## The Enigma of Franceschi's *Falso Scontro*

## An unknown battle between polyalphabetic and nomenclator

· · · · · · · · · · · · · · · · · · ·	Trement		And the state of the second state of the second		
2 same Example and a single				1 12 1 1 2 12 1 1 × ×	11624-124
STREET STREET,	States in succession in the	STREET, STREET	and the second division of the second divisio	Description of the local division of the loc	STREET, STREET
Contract of the local division in which the local division in the	2 2 3 15 5 4 5	The survey of th			the second s
CONTRACTOR DE LA CONTRACT		7.4 7.5 7 6 5	2 2 2 8 3 8 4 8 1 8	5 25 7 65 7 A F	4 4 4 7 8 14 15 4 14
	1 + + + 7 4- 1	5 6 6 7 6 6 4 10 1	5 6 2 11 2 4 7 9 2 5		CONTRACTOR DESCRIPTION
The state of the s	the second second	and the second second	and the second s	the second se	
					5 8 4 12 Km 4- 1 7
	1 0 5 0 4 0		1 - 2 - 3 - 3 - 4 - 4 - 4	4 2 3 2 2 4 3 4	
CONTRACTOR OF ADVISED BY ADVID	Provide Links	the second second	Contraction in the local division in the loc	and the second s	
	The state of the s	Contraction of Contra	a particular in the second second	The state of the s	1 1 9 H 01 8 8 M
THE R. P. LEWIS CO., LANSING MICH. & CO., LANSING, MICH. & CO., LA	· · · · · · · · ·	4 7 5 2 4 1 8 5	12 9 4 6 3 4 9 8 7 8	1 1 7 1 4 1 8 4	777 7 4 4 7 7 7 7
	COLUMN TO A	1 12 x 4 7 4 4 1	2 4 2 5 4 5 7 5 . 2	A 1 & 2 CONTRACTOR	Constant of the Party of the Pa
Statement Statement Statement	Statement Contractor	and the second second	the second se		
A REAL PROPERTY AND A REAL	1 7 4 1			7 2 3 1 210 3 0 5	5 3 8 7 JA 8 10 5
11 3 5 6 7 4 7 4 4 1 1 2 7 1 1 1 8 8 2	1 1 12 10 12 18	4 0 3 3 4 4 7 0			2 2 2 2 2 2 2 2 2 2 2 2
And the state of t	Station in the local division in the	Contraction of the local division of the loc			CONTRACTOR OF STREET,
STATE OF TAXABLE PARTY OF TAXABLE PARTY.	Street Street	Annual Annual Provent	Statistics in the local division in the loca	Statement of the local division of the local	3 8 3 4 6 3 3 7 1
3 2 6 8 8 A 11 6 6 11 A 7 A 17 11 A 1 7 1	r 0 6 9 3 0 -	741594 20	3 8 7 1 1 1 2 7 4 1	A 10 0 10 5 5 10 1	A 7 4 8 7/4 1 4 8
					the local of the local division in the local
	Martin Contraction	And I Have been dealers		COLUMN DESIGNATION OF TAXABLE PARTY	4 1 4 2 4 14 4 4 4 44
* * 12 11 + 4 12 7 0 12 0 7 12 0 1 7 5 4 1	1 1 3 6 1 2	6 5 7 4 5 8 9 9	E 2 5 0 2 1 E 5 5 0	112070 221	I FIA A T & S T A
	1. 1. 6 7 2 78	1 1 1 1 1 1 1 1			Section 201
STATES STATES STATES STATES IN STATES	5- 1 15 15 7 14	A COLUMN TWO IS NOT		Statement Statements	Manual Manual Providence
	Statistics in succession.	Contraction of the local division of the loc			124 445 215
A H & S T H & F & T S IL L F & G T F			5 2 7 8 8 0 1 3 4 B	EIA TIA C+ 1A	154147454
		7 5 1 4 5 7 5 8	* 1 5 1 2 6 1 1 5 0		The second distances in the se
Married Married Married Married Married	States and a state of the state	THE REAL PROPERTY AND INCOME.	and the second s	The second second second	The second second
the state of the s	States and States and	States and states			
1 2 1 2 3 2 7 2 1 J 2 2 1 3 2 1 J 1 7 1	E T L A M C .	7 4 4 6 6 7 9 7	1 1 1 2 3 7 7 3 3 1 10	E 11 A 12 / 1 A 1 7	Contraction of the local division of the loc
		States Include	and the second s	Manager and Street and Street	Statement Statement
NAMES OF TAXABLE PARTY OF TAXABLE PARTY.	States and a state of the	TRACTOR DESIGNATION OF TAXABLE	1 1 4 1 1 5 1 4 1	1 + + + A / / / +	4 0 - 2 2 4 8 3 H
7 8 8 3 3 1 8 4 3 6 3 7 4 3 1 8	1125143	5 4 7 8 8 4 4 2	5 + 7 3 3 7 4 10 + 0	41278 + 434	
			and the second s	TORSE AND DESCRIPTION	The second se
	Solo I and I and I	and the second second	Station in the local division in the local d	1 4 5 4P 7 7 4 5	1 . 7 0 3 F 7 10 9
1 4 41 5 40 L 1/ 2 2 7 2 L 1/ 1 / 4 3	2 11 3 3 4 1	C + + + + + + + + + + + + + + + + + + +	5 + 7 5 + 1 2 7 3 1	7 4 7 46 1 4 4 4	A.S. + 7 + 8 1 4 4
THE R. LEWIS CO. LANSING MICH.	2 6 5 2 6 10 3	124 654 25			A DECK DECK
	States of the second	NAME OF TAXABLE PARTY.		The state of the second	The state of the s
A H 4 3 61 7 12 6 7 13 6 7 13 10 10 10 10 10 10 10 10 10 10 10 10 10			The state of the s	5 8 4 Jale 1 4 1	A & A & A & A & A & A & A & A & A & A &
THE REAL PROPERTY OF THE PROPERTY OF THE REAL PROPE		2 2 2 2 2 2 2 2 2		es : e : 7 1 2	
			and Diversition in the local diversities of		The second division of
the state is a state of the sta				A C T STAALS	A 1 2 3 F 4 5 5 5 5
CONTRACTOR DE LA CONTRACT	1 × 1 × 1 7 5	1 4 9 5 7 8 4		2111 2 2 2 2 7	
		States and the second second	in the second second second	Note Barris and	The second se
	A COLORED	Contraction of the local division of the loc	The state of the s		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

y' s
gromaning ball
also a fin a sta a sur a ser a sin a
The second
A THAT A THAT A THAT A THAT A THAT A THAT AND A THAT A THA
A T & A B &
A REAL PROPERTY AND A REAL PROPERTY A REAL PROPERTY AND A REAL PROPERTY AND A REAL PRO
and the second and the second second

Miles Cars St Cell

 $f_{0} = g_{0} ( i_{1} > j_{2} > i_{1} < j_{2} > j_{1} < j_{1} > j_{2} > j_{1} < j_{2} > j_{2} < j_{2} > j_{2} < j_{2} > j_{$ 

c d e f g h i l m n o p q r s t u z

159

18 11 1 2 14 13 16 9 15 7

2 8 20

HistoCrypt 2022 Amsterdam © 2022 Paolo Bonavoglia

anoghceufszmiqptrbld

bld

a 20 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19

a 20 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19

### Foreword

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

- 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

- 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

Et y poter più facilme consequir queen bernificio, fro giudicato marssinioisformante in modo A babbino qualche similitudine, è conformita' con quelle del Belasi, del Tritemio, del Posta, et di almi simili scuitoni, in queeta professione, acció o quello oggiordinano suol temer ogni Principe,

#### 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.





DI MISSER GIOVAN BATTISTA BELLASO, GINTIL'HYOMO BRESCIANO.

CON LE SVE SINGOLARISSIME QVALITA To noui precetti, et regole, da effo nella bellifsima, O importantifsima arte di Cifrar ritrouate, O in luce poste.

#### LE SINGOLAR QUALITA DELLE CIFRE, SONO QUESTE,

L A 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 feconda è, che fono di tal prestezza da cifrare, & decifrare, attefa la loro fecurezza, che non ui fi trouerà pari, esfeudo in esfe esercitati.

La terza è, che col primo, terzo, quarto, & quinto modo di cifrare, fi può cifrar fenza far le minute delle lettere, ilche importa affai, & fe pure à principianti il cifrare farà di qualche incommodo, alli efercitati farà di piacere & [paffo.

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 fe le prime quattro cifre, per qualche accidente fi perdono, fi poffono fubito riformare con la dittione, con laquale fon composti gli alfabeti, come Stauan prima.

La festa è, che le cifre fi mutano, mutando la dittione, con laquale fon composti gli alfabeti, fenza mutar punto la forma della cifra, imperò che fi muta la fostanza, & 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.

Almin Euch mi sin Com

Messo is fire In di Francisch fo les His Indalle normal , + how to rain mie bischow and gares see one and job of one min summer alli Eart " sift api noi profori , et mi afforn darlo one tiffe lill quality profer in essen soon scara limandas alos promis the ofer adoptate noth correction men Para a rest of All the color accounter it motive part of a is atondous a quark growines, no fife base and bolk as Ablanis di sig "gournalor dille intelle prime name laper l'effetusion A ai fofore coper de che por in men 1000 to d'anis fighilo la quel Maderie & rate ligensis de U.S. Mar prifer la vera part li a office it quines con sole li une, co fe divino in a sa misso a cono d'inquesto dues all'anno oficionisseres de il contenione to la la quarie d'andele a come pocco più li cono ducas; on lass astrado alte simplier parale di un no diege source at an difer at un por la para an foores il reis conserve, rourne pur inverse quello mi si deserve des fri le prese anche dimanci dei wass li canto and and a come and grangers all alter a dell' qual so bor on nicordo cano doi delle Sig " to for I clar Con ginerities, on clar to Viene , on Clafer il here in some . In investige lago a sende it may seil and them and and sour a shop on mo in from To a some and dischiantion? I bringnam in with di quate part. Ond to enverse dage ton to que to no have a obligo aleuno for nose proces alle con " sig sand, or parlare and Ma promin di sua sout or dell' surtime Colleggio et lectioni as alamon quelle Dom alligne y la min some no anche me h' cost di que servite a quero sec a fondals a new l' allitter & an on he fut had the "3" " Plane" Marine he b' part you low's prine pal and Aqueta Tiple fafe mode the secure in note the sec populat alogoned is to other to plan cut " sof sand suffer in raffer une fir in et there & an for low be soon of Denie wel epin's & sun Sub " Pin's a melsa panto at a my frances in cachenon' at is house strip a quanto haucun promo to et et la min niften si porren acar braifn'an pro of fift notion to part. is mandum all' 5 D. How hewards wier & to have not for all'olligo mes, or I good sen doors della gratia, Jospico la suplico ad istar content li forme queston giurnin , & gres de su' som vicenut in gratin & sis pola 2 0 5 Mm la pais' ail Mar lon : li ze co grinnen & deschamenions of is hablin suplise al lobis mis is at y consequencia hall. netainen il bras fini pramofani, lora to a confinime di ottomir no ifirado mai solin' li . U.S. Allow hi mosther alle san overion di quella grasia di una nola gli have promi/or Is qual home mone' is sincreak m' mi sausmile .

#### 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.

La la Diffora mia quarté condicioni . di grandiscimo comodo et litilii Lover da questa peler si puo un significato finto comi a cueli falso, or voi amili. Sopa l'info Caractru, por to manifet l'auto uno fronto it in hut narroso at ogn uno ~ L'fauit a componer in qual o' unglis lingun 1+ impossibili D's intende mai se or de colori de de mi prime conosura le chiani o con hange Silquali's apri linh nor mio rinchiuso . 3 Si murano le chiaui o signi ad infinito, ni scupier si pono hinshi alai fien' alcune di quell' innignate s'haur fa'. 9 Non V'enna alun enation' inusil' o Vano m' hou' prikada o biciond na inscuna lokua soren' juna lie a mel uno bugiardo come nel utulia 5 Annalir oi puo la interneción societar sons l'uno del aniso finto our " suo Alabeto alun o contra ugue floti è ascai li minor topo i forica 6 Nel componer a rifer preditte banda puo l'aireto boun seriotori forma prisolo ni dubitation alcuna d'ofer constituro l'animo mis fin chi co'l agno so ecurlaso no lo habria a chi fare bisogno . / > Alla line sigillan V's quillo the si nursa ne accadi p ais sporter almi me ragging to my la replice fan'. Tanto por chil Kiquendent' in slaw mode in de m' prima accumate.

#### 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?

of sovier . i. omnipotens sempiterne Deus. 3. 19. 6. 4. 10. 3. 5. 1. 5. 9. 9. 1. 13. 12. 2. 5. 1. 7. 6. 1. 19. 1. 5. 9. 19. 11. 11. 15. 1. 19. 6. 19. 10 . 19. 10 . 10 . 10 . 10. 10. 19. 18. 53. 48. 31. 58. 12. 19. 41 f swingt ... 2. Signooi mei Sonovandissimi. 13.51.13.28.55. 34. 06. 12. 41. 48.49.39 .47.77. 35.47.31.37.44.18.48.18.17.37. 10.4.17.7.1.5.4.12.2.4.12.1.1.5.6.7.16.4.10.10.4.12.4. 23.55.30.35.56.39.60.34.44.52.65.40.54.78.40.53.38.53.48.35.58.1.19.41 1 Sories . 9. Il signor turco sta benisimo. ii 49. 10. 10. 38. 38. 56. 92. 37. 10. 62. 9. 39. 44. 25. 50. 47. 19. 59. ie is. 57. iz. 6. 5. it. it. 10. i. 4. 2. 7. 0. 2. ii. 4. 5. 7. 9. ig. 3. i. in. f. in. it. it. 4. 23.55. 20. 15. 56.39. 60.34.44.52.65.40.54.70.40.53.38.53. 48.35.58.22.19.41

# 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

	\$ maler i.
131390 35 36 9	9 6 34 44 52 6540 54 78 4053 3853 4 835 58 12 1941. 1 52 33 38 43 26 39 41.6 38 45 37 + ( 4234 48 21 14 32 )
3. i3. 6. n. in. 3 omnipo	tenssempiterredeus.
	t malar. 2.
23.51.30.35.56.3 13.51.13.28.11.3	9.60.34.44.54.65.40.54.78.40.53.30.53.40.35.58.12.14.45. 4.56.12.41.45.45.99.47.77.35.47.31.97.44.15.48.18.17.37.
io	imeisonorandissimi
	2 tralor . g.
23.55.30.35.56	· 39 · 60.94 44.52.65.40.54.78.40.53.38.59.48.3558 12.
i L s i g	i.q.2.7.8.2.11.4.5.7.9.13.3.1.12.5.12.14. norturcosta 6enisimo

## 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

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

Inside the sealed envelope a new fake key.

					E	inci	уp	t n	ewl	у	Em	npty	y ai	nd	res	tarl	t								
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	Ν	0	R	т	۷	R	С	0	S	т	Α	В	Е	Ν	I	S	I	М	0	
dood message	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	
			Dec	cryp	btι	ısin	g t	rue	ke	y	De	cry	γpt	usi	ng	fak	æ k	æy	s :	Г					
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	
Decipied text	S	I	G	Ν	0	R	I	М	Е	I	Н	0	Ν	0	R	Α	Ν	D	I	S	S	I	М	I	
					ł	Enc	ryp	t n	ew	y	En	npt	y a	nd	res	tar	t								
Good key:	63	37	41	35	79	Enc 53	ryp 62	t n 66	ew 60	у 80	<b>En</b> 52	1 <b>pt</b> 63	<mark>y a</mark> 76	nd 38	res 40	tar 58	67	46	67	54	58	60	78	34	
Good key:	63 I	37 L	41 S	35 I	79 G	Enc 53 N	ryp 62 0	<b>t n</b> 66 R	еw 60 т	у 80 V	En 52 R	npt 63 C	<mark>y a</mark> 76 0	nd 38 S	res 40 T	58 A	<mark>t</mark> 67 В	46 E	67 N	54 I	58 S	60 I	78 M	34 0	
Good key: Good message	63 I 12	37 L 06	41 S 05	35 I 12	79 G 18	53 53 N 01	<b>ryp</b> 62 0	t n 66 R 02	еw 60 т 07	y 80 V 08	En 52 R 02	<mark>1pt</mark> 63 C 11	<mark>y a</mark> 76 0	nd 38 S 05	<mark>res</mark> 40 т 07	58 58 09	<mark>t</mark> 67 В 13	46 E 10	67 N 01	54 I 12	58 S 05	60 I 12	78 M 14	34 0 04	
Good key: Good message Cryptogram:	63 I 12 75	37 L 06 43	41 S 05 46	35 I 12 47	79 G 18 97	53 53 01 54	62 0 04 66	<b>t n</b> 66 R 02 68	ew 60 T 07 67	9 80 V 08 88	En 52 R 02 54	npt 63 C 11 74	y a 76 04 80	nd 38 5 05 43	res 40 т 07 47	58 58 09 67	t 67 В 13 80	46 E 10 56	67 N 01 68	54 I 12 66	58 S 05 63	60 I 12 72	78 M 14 92	34 0 04 38	
Good key: Good message Cryptogram:	63 12 75	37 L 06 43	41 S 05 46	35 I 12 47	79 6 18 97	53 N 01 54 Jsin	ryp 62 04 66	t n 66 R 02 68	еw 60 т 07 67	9 80 V 08 88	En 52 R 02 54	100 63 C 11 74	y a 76 04 80	nd 38 95 43 Usi	res 40 Т 07 47	58 58 09 67	67 B 13 80	46 E 10 56	67 N 01 68 S	54 I 12 66	58 S 05 63	60 I 12 72	78 M 14 92	34 0 04 38	
Good key: Good message Cryptogram: Fake key	63 12 75 66	37 L 06 43 41	41 S 05 46 De 31	35 I 12 47 Cry 41	6 79 18 97 0t 1 94	53 N 01 54 Jsin 47	ryp 62 04 66 ng t	t n 66 R 02 68 rue 55	ew 60 T 67 67 66	80 V 08 88 <b>X</b> 88	En 52 R 02 54 De 36	11 63 c 11 74 cry 71	<mark>y a</mark> 76 04 80 <b>/pt</b> 74	nd 38 05 43 <b>USI</b>	40 T 07 47 <b>ng</b> 40	tar 58 A 09 67 fak 63	67 B 13 80 (e) 74	46 E 10 56 <b>(ey</b> 46	67 N 01 68 <b>S</b>	54 12 66 T 57	58 S 05 63 54	60 I 12 72 70	78 M 14 92 79	34 0 04 38 38	
Good key: Good message Cryptogram: Fake key Decrypted text	63 12 75 66 09	37 L 06 43 41 02	41 S 05 46 De( 31 15	35 I 12 47 <b>Cry</b> 41 06	6 79 6 18 97 01 ( 94 03	53 N 01 54 Jsin 47 07	ryp 62 04 66 19 t 64 02	t n 66 R 02 68 rue 55 13	ew 60 T 07 67 e ke 66 01	80 V 08 88 <b>2</b> 88 86 02	En 52 R 02 54 De 36	npt 63 C 11 74 2CN 71 03	y a 76 04 80 /pt 74 06	nd 38 05 43 <b>USI</b> 40 03	40 T 07 47 10 40 07	tar 58 09 67 fak 63 04	67 B 13 80 (ce) 74 06	46 E 10 56 (ey 46 10	67 N 01 68 5 66 02	54 I 12 66 <b>T</b> 57 09	58 S 05 63 54 09	60 I 12 72 70 02	78 M 14 92 79 13	34 0 04 38 38 36	

#### 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.
- 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

per Soiner B. C.D.I.T.G.H.I.L.M. H.O.P.Q.R.S.T.V.Z. 16. is. i. is. a. 4. ig. no. 8. i4. 7. is it. io. g. in. s. ii. 3. 6. 36. 97 . ai . 35 na . a4 . 99 - 28.74 17 . 97 . 98 . 70 . 29 . Ja. 25. Bi . 29. ab A. Aler 75 N. Qui - 26 B Balia \_ 60 Papert - 65 Imperator - 87 Else \_\_\_\_ st Imperator \_ s> Fsjedi \_\_\_\_ s> 1. La Regi Madre 6, 1 Sontita' sexmo Prefent - 77 c Con \_ Serta Isming - 49 - 46 Maestri - 40 Far -Cons! dix -si Signor Forment - 98 M. Molt - 78 Quant Constant ! - 90 sempre -Mente \_ mlique - 93 Per priver Galec \_\_ 43 Clarissim -58

Grata → 8	A →	16	16 - 8 = 8	La cifra di A è 8
Grata $\rightarrow 19$	$A \rightarrow$	36	36 - 19 = 17	La cifra di A è 17
Grata → 19	$A \rightarrow$	16	$16 - 19 = 17 \pmod{2}$	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, Whethe	or not r 'tis	: to be nobler	, th r in	at is f the mi	the que nd to :	estion, suffer	,																1	Plain text
								Clic	: qui	per	cifra	are c	on le	e cas	selle									Cifra A16-36 Grata Germania
							Sc	ovracif	ira co	n grat	a Ger	mania (S	Sacro R	lomano 1	Impero	) ~								
t	0	b	e	0	r	n	0	t	t	0	b	e	t	h	a	t	i	s	t	h	e	q	u	CIITà caselle
11 -	18 -	13 -	2 -	18 -	12 -	17 -	18 -	·   11 - '	11 -	18 - '	13 -	2 - 1	( <b>11</b> - '	20 - 1	16 -	11 -/	8 -	5 - /	11 -	20 -	2 - /	9 - /	3 - 1	
2	8	3	2	6	10	0	3	7	4	1	10	2	7	5	2	4	1	3	7	2	4	( 1 '	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		i		n	<u>h</u>	e	+	h	e	r	t	Γ <sub>i</sub>	s	n	•	ь		e		+	n	t	2 8 3 2 6 10 0 3 7 4 1 10 2 7 5 2 4 1 3 7 2 4 1 8
2 -	5 -	11 -	8 -	18 -	17 -	20 -	2 -	11 -	20 -	2 -	12 -	11 -	8 -	5 -	17 -	18 -	13 -	14 -	2 -	12 -	8 -	17 -	11 -	1         7         2         5         1         2         6         1         2         5         1         0         4         0         5         2         5         7         4         1         6         7         7         4         1         6         7         7         1         6         7
1	7	2	5	0	12	2	8	3	1	0	4	0	3	6	2	5	7	4	1	3	0	7	2	3       1       0       2       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
		I <sup>1</sup>	['			·   '	,	-  '		·   '		· '	( <u> </u>	'	I	'		'		-  '	· '	( <u> </u>	<u> </u>	6         0         3         1         5         1         7         1         0         2         8         1         3         81210         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
1	18	9	3	18	5	18	14	8	19	2	8	11 /	5	19	15	13	6	10 '	1	9	8	10 /	9	3 0 3 0 4 5 7 1 7 3 4 0 2 5 7 0 5 6 2 7 1 4 3 2
h	е	m	i	n	d	t	0	s	u	f	f	e	r		<u></u>		<u> </u>		<u> </u>					10         4         1         5         4         1         5         2         4         1         5         1         4         2         10         2         10         1         1         0         1         1         0         1         1         0         1         1         0         1         1         0         1         1         1         0         1         1         1         0         1
20 -	2 -	7 - '	8 -	17 -	15 -	11 -	18 -	- 5 -	3 -	4 -	4 -	2 -	12 -											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       3       5
5	2	6	$\begin{bmatrix} 1 \end{bmatrix}$	2	3	4	0	5	2	14	1	3	2											<b>3 9 6 8 1 4 2 5 0 1 7 3 1 4 0 8 110 2 7 2 1 5 3 6 1 0 5 1711 015 5 3 8 6 1 0</b>
		I — !	[]			·   '		-		·   '		. !	[]											2 0 15 11 0 17 18 2 4 1 14 3 5 2 9 6 1 4 3 7 2 6 1 7
15	0	1 '	7	15	12	7	18	0	1	10	3	19	10											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
										Cifrat	o da	trasm	ettere	£										2 5 5 7 3 4 0 8 9 6 1 12 11 10 2 7 0 14 2 1 4 4 2 12
9 10	) 10	0 12	2	17 15	4	7 17	3 0	) 4 1	5 14	7 7	2	4 18 2	18 8	15										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       1       2       5       8       3       6       3       9       4       2       2       8       5       1       3       4
1 18	39 31	3 18	5 12	18 14 7 18	81 60	9 2	8 11 3 19	. 519 310	3 15 °	13 6	10	19	8 10	9										6 1 7 2 5 8 3 2 7 4 4 0 6 1 14 3 2 11 15 0 14 3 6 7 13 1 4 7 3 6 0 4 1 2 5 7 4 6 12 4 7 14 0 5 11 10 3 8
	· -	1				1																		

Cifra delle Caselle - Esempio interattivo

#### **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     3     1     0     4     0     3     6     2     5     7     4     1     3     0     7     2     4     1     3     7     2     4     1     3     7     2     5     7     4     1     3     0     7     7       5     2     6     1     7     2     3     4     0     5     1     7     1     0     2     8     1     3     8     12     10     6     8     1     3     8     12     10     2     7     4     1     5     2     1     6       6     0     3     1     5     1     7     1     7     3     4     0     2     5     7     0     5     6     2     7     1     4     3     2     1     1     5     1     1     1     3     0     1     1     3     1     1     3     1 <t< th=""><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></t<>																								
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     7     2     4     1     7     2     4     1     7     2     4     1     7     2     5     1     5     1     7     2     5     7     0     1     7     2     5     1     6     2     7     5     3     6     8     2     5     1     3     8     12     10     2     7     4     1     7     2     1     4     0     2     5     7     0     5     6     2     7     1     4     3     2     1     1     8     1     3     8     1     1     3     1     1     1     3     1     1     3     1     1     3     1     1     3     1     1     1     3     1	ź	2 8	3	2	6	10	0	3	7	4	1	10	2	7	5	2	4	1	3	7	2	4	1	8
5       2       6       1       2       3       4       0       5       2       14       1       3       2       4       1       7       2       4       1       7       2       4       1       7       2       4       1       7       2       4       1       7       2       5       1       5       4       1       7       2       5       1       5       4       1       7       2       5       1       7       2       5       1       7       2       5       1       7       2       5       1       7       2       5       1       7       2       5       1       7       2       5       1       7       2       5       7       1       7       2       5       7       1       7       3       4       0       2       5       7       0       1       4       8       2       1       7       3       1       3       1       1       3       1       1       3       1       1       3       1       1       1       3       1       1       3       1       1	-	ן 7	2	5	0	12	2	8	3	1	0	4	0	3	6	2	5	7	4	1	3	0	7	2
3       1       10       2       0       4       1       7       2       8       0       2       5       1       5       4       1       7       2       5       8       1       7       2       5       8       1       7       2       5       8       1       7       2       5       8       1       7       2       5       8       1       3       8       12       10       2       7       4       1       5       2       1       4         4       2       7       5       3       6       8       2       5       7       0       5       6       2       7       1       4       3       2       6       1       8       7       2       5       6       6       2       7       1       4       3       2       6       1       3       7       1       8       3       2       4       1       5       0       1       1       3       3       1       1       3       1       1       3       1       1       3       1       1       3       1       1       1 <td>Ę</td> <td>52</td> <td>6</td> <td>1</td> <td>2</td> <td>3</td> <td>4</td> <td>0</td> <td>5</td> <td>2</td> <td>14</td> <td>1</td> <td>3</td> <td>2</td> <td>4</td> <td>1</td> <td>7</td> <td>2</td> <td>4</td> <td>1</td> <td>6</td> <td>2</td> <td>5</td> <td>0</td>	Ę	52	6	1	2	3	4	0	5	2	14	1	3	2	4	1	7	2	4	1	6	2	5	0
7       1       4       3       5       0       6       2       1       4       3       7       2       5       0       4       0       6       8       1       3       8       12       10       2       7       5       3       6       8       2       5       4       0       2       6       1       8       7       2       5       1       6       3       4       0       2       6       1       8       7       2       5       1       6       3       4       0       2       5       7       0       5       6       2       7       1       4       3       2       4       1       5       0       1       4       8       2       10       2       0       1       4       3       7       2       5       0       1       4       3       3       2       4       1       5       0       1       7       3       1       4       0       5       0       1       7       3       1       4       0       1       3       1       1       1       1       1       1	3	3 1	10	2	0	4	1	7	2	8	0	2	5	1	5	4	1	7	2	5	8	5	3	6
6       0       3       1       5       1       7       1       0       2       8       1       3       8       12       10       2       7       4       1       5       2       1       6       3       4       0       2       6       1       8       7       2       5       1       6       3       4       0       2       5       7       0       5       6       2       7       1       4       3       2       4       1       5       0       1       4       8       2       10       2       0       2       5       0       1       4       3       2       0       2       5       0       1       7       3       2       4       1       5       0       1       7       3       2       4       7       1       8       2       10       1       1       3       1       1       3       1       1       1       3       1       1       3       1       1       1       1       1       1       1       1       1       1       1       1       1       1       1 <td></td> <td>7 1</td> <td>4</td> <td>3</td> <td>5</td> <td>0</td> <td>6</td> <td>2</td> <td>1</td> <td>4</td> <td>3</td> <td>7</td> <td>2</td> <td>5</td> <td>0</td> <td>4</td> <td>0</td> <td>6</td> <td>8</td> <td>1</td> <td>3</td> <td>8</td> <td>0</td> <td>4</td>		7 1	4	3	5	0	6	2	1	4	3	7	2	5	0	4	0	6	8	1	3	8	0	4
4       2       7       5       3       6       8       2       5       4       0       2       6       1       8       7       2       5       1       6       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       2       5       0       6       9       1       7       3       2       4       1       5       0       1       7       3       2       5       0       1       7       3       1       1       5       0       1       7       1       1       3       1       1       1       3       1       1       1       1       3       1	e	5 0	3	1	5	1	7	1	0	2	8	1	3	8	12	10	2	7	4	1	5	2	1	6
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       2         10       4       11       3       0       9       4       1       7       6       1       7       2       0       2       5       0       6       9       1       7       3       2       4       7       1       8       2       5       0       4       1       5       2       11       7       1       1       8       2       5       0       4       1       3       5       2       4       7       1       8       2       5       0       4       1       5       0       1       1       1       1       5       1       1       1       1       1       1       1       1	4	12	7	5	3	6	8	2	5	4	0	2	6	1	8	7	2	5	1	6	3	4	0	4
6       3       1       4       2       7       5       4       1       8       3       2       4       1       5       0       1       4       8       2       10       2       0       2       5       0       6       9       1       7       3       2       7       3       2       7       3       2       7       3       2       7       3       2       7       3       2       7       3       2       7       3       2       7       3       2       7       3       3       7       7       3       1       7       0       10       3       12       2       8       1       3       4       1       5       3       8       6       1       7       3       1       4       0       8       1       10       2       7       2       1       5       3       8       6       1       7       3       1       4       0       1       1       1       5       1       1       1       1       1       1       1       1       1       1       1       1       1       1 <td>3</td> <td>3 0</td> <td>3</td> <td>0</td> <td>4</td> <td>5</td> <td>7</td> <td>1</td> <td>7</td> <td>3</td> <td>4</td> <td>0</td> <td>2</td> <td>5</td> <td>7</td> <td>0</td> <td>5</td> <td>6</td> <td>2</td> <td>7</td> <td>1</td> <td>4</td> <td>3</td> <td>2</td>	3	3 0	3	0	4	5	7	1	7	3	4	0	2	5	7	0	5	6	2	7	1	4	3	2
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       2       14       0       16       1       10       17       18       2       4       1       14       3       5       2       9       6       1       4       3       7       2       6       1       7       2       6       1       7       14       1       5       1       1       1       1       1       1       1       1       1       1       1       1	e	53	1	4	2	7	5	4	1	8	3	2	4	1	5	0	1	4	8	2	10	2	0	3
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       1       7       3       1       4       0       8       1       10       17       18       2       4       1       14       3       5       2       9       6       1       4       3       7       2       6       1       7       14       1       5       0       14       2       6       1       14       0       7       14       0       1       1	10	) 4	11	3	0	9	4	1	7	6	1	7	2	0	2	5	0	6	9	1	7	3	2	5
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       7       2       1       5       3       8       6       1       7         4       1       6       2       5       4       6       1       7       3       4       2       6       2       4       0       1       4       1       4       3       7       2       6       1       4       3       7       2       6       1       4       1       4       1       4       1       4       1       4       1       4       1       4       <	e	5 1	3	4	1	2	7	4	8	1	3	5	2	4	7	1	8	2	5	0	4	7	3	6
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       14       10       13       5       0       14       3       5       2       4       0       13       5       0       14       3       3       7       14       10       5       6       1       3       4       2       8       5       3       13       2       7       4       4       2       14       3       4       14       3       3       14       14	Į.	5 0	14	2	3	8	6	1	4	5	2	11	7	0	10	3	12	2	8	1	13	4	1	5
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       4       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       2       6       1       4       3       7       2       6       1       4       0       7       2       6       1       4       0       7       12       7       0       13       5       0       4       2       7       5       3       13       2       7       4       4       2       14       3       4       14       14       14       14       14       14       14       14       14       14       14       14 <td< td=""><td>3</td><td>39</td><td>6</td><td>8</td><td>1</td><td>4</td><td>2</td><td>5</td><td>0</td><td>1</td><td>7</td><td>3</td><td>1</td><td>4</td><td>0</td><td>8</td><td>1</td><td>10</td><td>2</td><td>7</td><td>2</td><td>1</td><td>5</td><td>3</td></td<>	3	39	6	8	1	4	2	5	0	1	7	3	1	4	0	8	1	10	2	7	2	1	5	3
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       14       3       4       2       16       14       3       14       3       4       14	e	52	7	4	1	3	2	7	4	5	4	0	6	1	17	12	0	15	5	3	8	6	1	0
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       14       1       14       1       14       1       14       1       14       1       14       1       14       1       14       1       14       1       14       1       14       1       14       1       14       1       14       1       14       1       14       1       14       1       14       1       14       1       1       1       14       1       14       1       14       1       14       1       14       1       14       1       14       1       14       1       14       1       14       1       14       1       14       14       14       14       14       14<	ź	2 0	15	11	0	17	18	2	4	1	14	3	5	2	9	6	1	4	3	7	2	6	1	7
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       17         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       8       4       1       12       13       4       7       3       2       1       4       4       12       14<	4	1 1	6	2	5	4	6	1	7	3	4	2	6	2	4	0	7	12	7	0	13	5	0	14
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       1         2       5       5       7       3       4       0       8       9       6       1       12       11       10       2       7       0       14       2       1       4       4       2       17         0       4       7       5       3       6       2       5       8       4       2       7       6       1       4       7       3       2       5       2       4       6       6       3       6       3       2       7       6       1       4       7       3       2       1       4       4       1       1       1       1       1       1	8	3 1	6	2	7	2	5	5	4	0	4	7	2	8	0	5	2	4	6	6	2	4	3	0
8       3       6       1       7       2       5       0       4       2       7       5       4       1       4       8       2       7       6       1       14       3       4       1         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       6       3         5       2       8       7       3       7       4       1       4       2       5       8       3       6       3       9       4       2       2       8       5       1       3       4       1       3       4       1       4       7       3       5       1       3       4       1       1       1       1       1       1       1       <	10	) 2	7	14	0	5	6	1	3	4	2	8	5	3	13	2	7	4	4	2	11	6	2	16
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 <td< td=""><td>8</td><td>3 3</td><td>6</td><td>1</td><td>7</td><td>2</td><td>5</td><td>0</td><td>4</td><td>2</td><td>7</td><td>5</td><td>4</td><td>1</td><td>4</td><td>8</td><td>2</td><td>7</td><td>6</td><td>1</td><td>14</td><td>3</td><td>4</td><td>11</td></td<>	8	3 3	6	1	7	2	5	0	4	2	7	5	4	1	4	8	2	7	6	1	14	3	4	11
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       6       3       9       4       2       2       8       5       1       3       4         6       1       7       2       5       8       3       2       1       14       4       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         12       1       4 <td>ź</td> <td>2 5</td> <td>5</td> <td>7</td> <td>3</td> <td>4</td> <td>0</td> <td>8</td> <td>9</td> <td>6</td> <td>1</td> <td>12</td> <td>11</td> <td>10</td> <td>2</td> <td>7</td> <td>0</td> <td>14</td> <td>2</td> <td>1</td> <td>4</td> <td>4</td> <td>2</td> <td>12</td>	ź	2 5	5	7	3	4	0	8	9	6	1	12	11	10	2	7	0	14	2	1	4	4	2	12
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       1       14       2       2       8       5       1       3       4         12       1       7       2       5       8       3       2       5       7       4       6       12       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         10       4       12       10       11       1       2       8       2       5       7       4       6       12       4       7       14       0       5       11       10       3       8       4       6       <	(	) 4	7	5	3	6	2	5	8	4	2	7	6	1	4	7	3	2	5	2	4	6	6	3
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       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       0       6       1       7       3       2<		5 2	8	7	3	7	4	1	14	2	5	8	3	6	3	9	4	2	2	8	5	1	3	4
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	(	5 1	7	2	5	8	3	2	7	4	4	0	6	1	14	3	2	11	15	0	14	3	6	7
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	12	2 1	4	7	3	6	0	4	1	2	5	7	4	6	12	4	7	14	0	5	11	10	3	8
6       5       3       0       4       6       1       4       5       3       6       4       2       5       8       4       4       0       6       1       7       3       2       7	(	) 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 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.

74		Wo uppoint	
A B 4 cis air as fin co fo gir die de his his hi ano giy gr	D E T L $a_{12}$ 'int as a $c_{12}$ int as a $c_{12}$ in $c_{13}$ c $c_{14}$ c $c_{14}$ c $c_{15}$ c $c_{1$	g H I L M N O P g H I L M N O P $g a a^{10} a^{10} a^{10} a^{11} a^{11} a^{11} a^{11} a^{11}$ $g^{11} g^{11} g^{11} g^{11} g^{11} g^{11} g^{11} g^{11} g^{11}$ $g^{12} g^{12} g^{12} g^{12} g^{12} g^{13} g^{13} g^{13} g^{11} g^{11}$ $g^{13} g^{12} g^{12} g^{12} g^{13} g^{13} g^{13} g^{11} g^{11}$	Q P S T V $\gamma$
Accordo ···································	apide of api	$m = a_{68} q_1 = a_{64} a_{64} a_{64} a_{64}$	Mal _ 452 pri _ eiz hu Malmo _ 1.52 (n _ eiz hu (u

#### Alfabeto

	а	b	С	d	е	f	g	h	i		m	n	0	р	q	r	s	t	u	Z
	a <sup>20</sup>	a <sup>17</sup>	a <sup>5</sup>	a <sup>19</sup>	a <sup>6</sup>	a <sup>8</sup> -	a <sup>3</sup>	a <sup>4</sup>	a <sup>12</sup>	a <sup>18</sup>	a <sup>11</sup>	a <sup>1</sup>	a <sup>2</sup>	a <sup>14</sup>	a <sup>13</sup>	a <sup>16</sup>	<b>a</b> 9	a <sup>15</sup>	a <sup>7</sup>	a <sup>10</sup>
	c <sup>15</sup>	c <sup>12</sup>	c <sup>20</sup>	<b>c</b> <sup>14</sup>	c١	<b>c</b> <sup>3</sup>	c <sup>18</sup>	c <sup>19</sup>	c7	<mark>د</mark> 13	с <sup>6</sup>	<b>c</b> <sup>16</sup>	c <sup>17</sup>	с <sup>9</sup>	с <sup>8</sup>	<b>c</b> 11	c <sup>4</sup>	c <sup>10</sup>	c <sup>2</sup>	c5
	dl	d <sup>18</sup>	d <sup>6</sup>	d <sup>20</sup>	d7	d <sup>9</sup>	d <sup>4</sup>	ds	d <sup>13</sup>	d <sup>19</sup>	d <sup>12</sup>	d <sup>2</sup>	d <sup>3</sup>	d <sup>15</sup>	d <sup>14</sup>	d <sup>17</sup>	d <sup>10</sup>	d <sup>16</sup>	d <sup>8</sup>	d11
	f <sup>12</sup>	f <sup>9</sup> 14	f <sup>1</sup> /	f''	f <sup>18</sup>	f <sup>20</sup>	-20	f10	f <sup>4</sup>	f <sup>10</sup>	f <sup>3</sup>	f <sup>14</sup>	f <sup>14</sup>	f° l.l	f? 10	f <sup>ø</sup> "13	f <sup>l</sup>	f′ 12	f <sup>19</sup>	f <sup>2</sup>
	g'' h <sup>16</sup>	g'" h <sup>13</sup>	9² h <sup>1</sup>	g'' h <sup>15</sup>	g² h²	9 <sup>-</sup>   h <sup>4</sup>	g20 h19	g' h <sup>20</sup>	g² h <sup>8</sup>	g' <sup>3</sup> h <sup>14</sup>	g° h <sup>7</sup>	g'' h <sup>17</sup>	g' <sup>9</sup> h <sup>18</sup>	g'' h <sup>10</sup>	g'° h <sup>9</sup>	g'' h <sup>12</sup>	g∽ h <sup>5</sup>	g'² h <sup>11</sup>	g <sup>-</sup> h <sup>3</sup>	gʻ h <sup>6</sup>
	а	b	с	d	е	f	g	h	i	I	m	n	0	р	q	r	s	t	u	z
а	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
с	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
е	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
Т	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
ο	18	15	3	17	4	6	1	2	10	16	9	19	20	12	11	14	7	13	5	8
р	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?

	а	b	с	d	е	f	g	h	i	1	m	n	0	р	q	r	s	t	u	z
а	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
с	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
1	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
0	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

#### LdaqcbdanbubusdeLf

Quano w Hingno de Transtechi mil sons deine nato Ballo. et defligerant anuiren | de que so sort mo Oominio | in racundar disurs word falle saulte ner wo sons l'aluse inter de oto nel usar & refer franco pin nerger a dimosnarmi obe deinar. col motor in senistano que de Opin us la ginante in pricultor di cosmi occolliner collo aline muser nere Ula quine des

Quanto io Hieronimo di Franceschi mi sono dimostrato ...

115 68

Q	U	Α	Ν	Т	0	I	0	Н	Ι	Ε	R	0	Ν		Μ	0	D		
15	8	20	8	10	5	13	2	3	15	19	19	15	12	13	12	4	11		
L	d	а	q	С	b	d	а	n	b	u	b	u	S	d	е	L	f		
Ι	F	R	Α	Ν	С	Е	S	С	Н	Ι	Μ	I	S	0	Ν	0	D	I	Μ
5	19	5	9	19	20	1	34	9	15	13	8	10	17	6	3	4	9	3	6
u	S	m	m	0	С	С	t	r	S	d	g	0	i	r	L	L	d	S	С

115 1 * 1 2 to 65 1 13 2 2 3 6 15 1 19 6 9 115 5 2 13 2 19 54
1 + r a n & r 4 9 15 15 mis on odim s 19 5 9 19 10 1 49 15 15 mis on odim 4 5 mm 0 c c + r s d g 0 1 r L 2 s c
1 5 + 7 a + 0 f r d r l r v + d i l i g P o 1 5 + 7 a + 0 i 1 4 9 5 2 5 C 13 18 7 2 4 17 10 17 C h h h a c 2 j 9 j h g a g b i 2 p + g s
2 n + P s P r u i to r P d i g u P st 1 2 t a s r g i g g u H P n g z z i g 1 2 t a s s i m o d o m i n g i g 1 2 t a s s i m o d o m i n g i g 1 2 t a s s i m o d o m i n g i g 1 2 t a s s i m o d o m i n g i g 1 2 t a s s i m o d o m i n g i g 1 2 t a s s i m o d o m i n g i g 1 2 t a s s i m o d o m i n g i g 1 2 t a s s i m o d o m i n g i g 1 2 t a s s i m o d o m i n g i g 1 2 t a s s i m o d o m i n g i g 1 2 t a s s i m o d o m i n g i g 1 2 t a s s i m o d o m i n g i g 1 2 t a s s i n g o d o m i n g i g 1 2 t a s s i m o d o m i n g i g 1 2 t a s s i m o d o m i n g i g 1 2 t a s s i n g o d o m i n g i g 1 2 t a s s i n g o d o m i n g
n rac cordard in 11 r s. r. h of t Pa r r s r s r g t h c t r h t f r h t t t t t t t t t t t t t t t t t t
10 A d i m o strap m i o 6 P d i 17 17 17 17 14 17 10 10 17 11 13 3 3 13 17 1 2 14 7 10 14 13 7 10 C C C C F S 3 13 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
in a c L d y <sup>3</sup> L n.m L + r m m L a f h a d n o q u γ. L o c h p i u μ o f + p n.r a st c c t <sup>3</sup> y <sup>5</sup> f <sup>4</sup> 0 <sup>3</sup> h <sup>4</sup> 0 (g) (h d) g + 1 <sup>5</sup> ρ β ρ c i i c p
1 n a n + i a n n e c tis s o n ti for 214

### 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)?

	а	b	с	d	е	f	g	h	i	1	m	n	0	р	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
с	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
I.	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
0	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 [...]

quants alla putit na por certificante, qual delle he is service a my jor putit , co beach to an () when formate and hacent mantho Whom som were juste let horeach on it scontro a lui dato del l'arthenio ; ma grando s. venne all'atto della mora, l'Ami 1 as when nemin , Ala concorrente, 10. La carla gli un tha buerefind in morte And enpends, his box somme, cr withing a monus mimo di sericietta of the more low h' di mar to il homesul di miningente serius hei la me mornie, er illinne ti à la mhina, seriuesse quelle del Contromio, los. condigens nother contentite con lines ; of hounds dife

### 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.

	5	Р	I	R	Т	Q	۷	A	N	D	С	0	Н	L	F	Ζ	G	Ε	м	В
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
м	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
0	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4
Р	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
5	9	10	11	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8
Т	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
В	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13
С	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
Н	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