sequence of number (+the square)?



L d a q c b d a n b u b u s d e L f

Quanto io Hieronimo di Franceschi
mi sono dimostrato …



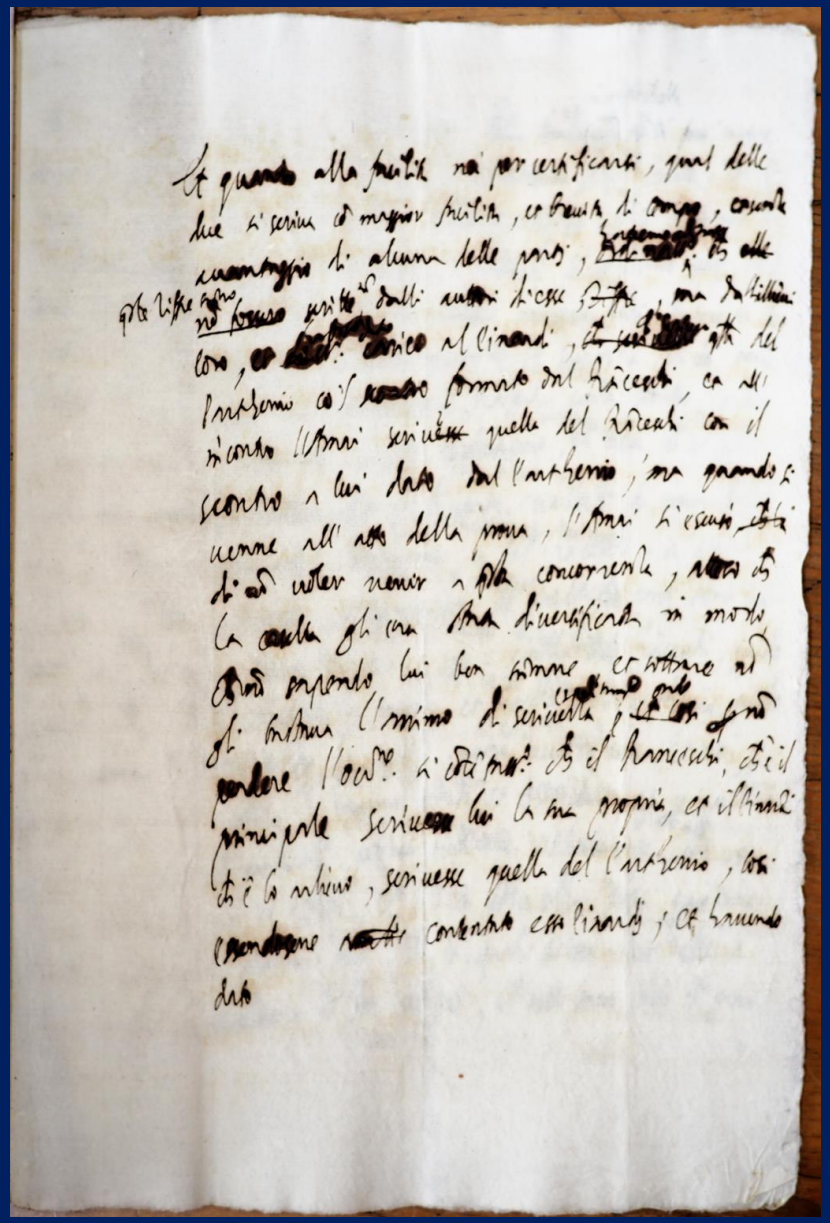
Q	U	A	N	T	O	I	O	H	I	E	R	O	N	I	M	O	D		
15	8	20	8	10	5	13	2	3	15	19	19	15	12	13	12	4	11		
L	d	a	q	c	b	d	a	n	b	u	b	u	s	d	e	L	f		
I	F	R	A	N	C	E	S	C	H	I	M	I	S	O	N	O	D	I	M
5	19	5	9	19	20	1	34	9	15	13	8	10	17	6	3	4	9	3	6
u	s	m	m	o	c	c	t	r	s	d	g	o	i	r	L	L	d	s	c

	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

The conclusion of the Franceschi-Partenio dispute.

[…] ma quando si uenne all'atto della proua, l'Amai si escusò di non uoler uenir a questa concorrenza, atteso che la casella gli era stata diuersificata in modo se ben secondo l'ordine del Franceschi in modo che non sapendo lui ben summare et sottrare non gli bastaua l'animo di scriuerla espeditamente, onde per non perdere l'occasione, si contentasse che il Franceschi che è il principale scriuesse lui la sua propria […]

[…] but when it came to the act of the test, Amai excused himself not to want to join this competition, given that the box had been diversified in such a way if well according to the order of Franceschi so that not knowing how to add and subtracting is not enough for him to write it expeditiously, so as not to miss the opportunity, he would content himself with the fact that Franceschi, who is the principal, wrote his own […]



The last cipher of Partenio

In 1605, five years after the sad conclusion of the dispute with Franceschi and his death, Pietro Partenio wrote a long letter to the CX deprecating the poor quality of the ciphers used in those years, a sign that both Franceschi's ana Partenio's cipher were still used. And he also offered to write a new booklet of more safe ciphers .
The last cipher of the booklet (still present in the Venetian Archives), uses a square equivalent to Franceschi's, but with a key transposition as the first cipher.

	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

```
__E__N__L__E__X__T__V__A__M__E__D__I__T__A__T__I__O__M__E__A__I__N__C__O__R__D__E__M__E__O__
_06_19_15_07____25_28_00_16_08_04_12_26_01_27_13_21_17_09_02_14_20_03_22_24_05_10_18_11_23
__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
```

Thank you
for your attention