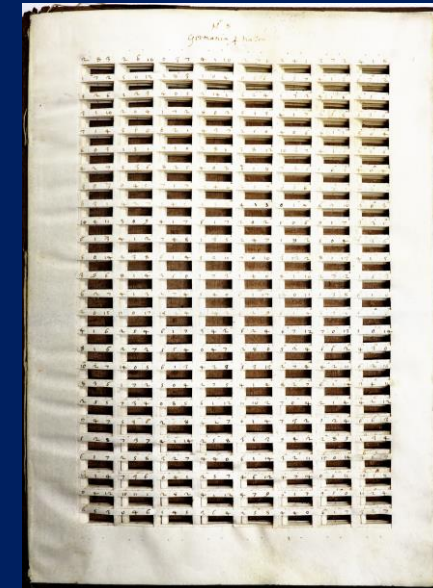




Martedì 30 marzo 2021 17:30

François Viète e le cifre veneziane

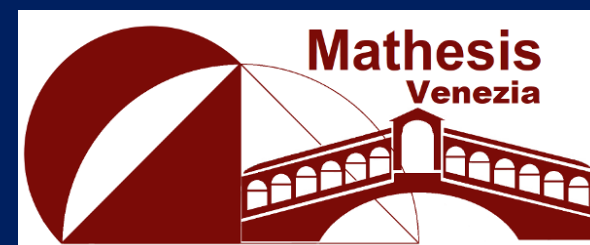


[Archivio di Stato di Venezia](#)



29 agosto 2017 –
Entra in vigore la
legge che liberalizza
le riproduzioni
digitali ...con mezzo
proprio in biblioteche
e archivi pubblici per
finalità culturali.

Ospitato e organizzato da



© 2021 Paolo Bonavoglia

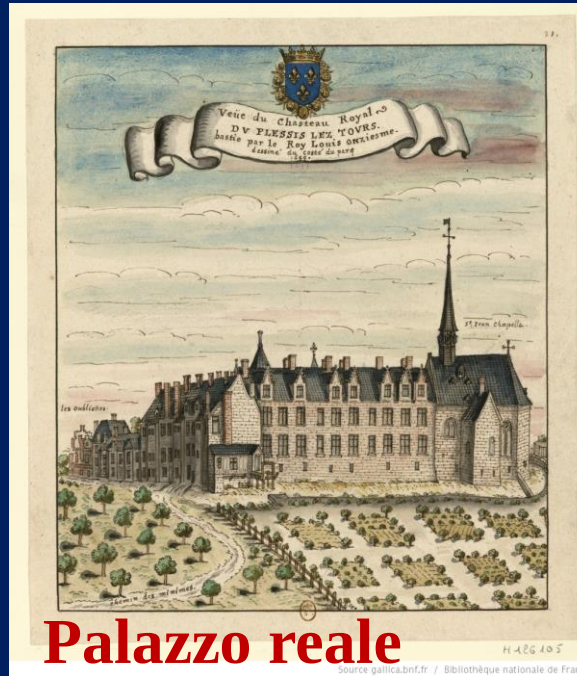
V. 02 04 2021

Serie 1



Enrico IV

Viète
chi era costui?



Tours 1589

Venezia 1595



Cosa vuol dire CX? Consiglio di Dieci

Nella Repubblica di Venezia non c'era un ufficio cifra a se stante, le cifre erano competenza del Consiglio di Dieci (**Cons° di X - CX**)

Il CX era un tribunale irrevocabile che si occupava in particolare della sicurezza dello stato e quindi anche delle cifre.

I dieci membri effettivi erano eletti dal Maggior Consiglio al suo interno, dovevano essere nobili.

Alle riunioni del CX partecipavano di diritto il doge e i sei consiglieri ducali

E quindi i **dieci** erano in effetti **diciasette**.



François Viète

il matematico

Nell' *In artem analyticam isagoge* Viète introduce le lettere per rappresentare incognite. Suggerisce di usare lettere come simboli per quantità, note o incognite. Usa lettere maiuscole, le vocali come incognite, le consonanti come costanti, come in questo esempio:

$$A^3 + B^2A = B^2Z$$

Ma Viète è ancora molto legato alla geometria, quindi questa equazione per lui ha senso perché significa una somma di volumi. Ma la seguente

$$A = B^3 + B^2$$

... non ha senso perché non ha senso sommare volumi, aree e lunghezze.

Sarà poi Cartesio a introdurre la geometria analitica e le minuscole x , y , z per le variabili, dove anche queste somme hanno un senso ben preciso. $y = x^3 + x^2$ rappresenta ...



[Viète su MacTutor](#)

François Viète

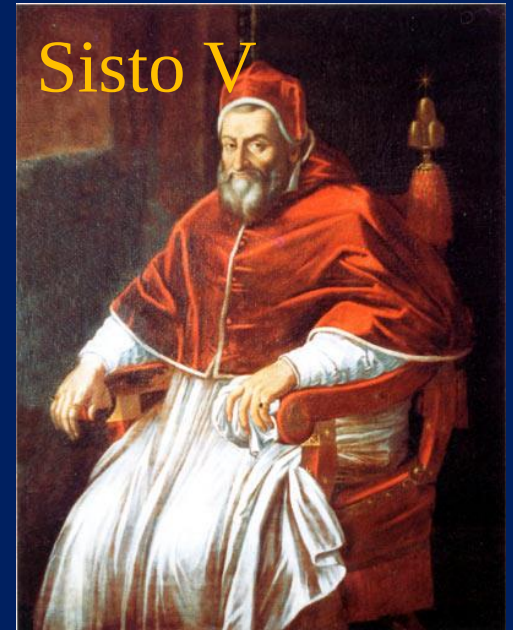
il crittanalista

Viète oltre che come matematico fu un valente crittanalista al servizio di Enrico IV re di Navarra, e dal 1598 re di Francia. Riuscì a decrittare messaggi cifrati del Re di Spagna e dell'Imperatore.

Filippo II di Spagna quando venne a sapere che i suoi dispacci cifrati venivano decrittati, scrisse al papa accusando Viète di praticare le scienze occulte; non è chiaro se ci credesse o se sperasse che Viète fosse condannato al rogo.

Il papa Sisto V non ne fu molto impressionato, aveva un ufficio cifra molto efficiente dove è verosimile ci fossero crittanalisti capaci di fare altrettanto.

In effetti Viète riprese la tecnica dell'*analisi delle frequenze* già nota ai crittanalisti veneziani (Giacomo Soro) e romani (gli Argenti), e prima ancora agli arabi (Al-Kindi) che vedremo tra poco.



Tours 1589: Giovanni Mocenigo ambasciatore veneziano in Francia, riceve una strana visita

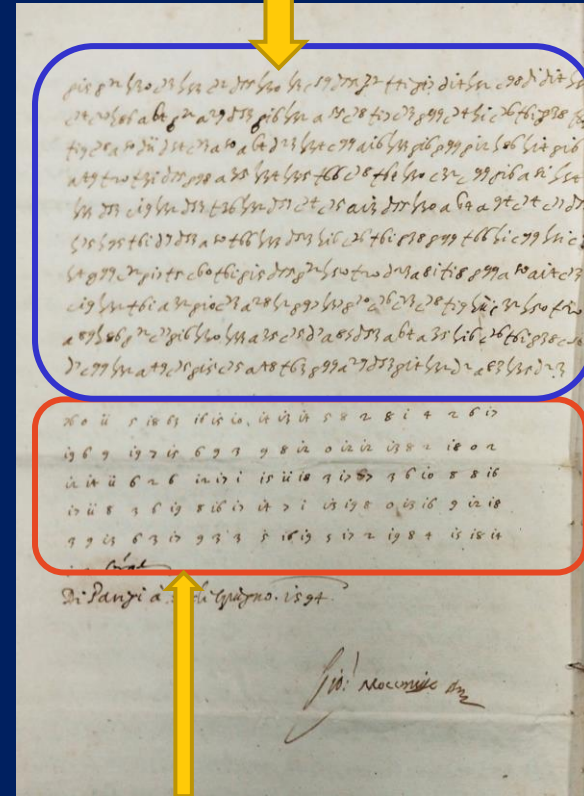
Giovanni alias *Zuane* Mocenigo era ambasciatore veneziano a Tours, nel 1589 quando Enrico di Borbone re di Navarra divenne **Enrico IV** re di Francia; solo nel 1594 poté entrare in Parigi dopo essersi convertito al cattolicesimo («*Parigi val bene una messa*»).

Nel 1589 Mocenigo ricevette la visita di «persona molto intendente di cifre» inviata a portare come omaggio di Enrico IV a Venezia un pacco di lettere di Filippo II re di Spagna da lui decrittate e piuttosto inquietanti per la Repubblica di Venezia.

Si trattava quasi certamente di **François Viète**.

Mocenigo scriveva i suoi dispacci in cifra, usandone una più facile, la *ziffra prima* per le cose ordinarie e una più sicura per le cose più segrete la *cifra delle caselle* di Hieronimo di Franceschi il principale *deputato alle cifre* veneziano di quegli anni.

Ziffra prima



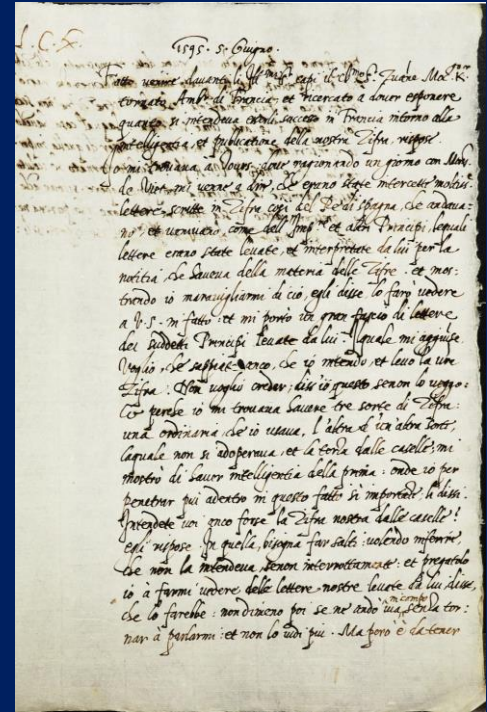
Cifra caselle

**ASVe Senato dispacci
amb. Francia filza 23**

Venezia, 5 giugno 1595 – Giovanni Mocenigo compare davanti al CX

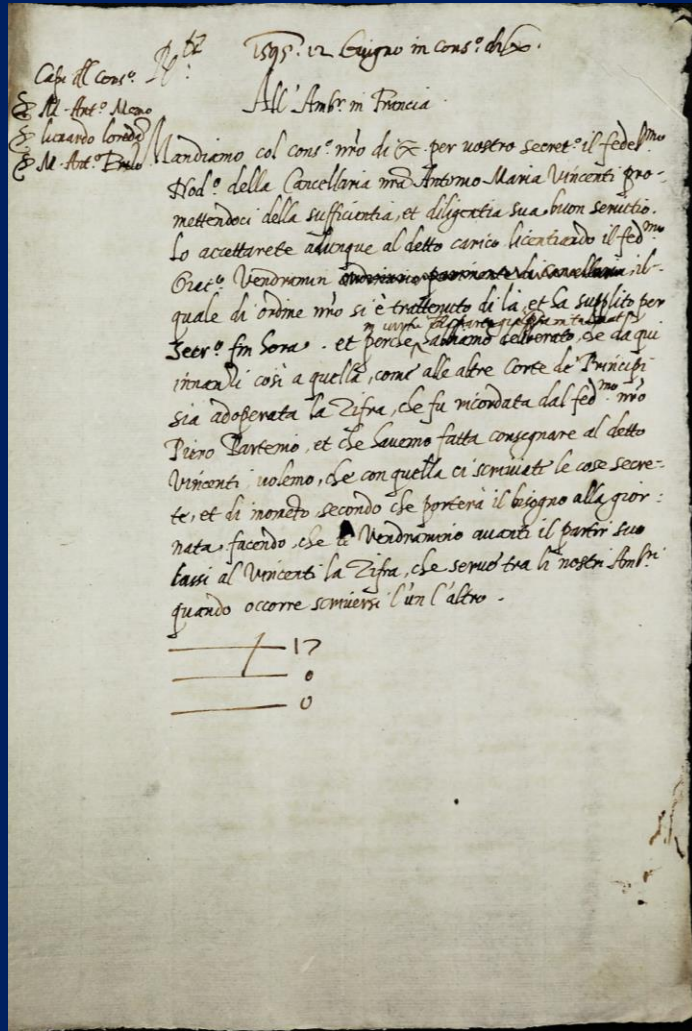


Io mi trouaua a Tours doue *ragionando un giorno con Mons. de Viet* mi uenne a dire che erano intercette moltissime lettere scritte in zifra così del Re di Spagna, che andauano et ueniuano, così come dell'Imperatore et altri Principi, le quali lettere erano state leuate et interpretate da lui per la notitia che haueua della materia delle zifre, et mostrando io marauigliarmi di ciò, *egli disse lo farò vedere a V.S. in fatto; et mi portò un gran fascio di lettere dei suddetti Principi leuate da lui.* Il quale mi aggiunse: *Voglio che sappiate anco che io intendo et leuo la u[ostra] zifra; non uoglio creder, diss'io, questo se non lo ueggo, ciò perché io mi trouaua hauere tre sorte di zifra : una ordinaria che io usaua, l'altra d'un'altra sorta la quale non si adoperaua, et la terza delle caselle; mi mostrò di hauer intelligenza della prima; onde io per penetrar più addentro in questo fatto sì importante, li dissi: intendete uoi anco forse la zifra nostra delle caselle? Egli rispose: **In quella bisogna far salti**; uolendo inferire che non la intendeua e non interrottamente, et pregatolo io à farmi uedere delle lettere nostre leuate da lui, disse che lo farebbe; nondimeno poi se ne andò ma senza tornare a parlarmi; et non lo uidi più.*



**ASVe CX parti segrete
filza 26 – 5 giu 1595**

Una settimana dopo il CX decreta ...



**ASVe CX parti secrete
filza 26 – 12 giu 1595**

Una settimana dopo, il 12 giugno 1595, il CX decretò all'unanimità, 17 su 17 compreso quindi il doge Marin Grimani che presiedeva, di inviare un nuovo segretario a Parigi, [...] *Et perché habbiamo deliberato che da qui innanzi così a quella come ad altre corti de' Principi sia adoperata la zifra che fu ricordata dal fedelissimo nostro Pietro Partenio [...] uolemo che con quella ci scriuiate le cose secrete et di momento [...]*

Questa delibera del CX riportata dal Baschet nel suo libro, è stata ripresa da molti autori che ne hanno tratto conseguenze un po' azzardate:

- Partenio sarebbe diventato il nuovo deputato alle cifre del CX.
- Le cifre del Partenio divennero quelle correnti per le ambasciate veneziane.

Come vedremo dalle carte originali emerge una storia un po' diversa.

Qualche domanda viene spontanea ...

1. Cosa era **la cifra delle caselle**?
 2. Chi era **Hieronimo di Franceschi**?
 3. Chi era **Pietro Partenio**?
 4. Cos'è un **nomenclatore**?
1. Un cifrario di massima sicurezza.
 2. Un segretario deputato alle cifre dal CX, inventore della cifra delle caselle.
 3. Un notaio veneziano geniale inventore di cifre.
 4. Un cifrario misto che cifra lettere, sillabe e parole(nomi)
- L'incontro con Viète di cui riferisce nel 1595 è quello del 1589?
 - Se è così perché Mocenigo aspettò sei anni, il ritorno a Venezia, per riferire al CX?
 - E perché accettò di usare la cifra delle caselle?
 - Oppure vi fu un secondo incontro con Viète?

Serie 2

L'ABC

Cos'è la crittografia?

Cos'è la crittanalisi?

Crittanalisi è ... Settimana Enigmistica!?

Parole in chiaro

Spazi visibili

20 numeri usati
sottintendono una
sostituzione
monoalfabetica
corrispondenza
1:1 tra numeri e
lettere.

57108. L'ANEDDOTO CIFRATO

1	2	3	4	5	6	—	7	4	8	3	4
9	7	6	4	3	—	5	7	—	10	7	11
1	11	3	—	12	4	—	13	7	14		
15	—	5	7	fantascienza,	12	4	—				
13	1	15	6	16	6	—	11	3	10		
7	16	8	1	—	17	18	7	3	16	3	
—	7	4	2	1	4	6	—	1	7	Lloyd's	
5	7	—	14	6	4	5	11	1	—	5	
7	—	1	16	16	7	17	12	11	1		
11	14	6	contro	14	3	—	19	3			
11	5	7	3	—	17	18	3	—	1		
2	11	3	20	20	3	—	16	12	20		
7	8	6	—	16	3	—	5	3	10	14	
7	—	1	14	7	3	4	7	fossero	16		
8	1	8	7	—	16	17	6	19	3	11	
8	7	—	19	11	7	15	1	—	5	3	
14	lancio	5	3	14	14	1	—	19			
3	14	14	7	17	6	14	1	.			

Sostituite una lettera ad ogni numero.

36 N. 4457 LA SETTIMANA ENIGMISTICA

57104. REBUS (3 1 8) (Braco)

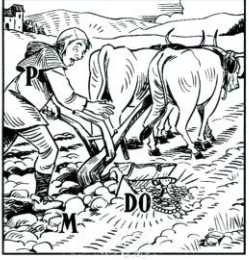


57105. REBUS A ROVESCIO (6 5 2 4) (Gianna)

Es.: OB ragno; ceri GA = Agire con garbo



57106. REBUS (9 6) (M. Barile)



57107. FRASI IN... COCCI

1	...
2	...
3	...
4	...
5	...
6	...
7	...
8	...
9	...

57108. L'ANEDDOTO CIFRATO

1	2	3	4	5	6	—	7	4	8	3	4
9	7	6	4	3	—	5	7	—	10	7	11
1	11	3	—	12	4	—	13	7	14		
15	—	5	7	fantascienza,	12	4	—				
13	1	15	6	16	6	—	11	3	10		
7	16	8	1	—	17	18	7	3	16	3	
—	7	4	2	1	4	6	—	1	7	Lloyd's	
5	7	—	14	6	4	5	11	1	—	5	
7	—	1	16	16	7	17	12	11	1		
11	14	6	contro	14	3	—	19	3			
11	5	7	3	—	17	18	3	—	1		
2	11	3	20	20	3	—	16	12	20		
7	8	6	—	16	3	—	5	3	10	14	
7	—	1	14	7	3	4	7	fossero	16		
8	1	8	7	—	16	17	6	19	3	11	
8	7	—	19	11	7	15	1	—	5	3	
14	lancio	5	3	14	14	1	—	19			
3	14	14	7	17	6	14	1	.			

Sostituite una lettera ad ogni numero.

57109. PAROLE CONVERGENTI

1	2	3	4	5	6	7	8	9
1								
2								
3								
4								
5								
6								
7								
8								
9								

In ogni riga la prima parola definita va scritta da sinistra a destra e la seconda, invece, da destra a sinistra. In ogni colonna, la prima va scritta dall'alto in basso e la seconda dal basso in alto.

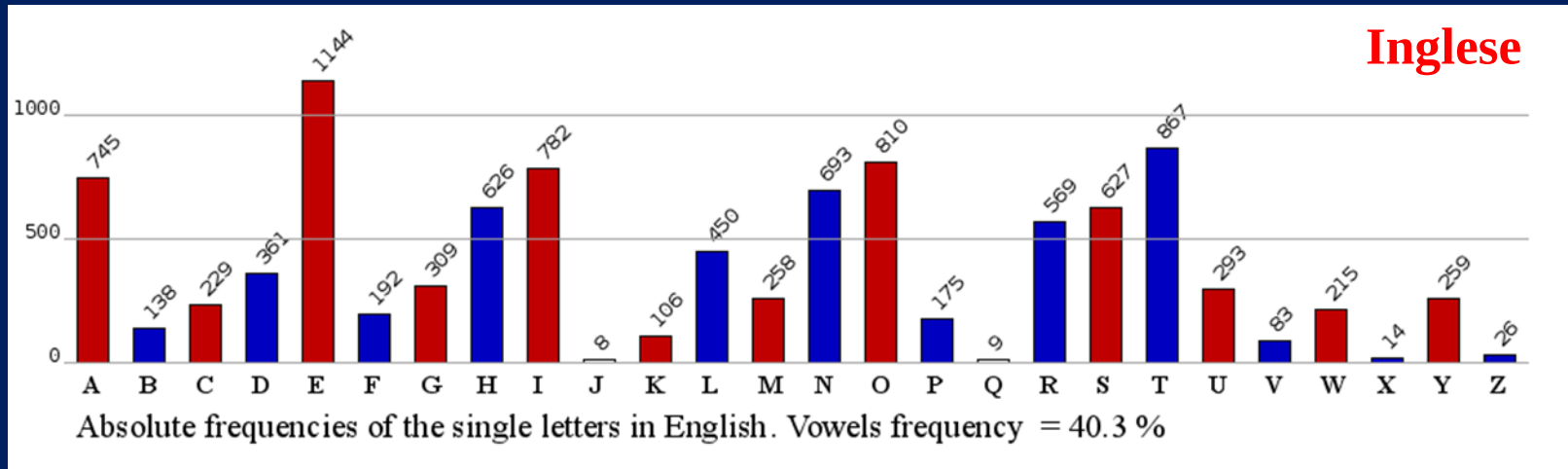
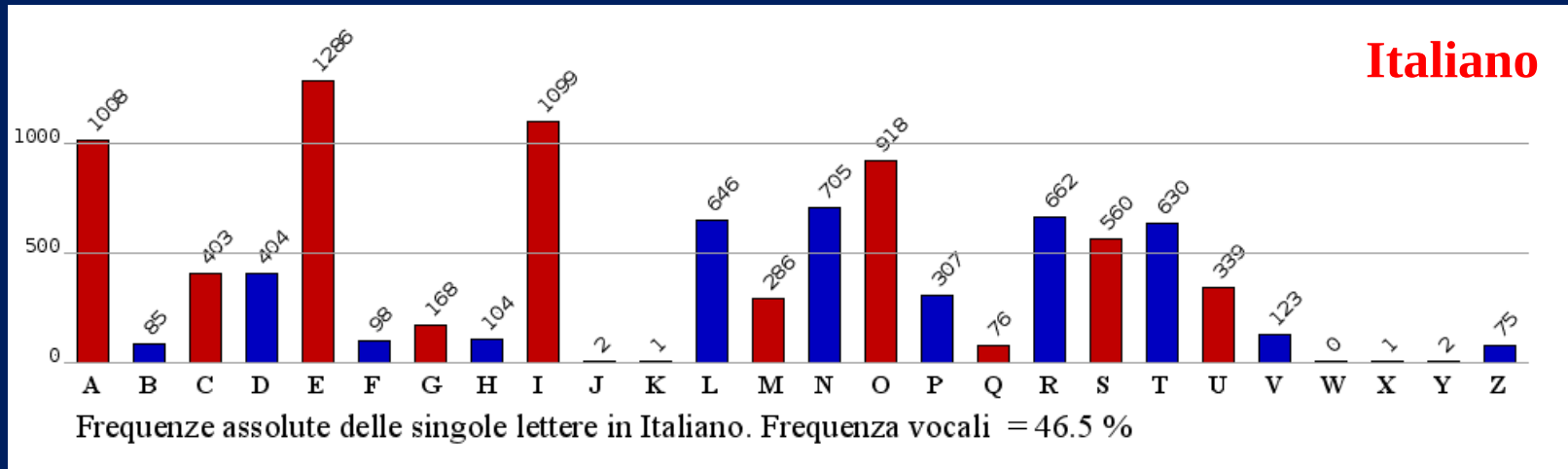
ORIZZONTALE: 1. Tutt'altro che al dente — L'involto... che si suona - 2. Dolce di mandorle — Divertente in compagnia - 3. Il re longobardo d'un famoso editto — Ironia graffiante - 4. Vertici da raggiungere — Un antico popolo greco - 5. Una città sul Lario — Il callo che si forma dopo la frattura - 6. Fa alzare il tono della voce — Ciarla, pettegolezzo - 7. Il Lago di Garda — Tetro, scuro - 8. Ben protette da caldo e freddo — La ispirano gli infelici - 9. Una cornice dei mobili — Cetaceo vorace e intelligente.

VERTICALE: 1. Poetiche frecce — Arrivano allo stomaco attraverso l'esofago - 2. Una delle Mini — Il dipartimento con Grenoble - 3. Se la si tocca, punge — Lo sono gli Olivetani - 4. Il segno da seguire — Nel calcio c'è quella tornante - 5. Il Th del chimico — Quel che si può sapere di cose - 6. Una gemma color unghia — Le sillabe prive di accento - 7. Fu fatto uccidere dal fratello Caracalla — La ciliegia... nel Meridione - 8. Gli sposi all'altare promettono di farlo — Funzioni tradizionali - 9. Grandezza pomposa — Niente affatto lucido.

5 7 è molto frequente, quasi certamente è

Analisi delle frequenze, italiano vs inglese

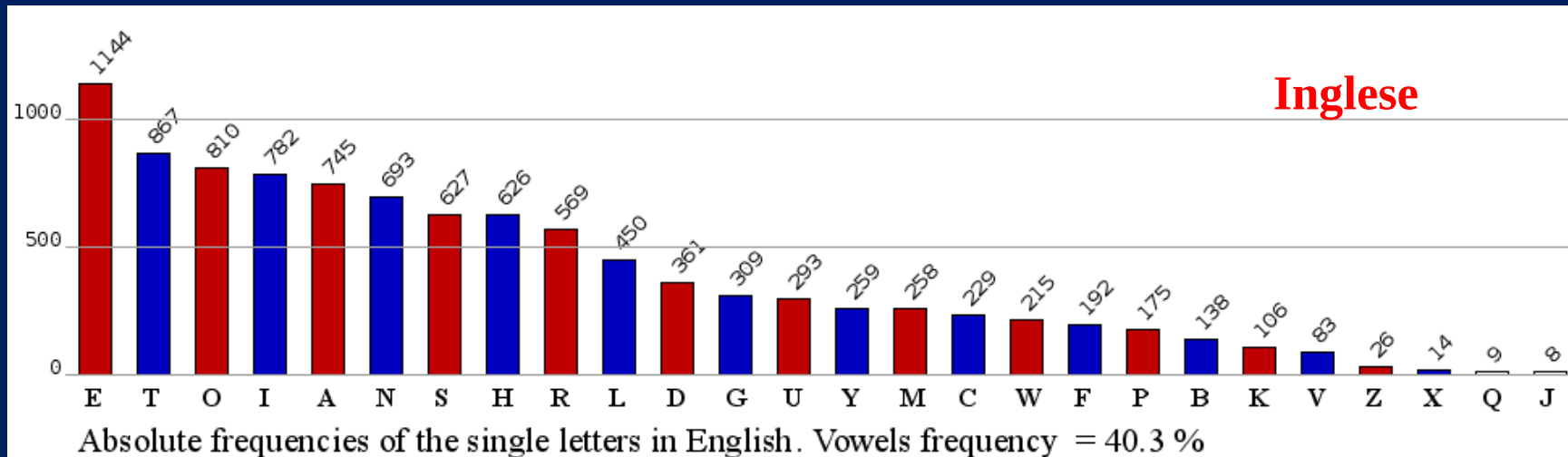
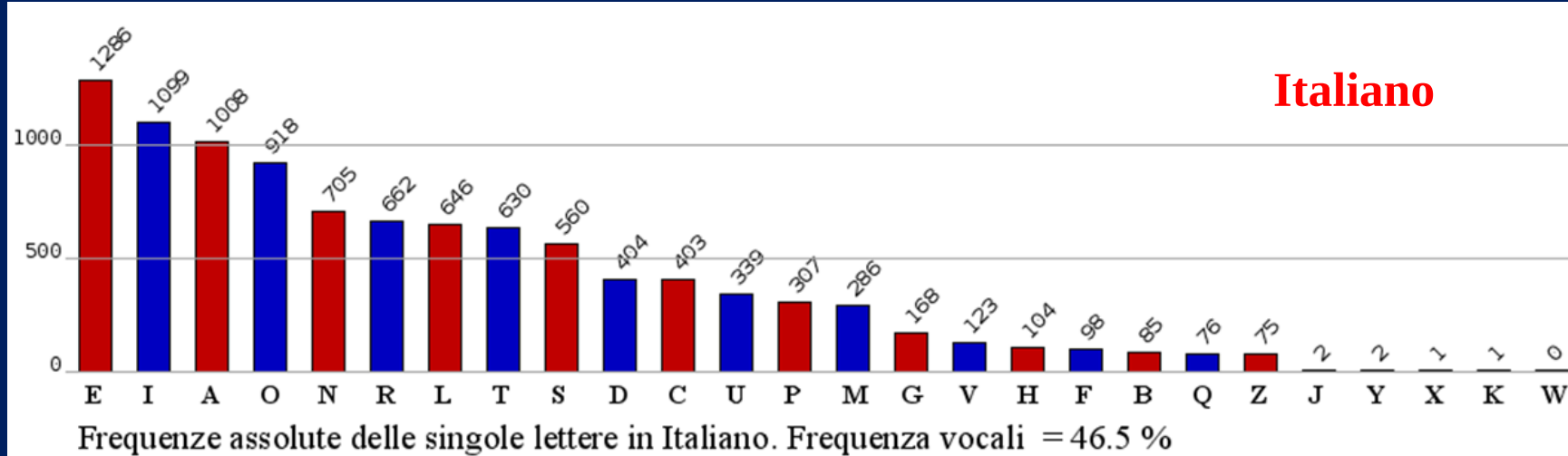
http://www.crittologia.eu/critto/php/frequenze_lingua.phtml



Al –Kindi(801-873)

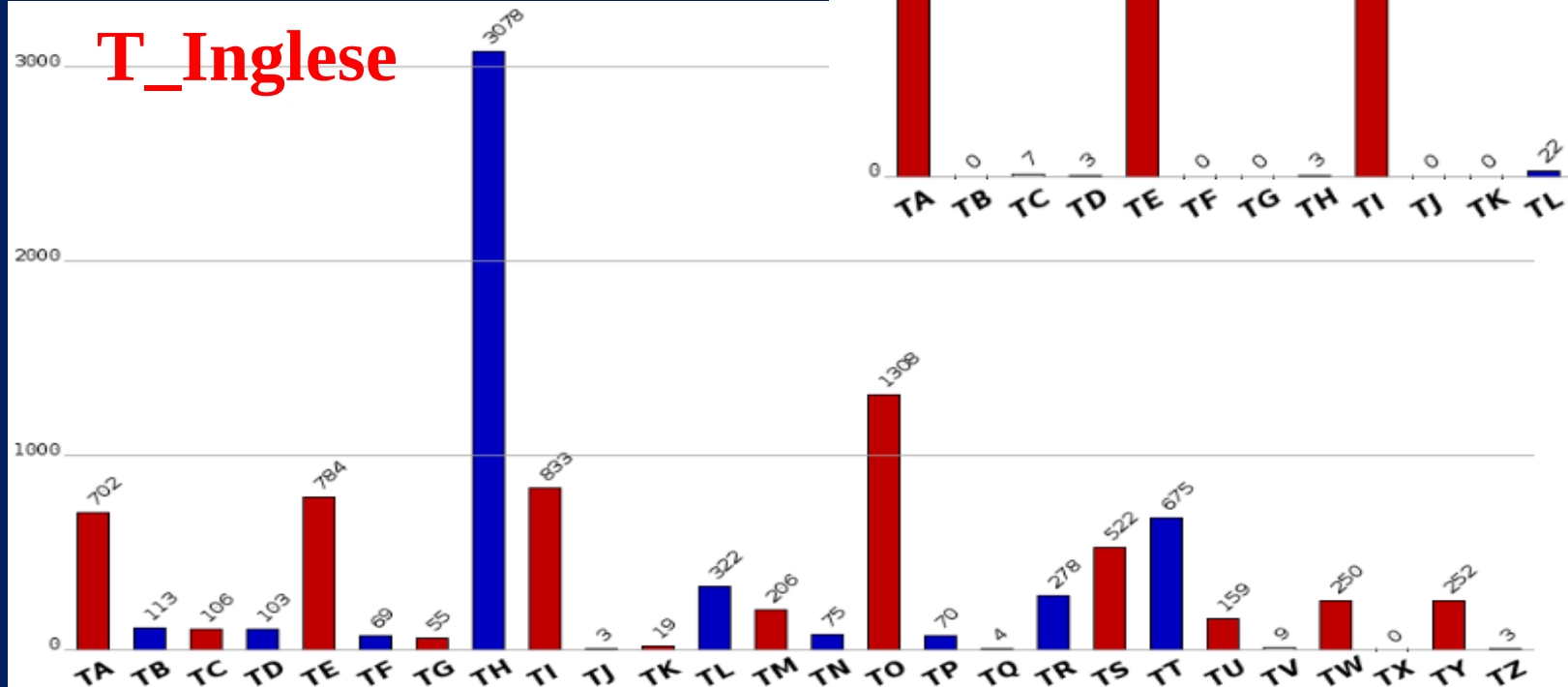
Analisi delle frequenze, italiano vs inglese

[Pagina Web](#)

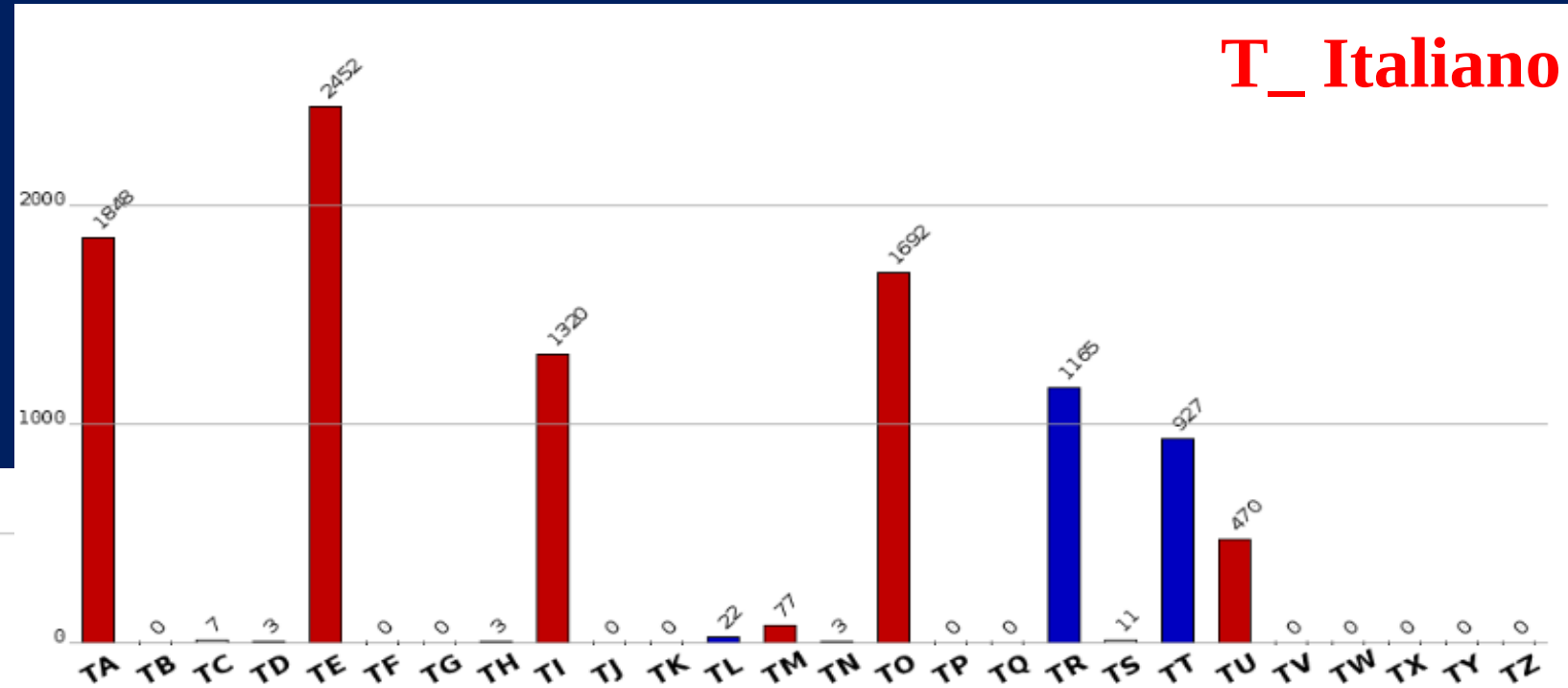


Analisi delle frequenze dei digrammi T_

T_Inglese

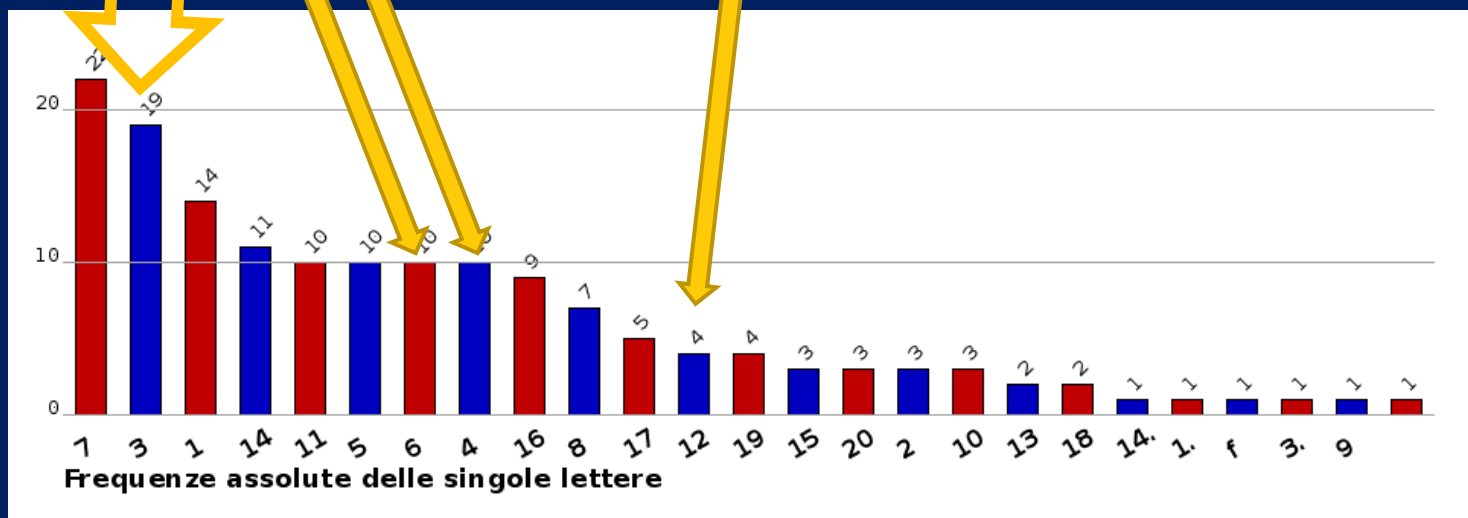
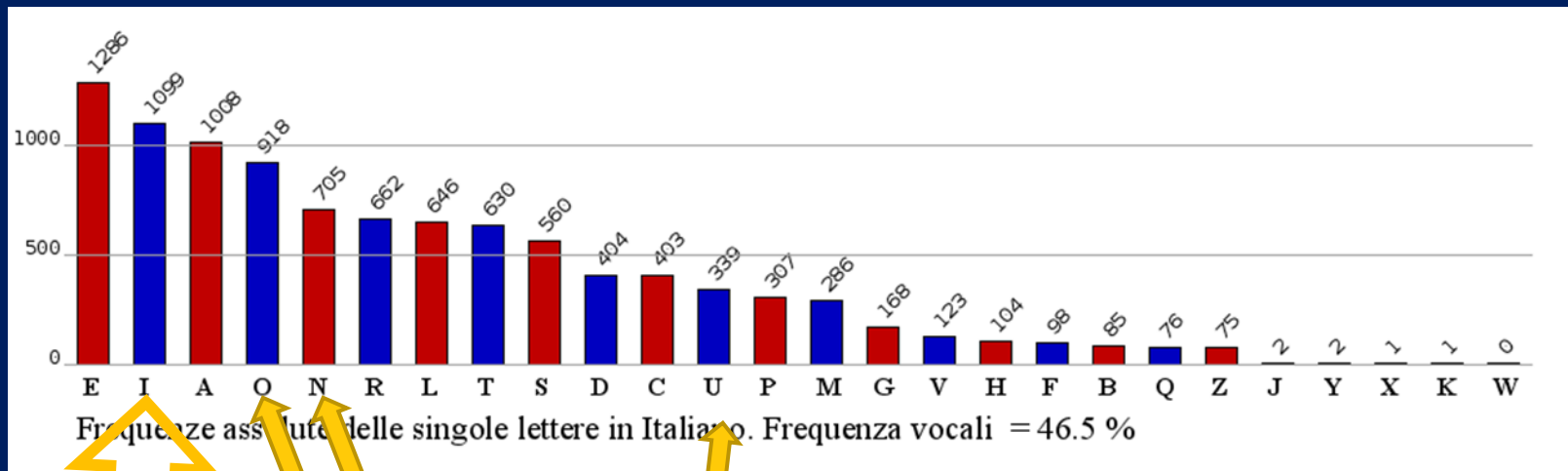


T_Italiano



Un confronto ...

7, 3, 1 E I A
 5 = D (L) 7 = I (A)
 6 = O
 12 = U 4 = N



57108. **L'ANEDDOTO CIFRATO**

1	2	3	4	5	6	—	7	4	8	3	4
9	7	6	4	3	—	5	7	—	10	7	11
1	11	3	—	12	4	—	13	7	14		
15	—	5	7	fantascienza,	12	4	—				
13	1	15	6	16	6	—	11	3	10		
7	16	8	1	—	17	18	7	3	16	3	
—	7	4	2	1	4	6	—	1	7	Lloyd's	
5	7	—	14	6	4	5	11	1	—	5	
7	—	1	16	16	7	17	12	11	1		
11	14	6	contro	14	3	—	19	3			
11	5	7	8	3	—	17	18	3	—	1	
2	11	3	20	20	3	—	16	12	20		
7	8	6	—	16	3	—	5	3	10	14	
7	—	1	14	7	3	4	7	fossero	16		
8	1	8	7	—	16	17	6	19	3	11	
8	7	—	19	11	7	15	1	—	5	3	
14	lancio	5	3	14	14	1	—	19			
3	14	14	7	17	6	14	1	.			

Sostituire una lettera ad ogni numero.

Un confronto ...

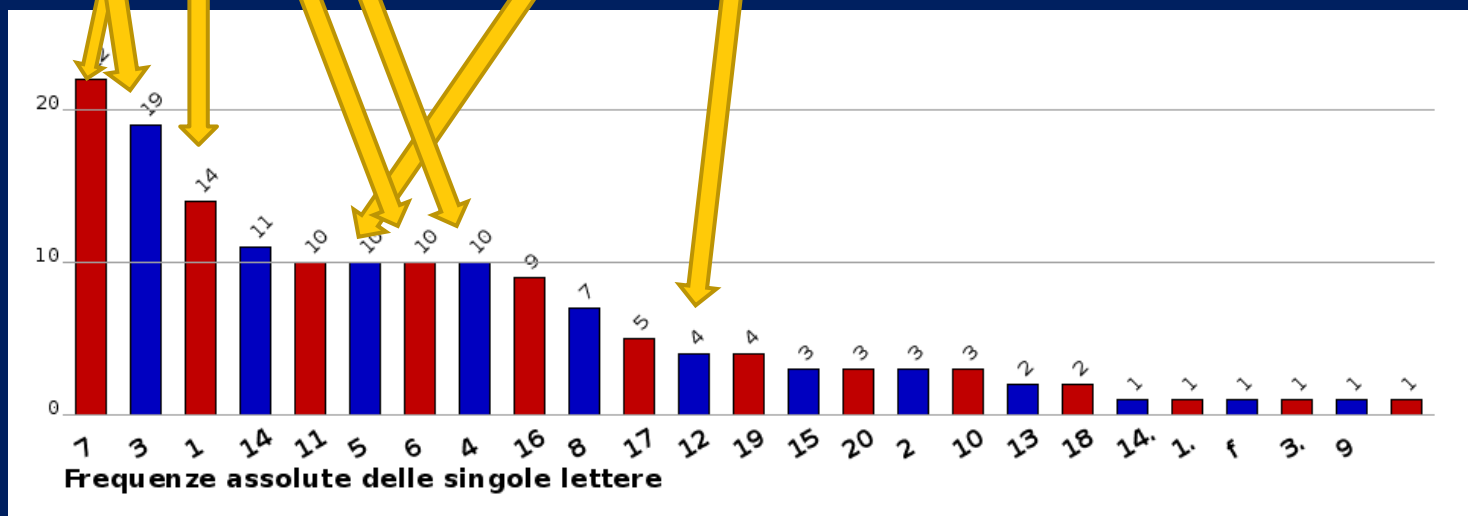
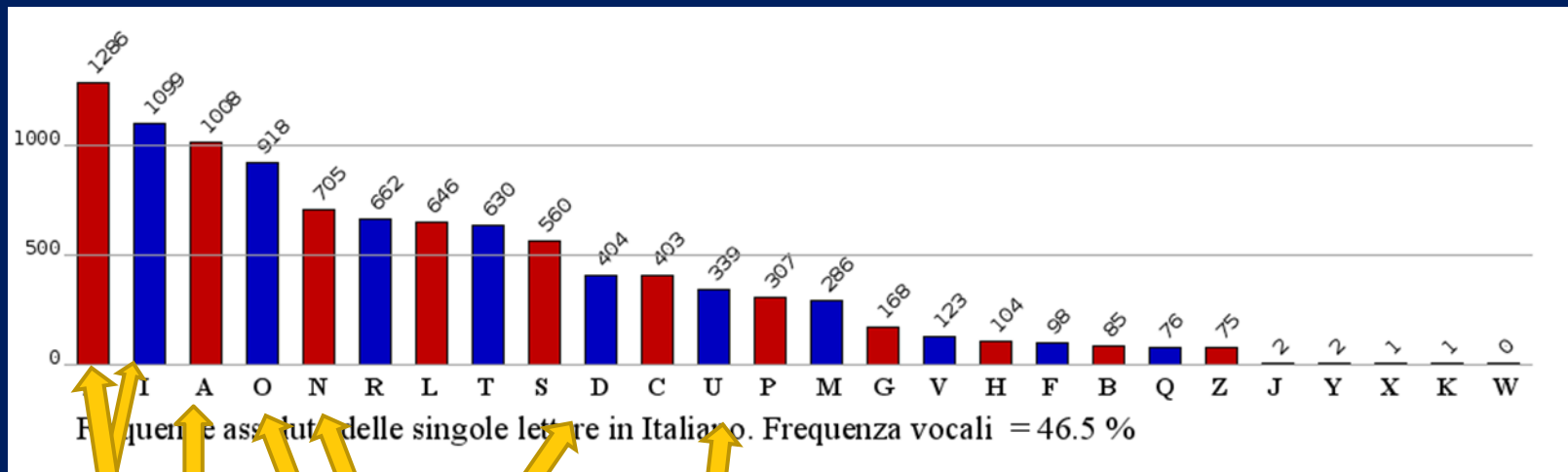
5 7 DI
5 7 LA

5 = D 7 = I
3 = E 1 = A
12 = U 4 = N



Ricuperare la **chiave**

Ricuperare il testo chiaro



57108. L'ANEDDOTO CIFRATO

1 2 3 4 5 6 — 7 4 8 3 4
 9 7 6 4 5 — 5 7 — 10 7 11
 1 11 5 — 12 4 — 13 7 14
 15 — 5 1 fantascienza, 12 4 —
 13 1 15 6 16 6 — 11 3 10
 7 16 8 1 — 17 18 7 3 16 3
 — 7 4 2 1 4 6 — 1 7 Lloyd's
 5 7 — 14 6 4 5 11 1 — 5
 7 — 1 16 16 7 17 12 11 1
 11 14 6 contro 14 3 — 19 3
 11 5 7 8 3 — 17 18 3 — 1
 2 11 3 20 20 3 — 16 12 20
 7 8 6 — 16 3 — 5 3 10 14
 7 — 1 14 7 3 4 7 fossero 16
 8 1 8 7 — 16 17 6 19 3 11
 8 7 — 19 11 7 15 1 — 5 3
 14 lancio 5 3 14 14 1 — 19
 3 14 14 7 17 6 14 1 .

Sostituire una lettera ad ogni numero.

Crittografia: due operazioni (funzioni ?)

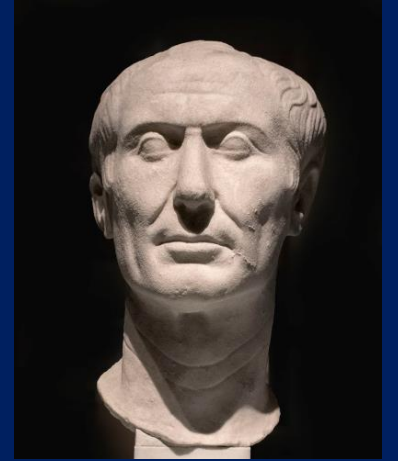


Crittanalisi: altre due funzioni



Cifrare per ... sostituzione (o trasposizione)

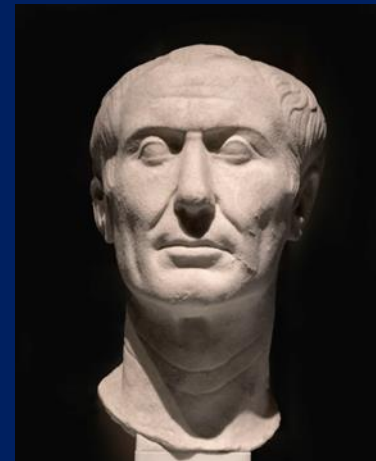
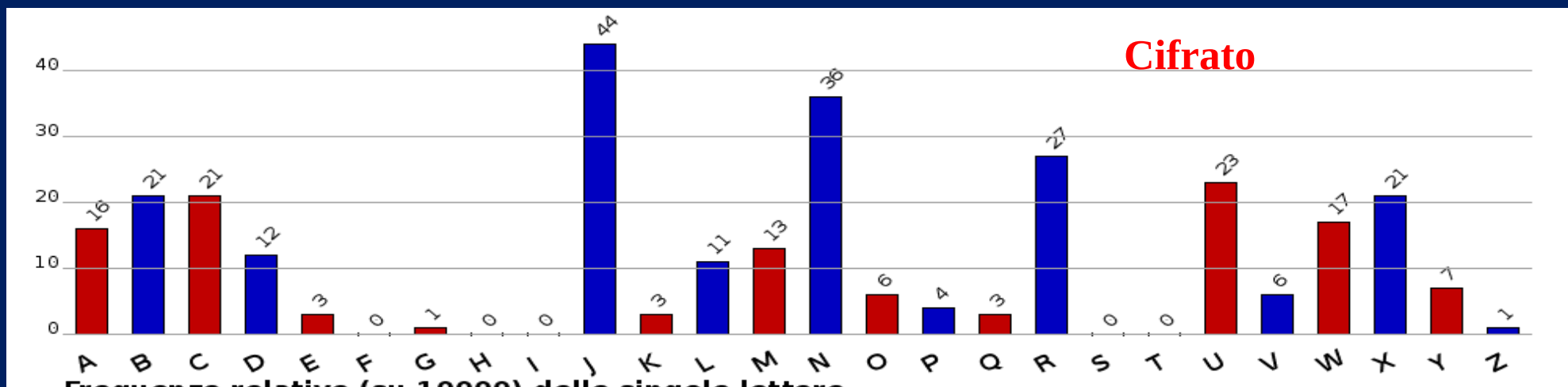
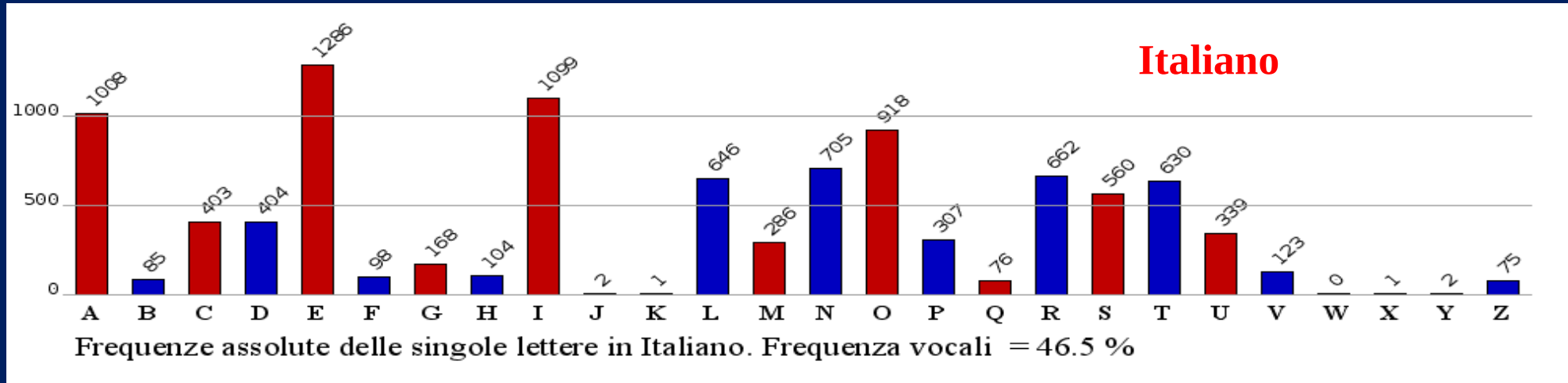
- Una *cifra* è una **relazione** tra un insieme di lettere in chiaro, e un insieme di lettere, simboli o numeri che sostituiscono le lettere chiare in modo da occultare il significato del testo; questo è il metodo più comune, detto **sostituzione**: ogni lettera o gruppo di lettere del testo chiaro viene sostituita da un segno cifrante.
- Un altro metodo che qui non trattiamo è quello della **trasposizione** le lettere del testo chiaro vengono rimescolate secondo una qualche regola convenuta. Equivale ad un anagramma.
- Per esempio ecco una lista cifrante di **sostituzione** molto semplice (alfabeto latino classico):
- Chiaro ABCDEFGHIKLMNOPQRSTVX
Cifrato **DEFGHIKLMNOPQRSTVXABC**
- E' la **cifra di Cesare**, descritta da Svetonio, spostamento di tre passi lungo l'alfabeto, la più semplice di tutte le sostituzioni; oggi viene detta più in generale cifra di Cesare una cifra con spostamento N qualsiasi, usando l'alfabeto di oggi, di 26 lettere, quindi ci sono 25 cifre di Cesare possibili. Perché non 26?



IVLIVSCAESAR
MBOMBXFDHXDV

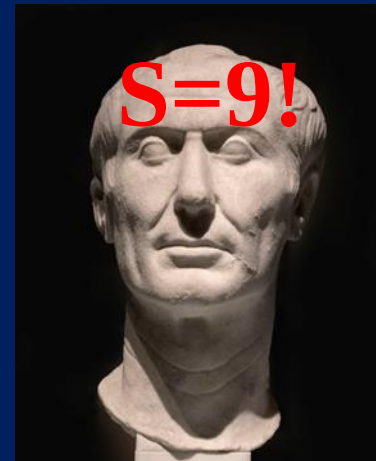
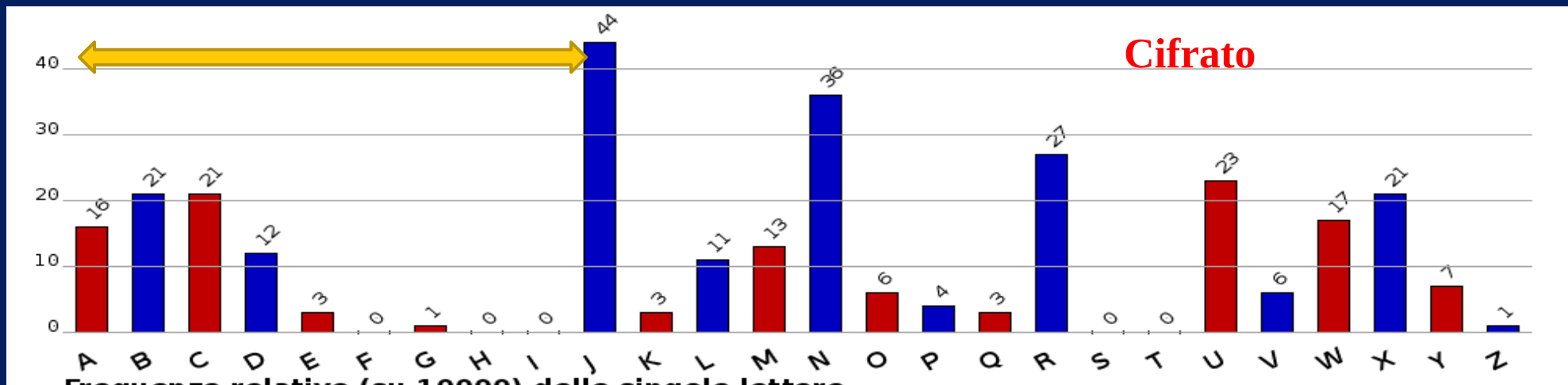
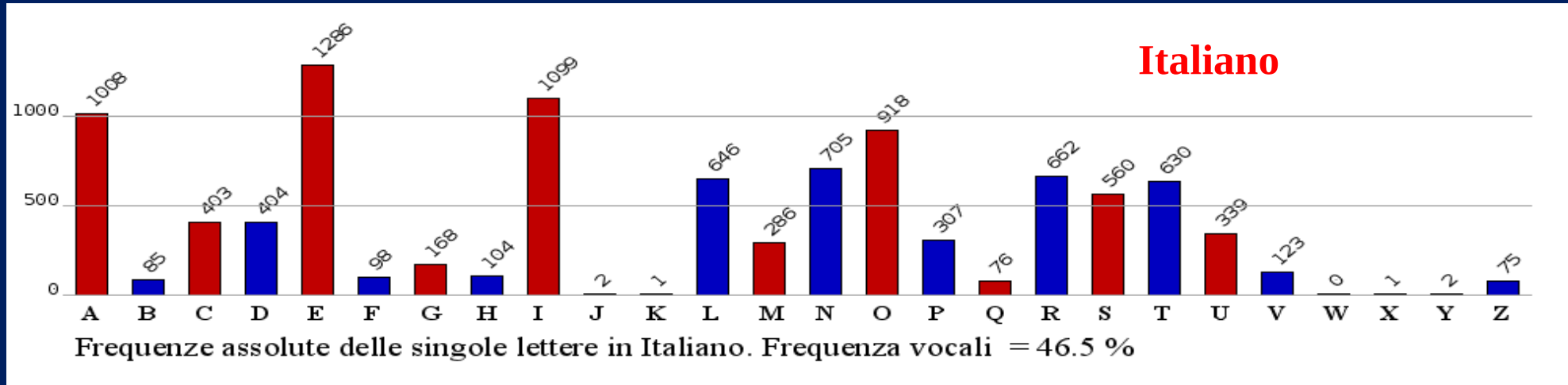
Cesare svelato dalle frequenze

http://www.crittologia.eu/critto/php/frequenze_lingua.phtml



Cesare svelato dalle frequenze

http://www.crittologia.eu/critto/php/frequenze_lingua.phtml



Sostituzione monoalfabetica (MASC)

- ▶ La cifra di Cesare non è affatto sicura; bastano $N-1$ tentativi (N numero di lettere dell'alfabeto) per trovare la soluzione.
- ▶ Molto più sicuro sarebbe usare un alfabeto cifrante disordinato, per esempio (alfabeto odierno di 26 cifre)

Chiave	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cifra	HXAIULJMGWQREKFCSTVBNYZOPD

} Chiave
lista cifrante

GIULIOCESARE
JGNRGFAUVHTU

- ▶ Quanti sono gli alfabeti cifranti possibili?
- ▶ Prima lettera, una su 26, seconda una su 25 ...
- ▶ $26 \times 25 \times 24 \dots 1 = 26! = 403.291.461.126.605.635.584.000.000$
- ▶ Numero astronomico, quindi impossibile da decifrare? **Spazio delle chiavi**
- ▶ Non proprio, come abbiamo visto basta un po' di statistica

Nasce la crittografia ma come confondere la statistica?

- ▶ La crittografia moderna nasce tra il XIV e XV secolo quando le varie città stato italiane, ebbero l'idea di scambiarsi ambasciatori residenti che mantenessero aperto un dialogo con il principe locale e riferissero ai loro principi.
- ▶ *[non esistevano mezzi di comunicazione più veloci del corriere a cavallo! Niente telegrafo, niente radio ...]*
- ▶ Ma come potevano gli ambasciatori comunicare in modo riservato con i loro principi?
- ▶ Con la crittografia!
- ▶ Nel 1476 Cicco Simonetta, reggente del ducato di Milano , essendo Gian Galeazzo Sforza infante, scrisse una serie di regole di decrittografia, primo esempio di testo di crittoanalisi, anche se a un livello molto basso persino per quei tempi, niente analisi delle frequenze ... a mala pena sufficienti per i monoalfabetici della settimana enigmistica.
- ▶ In realtà erano già in uso da diversi decenni vari espedienti per aumentare la sicurezza, che vuol dire soprattutto confondere l'analisi delle frequenze. Il monoalfabetico non bastava già più.

Confondere la statistica

Per rendere più sicura una funzione Cifra per sostituzione, sin dal XV secolo si sono inventati diversi modi, in breve la cifra non deve essere 1:1(biiettiva)

- 1. Alcuni segni non vengono cifrati:** tipicamente spazi, segni di interpunzione non vengono cifrati, anche alcune lettere rare e mute come la H possono essere trascurate. *Matematicamente:* la relazione **cifra** non è più **ovunque definita**
- 2. Omofoni:** alcune lettere, anche tutte ma per lo meno le più frequenti, hanno diverse cifre, da variare di volta in volta, *a caso, a discrezione del cifratore*; così si confonde la statistica. *Matematicamente:* la relazione non è più **univoca**, non è una funzione in senso stretto.
- 3. Nulle:** segni che non significano nulla, vanno inseriti a casaccio a inizio, fine o in mezzo al testo, sempre per confondere le statistiche. *Matematicamente:* la relazione non è più **suriettiva**, alcuni segni cifranti non hanno contro-immagine.
- 4. Polifoni:** più lettere diverse si cifrano con lo stesso numero; strumento da usare con cautela perché la decifra (funzione inversa) non è più univoca, e va fatta in base al contesto. *Matematicamente:* la relazione non è più **iniettiva**, alcuni segni cifranti hanno più di una contro-immagine.

Cifrare per gruppi di lettere

Un altro modo di rendere più sicuro un cifrario per sostituzione è quello di cifrare per gruppi di lettere invece che lettera per lettera:

lessicale

1. Cifrari **digrafici**. Alcuni o tutti i gruppi di due lettere sono cifrati con un solo segno;
2. **Sillabario**: si cifra per sillabe gruppi di lettere formati da una o più consonanti e terminanti con una vocale; p.es. **ba be bi bo bu ca ce ci co cu ...**

semantico

3. **Dizionario**: si cifra per parole, o gruppi di parole (p.es. Re di Francia), o radici (p.es. esse, haue, ment).
4. **Frasario**: si cifrano intere frasi comuni. (*Radio Londra durante la II guerra mondiale*)

I nomenclatori *Non di sole lettere sono fatti i cifrari*

Il nomenclatore è un cifrario che contiene un po' di tutto, i nomenclatori del Rinascimento consistevano di ...

1. **Alfabeto**, di solito con omofoni (*quasi sempre*).
2. **Nulle**, più o meno numerose (*spesso*).
3. **Sillabario**, 20 – 30 gruppi, quindi 100 - 150 sillabe. Nelle cifre più grandi.
4. **Dizionario**: si cifra per parole, o gruppi di parole (p.es. Re di Francia), o radici (p.es. esse, haue, ment). Quasi sempre, da 50 a qualche centinaio di termini.
5. **Frasario**: solo nelle cifre più antiche.

Se ben progettato e usato correttamente un nomenclatore è molto difficile, se non impossibile da decrittare.

E finalmente ... una cifra veneziana

Ziffra piccola A16-36

E' un nomenclatore molto semplice, a due cifre, solo 99 segni, piccolo appunto.

Alfabeto con due omofoni per lettera tranne la H.

Dizionarietto di 60 parole.

Perché la differenza di 20?
Perché non anche 0?

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

Dizionario											
accio	41	alanson	66	altr	44	anno	47	bassa	63		
che	69	Clarissim	58	come	70	con	50	consiglio di X	51		
Costantinopoli	90	dal	56	del	52	deside	59	dett	53		
donde	55	duca di Sauogia	88	espedi	57	esse	54	far	46		
forment	48	galee	43	giorn	42	gran	92	habbia	61		
haue	62	illustr	84	Imperatore	87	Maestà	80	mente	72		
molt	78	necess	45	noi	98	non	89	nostr	99		
ordin	82	passat	65	per	79	present	77	princip	49		
qua	93	quant	97	que	94	Re cristianissimo	74	Re di Nauara	76		
Re di Spagna	73	Regina d Inghilterra	71	rispo	75	Santità	40	sempre	85		
Serenissimo	81	Serenità	83	Signor	60	sua	86	tant	95		
Turch	68	tutt	64	uoi	96	uostr	91	Vostra Serenità	67		

Ziffra prima

Un esempio di nomenclatore più ampio con segni del tipo

lettera-numero di una o due cifre;
usando tutte le 20 lettere e 99 numeri, si hanno 1980 segni cifranti possibili, in genere ne venivano usati meno della metà.

Si tratta della *ziffra prima* del libro delle cifre realizzato da Hieronimo di Franceschi in esecuzione della delibera del CX del 30 agosto 1577. Alcune cifre furono realizzate dal segretario Milledonne collaboratore del Franceschi.

Usata come cifra corrente da molte ambasciate veneziane tra il 1580 e il 1595 e anche da Giovanni Mocenigo.

Nulle ↓

Nulle											
a ⁹¹	g ⁶⁰	g ⁵⁴	g ⁵²	f ⁶⁵	f ⁵⁶	f ⁵¹	d ⁵⁹	d ⁴⁷	d ⁴⁰	c ⁹⁵	h ⁸³

Omofoni →

Alfabeto																
a	b	c	d	e	g	i	l	m	n	o	p	r	s	t	u	z
d^{53}	d^{54}	a^{94}	c^{98}	f^{61}	d^{63}	d^{58}	d^{62}	a^{38}	d^{55}	d^{57}	d^{85}	c^{99}	a^{96}	f^{54}	d^{51}	f^{55}
d^{96}	d^{60}	d^{56}	f^{68}	g^{55}	d^{90}	d^{61}	f^{64}	g^{65}	f^{69}	d^{95}	f^{70}	f^{71}	f^{85}	g^{58}	d^{64}	g^{74}
f^{67}	f^{74}	f^{80}	g^{89}	h^{91}	f^{62}	f^{63}	g^{63}	h^{85}	g^{67}	f^{84}	g^{53}	g^{69}	g^{64}	h^{90}	f^{66}	h^{89}
g^{56}						g^{62}				g^{71}					g^{66}	
h^{87}						h^{99}				h^{86}					g^{68}	
															h^{88}	

Sillabario →

Dizionario (estratto) ↓

Sillabario																			
ba	be	bi	bo	bu	ca	ce	ci	co	cu	cra	cre	cri	cro	cru	da	de	di	do	du
a ¹⁶	a ¹⁵	a ¹⁴	a ¹³	a ¹²	a ⁵²	a ⁵¹	a ⁵⁰	a ⁴⁹	a ⁴⁸	a ⁵⁷	a ⁵⁶	a ⁵⁵	a ⁵⁴	a ⁵³	g ⁷⁰	g ⁷²	g ⁹⁹	g ⁹⁸	g ⁹⁷
fra	fre	fri	fro	fru	ga	ge	gi	go	gu	gna	gne	gni	gno	gnu	gra	gre	gri	gro	gru
a ⁷⁸	a ⁷⁷	a ⁷⁶	a ⁷⁵	a ⁷⁴	c ²⁹	c ²⁸	c ²⁷	c ²⁶	c ²⁵	c ²⁴	c ²³	c ²²	c ²¹	c ²⁰	c ¹⁹	c ¹⁸	c ¹⁷	c ¹⁶	c ¹⁵
ia	ie	ii	io	iu	la	le	li	lo	lu	lla	lle	lli	llo	llu	ma	me	mi	mo	mu
c ⁴²	c ⁴³	c ⁴⁴	c ⁴⁵	c ⁴⁶	c ⁷⁵	c ⁷⁴	c ⁷³	c ⁷²	c ⁷¹	c ⁷⁰	c ⁶⁹	c ⁶⁸	c ⁶⁷	c ⁶⁶	c ⁷⁶	c ⁷⁷	c ⁷⁸	c ⁷⁹	c ⁸⁰
pa	pe	pi	po	pu	pra	pre	pri	pro	pru	qua	que	qui	quo	quu	ra	re	ri	ro	ru
d ⁷	d ⁸	d ⁹	d ¹⁰	d ¹¹	d ¹²	d ¹³	d ¹⁴	d ¹⁵	d ¹⁶	g ¹	g ²	g ³	g ⁴	g ⁵	g ¹⁴	g ¹⁵	g ¹⁶	g ¹⁷	g ¹⁸
sca	sce	sci	sco	scu	spa	spe	spi	spo	spu	ssa	sse	ssi	sso	ssu	sta	ste	sti	sto	stu
h ⁶	f ³¹	f ³²	f ³³	f ³⁴	f ³⁵	f ³⁶	f ³⁷	g ³⁶	g ³⁷	f ⁴⁰	f ⁴¹	f ⁴²	g ⁴¹	g ⁴²	g ³⁸	g ³⁹	g ⁴⁰	h ⁷	h ⁸
ta	te	ti	to	tu	tra	tre	tri	tro	tru	tta	tte	tti	tto	ttu	ua	ue	ui	uo	uu
h ³⁰	h ³¹	h ³²	h ³³	h ³⁴	h ⁴⁰	a ⁸⁴	a ⁸⁵	a ⁸⁶	a ⁸⁷	h ³⁵	h ³⁶	h ³⁷	h ³⁸	h ³⁹	h ⁵⁰	h ⁵¹	h ⁵²	h ⁵³	h ⁵⁴

Dizionario					
al	f ⁵	alcun	f ⁶	altr	f ⁹
armata	f ¹⁴	Candia	a ¹⁵	capit	a ²¹
come	a ³²	communica	a ³⁴	con	a ³⁵
Costantinopoli	a ³⁹	Cypro	a ³⁰	dal	g ⁷³
ditt	h ⁹²	duca	h ⁹⁶	espedi	a ⁵⁸
et	a ⁶⁴	far	a ⁶⁵	Francia	a ⁷¹
gli	c ¹⁰	grand	c ¹¹	habbia	c ³⁰
hora	c ³⁶	il	c ⁴⁷	illustrissim	c ⁵¹
la qual	c ⁶⁰	lettere	h ¹⁷	luogo	c ²⁶
molt	c ⁹¹	mons.r	c ⁹²	necess	f ²⁵
				non	f ²⁷
				ogno	d ¹

Confondiamo un po' la statistica

La tavola di Tritemio e Vigenère

Un altro modo di confondere l'analisi delle frequenze è dato dalla tavola di Vigenère, derivata da quella dell'abate Tritemio; ad ogni passo si cambia alfabeto cifrante: *cifra polialfabetica*.

La tavola in sostanza ha una cifra di Cesare per ogni riga. Vigenère usa **una parola chiave** ripetuta fino al necessario.

x Chiaro	ARRIVANOIRINFORZIDOMANI
y Chiave	VIGENERE VIGENEREVIGENER
z Cifrato	VDBOLEGSGDQRSSMDGNVQNRD

Matematicamente equivale ($A=0$; $B = 1 \dots$) a una somma modulo N

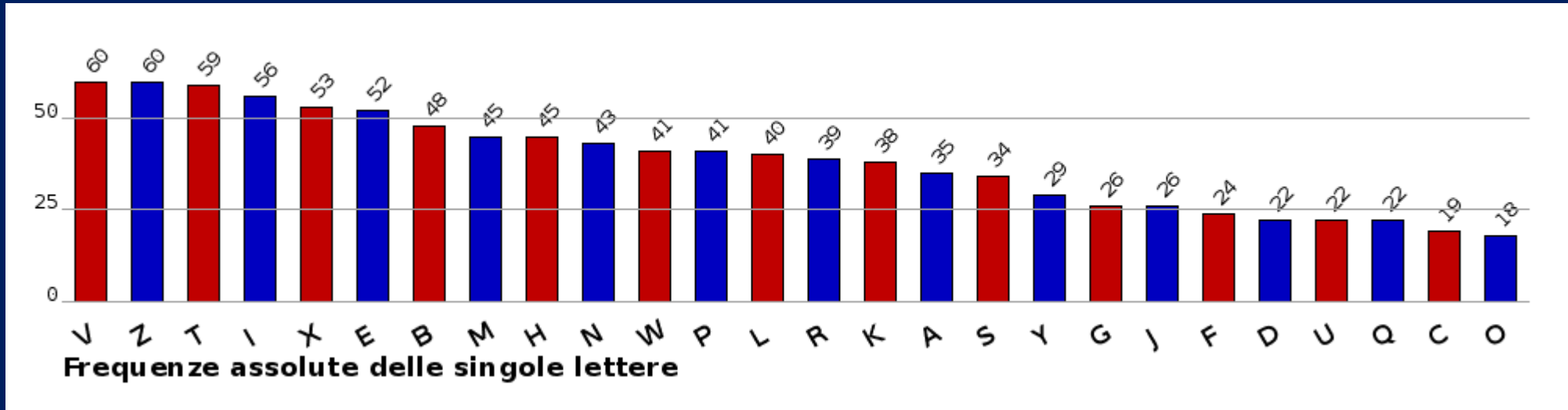
$$V = V + A; D = R + I \quad z = x + y \pmod{20}$$

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

La tavola di Vigenère

Confondiamo un po' la statistica

Analisi delle frequenze di un Vigenère



Ecco l'analisi delle frequenze di un cifrato con Vigenère; come si vede la distribuzione è stata spianata almeno in parte, e non ci sono più grosse differenze; insomma non ci dice più nulla di significativo. (*La cifra di Vigenère fu per questo ritenuta indecifrabile ... a torto*). Però a qualcosa serve: se ci troviamo di fronte a un diagramma del genere possiamo subito concludere che non si tratta di una cifra monoalfabetica.

Perché non furono quasi mai usate?

David Kahn fece notare che la crittografia rinascimentale era in certo modo schizofrenica; da una parte illustri autori pubblicavano ingegnose cifre polialfabetiche come indecifrabili. Dall'altra diplomatici e militari continuarono ad usare i nomenclatori.

Le cifre polialfabetiche, Tritemio, Bellaso, Vigenère non furono quasi mai usate perché troppo complicate per messaggi lunghi e soprattutto troppo esposte ad errori dei segretari; un errore può compromettere tutto il resto del messaggio.

x Chiaro	ARRIVANOIRINFORZIDOMANI
y Chiave	VIGENERE VIGNEREVIGENERE
z Cifrato	VDBOLEGSGDQ CLHZTSLSBEGO VDBOLEGSGDQRSSMDGNVQNRD

Meglio i nomenclatori ...

Le cifre polialfabetiche alla riscossa nel XX secolo con le macchine cifranti: il Vernam

Nel 1919 Gilbert Vernam propose una macchina cifrante basata sull'operatore logico XOR, aritmeticamente una somma modulo 2; equivale ad un Vigenère con *chiave infinitamente lunga e casuale*, e Claude Shannon nel 1949 dimostrò che il Vernam è il cifrario perfetto, nel senso che è inattaccabile dall'analisi statistica.

Addizione di caratteri con il codice Baudot										
chiaro c	A 11000	T 00001	T 00001	E 10000	N 00110	Z 10001	I 01100	O 00011	N 00110	E 10000
verme v	W 11001	I 01100	A 11000	P 01101	F 10110	I 01100	L 01001	K 11110	M 00111	S 10100
cifrato c XOR v	00001 T	01101 P	11001 W	11101 Q	10000 E	11101 Q	00101 H	11101 Q	00001 T	00100 {sp}

Matematicamente equivale
a una somma modulo 2

$$z = x + y \pmod{2}$$

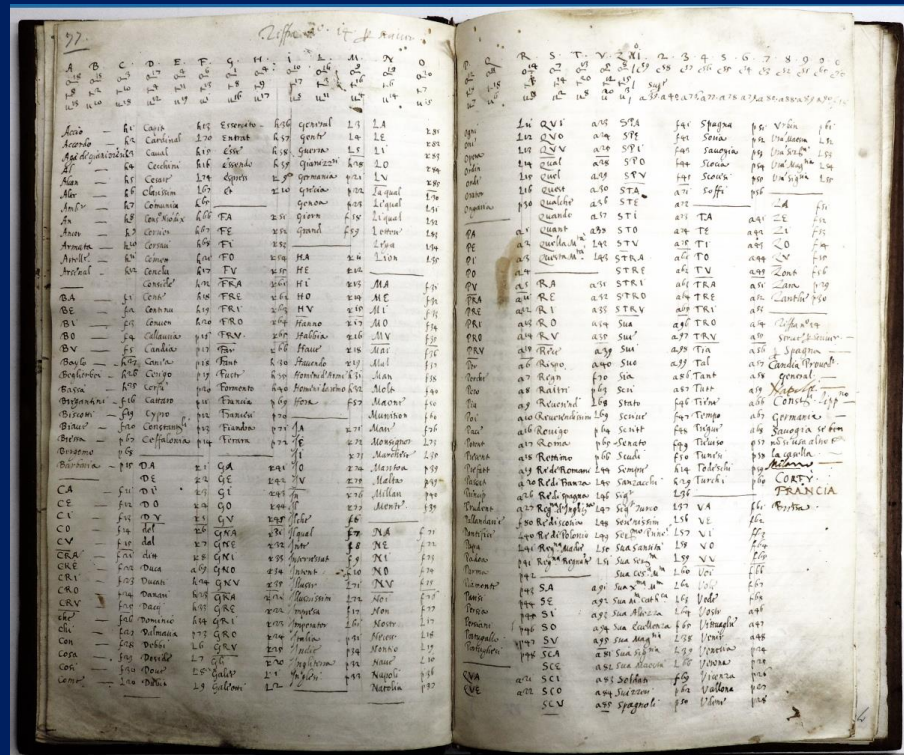
$$z = x \text{ XOR } y$$

Indecifrabile ... a condizione che il verme sia una *sequenza casuale* di 0 e 1

Un esempio di nomenclatore: la ziffra granda

Uno dei pezzi più interessanti negli archivi è questo libretto di cifre. La grafia è molto probabilmente quella del Franceschi.

Accanto la cifra 14, noto come *ziffra granda*, un grande nomenclatore di circa 300 segni, utilizzato dalla maggior parte degli ambasciatori alla fine del XVI secolo. Niente di rivoluzionario, un normale nomenclatore come tanti altri usati a Venezia e altrove in Europa.



ASVe – CX chiavi di cifra ... b. 4. c.77

Serie 3

I due antagonisti

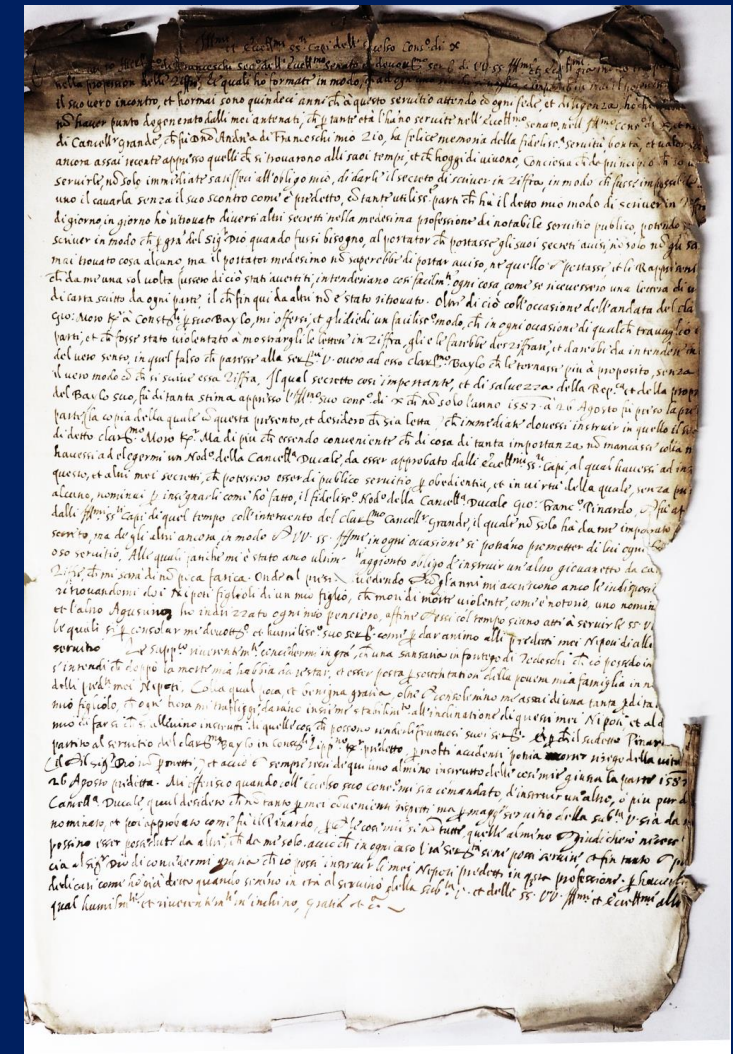
Hieronimo di Franceschi, Pietro Partenio

Hieronimo di Franceschi

Hieronimo (o Girolamo) di Franceschi (1540-~1600), segretario del Senato, fu tra il 1575 e il 1597 deputato alle cifre, uomo chiave della crittografia veneziana.

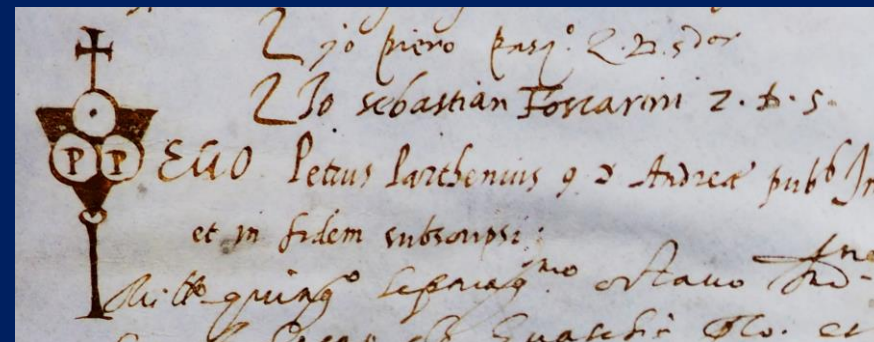
Noto soprattutto come inventore della *cifra delle caselle* una cifra menzionata da diversi autori, tra i quali Pasini e Preto, ma senza alcun dettaglio o ipotesi sulla sua natura.

Della sua vita si sa molto poco, unica fonte autografa questa lunga supplica al CX del 1590 nella quale chiede il permesso di insegnare l'arte delle cifre ai suoi nipoti Agustin e Vettor, e ricorda che la sua famiglia aveva origini antiche, e aveva avuto molti segretari del Senato oltre al cancellier grande Andrea di Franceschi, suo zio.



ASVe – CX parti segrete ...
allegato a parte 8 giugno 1590

Pietro Partenio



Pietro Partenio (1538-~1620), fu notaio attivo dal 1563 al 1618 secondo il registro degli atti notarili conservato nell'archivio veneziano. Fu diverse volte membro del collegio notarile di Venezia.

Diversi atti notarili del Partenio menzionano come procuratore Hieronimo di Franceschi, a riprova che Partenio e Franceschi si conoscevano e avevano legami professionali.

E nel 1592 e 1593 Partenio presentò e donò al CX in tutto sette cifrari, che furono trascritti su un elegante volume in pergamena; il CX apprezzò molto e gli garantì per riconoscenza un vitalizio. Altre cifre presentò nel giugno 1606 in un libretto destinato agli studenti di un corso che si offrì di tenere.

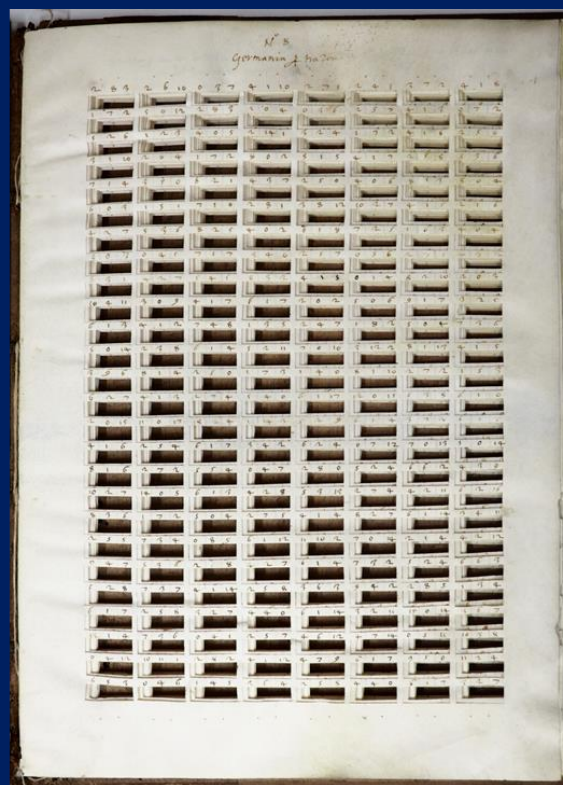
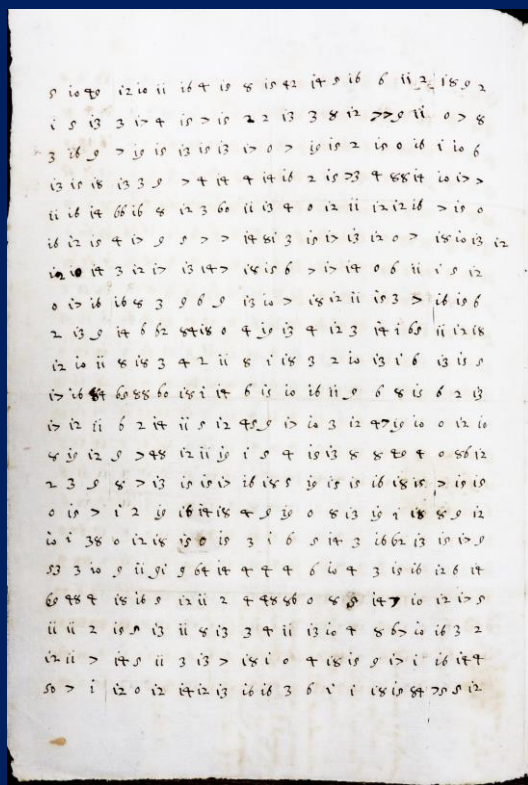
Nel 1596 fu protagonista di una brutta polemica con Franceschi che si concluse male per entrambi.

**ASVe – Notarile 168676 Pietro Partenio
Foglio 5 agosto 1579**

Serie 4

Le chiffre

La cifra delle caselle di Hieronimo di Franceschi

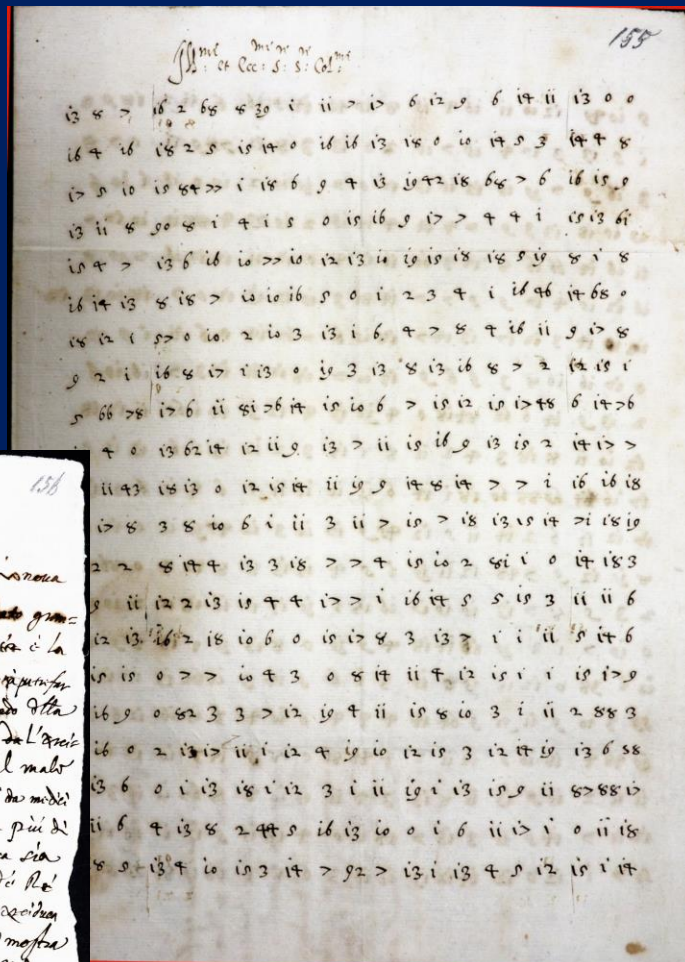


Uno strano messaggio

Nel dicembre 2018, mi fu proposto questo problema irrisolto un dispaccio cifrato dell'ambasciatore veneziano a Praga (Sacro Romano Impero) aveva allegata la decifra di cancelleria, ma non si riusciva a ricostruire la cifra usata.

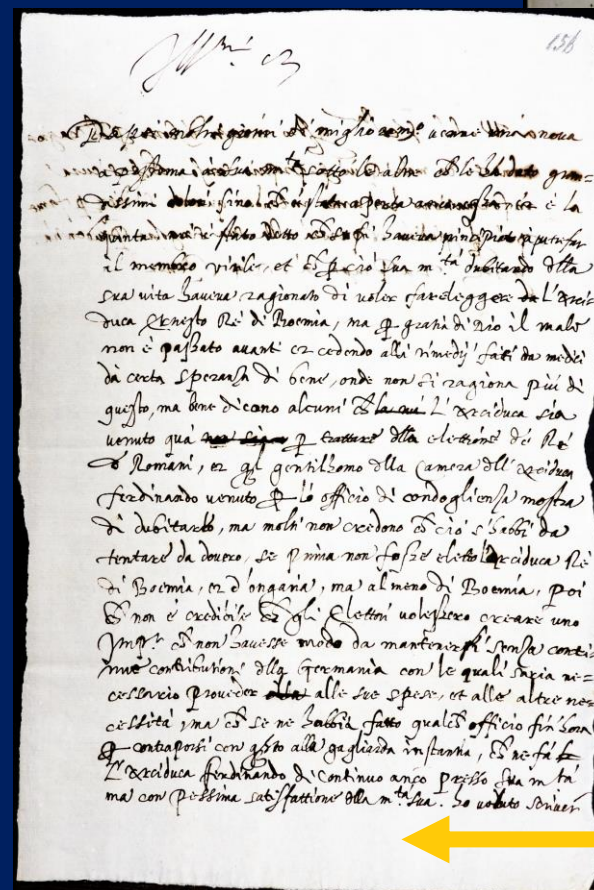
Insolita appariva la disposizione molto ordinata del cifrato ... come se fosse stato scritto attraverso una maschera, una griglia.

**Dispaccio cifrato
Dell'ambasciatore
Alberto Badoer
Praga,
1581 gen 25**



Cifrato

Decifrato



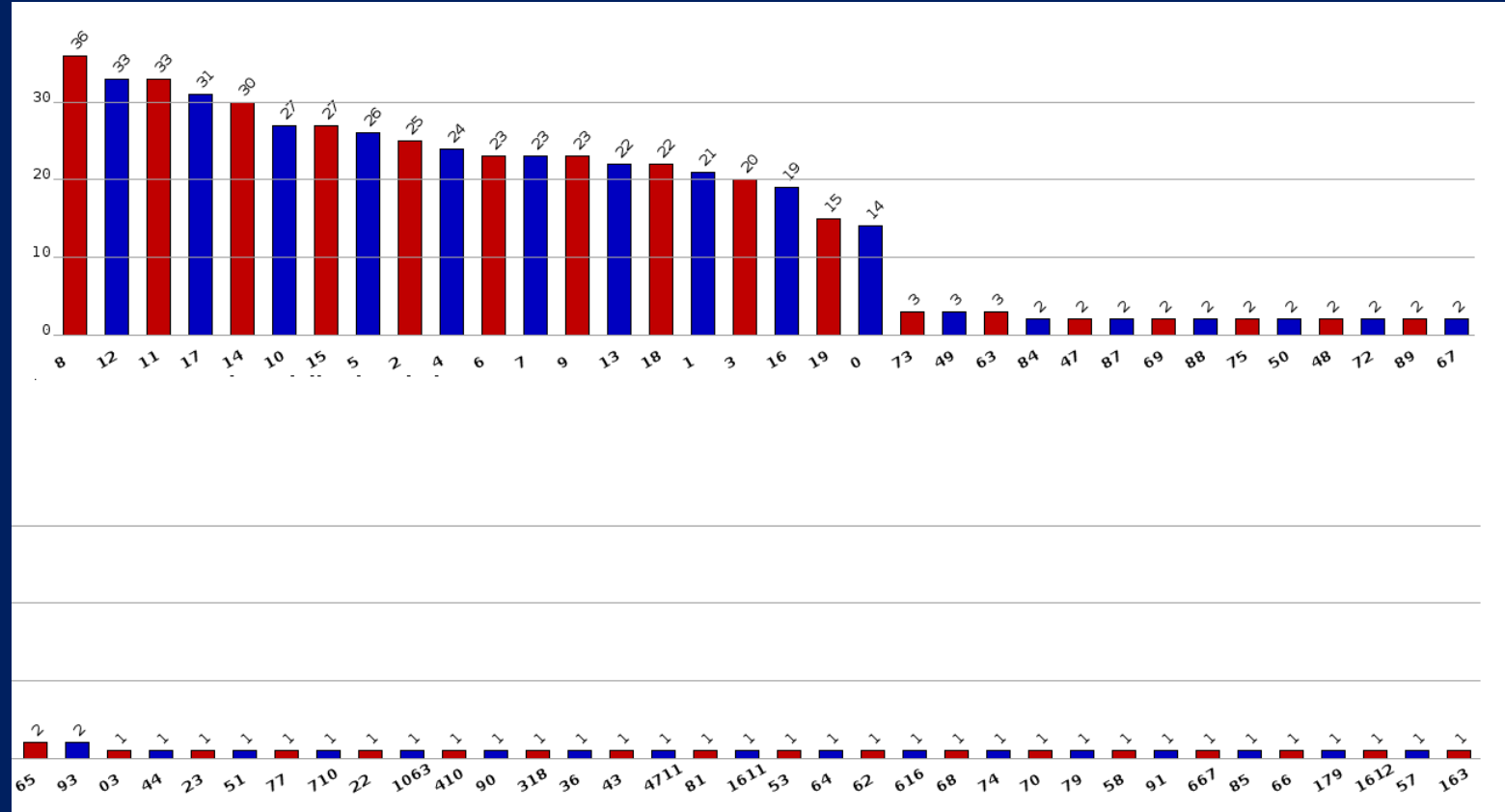
Analisi delle frequenze

L'analisi delle frequenze è sorprendente, ci sono venti numeri con frequenze elevate senza troppe differenze tra di loro, altri sessanta numeri con frequenze minime.

Prima ovvia congettura: le prime venti sono le lettere dell'alfabeto, le altre sono parole del dizionario, proprio come nella cifra piccola!

Ma non funziona, la distribuzione delle frequenze delle lettere è troppo uniforme non ci sono le forti differenze tra lettere comuni e lettere rare.

C'è qualcosa che non quadra! Ha tutta l'aria di una cifra polialfabetica!!!



Una cifra polialfabetica e al tempo stesso un nomenclatore?

- ▶ In altre parole una cifra in due passaggi
- ▶ Un cifra composta, matematicamente equivale ad una funzione composta, non è una novità in crittografia, ma cifre simili entrarono in uso solo nel XIX secolo.
- ▶ Qualche esempio teorico di cifre in qualche modo composte di due passaggi si possono ritrovare in letteratura, persino in Al-Kindi, ma questo è il primo caso di cifra composta effettivamente usata nel mondo reale.

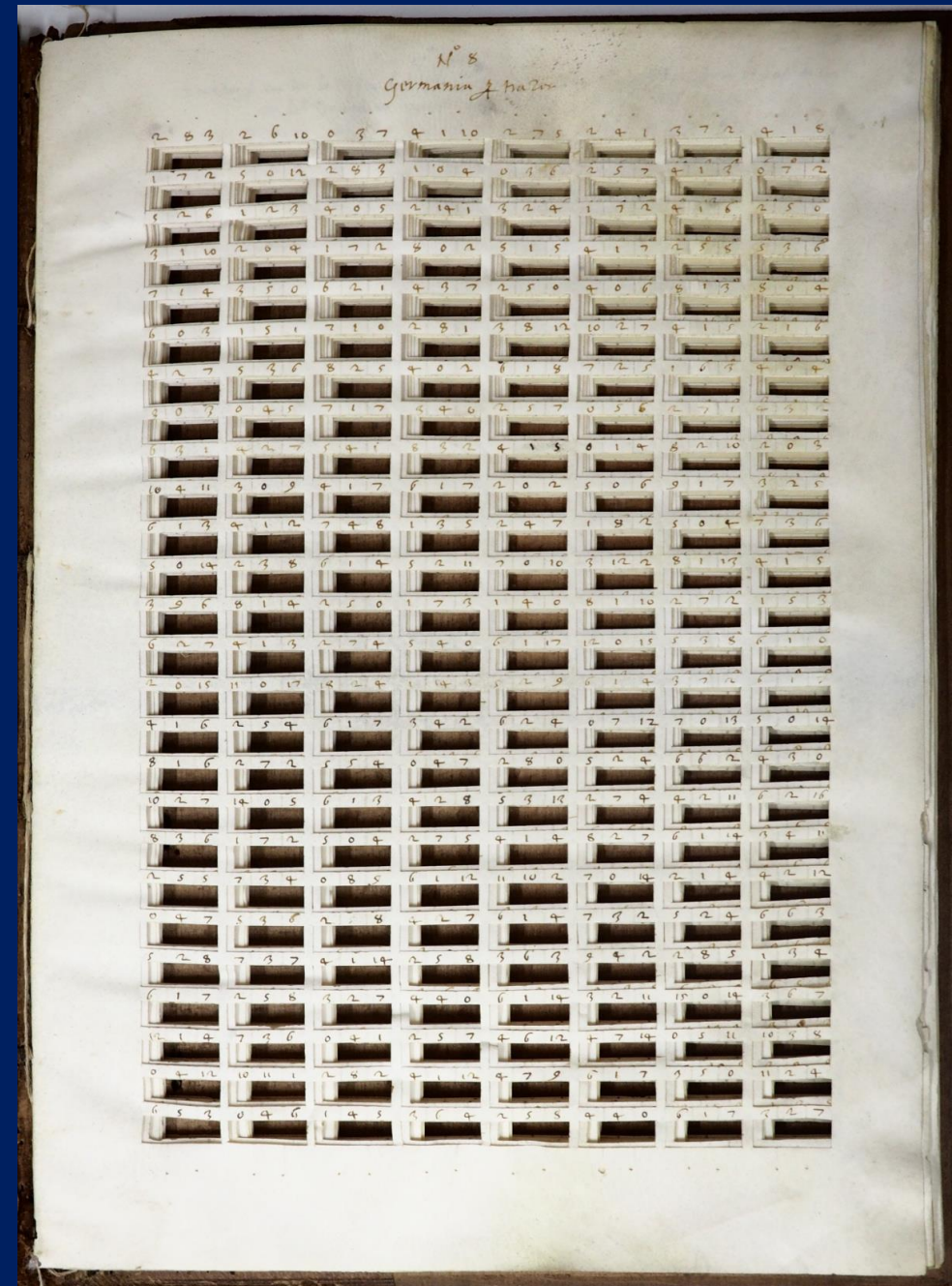


Un libro di *grade* o ... caselle!

La mia fortuna fu che poche settimane prima avevo visto questo libro in archivio che conteneva molte pagine con finestrelle rettangolari, intitolate : Germania, Francia, Spagna e Costantinopoli.

Ogni griglia ha 8 colonne e 26 file di piccole finestre (caselle). Ogni finestra ha tre numeri a 2 cifre sopra.

Questa è la seconda chiave (o secondo *scontro*)

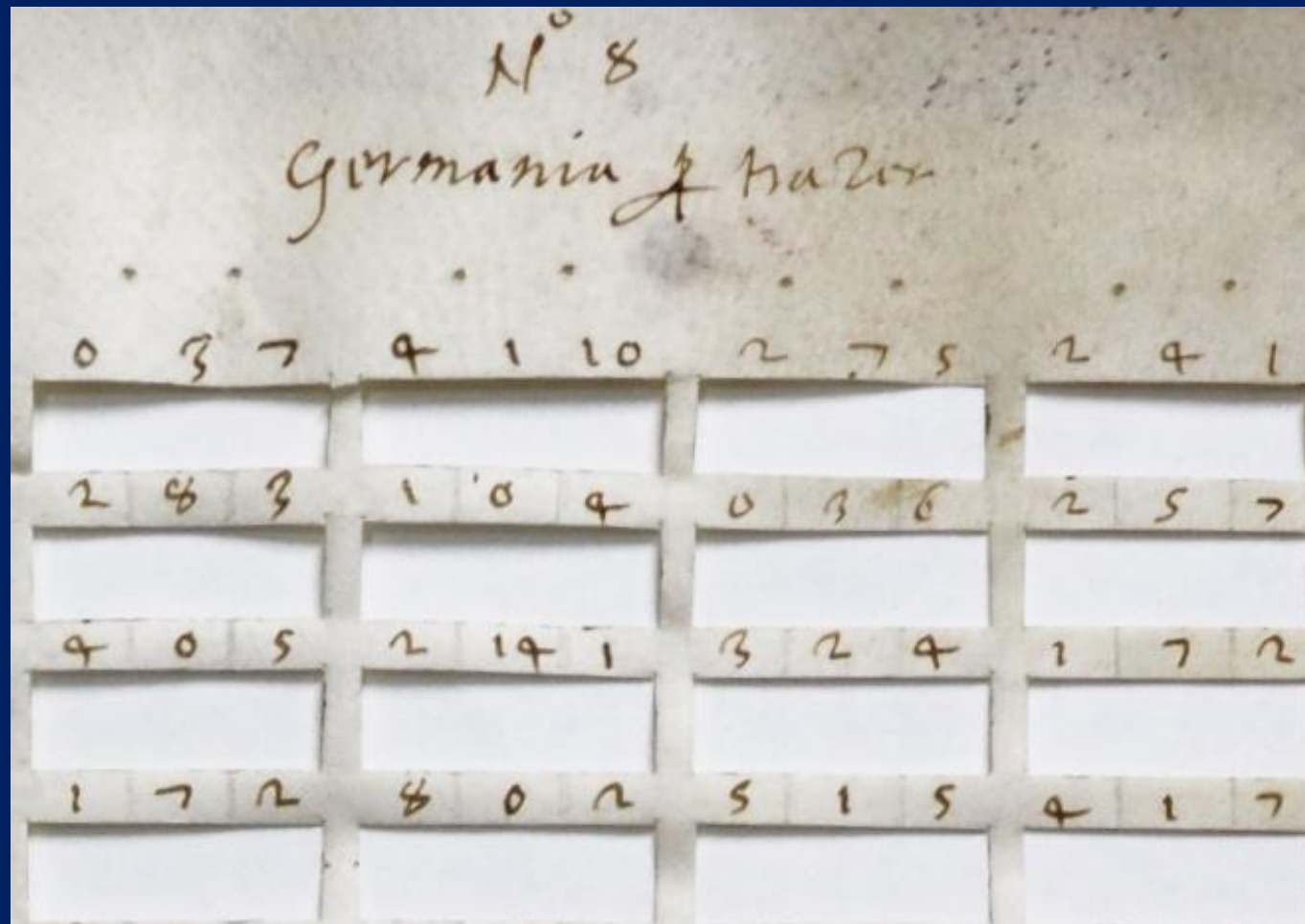


Le caselle!

Ogni griglia ha 8 colonne e 26 file di piccole finestre (caselle).

Ogni finestra ha tre numeri a 2 cifre compresi tra 0 e 19 sopra come si vede a destra.

La decifra è ora chiara: si inserisce il foglio cifrato sotto la griglia e i numeri della griglia devono essere sommati (o sottratti) ai numeri corrispondenti del crittogramma.



Sommando i numeri della griglia «Germania» con i numeri del messaggio di Badoer e confrontando questi numeri con il testo decifrato, è stato facile recuperare il cifrario di base, una ziffra piccola, ed era esattamente la cifra A16 36.

Il motivo della differenza di 20 è ora chiaro; un espediente per fare quella che oggi si chiama aritmetica modulo 20.

La prima cifra era la ziffra piccola A 16 36

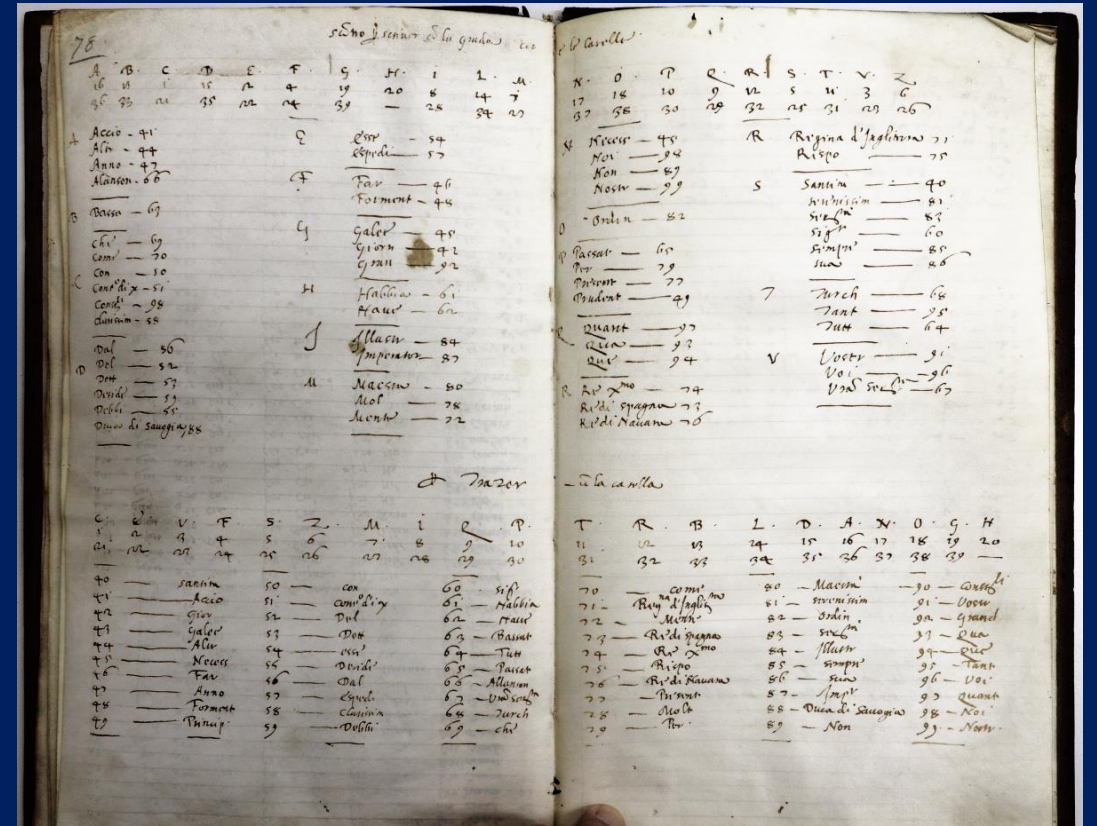
Sono per scriuer con la grada e le caselle

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

Per trazer con la casella

Dizionario									
accio	41	alanson	66	altr	44	anno	47	bassa	63
che	69	Clarissim	58	come	70	con	50	consiglio di X	51
Costantinopoli	90	dal	56	del	52	deside	59	dett	53
donde	55	duca di Sauogia	88	espedi	57	esse	54	far	46
forment	48	galee	43	giorn	42	gran	92	habbia	61
haue	62	illustr	84	Imperatore	87	Maestà	80	mente	72
molt	78	necess	45	noi	98	non	89	nostr	99
ordin	82	passat	65	per	79	present	77	princip	49
qua	93	quant	97	que	94	Re cristianissimo	74	Re di Nauara	76
Re di Spagna	73	Regina d Inghilterra	71	rispo	75	Santità	40	sempre	85
Serenissimo	81	Serenità	83	Signor	60	sua	86	tant	95
Turch	68	tutt	64	uoi	96	uostr	91	Vostra Serenità	67

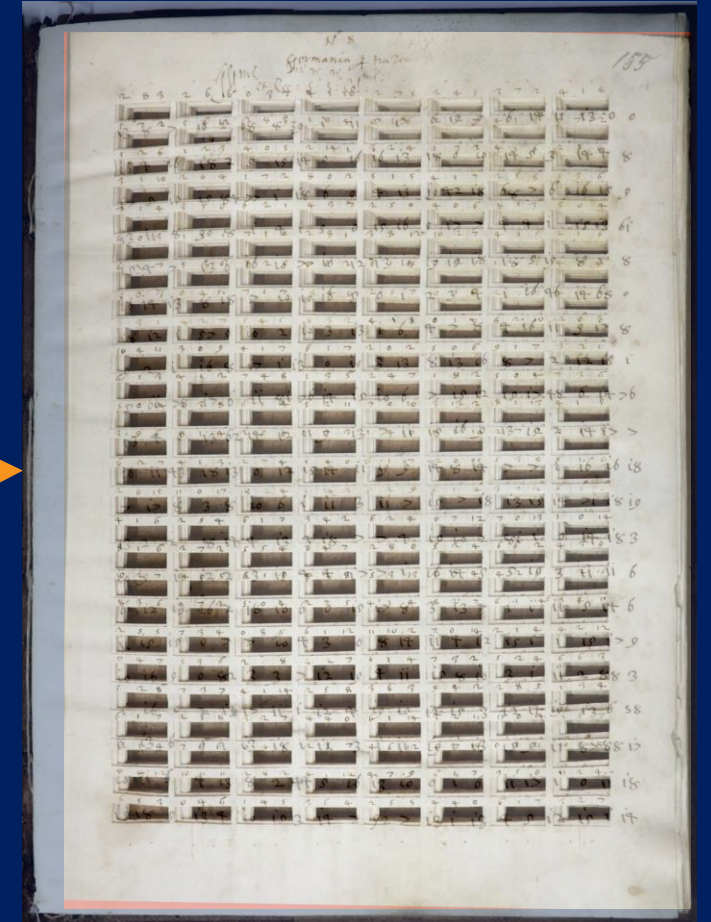
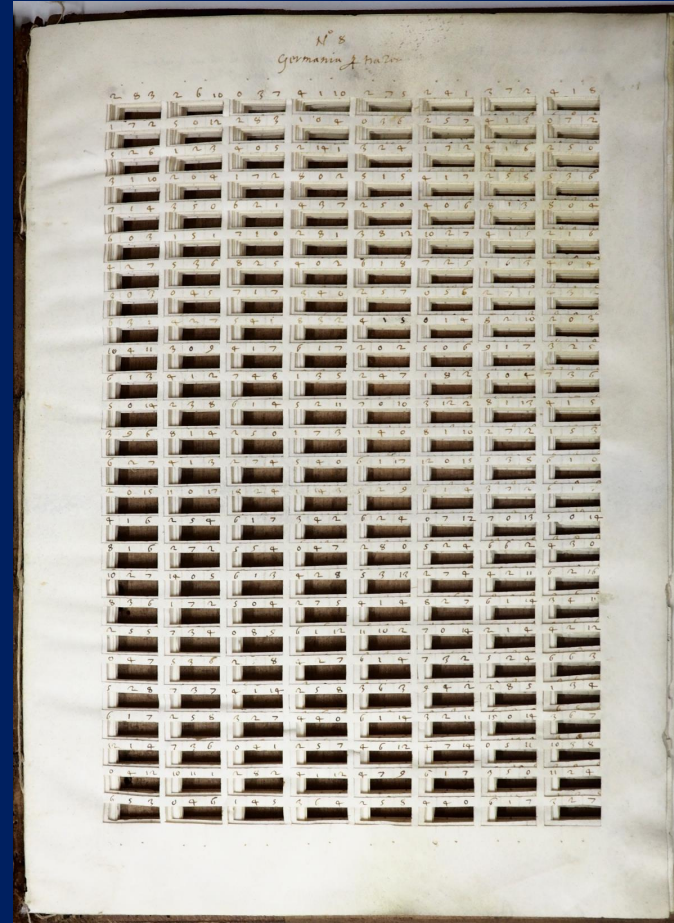
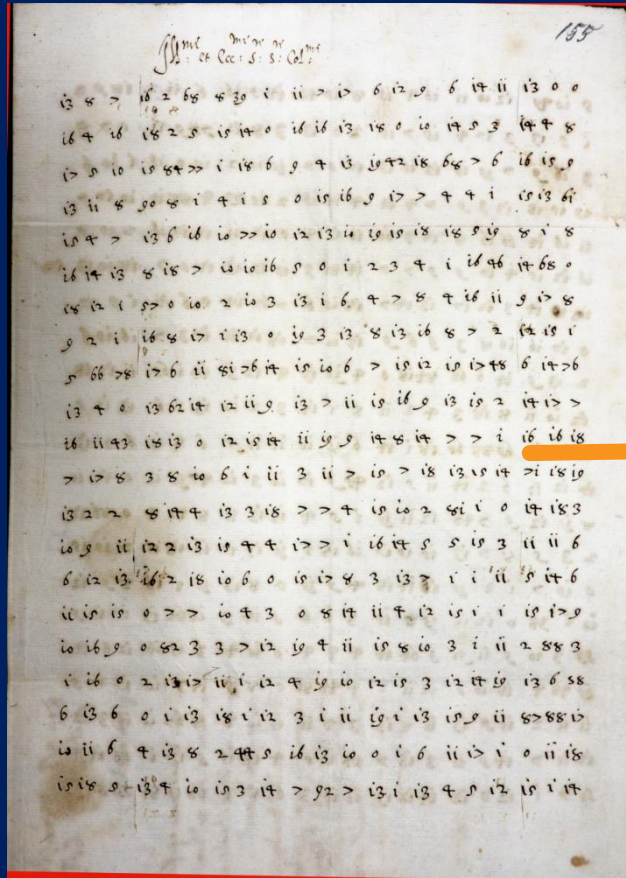
Ritroviamo così la cifra piccola, solo 20 lettere dell'alfabeto con due omofoni ciascuna, che differiscono di 20, più 60 parole comuni. Perché quella differenza di 20? Ora il motivo è chiaro



ASVe – CX chiavi di cifra ... busta 4.

Fasc. 16 Libro delle cifre di H. di Franceschi

Come si decifra con le caselle



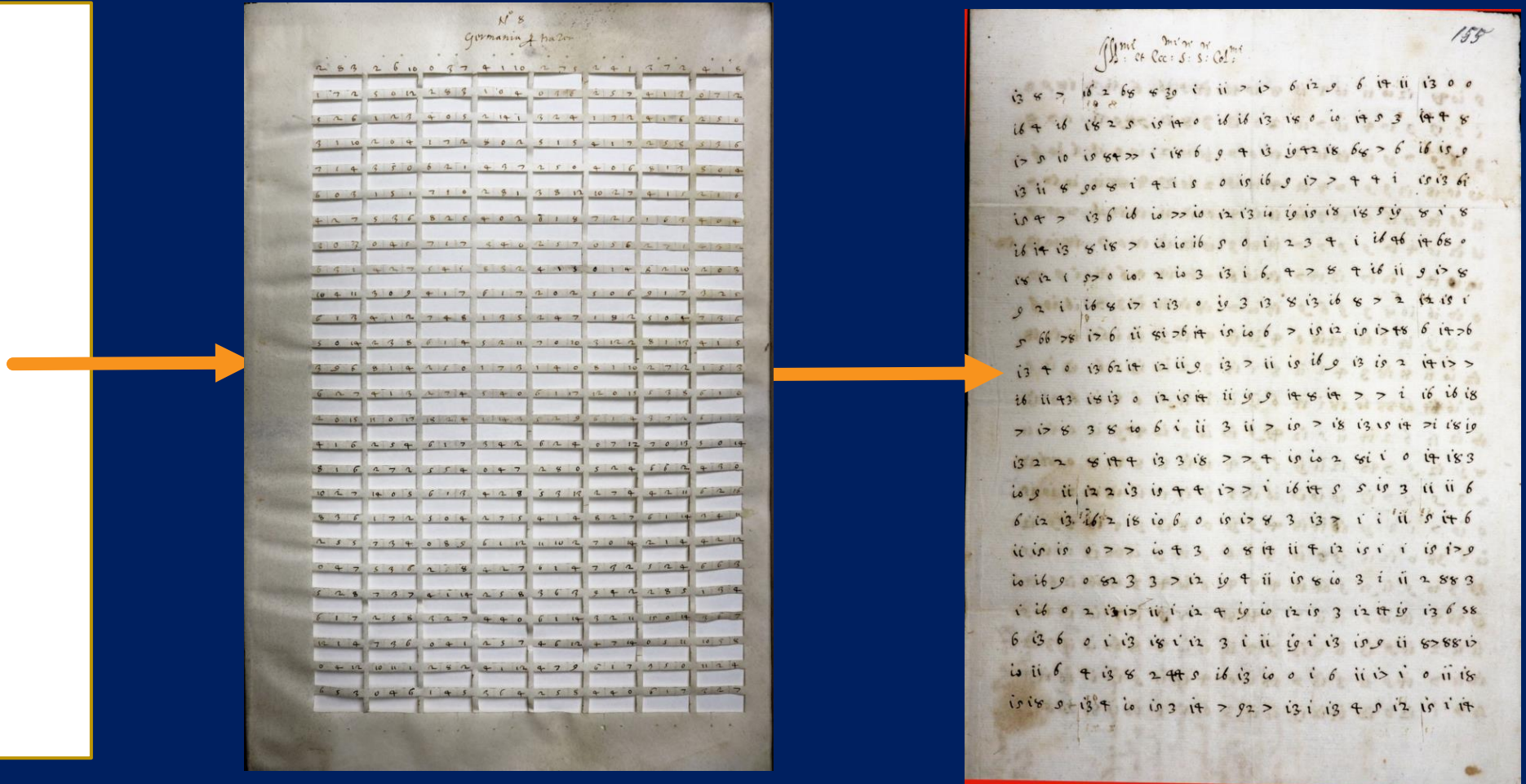
$$c + g = p$$

ASVe – CCX lettere ambasciatori
in Germania f.13 c.155

ASVe – CX chiavi di cifra ...
b. 4. reg.8 Germania

Come si cifra con le caselle?

[Prova a cifrare](#)



Mancano le istruzioni: si presume una sottrazione, ma evitando i negativi.

$$c = p - g(\text{mod } 20)$$

La conferma

Realizzai uno strumento software per decifrare i nomenclatori, aggiungendo una funzione per aggiungere i numeri. Tutti i numeri della griglia Germania sono stati copiati in un database e lo stesso per i messaggi crittografati. Il software decifra l'intero messaggio di Badoer (2 pagine e mezzo) in una frazione di secondo.

Altri messaggi cifrati con le caselle sono stati decrittati, anche quelli senza decifra. Questa è stata la prova migliore, la soluzione era corretta, anche se le istruzioni originali non sono state trovate.

1580-01-24 Dispaccio dell'ambasciatore in Germania Alberto Badoer 1084 gruppi

13	08	07	16	02	68	08	39	01	11	07	17	06	12	09	06	14	11	13	00	00
2	8	3	2	6	10	0	3	7	4	1	10	2	7	5	2	4	1	3	7	2
15	16	10	18	8	58	8	22	8	15	8	7	8	19	14	8	18	12	16	7	2
d	a	p	o	i	molt	i	giorn	i	d	i	m	i	g	l	i	o	r	a	m	e
16	04	16	18	02	05	15	14	00	16	16	13	18	00	10	14	05	03	14	04	08
1	7	2	5	0	12	2	8	3	1	0	4	0	3	6	2	5	7	4	1	3
17	11	18	3	2	17	17	2	3	17	16	17	18	3	16	16	10	10	18	5	11
n	t	o	u	e	n	n	e	u	n	a	n	o	u	a	a	p	p	o	s	t

1581-01-24 Dispaccio dell'ambasciatore Alberto Badoer 1084 gruppi

13	08	07	16	02	68	08	39	01	11	07	17	06	12	09	06	14	11	13	00	00
2	8	3	2	6	10	0	3	7	4	1	10	2	7	5	2	4	1	3	7	2
15	16	10	18	8	78	8	42	8	15	8	27	8	19	14	8	18	12	16	7	2
d	a	p	o	i	molt	i	giorn	i	d	i	m	i	g	l	i	o	r	a	m	e
16	04	16	18	02	05	15	14	00	16	16	13	18	00	10	14	05	03	14	04	08
1	7	2	5	0	12	2	8	3	1	0	4	0	3	6	2	5	7	4	1	3
17	11	18	23	2	17	17	22	3	17	16	17	18	3	16	16	10	10	18	5	11
n	t	o	u	e	n	n	e	u	n	a	n	o	u	a	a	p	p	o	s	t

12	01	42	00	02	02	04	00	13	10	16	03	10	14	02	00	00	00	00	00	00
r	e	f	a	r	e	i	l	m	e	m	b	p	o	u	i	r	i	l	e	e
05	66	78	17	06	11	81	76	14	15	10	06	07	15	12	15	17	48	06	14	76
6	3	1	4	2	7	5	4	1	8	3	2	4	1	5	0	1	4	8	2	10
11	49	59	1	8	18	66	60	15	3	13	8	11	16	17	15	18	32	14	16	66
t	che	per	c	i	o	sua	Maestà	d	u	b	i	t	a	n	d	o	del	l	a	sua
13	04	00	13	62	14	12	11	09	13	07	11	15	16	09	13	15	02	14	17	07
10	4	11	3	0	9	4	1	7	6	1	7	2	0	2	5	0	6	9	1	7
3	8	11	16	42	3	16	12	16	19	8	18	17	16	11	18	15	8	3	18	14
u	i	t	a	haue	u	a	r	a	g	i	o	n	a	t	o	d	i	u	o	l
16	11	43	18	13	00	12	15	14	11	19	09	14	08	14	07	07	01	16	16	18
6	1	3	4	1	2	7	4	8	1	3	5	2	4	7	1	8	2	5	0	4
2	12	26	2	14	2	19	19	2	12	2	14	16	12	1	8	15	3	1	16	2
e	r	far	e	l	e	g	e	r	e	l	a	r	c	i	d	u	c	a	e	
07	17	08	03	08	10	06	01	11	03	11	07	15	07	18	13	15	14	71	18	19
5	0	14	2	3	8	6	1	4	5	2	11	7	0	10	3	12	2	8	1	13
12	17	2	5	11	18	12	2	15	8	13	18	2	7	8	16	7	16	59	19	12
r	n	e	s	t	o	r	e	d	i	b	o	e	m	i	a	m	a	per	g	r
13	02	02	08	14	04	13	03	18	07	07	04	15	10	02	81	01	00	14	18	03
3	9	6	8	1	4	2	5	0	1	7	3	1	4	0	8	1	10	2	7	2
16	11	8	16	15	8	15	8	18	8	14	7	16	14	2	69	2	10	16	5	5
a	t	i	a	d	i	d	i	o	i	l	m	a	l	e	non	e	p	a	s	s
10	09	11	12	02	13	15	04	04	17	07	01	16	14	05	05	15	03	11	11	06
6	2	7	4	1	3	2	7	4	5	4	0	6	1	17	12	0	15	5	3	8
16	11	18	16	3	16	17	11	8	2	11	1	2	15	2	17	15	18	16	14	14
a	t	o	a	u	a	n	t	i	e	t	c	e	d	e	n	d	o	a	l	l

La cifra 5 di Pietro Partenio

Partenio

100 A	150 cam	200 ruca	250 gno	300 indy	350 nte	400 lancia	450 sca	500 sua mag	550 Vorma
101 al	151 cor	201 ducab	251 gnu	301 ingultra	351 nte	401 papa	451 sca	501 sua sig	551 vorma
102 an	152 cor	202 denari	252 gnu	302 ingultra	352 nte	402 padra	452 sca	502 sua sig	552 vorma
103 ar	153 cor	203 denari	253 gnu	303 ingultra	353 nte	403 padra	453 sca	503 sua sig	553 vorma
104 ar	154 cor	204 denari	254 gnu	304 ingultra	354 nte	404 padra	454 sca	504 sua sig	554 vorma
105 ar	155 cor	205 denari	255 gnu	305 ingultra	355 nte	405 padra	455 sca	505 sua sig	555 vorma
106 ar	156 cor	206 denari	256 gnu	306 ingultra	356 nte	406 padra	456 sca	506 sua sig	556 vorma
107 ar	157 cor	207 denari	257 gnu	307 ingultra	357 nte	407 padra	457 sca	507 sua sig	557 vorma
108 ar	158 cor	208 denari	258 gnu	308 ingultra	358 nte	408 padra	458 sca	508 sua sig	558 vorma
109 ar	159 cor	209 denari	259 gnu	309 ingultra	359 nte	409 padra	459 sca	509 sua sig	559 vorma
110 ar	160 cor	210 denari	260 gnu	310 ingultra	360 nte	410 padra	460 sca	510 sua sig	560 vorma
111 ar	161 cor	211 denari	261 gnu	311 ingultra	361 nte	411 padra	461 sca	511 sua sig	561 vorma
112 ar	162 cor	212 denari	262 gnu	312 ingultra	362 nte	412 padra	462 sca	512 sua sig	562 vorma
113 ar	163 cor	213 denari	263 gnu	313 ingultra	363 nte	413 padra	463 sca	513 sua sig	563 vorma
114 ar	164 cor	214 denari	264 gnu	314 ingultra	364 nte	414 padra	464 sca	514 sua sig	564 vorma
115 ar	165 cor	215 denari	265 gnu	315 ingultra	365 nte	415 padra	465 sca	515 sua sig	565 vorma
116 ar	166 cor	216 denari	266 gnu	316 ingultra	366 nte	416 padra	466 sca	516 sua sig	566 vorma
117 ar	167 cor	217 denari	267 gnu	317 ingultra	367 nte	417 padra	467 sca	517 sua sig	567 vorma
118 ar	168 cor	218 denari	268 gnu	318 ingultra	368 nte	418 padra	468 sca	518 sua sig	568 vorma
119 ar	169 cor	219 denari	269 gnu	319 ingultra	369 nte	419 padra	469 sca	519 sua sig	569 vorma
120 ar	170 cor	220 denari	270 gnu	320 ingultra	370 nte	420 padra	470 sca	520 sua sig	570 vorma
121 ar	171 cor	221 denari	271 gnu	321 ingultra	371 nte	421 padra	471 sca	521 sua sig	571 vorma
122 ar	172 cor	222 denari	272 gnu	322 ingultra	372 nte	422 padra	472 sca	522 sua sig	572 vorma
123 ar	173 cor	223 denari	273 gnu	323 ingultra	373 nte	423 padra	473 sca	523 sua sig	573 vorma
124 ar	174 cor	224 denari	274 gnu	324 ingultra	374 nte	424 padra	474 sca	524 sua sig	574 vorma
125 ar	175 cor	225 denari	275 gnu	325 ingultra	375 nte	425 padra	475 sca	525 sua sig	575 vorma
126 ar	176 cor	226 denari	276 gnu	326 ingultra	376 nte	426 padra	476 sca	526 sua sig	576 vorma
127 ar	177 cor	227 denari	277 gnu	327 ingultra	377 nte	427 padra	477 sca	527 sua sig	577 vorma
128 ar	178 cor	228 denari	278 gnu	328 ingultra	378 nte	428 padra	478 sca	528 sua sig	578 vorma
129 ar	179 cor	229 denari	279 gnu	329 ingultra	379 nte	429 padra	479 sca	529 sua sig	579 vorma
130 ar	180 cor	230 denari	280 gnu	330 ingultra	380 nte	430 padra	480 sca	530 sua sig	580 vorma
131 ar	181 cor	231 denari	281 gnu	331 ingultra	381 nte	431 padra	481 sca	531 sua sig	581 vorma
132 ar	182 cor	232 denari	282 gnu	332 ingultra	382 nte	432 padra	482 sca	532 sua sig	582 vorma
133 ar	183 cor	233 denari	283 gnu	333 ingultra	383 nte	433 padra	483 sca	533 sua sig	583 vorma
134 ar	184 cor	234 denari	284 gnu	334 ingultra	384 nte	434 padra	484 sca	534 sua sig	584 vorma
135 ar	185 cor	235 denari	285 gnu	335 ingultra	385 nte	435 padra	485 sca	535 sua sig	585 vorma
136 ar	186 cor	236 denari	286 gnu	336 ingultra	386 nte	436 padra	486 sca	536 sua sig	586 vorma
137 ar	187 cor	237 denari	287 gnu	337 ingultra	387 nte	437 padra	487 sca	537 sua sig	587 vorma
138 ar	188 cor	238 denari	288 gnu	338 ingultra	388 nte	438 padra	488 sca	538 sua sig	588 vorma
139 ar	189 cor	239 denari	289 gnu	339 ingultra	389 nte	439 padra	489 sca	539 sua sig	589 vorma
140 ar	190 cor	240 denari	290 gnu	340 ingultra	390 nte	440 padra	490 sca	540 sua sig	590 vorma
141 ar	191 cor	241 denari	291 gnu	341 ingultra	391 nte	441 padra	491 sca	541 sua sig	591 vorma
142 ar	192 cor	242 denari	292 gnu	342 ingultra	392 nte	442 padra	492 sca	542 sua sig	592 vorma
143 ar	193 cor	243 denari	293 gnu	343 ingultra	393 nte	443 padra	493 sca	543 sua sig	593 vorma
144 ar	194 cor	244 denari	294 gnu	344 ingultra	394 nte	444 padra	494 sca	544 sua sig	594 vorma
145 ar	195 cor	245 denari	295 gnu	345 ingultra	395 nte	445 padra	495 sca	545 sua sig	595 vorma
146 ar	196 cor	246 denari	296 gnu	346 ingultra	396 nte	446 padra	496 sca	546 sua sig	596 vorma
147 ar	197 cor	247 denari	297 gnu	347 ingultra	397 nte	447 padra	497 sca	547 sua sig	597 vorma
148 ar	198 cor	248 denari	298 gnu	348 ingultra	398 nte	448 padra	498 sca	548 sua sig	598 vorma
149 ar	199 cor	249 denari	299 gnu	349 ingultra	399 nte	449 padra	499 sca	549 sua sig	599 vorma
150 ar	200 cor	250 denari	300 gnu	350 ingultra	400 nte	450 padra	500 sca	550 sua sig	600 vorma

0	1	2	3	4	5	6	7	8	9
h	c	e	b	f	d	a	m	i	g
p	t	r	u	l	s	z	n	o	q

ASVe – CX cifre, chiavi e scontri di cifra ... b,2 r. 13 Partenio, cifra A 100

La cifra 5 di Pietro Partenio (1593-95)

Ed ecco la cifra di Partenio adottata dal CX al posto delle caselle.

Anche questa è una cifra composta, ma il nomenclatore è molto più ampio a 3 cifre, circa 500 segni. Più semplice la seconda cifra.

pi	et	ro	pa	r	te	ni	o
379	211	424	377	420	514	344	365

Partenio

100 A	150 cam	200 duca	250 gno	300 indip	350 nti	400 Pontific	450 sca	500 sua mag	550 Verona
101 al	151 sar	201 duca	251 gnu	301 inghilterra	351 nti	401 papa	451 sca	501 sua mag	551 Verona
102 an	152 cor	202 ducan	252 gnu	302 ingh	352 nti	402 padon	452 sca	502 sua mag	552 Verona
103 ar	153 cor	203 ducij	253 gre	303 L	353 nti	403 padon	453 sca	503 sua mag	553 Verona
104 accia	154 cor	204 ducina	254 gre	304 L	354 nti	404 padon	454 sca	504 sua mag	554 Verona
105 accia	155 cor	205 ducina	255 gre	305 L	355 nti	405 padon	455 sca	505 sua mag	555 Verona
106 accia	156 cor	206 ducina	256 gre	306 L	356 nti	406 padon	456 sca	506 sua mag	556 Verona
107 accia	157 cor	207 ducina	257 gre	307 L	357 nti	407 padon	457 sca	507 sua mag	557 Verona
108 accia	158 cor	208 ducina	258 gre	308 L	358 nti	408 padon	458 sca	508 sua mag	558 Verona
109 accia	159 cor	209 ducina	259 gre	309 L	359 nti	409 padon	459 sca	509 sua mag	559 Verona
110 accia	160 cor	210 ducina	260 gre	310 L	360 nti	410 padon	460 sca	510 sua mag	560 Verona
111 accia	161 cor	211 ducina	261 gre	311 L	361 nti	411 padon	461 sca	511 sua mag	561 Verona
112 accia	162 cor	212 ducina	262 gre	312 L	362 nti	412 padon	462 sca	512 sua mag	562 Verona
113 accia	163 cor	213 ducina	263 gre	313 L	363 nti	413 padon	463 sca	513 sua mag	563 Verona
114 accia	164 cor	214 ducina	264 gre	314 L	364 nti	414 padon	464 sca	514 sua mag	564 Verona
115 B	165 cor	215 ducina	265 gre	315 L	365 nti	415 padon	465 sca	515 sua mag	565 Verona
116 B	166 cor	216 ducina	266 gre	316 L	366 nti	416 padon	466 sca	516 sua mag	566 Verona
117 B	167 cor	217 ducina	267 gre	317 L	367 nti	417 padon	467 sca	517 sua mag	567 Verona
118 B	168 cor	218 ducina	268 gre	318 L	368 nti	418 padon	468 sca	518 sua mag	568 Verona
119 B	169 cor	219 ducina	269 gre	319 L	369 nti	419 padon	469 sca	519 sua mag	569 Verona
120 B	170 cor	220 ducina	270 gre	320 L	370 nti	420 padon	470 sca	520 sua mag	570 Verona
121 B	171 cor	221 ducina	271 gre	321 L	371 nti	421 padon	471 sca	521 sua mag	571 Verona
122 B	172 cor	222 ducina	272 gre	322 L	372 nti	422 padon	472 sca	522 sua mag	572 Verona
123 B	173 cor	223 ducina	273 gre	323 L	373 nti	423 padon	473 sca	523 sua mag	573 Verona
124 B	174 cor	224 ducina	274 gre	324 L	374 nti	424 padon	474 sca	524 sua mag	574 Verona
125 B	175 cor	225 ducina	275 gre	325 L	375 nti	425 padon	475 sca	525 sua mag	575 Verona
126 B	176 cor	226 ducina	276 gre	326 L	376 nti	426 padon	476 sca	526 sua mag	576 Verona
127 B	177 cor	227 ducina	277 gre	327 L	377 nti	427 padon	477 sca	527 sua mag	577 Verona
128 B	178 cor	228 ducina	278 gre	328 L	378 nti	428 padon	478 sca	528 sua mag	578 Verona
129 B	179 cor	229 ducina	279 gre	329 L	379 nti	429 padon	479 sca	529 sua mag	579 Verona
130 B	180 cor	230 ducina	280 gre	330 L	380 nti	430 padon	480 sca	530 sua mag	580 Verona
131 B	181 cor	231 ducina	281 gre	331 L	381 nti	431 padon	481 sca	531 sua mag	581 Verona
132 B	182 cor	232 ducina	282 gre	332 L	382 nti	432 padon	482 sca	532 sua mag	582 Verona
133 B	183 cor	233 ducina	283 gre	333 L	383 nti	433 padon	483 sca	533 sua mag	583 Verona
134 B	184 cor	234 ducina	284 gre	334 L	384 nti	434 padon	484 sca	534 sua mag	584 Verona
135 B	185 cor	235 ducina	285 gre	335 L	385 nti	435 padon	485 sca	535 sua mag	585 Verona
136 B	186 cor	236 ducina	286 gre	336 L	386 nti	436 padon	486 sca	536 sua mag	586 Verona
137 C	187 cor	237 ducina	287 gre	337 L	387 nti	437 padon	487 sca	537 sua mag	587 Verona
138 C	188 cor	238 ducina	288 gre	338 L	388 nti	438 padon	488 sca	538 sua mag	588 Verona
139 C	189 cor	239 ducina	289 gre	339 L	389 nti	439 padon	489 sca	539 sua mag	589 Verona
140 C	190 cor	240 ducina	290 gre	340 L	390 nti	440 padon	490 sca	540 sua mag	590 Verona
141 C	191 cor	241 ducina	291 gre	341 L	391 nti	441 padon	491 sca	541 sua mag	591 Verona
142 C	192 cor	242 ducina	292 gre	342 L	392 nti	442 padon	492 sca	542 sua mag	592 Verona
143 C	193 cor	243 ducina	293 gre	343 L	393 nti	443 padon	493 sca	543 sua mag	593 Verona
144 C	194 cor	244 ducina	294 gre	344 L	394 nti	444 padon	494 sca	544 sua mag	594 Verona
145 C	195 cor	245 ducina	295 gre	345 L	395 nti	445 padon	495 sca	545 sua mag	595 Verona
146 C	196 cor	246 ducina	296 gre	346 L	396 nti	446 padon	496 sca	546 sua mag	596 Verona
147 C	197 cor	247 ducina	297 gre	347 L	397 nti	447 padon	497 sca	547 sua mag	597 Verona
148 C	198 cor	248 ducina	298 gre	348 L	398 nti	448 padon	498 sca	548 sua mag	598 Verona
149 C	199 cor	249 ducina	299 gre	349 L	399 nti	449 padon	499 sca	549 sua mag	599 Verona

[Pagina sul sito](#)

Ibidem

La cifra 5 di Pietro Partenio (1593-95)

beghir bei	128	bei	122	bergamo	136	bianc	129
bile	130	biscotti	131	bisogn	132	bon	123
bra	124	bre	125	brescia	135	brigantini	133
calunnia	176	cam	150	Candia	177	Canea	178
capit	160	car	151	cardinal	161	cataro	179
caual	162	cechini	163	Ceffalonia	181	censo	180
cer	152	cesare	164	che	153	chi	154
cio	144	Cipro	182	clarissim	165	col	155
come	159	comen	170	comunic	166	con	156
conclu	171	consiglio	172	consiglio nostro di X	167	conte	173
contenu	174	conuen	175	Corfu	184	corrier	168
corsari	169	cosa	157	così	158	Costantinopoli	183
dal	194	Dalmatia	205	debbi	206	decij	203
dei	193	del	165 195	delibera	198	denari	202
deside	207	dice	199	ditt	196	dominis	204
doue	208	dra	191	dre	192	dubit	209
duca	200	ducati	201	dun	197	entrat	213
era	217	esercit	212	espress	216	esse	214
essendo	215	et	211	fan	231	fant	232

0	1	2	3	4	5	6	7	8	9
h	c	e	b	f	d	a	m	i	g
p	t	r	u	l	s	z	n	o	q

Alfabeto																					
a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	z		
100	115	137	185	210	218	239	270	283	303	317	341	365	376	408	420	444	512	535	559		

Sillabario																													
ba	be	bi	bo	bu	ca	ce	ci	co	cu	cra	cre	cri	cro	cru	da	de	di	do	du	fa	fe	fi	fo	fu					
116	117	118	119	120	138	139	140	141	142	145	146	147	148	149	186	187	188	189	190	219	220	221	222	223					
fra	fre	fri	fro	fru	ga	ge	gi	go	gu	gna	gne	gni	gno	gnu	gra	gre	gri	gro	gru	ha	he	hi	ho	hu					
224	225	226	227	228	240	241	242	243	244	247	248	249	250	251	252	253	254	255	256	271	272	273	274	275					
ia	ie	ii	io	iu	la	le	li	lo	lu	ma	me	mi	mo	mu	na	ne	ni	no	nu	nta	nte	nti	nto	ntu					
284	285	286	287	288	304	305	306	307	308	318	319	320	321	322	342	343	344	345	346	349	350	351	352	...					
pa	pe	pi	po	pu	pra	pre	pri	pro	pru	qua	que	qui	quo	quu	ra	re	ri	ro	ru	sa	se	si	so	su					
377	378	379	380	381	382	383	384	385	386	409	410	411	412	...	421	422	423	424	425	445	446	447	448	449					
sca	sce	sci	sco	scu	spa	spe	spi	spo	spu	ssa	sse	ssi	sso	ssu	sta	ste	sti	sto	stu	stra	stre	stri	stro	stru					
450	451	452	453	454	455	456	457	458	459	470	471	472	473	474	460	461	462	463	464	465	466	467	468	469					
ta	te	ti	to	tu	tra	tre	tri	tro	tru	ua	ue	ui	uo	uu	za	ze	zi	zo	zu										
513	514	515	516	517	518	519	520	521	522	536	537	538	539	540	560	561	562	563	564										

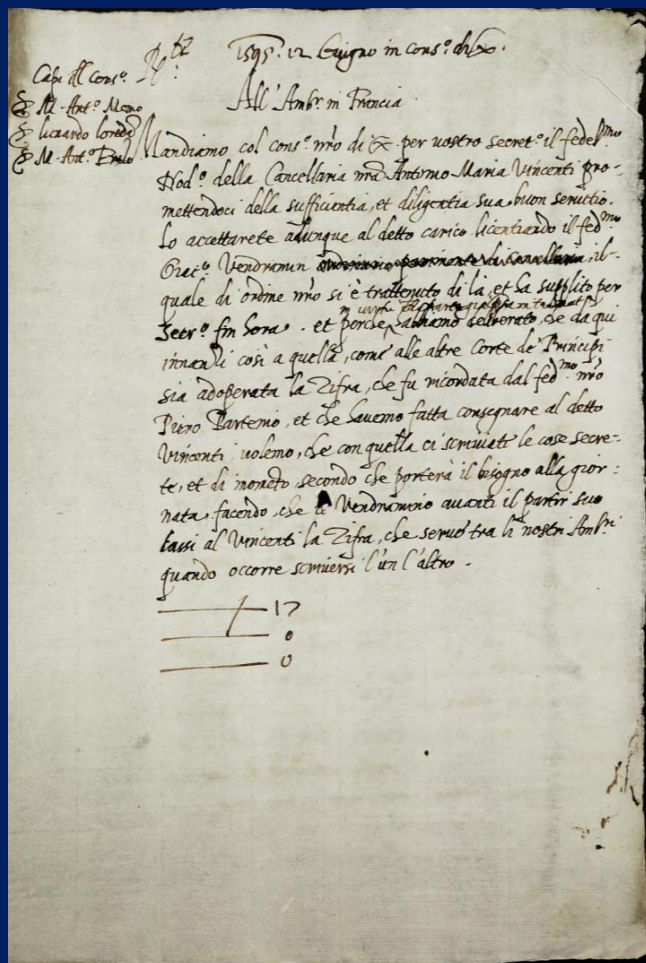
pi	et	ro	pa	r	te	ni	o
379	211	424	377	420	514	344	365
umg	rtt	frf	unm	lrp	scl	ull	bzs

Serie 5

La sfida

Partenio vs Franceschi
una sfida senza vincitori

Una settimana dopo il CX decreta ...



Il 12 giugno 1595, il CX decretò all'unanimità, 17 su 17, che d'ora in poi l'ambasciatore di Francia usasse una nuova cifra di Pietro Partenio al posto di quella delle caselle, per le questioni più riservate.

Fu scelta la cifra n.5 tra le sette che Partenio aveva donato al CX nel 1592 e 1593.

Come abbiamo visto si trattava di una cifra in due passaggi, sovracifratura.

Partenio sosteneva che se anche il nemico fosse venuto in possesso del nomenclatore, non sarebbe mai riuscito a decifrare i dispacci cifrati senza conoscere la tabellina.

ASVe CX parti secrete filza
26 15 05 1595

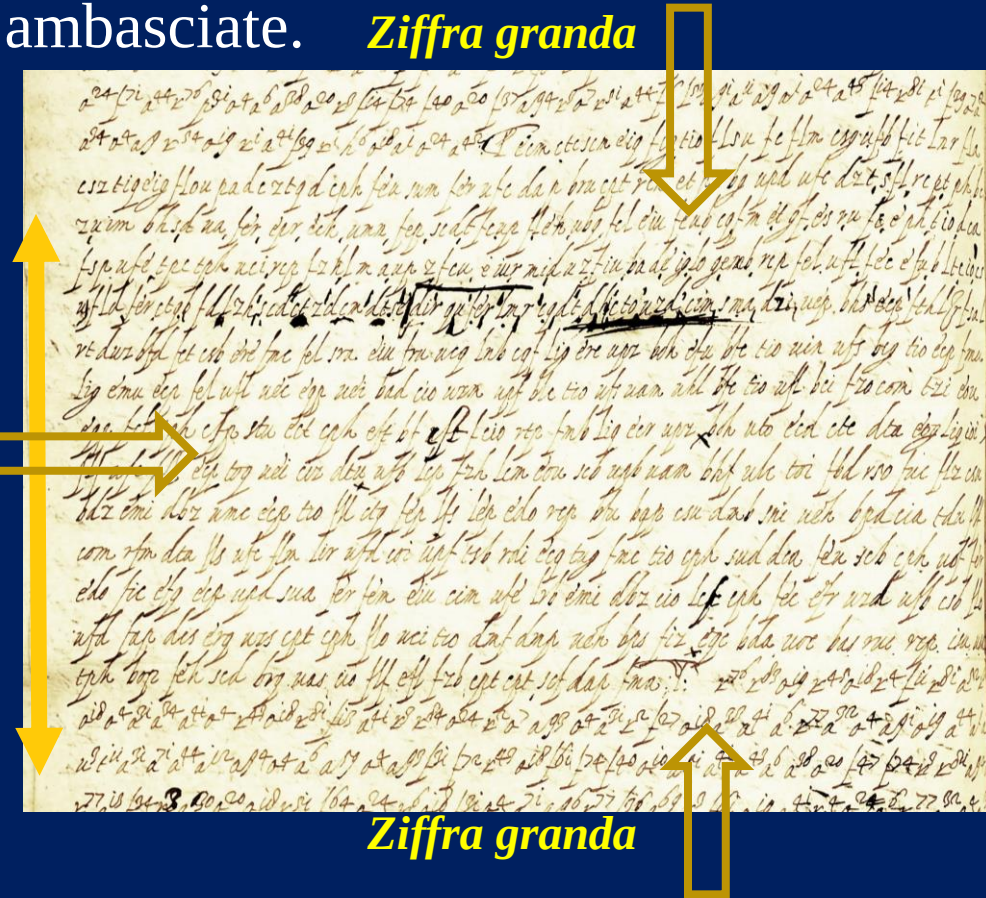
Il CX adottò le cifre del Partenio?

Questa delibera del CX riportata dal Baschet nel suo libro, è stata ripresa da molti autori che ne hanno tratto conseguenze un po' azzardate:

- Partenio sarebbe diventato il deputato alle cifre del CX.
- Le cifre del Partenio divennero quelle correnti per le ambasciate. **Ziffra granda**

L'esame delle carte d'archivio fornisce una storia un po' diversa: la cifra 5 del Partenio risulta usata solo tre volte tra luglio e agosto 1595, e solo per la parte più delicata del dispaccio, come nell'esempio a lato, il resto usa la *ziffra granda*; poi non se ne trova più traccia.

Cifra corrente per le ambasciate restò la *ziffra granda* n. 14 del libro di Franceschi.

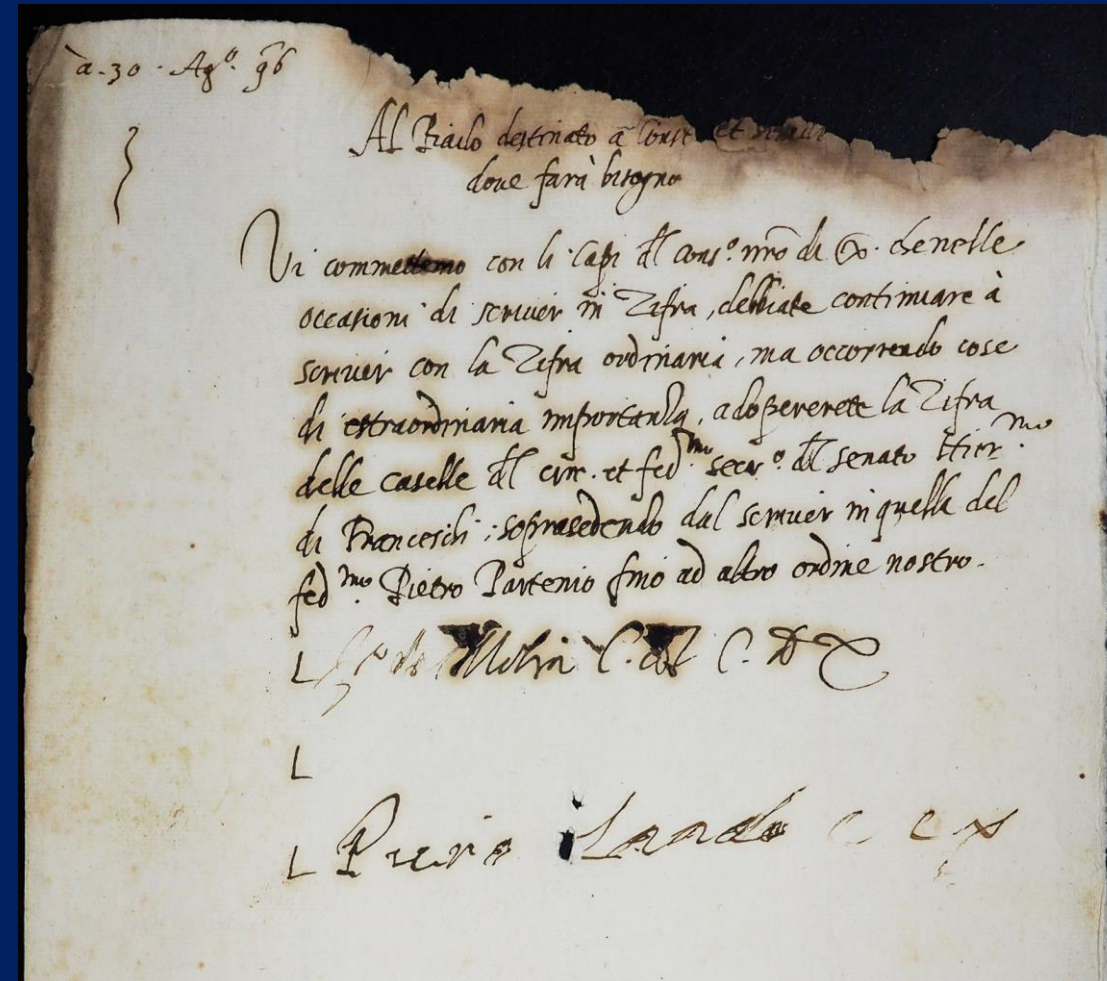


Ma un anno dopo ...

Un anno dopo il 30 agosto 1596, il CX scrisse questa *sorprendente* lettera al nuovo Baylo a Costantinopoli:

Vi commetemo con li Capi del Cons^o nostro di X che nelle occasioni di scriuer in zifra dobbiate continuar à scriuer con la zifra ordinaria; ma occorrendo cose di straordinaria importanza adopererete la zifra delle caselle del circ. et fed^{mo} sec^o al Senato H^{mo} di Franceschi, soprasedendo dal scriuer in quella del fed^{mo} Pietro Partenio fino ad altro ordine nostro.

Cosa aveva provocato questa improvvisa inversione di rotta?



ASVe CCX lettere secrete f. 11 30 08 1596

La sfida di Franceschi

La risposta si trova in una relazione del CX datata 8 agosto 1596.

Franceschi non aveva digerito la dismissione della sua cifra a favore di una cifra di Partenio che era un notaio privato, estraneo alla cancelleria. Ed evidentemente non era affatto convinto che la sua cifra fosse stata forzata dal Viète.

Si presentò al CX nel luglio 1596 affermando che **Partenio era in errore quando diceva che senza la tabellina di sovracifra, nessuno poteva decifrare un dispaccio così cifrato**, nemmeno se fosse venuto in possesso dello scontro (nomenclatore) e lanciò la sfida. «preparatemi un testo cifrato con una tabellina diversa, io sarò in grado di decrittarlo».

E così fu: il CX incaricò un altro segretario, tale Comino, di preparare il cifrato con una tabellina segreta e consegnarlo a Franceschi. Dopo pochi giorni Franceschi si ripresentò al CX accompagnato dal suo pupillo Pietro Amai, con la decifra completa, parola per parola !

Partenio convocato dal CX

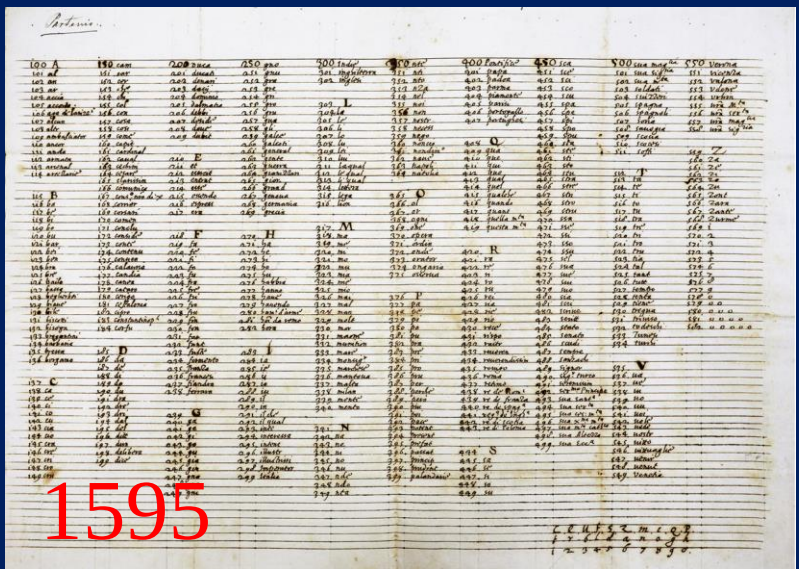
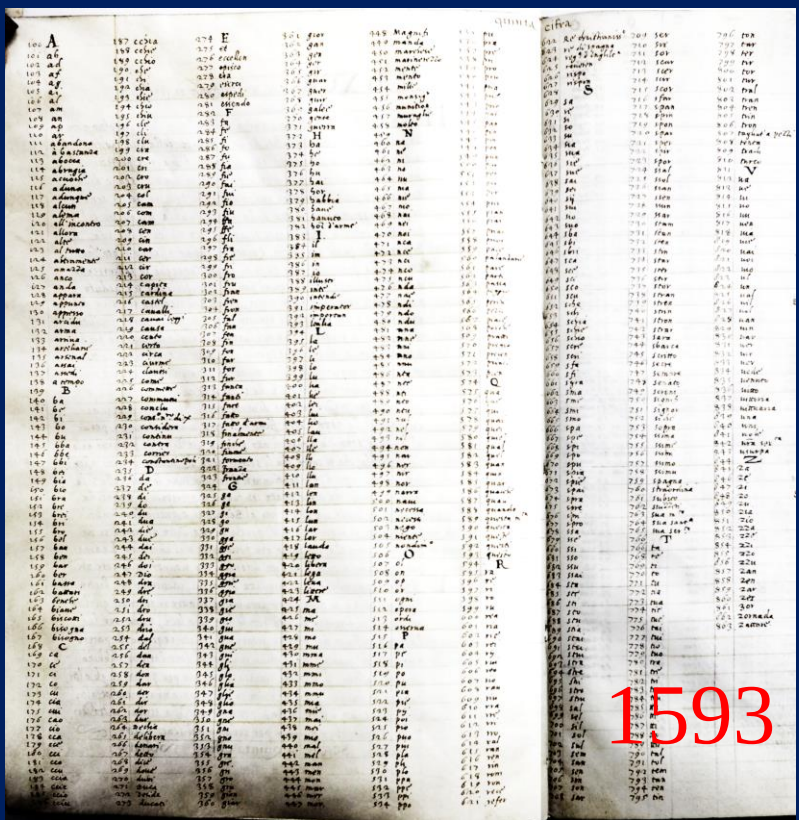
Convocato d'urgenza dal CX Pietro Partenio per dire quanto poteva essere di suo interesse, si difese a fatica, Disse che, sì, la sua cifra era *trazibile* perché invece delle 1000 parole della versione originale del 1593, il suo nomenclatore era stato ridotto a circa 500 parole indebolendolo seriamente.

Il CX non fu affatto convinto, qualcuno parlò anche di revocare il vitalizio assegnato nel 1592, e si decise di tornare alla cifra delle caselle del Franceschi.

E qualche giorno dopo il CX inviò al nuovo Baylo il messaggio su riportato.

Non risultano più usate altre cifre del Partenio nei dispacci diplomatici.

ASVe – CCX Raccordi n.1 c.31 cifra 5 Partenio
ASVe – CX cifre, chiavi e scontri di cifra ... b,2 r. 13 Partenio, cifra A 100

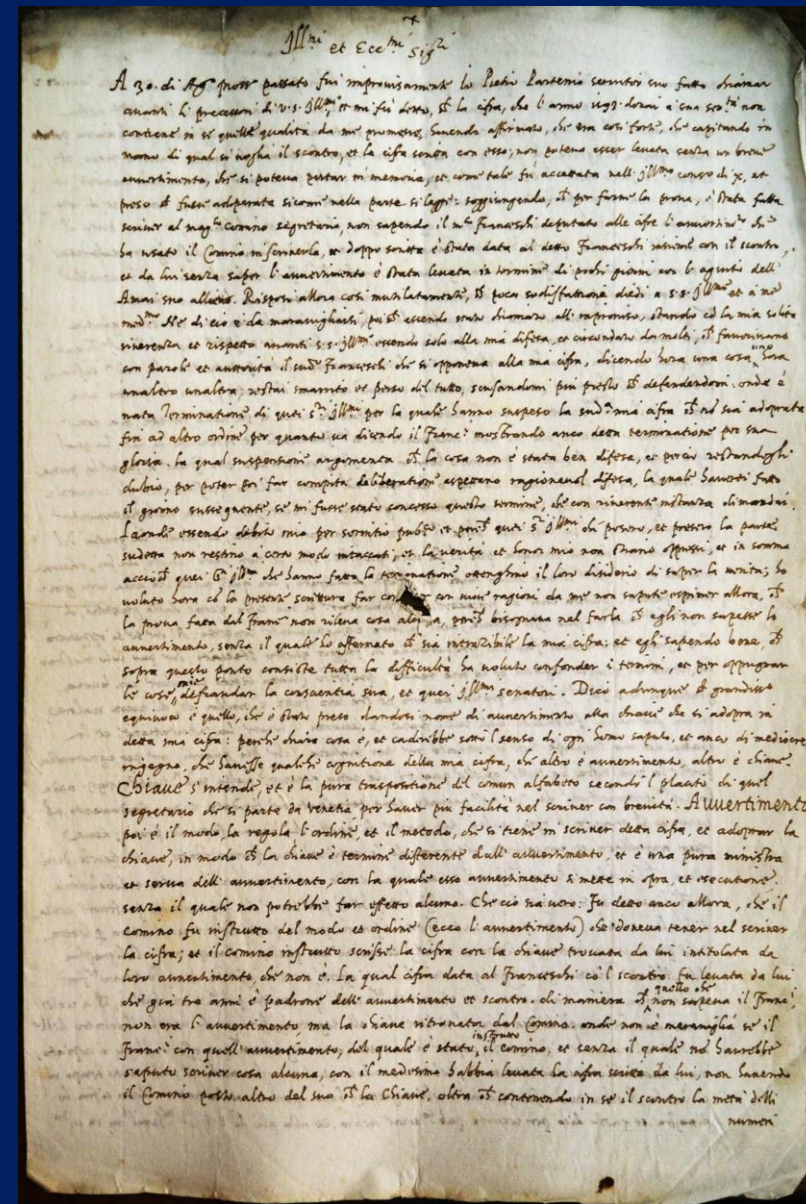


Partenio furioso ...

Dopo qualche giorno Partenio scrisse una lunghissima lettera al CX scusandosi per aver risposto in modo poco convincente, non avendo avuto tempo di riflettere sul problema.

Partenio parte al contrattacco, introducendo un nuovo argomento: la sua cifra era sicura a patto di non conoscere l'*auvertimento* e con questa parola intendendo non solo la tabellina ma anche le istruzioni per l'uso, il metodo.

La cosa è discutibile, oggi si accetta il principio di Kerckhoff, la sicurezza di una cifra deve basarsi solo sulla chiave non sulla conoscenza del metodo. D'altra parte questo principio è del XIX secolo, nei secoli precedenti fu ignorato sistematicamente.

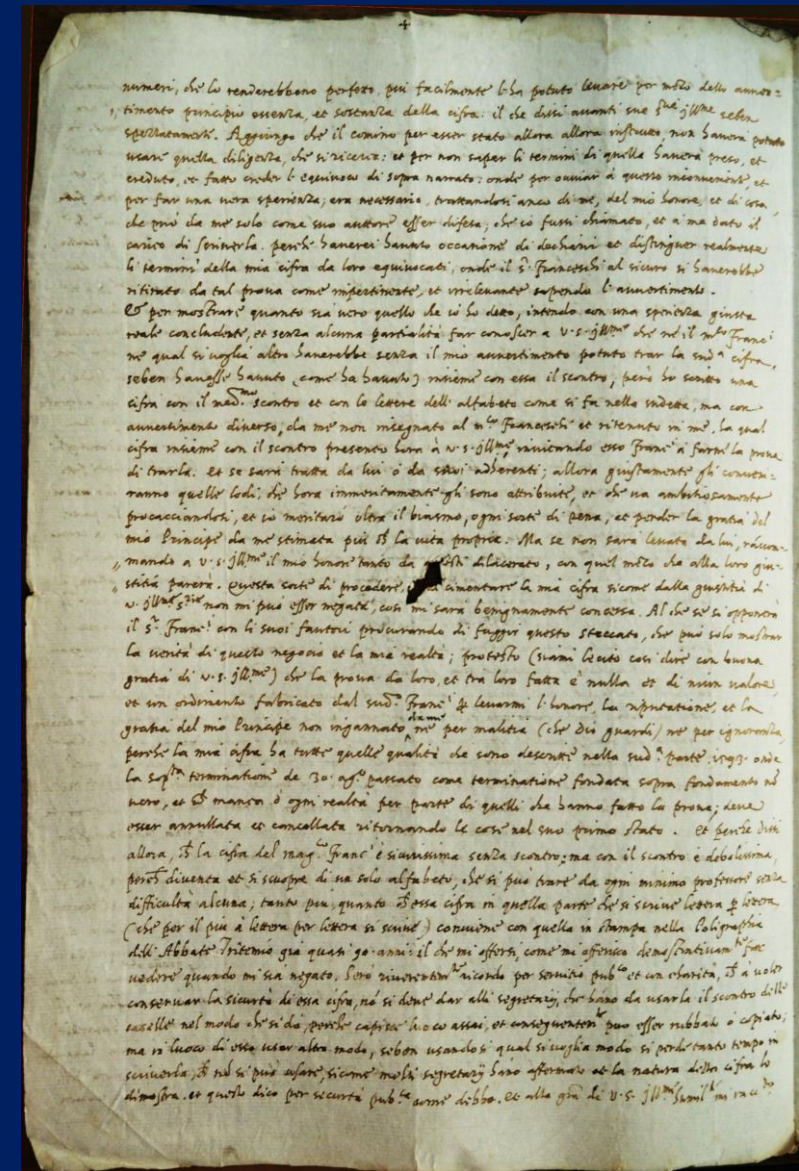


... e la polemica si fa aspra

Partenio continua con altre argomentazioni, per esempio che il segretario Comino non era stato istruito a sufficienza, e arriva a scrivere che

«la proua da loro fatta è nulla et di niun ualore et un ordimento fabricato dal sud^o Franceschi per leuarmi l'honore la riputatione et la gratiia del mio Principe»

Dopo di ché chiede l'annullamento del decreto del CX e conclude contestando la sicurezza della cifra delle caselle, che riconosce sicurissima senza lo scontro (la grata) ma con la grata «è debolissima perché si scuopre di un solo alfabeto, che di può trarre da ogni minimo professore senza difficoltà alcuna» e che tanto varrebbe usare «quella in stampa nella Poligraphia dell'Abbate Tritemio già quasi 90 anni»,



E tutto finisce nel nulla, perdono tutti!

Di fronte a questa lettera, il CX si riunisce di nuovo il 16 settembre 1596, e si spacca tra sostenitori del Franceschi e del Partenio.

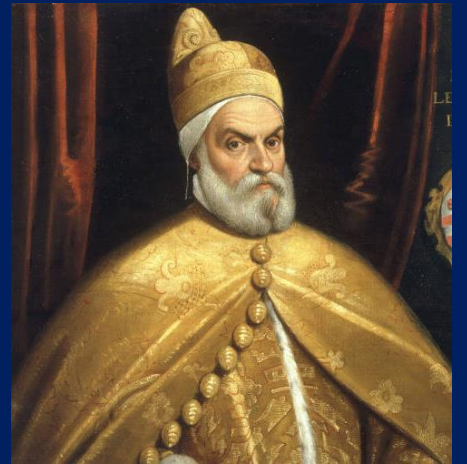
Per deliberare occorreva una maggioranza dei $\frac{3}{4}$, e alla fine essendo impossibile concludere qualcosa, le due cifre vennero entrambe sospese, e la decisione demandata a una commissione formata da cinque nobili, invitata ad esprimere un parere entro due mesi.

Vennero eletti Leonardo Donato (futuro doge dal 1605), Giacomo Foscarini, Paolo Paruta, Giovanni Soranzo e Nicolò Gussoni, tutti con esperienza di ambasciatori in varie sedi.

I cinque se la presero comoda se è vero che il 10 febbraio 1598 il CX prese atto di non aver ancora ricevuta una risposta e sollecitò i cinque; dopodiché di questa vicenda non si trovano altri documenti in archivio.



Marin Grimani



Leonardo Donà

Franceschi vs Partenio: conclusioni

- ▶ Franceschi ha il merito di aver introdotto la sovracifratura, con la cifra delle caselle, a mia conoscenza la prima cifra del genere ad essere stata effettivamente usata, essendo tutto sommato alla portata dei segretari.
- ▶ Partenio riprende l'idea di Franceschi ma insiste su chiavi di sovracifratura leggere e facili da ricordare a memoria o da ricostruire, e insiste molto sul fatto che in questo modo se anche lo scontro cade in mano al nemico, questi non potrà decrittare i dispacci cifrati. Un'idea questa in anticipo di due secoli, diverrà di uso comune solo nell'Ottocento.
- ▶ I pupilli di Franceschi e Partenio, Pietro Amai e Ottavian Medici tornarono ai normali noomenclatori in un solo passaggio, tanto familiari ai segretari.
- ▶ **L'età d'oro della crittografia veneziana era finita.**

Ma in definitiva Viète aveva veramente decrittato le cifre veneziane?

Per rispondere la cosa migliore è di fare riferimento all'articolo su Cryptologia di P. Pesic, dedicato alle abilità crittanalitiche del Viète.

Viète si era specializzato nel decrittare i nomenclatori con omofoni che erano le cifre di gran lunga più usate dalle diplomazie europee. E' quindi verosimile che possa aver decrittato la *ziffra prima* che abbiamo visto in precedenza.

Viceversa Pesic conclude che Viète non sembra aver avuto nozione delle cifre polialfabetiche tipo *Tritemio*, *Bellaso*, *Vigenere* che peraltro non furono quasi mai usate dalle diplomazie. Sembra quindi poco probabile che possa aver decrittato le caselle che comportavano una sovracifratura di tipo polialfabetico.

Quello di Viète fu forse un bluff, un ballon d'essai ...



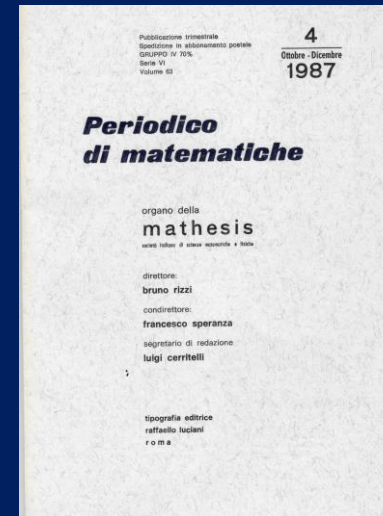
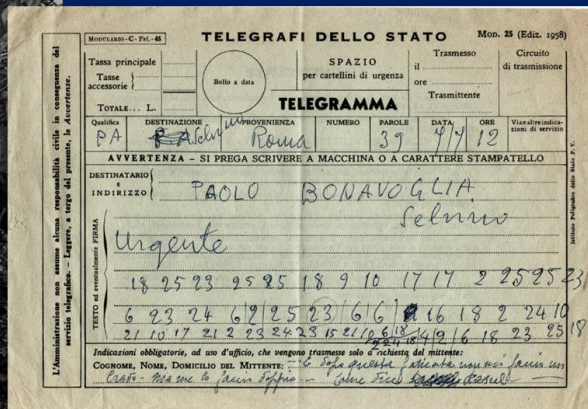
**Grazie per avermi
seguito fin qui!!**



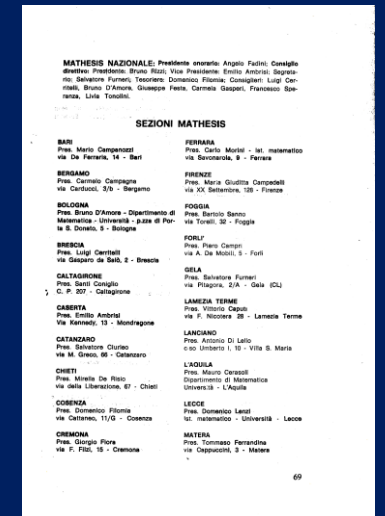
Roma 1947



Roma aprile 1955



Roma 1987



Luigia Berardi e Bruno Rizzi

**La funzione di Eulero torna alla ribalta
nei codici RSA: uno sguardo a questo settore**

Sommario: Un grande numero di messaggi viaggiano su canali elettronici: posta elettronica, telex, moneta elettronica, ordini e transazioni bancarie. Molti dati riservati sono archiviati in un computer. Sembra che l'unico modo di proteggere messaggi e dati da oscuri malintenzionati sia un buon prodotto (codice) crittografico al quale le Aziende devono ricorrere per proteggere la «privacy» sia essa individuale, commerciale o governativa. Gli Autori trattengono le più interessanti idee che il settore presenta.

Indice

1. Introduzione.
2. Molto rumore per niente: significati della parola « codice ».
3. - Non conosciamo i numeri primi: questa è proprio una brutta storia dice il Matematico teorico.
4. - Non conosciamo i numeri primi: meno male, ci possiamo fare, codice indecifrabile dice il Matematico applicato. Il codice RSA.
5. - Un Notale elettronico di nome RSA autentica i messaggi e permette la firma (elettronica) dei documenti.
6. - Potenza di una multinazionale: si impone commercialmente un codice standard, il Data Encryption Standard detto DES.
7. - Concludendo: un buon Vernam non si rifiuta mai, ovvero alla ricerca di nuove sequenze pseudocasuali.

Bibliografia minima

Bibliografia

- ▶ Ibrahim Al-Kadi. 1992. *Origins of Cryptology: the Arab Contributions*. Cryptologia, 16:2,97-126, Philadelphia, Pa. DOI: 10.1080/0161-119291866801
- ▶ Armand Baschet, *Les Archives de Venise - Histoire de la chancellerie secrète*, Henri Plon, Paris, 1870.
- ▶ Friedrich Ludwig Bauer, 1997. *Decrypted Secrets*. Springer, Berlin. ISBN: 3-540-24502-2
- ▶ Paolo Bonavoglia. 2019. *The Cifra delle Caselle, a superencrypted XVI Century Cipher*. Cryptologia, Philadelphia, Pa. DOI:10.1080/01611194.2019.1609132
- ▶ Paolo Bonavoglia. 2019. *Hieronimo di Franceschi and Pietro Partenio: Two Unknown Venetian Cryptologists*. Proceedings of the 2nd International Conference on Historical Cryptology, HistoCrypt 2019, June 23-26, 2019, Mons, Belgium
- ▶ David Kahn. 1967. *Codebreakers*. Scribner, New York, NY. ISBN: 978-0-684-83130-5
- ▶ Auguste Kerckhoffs. 1883. *La cryptographie militaire*. Paris.
- ▶ Luigi Pasini 1872, 2019. *Delle scritture in cifra usate nella Repubblica di Venezia*. Aracne, Roma ISBN: 978-88-255-1926-6
- ▶ Luigi Pasini. 1885. *Archivio di Stato di Venezia. Consiglio di Dieci - Cifre, Chiavi e Scontri di cifra ...*, a cura di L. Pasini e G. Giomo.
- ▶ Peter Pesic, *François Viète, father of modern cryptanalysis*, Cryptologia, Philadelphia, Pa
- ▶ Paolo Preto 1994. *I servizi segreti di Venezia*. EST, Milano
- ▶ Luigi Sacco. 1958, *Un primato italiano, la crittografia nei secoli XV e XVI*. Ist.Poligrafico dello Stato, Roma, Italy.

N3 N3

©1996-2020 PAOLO BONAVOGLIA -

La Crittografia da
Atbash a RSA

©2021 Paolo Bonavoglia

La Crittografia da Atbash a RSA

ENHANCED BY Google

LA

Crittografia classica

- Classificazione dei cifrari
- Cifrari per trasposizione.
 - Trasposizione a chiave
 - Griglia
- Cifrari monoalfabetici.
 - Omofoni
 - Polifoni
 - Dimensione variabile
- Cifrari polialfabetici.
 - Disco di L. B. Alberti
 - Tavola Tritemo
 - Tavola Bellaso (1553)
 - Tavola di Vigenère
 - Cifrario di Vernam
- Cifrari poligrafici.
- Cifrari composti (sovaccifratura)
- Codici e nomenclatori
 - Nomenclatori veneziani XVI-XVIII secolo
 - Il cifrario Mengarini
- Macchine cifranti.
 - Cilindro di Jefferson
 - Macchina Enigma
 - Macchina Lorenz
- Le sei regole di Kerckhoffs

Crittografia contemporanea

- Cifrari a chiave non riutilizzabile
- Cifrari a chiave segreta.
- Cifrari a chiave pubblica.

Steganografia

- Ave Maria del Tritemo
- Griglia di Cardano
- Cifrario di Francis Bacon

Crittanalisi

- Cifrari monoalfabetici
- Cifrari polialfabetici
- Crittanalisi automatica

Matematica per la Crittografia

- I Gruppi
- Le Aritmetiche finite (o modulari)
- Teoria dei numeri
- Statistica e lingue

La crittografia

Crittografia è parola di origine greca per *scrittura segreta*, si tratta quindi dell'arte di scrivere messaggi segreti che possano essere letti e compresi solo dal destinatario; una tecnica che risale alla più remota antichità, se già la Bibbia parla di un cifrario segreto per scrivere il nome di Babel (Atbash).

Per secoli la crittografia è stata appannaggio quasi esclusivo di militari e diplomatici, e i messaggi segreti viaggiavano materialmente affidati a corrieri fidati.

Tra XIX e XX secolo questo quadro è radicalmente cambiato: l'invenzione del telegrafo, del telefono e della radio hanno reso possibile la trasmissione pressoché istantanea di messaggi da un punto all'altro del globo terrestre; le comunicazioni via radio più ancora di quelle telefoniche sono esposte all'intercettazione da parte di estranei, di là la necessità di cifrare tutti i messaggi riservati trasmessi per radio.

Nella seconda metà del XX secolo l'invenzione del computer e di internet hanno cambiato in modo ancora più radicale lo scenario: i vecchi sistemi crittografici, manuali o macchine, sono diventati di colpo obsoleti vuoi per la facilità con la quale possono essere forzati con l'aiuto del computer, vuoi per la scomodità e lentezza d'uso.

La necessità di comunicare informazioni in modo riservato e quindi di cifrare i messaggi si è estesa ben al di là dell'ambito diplomatico-militare. Oggi chi preleva denaro con il Bancomat, chi effettua acquisti su internet con la carta di credito, chi fa una telefonata con il cellulare fa uso, spesso senza rendersene conto, di tecniche crittografiche.

Inevitabile in questo contesto la nascita di cifrari completamente nuovi come il DES della IBM e il rivoluzionario RSA capostipite dei cifrari a chiave pubblica, e all'inizio del XXI secolo il nuovo AES che ha sostituito il DES, ormai obsoleto.

Storia della crittografia

- Il cifrario Atbash
- Il cifrario di Cesare
- Il Rinascimento
 - Repubblica di Venezia
 - Leon Battista Alberti
 - Le cifre di G.B. Bellaso
 - Blaise de Vigenère
- La I guerra mondiale
 - Il taccuino di Luigi Sacco (1916)
- Il cifrario di Vernam
- La II guerra mondiale
- La crittografia nell'era del computer
- I grandi nomi della storia della crittografia

Varie

- Cronistoria di questo ipertesto
- Bibliografia
- Questo ipertesto è dedicato a Luigi Sacco.

Aggiornamenti e notizie

Conferenza internazionale di crittografia storica 2021, Amsterdam, 20-22 settembre

- HistoCrypt 2021 – International Conference on Historical Cryptology

Conferenza internazionale di crittografia storica 2020, Budapest, 15-17 giugno

- HistoCrypt 2020 – International Conference on Historical Cryptology (Conferenza annullata per la pandemia Covid)
- Proceedings (Atti)

Precedenti conferenze internazionali di crittografia storica

Risolto l'enigma della Cifra delle caselle

- La cifra delle caselle di Hieronimo di Franco
- La cifra delle caselle in dettaglio

Ritrovata a Venezia la cifra di G.B. Bellaso del 1552

- La cifra zero di G.B. Bellaso

Conferenza internazionale di crittografia storica 2018, Uppsala

- HistoCrypt 2018 – International Conference on Historical Cryptology, in Uppsala
- A video of Klaus Schmeh and many photos
- Foto della conferenza (Google Foto)

Convegno europeo di cifre storiche 2017, Smolenice

- European HCC 2017 – Smolenice – galleria
- European Historical Ciphers Colloquium 2017 – Smolenice
- Programma (18-19 maggio 2017)

Decrittato dopo un secolo e mezzo l'ultimo poema di Pietro Giannone

- Decrittato l'ultimo poema di Pietro Giannone
- Come ho forzato il codice di Giannone

I cifrari di Antonio Marzi

- I messaggi cifrati di Antonio Marzi partigiano e informatore degli inglesi nella II guerra mondiale
- Archivio cifrati di Antonio Marzi 1945

STORIA DELLA CRIPTOGRAFIA – CIPRANI – CIPRANI POLJAK – LE CIBRE DI G. B. BELLASO

Cifra Bellaso del 1553

LA CIBRA ZERO DI BELLASO 1552 - TAVOLA BELLASO 1555 - TAVOLA BELLASO 1564 - TAVOLA DELLA PORTA

Giouan Battista Bellaso pubblicò il 21 luglio 1553 un opuscolo con una cifra di sua invenzione, che dice derivata da quella presentata l'anno precedente 1552 a diversi illustri personaggi tra i quali Girolamo Ruscelli, umanista poligrafo, che si era occupato anche di cifre, come scrive nella prefazione dedicata allo stesso Ruscelli:

«...[I]t così l'anno a dietro essendo io in Venetia opera col mezzo de' molto illustri Signori il Signor Conte Giouan Francesco da Cambrara, et il Sig. Conte Paolo Auogadro, di venire a conoscere V.S. e senza manifestarmi per autore di quella mia Cifra, feci che quei Signori gliela mostraron, et le fecero uedere il modo d'usarla, facendola scrivere da un fanciullo, senza pur mirar nella contra cifra, la quale hauea tutta a mente. [...]Percheché essendosi l'anno passato stampate una quantità di dette mie cifre in una sola facciata d'un foglio, senza il modo d'usarla, sono già distribuite tutte, et ogni giorno me ne sono con lettere et a bocca richieste da ogni parte, et non trouandome delle stampate mi conuene di continuo parlar fastidio in farne a penna. La onde a preghi et consigli di molti, et per mio minor fastidio, mi sono risoluto di farne ristampare per comune satisfactione, et seruiro de Principi Crisiani, et holla oltre a ciò ridotta alla quarta parte di quello che era prima, et a tanta breuita et ageuolezza, che una sola ristorta d'occhio la comprende tutta, che potrebbesi ancora in breuissimo spatio di tempo imparare a mente [...]»

Insia bellezza, che tutto il modo potrà usarla, & intendimento, l'uno non potrà leggere quello che scrue l'altro; se no; s; come in questo medesimo foglio s'insiega, insieme con la sua dichiarazione, & col modo d'adoperarla.

di uno dei primi esempi di cifra polialfabetica, preceduto solo dal trattato di L. B. Alberti, che non era ancora slaso introduce l'idea di una parola chiave da scrivere ripetutamente sotto o sopra il testo chiaro. Quindi ha

da concordare tra i due corrispondenti e da scrivere sotto il testo chiaro lettera per lettera come in questo rende come contrassegno **Virtuti omnia parent** e come testo chiaro: "L'armata turческа partirà a cinque di

al libro. Vedi i dettagli nella procedura di cifra qui sotto.

dalla prima metà dell'alfabeto ordinata, e dalla seconda metà scritta in modo ordinato, ma spostato di qualche di lettere che faranno vicendevolmente il ruolo di cifra/decifra. Nell'esempio a destra, che è quello originale di 1, 6, 2, 7, 3, 8, 9, 4, 10, che ricadde nella prima parte la tavola del 1552.

di una o più parole; Bellaso scrive che la lunghezza "non importa" ma vale sempre la regola: più lungo il verme,

rme ripetuto a sufficienza, per ogni lettera del chiaro e del verme, cercare nella tavola la riga con la lettera del a lettera accoppiata, sotto o sopra.

chiamo nella riga VX la lettera del chiaro L e sotto la L troviamo S; la cifra quindi è S. Continuando si ottiene:

ica, usando liste involutorie, che sono vicendevolmente cifra/decifra dell'altra; in altri termini la procedura di cifra è identica a quella di decifra; per decifrare quindi si

STORIA DELLA CRIPTOGRAFIA – MACCHINE CIPRANI

Macchina Hagelin RT (Random Tape)

Macchina Hagelin RT (RT sta per *Random Tape* = nastro casuale) fu prodotta negli anni Cinquanta del Novecento dalla Hagelin Cryptos come Crypto AC. Le immagini a lato sono quelle dell'esemplare in possesso del Ministero Affari Esteri (Farnesina) a Roma, che fu esposta alla mostra del maggio 2015.

di una macchina che realizza in pieno il cifrario di Vernam. Cuore del sistema è il nastro perforato a 5 fori (usa quindi il codice Baudot),

vere generano con un procedimento casuale; in questo caso veniva usato un procedimento chimico che dava fori distribuiti in modo

le cose funzionano come segue:

rispondenti, per esempio il ministro **M** e il diplomatico **D** destinato all'un'ambasciata, si scambiano all'inizio due nastri identici e due

ne identiche.

un messaggio ad **M** posizionando il nastro nell'ultima posizione usata e scrivendo il messaggio con la tastiera collegata al modulo, ogni viene tradotta in un codice Baudot che viene sommato (addizione XOR) al corrispondente codice del nastro casuale. la somma dà il

e cifrato da trasmettere.

il messaggio così cifrato e non fa altro che inserirlo nella macchina gemella in parallelo al nastro identico; la macchina fa nuovamente

one XOR tra il cifrato e nastro e riottiene il messaggio originale.

il nastro è finito, occorre generare uno nuovo in due copie identiche e trasportarlo in modo sicuro dal ministero all'ambasciata.

STORIA DELLA CRIPTOGRAFIA – CIPRANI – CIPRANI POLJAK – LE CIBRE DI G. B. BELLASO

Cifra Bellaso del 1553

LA CIBRA ZERO DI BELLASO 1552 - TAVOLA BELLASO 1555 - TAVOLA BELLASO 1564 - TAVOLA DELLA PORTA

Giouan Battista Bellaso pubblicò il 21 luglio 1553 un opuscolo con una cifra di sua invenzione, che dice derivata da quella presentata l'anno precedente 1552 a diversi illustri personaggi tra i quali Girolamo Ruscelli, umanista poligrafo, che si era occupato anche di cifre, come scrive nella prefazione dedicata allo stesso Ruscelli:

«...[I]t così l'anno a dietro essendo io in Venetia opera col mezzo de' molto illustri Signori il Signor Conte Giouan Francesco da Cambrara, et il Sig. Conte Paolo Auogadro, di venire a conoscere V.S. e senza manifestarmi per autore di quella mia Cifra, feci che quei Signori gliela mostraron, et le fecero uedere il modo d'usarla, facendola scrivere da un fanciullo, senza pur mirar nella contra cifra, la quale hauea tutta a mente. [...]Percheché essendosi l'anno passato stampate una quantità di dette mie cifre in una sola facciata d'un foglio, senza il modo d'usarla, sono già distribuite tutte, et ogni giorno me ne sono con lettere et a bocca richieste da ogni parte, et non trouandome delle stampate mi conuene di continuo parlar fastidio in farne a penna. La onde a preghi et consigli di molti, et per mio minor fastidio, mi sono risoluto di farne ristampare per comune satisfactione, et seruiro de Principi Crisiani, et holla oltre a ciò ridotta alla quarta parte di quello che era prima, et a tanta breuita et ageuolezza, che una sola ristorta d'occhio la comprende tutta, che potrebbesi ancora in breuissimo spatio di tempo imparare a mente [...]»

Insia bellezza, che tutto il modo potrà usarla, & intendimento, l'uno non potrà leggere quello che scrue l'altro; se no; s; come in questo medesimo foglio s'insiega, insieme con la sua dichiarazione, & col modo d'adoperarla.

di uno dei primi esempi di cifra polialfabetica, preceduto solo dal trattato di L. B. Alberti, che non era ancora slaso introduce l'idea di una parola chiave da scrivere ripetutamente sotto o sopra il testo chiaro. Quindi ha

da concordare tra i due corrispondenti e da scrivere sotto il testo chiaro lettera per lettera come in questo rende come contrassegno **Virtuti omnia parent** e come testo chiaro: "L'armata turческа partirà a cinque di

al libro. Vedi i dettagli nella procedura di cifra qui sotto.

dalla prima metà dell'alfabeto ordinata, e dalla seconda metà scritta in modo ordinato, ma spostato di qualche di lettere che faranno vicendevolmente il ruolo di cifra/decifra. Nell'esempio a destra, che è quello originale di 1, 6, 2, 7, 3, 8, 9, 4, 10, che ricadde nella prima parte la tavola del 1552.

di una o più parole; Bellaso scrive che la lunghezza "non importa" ma vale sempre la regola: più lungo il verme,

rme ripetuto a sufficienza, per ogni lettera del chiaro e del verme, cercare nella tavola la riga con la lettera del a lettera accoppiata, sotto o sopra.

chiamo nella riga VX la lettera del chiaro L e sotto la L troviamo S; la cifra quindi è S. Continuando si ottiene:

ica, usando liste involutorie, che sono vicendevolmente cifra/decifra dell'altra; in altri termini la procedura di cifra è identica a quella di decifra; per decifrare quindi si

STORIA DELLA CRIPTOGRAFIA – MACCHINE CIPRANI

Macchina Hagelin RT (Random Tape)

Macchina Hagelin RT (RT sta per *Random Tape* = nastro casuale) fu prodotta negli anni Cinquanta del Novecento dalla Hagelin Cryptos come Crypto AC. Le immagini a lato sono quelle dell'esemplare in possesso del Ministero Affari Esteri (Farnesina) a Roma, che fu esposta alla mostra del maggio 2015.

di una macchina che realizza in pieno il cifrario di Vernam. Cuore del sistema è il nastro perforato a 5 fori (usa quindi il codice Baudot),

vere generano con un procedimento casuale; in questo caso veniva usato un procedimento