

# Franceschi vs Partenio

Una disputa crittografica  
nella Venezia del Cinquecento



A grid of numbers and letters, likely a cipher key or table, with a red border around the right side:

Grid A		Grid B		Grid C		Grid D		Grid E		Grid F		Grid G		Grid H		Grid I		Grid J		Grid K		Grid L		Grid M		Grid N		Grid O		Grid P		Grid Q		Grid R		Grid S	
101	A	102	B	103	C	104	D	105	E	106	F	107	G	108	H	109	I	110	J	111	K	112	L	113	M	114	N	115	O	116	P	117	Q	118	R	119	S
121	aa	122	ab	123	ac	124	ad	125	ae	126	af	127	ag	128	ah	129	ai	130	aj	131	ak	132	al	133	am	134	an	135	ao	136	ap	137	aq	138	ar	139	as
141	aa	142	ab	143	ac	144	ad	145	ae	146	af	147	ag	148	ah	149	ai	150	aj	151	ak	152	al	153	am	154	an	155	ao	156	ap	157	aq	158	ar	159	as
161	aa	162	ab	163	ac	164	ad	165	ae	166	af	167	ag	168	ah	169	ai	170	aj	171	ak	172	al	173	am	174	an	175	ao	176	ap	177	aq	178	ar	179	as
181	aa	182	ab	183	ac	184	ad	185	ae	186	af	187	ag	188	ah	189	ai	190	aj	191	ak	192	al	193	am	194	an	195	ao	196	ap	197	aq	198	ar	199	as
201	aa	202	ab	203	ac	204	ad	205	ae	206	af	207	ag	208	ah	209	ai	210	aj	211	ak	212	al	213	am	214	an	215	ao	216	ap	217	aq	218	ar	219	as
221	aa	222	ab	223	ac	224	ad	225	ae	226	af	227	ag	228	ah	229	ai	230	aj	231	ak	232	al	233	am	234	an	235	ao	236	ap	237	aq	238	ar	239	as
241	aa	242	ab	243	ac	244	ad	245	ae	246	af	247	ag	248	ah	249	ai	250	aj	251	ak	252	al	253	am	254	an	255	ao	256	ap	257	aq	258	ar	259	as
261	aa	262	ab	263	ac	264	ad	265	ae	266	af	267	ag	268	ah	269	ai	270	aj	271	ak	272	al	273	am	274	an	275	ao	276	ap	277	aq	278	ar	279	as
281	aa	282	ab	283	ac	284	ad	285	ae	286	af	287	ag	288	ah	289	ai	290	aj	291	ak	292	al	293	am	294	an	295	ao	296	ap	297	aq	298	ar	299	as
291	aa	292	ab	293	ac	294	ad	295	ae	296	af	297	ag	298	ah	299	ai	300	aj	301	ak	302	al	303	am	304	an	305	ao	306	ap	307	aq	308	ar	309	as
311	aa	312	ab	313	ac	314	ad	315	ae	316	af	317	ag	318	ah	319	ai	320	aj	321	ak	322	al	323	am	324	an	325	ao	326	ap	327	aq	328	ar	329	as
331	aa	332	ab	333	ac	334	ad	335	ae	336	af	337	ag	338	ah	339	ai	340	aj	341	ak	342	al	343	am	344	an	345	ao	346	ap	347	aq	348	ar	349	as
351	aa	352	ab	353	ac	354	ad	355	ae	356	af	357	ag	358	ah	359	ai	360	aj	361	ak	362	al	363	am	364	an	365	ao	366	ap	367	aq	368	ar	369	as
371	aa	372	ab	373	ac	374	ad	375	ae	376	af	377	ag	378	ah	379	ai	380	aj	381	ak	382	al	383	am	384	an	385	ao	386	ap	387	aq	388	ar	389	as
391	aa	392	ab	393	ac	394	ad	395	ae	396	af	397	ag	398	ah	399	ai	400	aj	401	ak	402	al	403	am	404	an	405	ao	406	ap	407	aq	408	ar	409	as
411	aa	412	ab	413	ac	414	ad	415	ae	416	af	417	ag	418	ah	419	ai	420	aj	421	ak	422	al	423	am	424	an	425	ao	426	ap	427	aq	428	ar	429	as
431	aa	432	ab	433	ac	434	ad	435	ae	436	af	437	ag	438	ah	439	ai	440	aj	441	ak	442	al	443	am	444	an	445	ao	446	ap	447	aq	448	ar	449	as
451	aa	452	ab	453	ac	454	ad	455	ae	456	af	457	ag	458	ah	459	ai	460	aj	461	ak	462	al	463	am	464	an	465	ao	466	ap	467	aq	468	ar	469	as
471	aa	472	ab	473	ac	474	ad	475	ae	476	af	477	ag	478	ah	479	ai	480	aj	481	ak	482	al	483	am	484	an	485	ao	486	ap	487	aq	488	ar	489	as
491	aa	492	ab	493	ac	494	ad	495	ae	496	af	497	ag	498	ah	499	ai	500	aj	501	ak	502	al	503	am	504	an	505	ao	506	ap	507	aq	508	ar	509	as
511	aa	512	ab	513	ac	514	ad	515	ae	516	af	517	ag	518	ah	519	ai	520	aj	521	ak	522	al	523	am	524	an	525	ao	526	ap	527	aq	528	ar	529	as
531	aa	532	ab	533	ac	534	ad	535	ae	536	af	537	ag	538	ah	539	ai	540	aj	541	ak	542	al	543	am	544	an	545	ao	546	ap	547	aq	548	ar	549	as
551	aa	552	ab	553	ac	554	ad	555	ae	556	af	557	ag	558	ah	559	ai	560	aj	561	ak	562	al	563	am	564	an	565	ao	566	ap	567	aq	568	ar	569	as
571	aa	572	ab	573	ac	574	ad	575	ae	576	af	577	ag	578	ah	579	ai	580	aj	581	ak	582	al	583	am	584	an	585	ao	586	ap	587	aq	588	ar	589	as
591	aa	592	ab	593	ac	594	ad	595	ae	596	af	597	ag	598	ah	599	ai	600	aj	601	ak	602	al	603	am	604	an	605	ao	606	ap	607	aq	608	ar	609	as
611	aa	612	ab	613	ac	614	ad	615	ae	616	af	617	ag	618	ah	619	ai	620	aj	621	ak	622	al	623	am	624	an	625	ao	626	ap	627	aq	628	ar	629	as
631	aa	632	ab	633	ac	634	ad	635	ae	636	af	637	ag	638	ah	639	ai	640	aj	641	ak	642	al	643	am	644	an	645	ao	646	ap	647	aq	648	ar	649	as
651	aa	652	ab	653	ac	654	ad	655	ae	656	af	657	ag	658	ah	659	ai	660	aj	661	ak	662	al	663	am	664	an	665	ao	666	ap	667	aq	668	ar	669	as
671	aa	672	ab	673	ac	674	ad	675	ae	676	af	677	ag	678	ah	679	ai	680	aj	681	ak	682	al	683	am	684	an	685	ao	686	ap	687	aq	688	ar	689	as
691	aa	692	ab	693	ac	694	ad	695	ae	696	af	697	ag	698	ah	699	ai	700	aj	701	ak	702	al	703	am	704	an	705	ao	706	ap	707	aq	708	ar	709	as
711	aa	712	ab	713	ac	714	ad	715	ae	716	af	717	ag	718	ah	719	ai	720	aj	721	ak	722	al	723	am	724	an	725	ao	726	ap	727	aq	728	ar	729	as
731	aa	732	ab	733	ac	734	ad	735	ae	736	af	737	ag	738	ah	739	ai	740	aj	741	ak	742	al	743	am	744	an	745	ao	746	ap	747	aq	748	ar	749	as
751	aa	752	ab	753	ac	754	ad	755	ae	756	af	757	ag	758	ah	759	ai	760	aj	761	ak	762	al	763	am	764	an	765	ao	766	ap	767	aq	768	ar	769	as
771	aa	772	ab	773	ac	774	ad	775	ae	776	af	777	ag	778	ah	779	ai	780	aj	781	ak	782	al	783	am	784	an	785	ao	786	ap	787	aq	788			

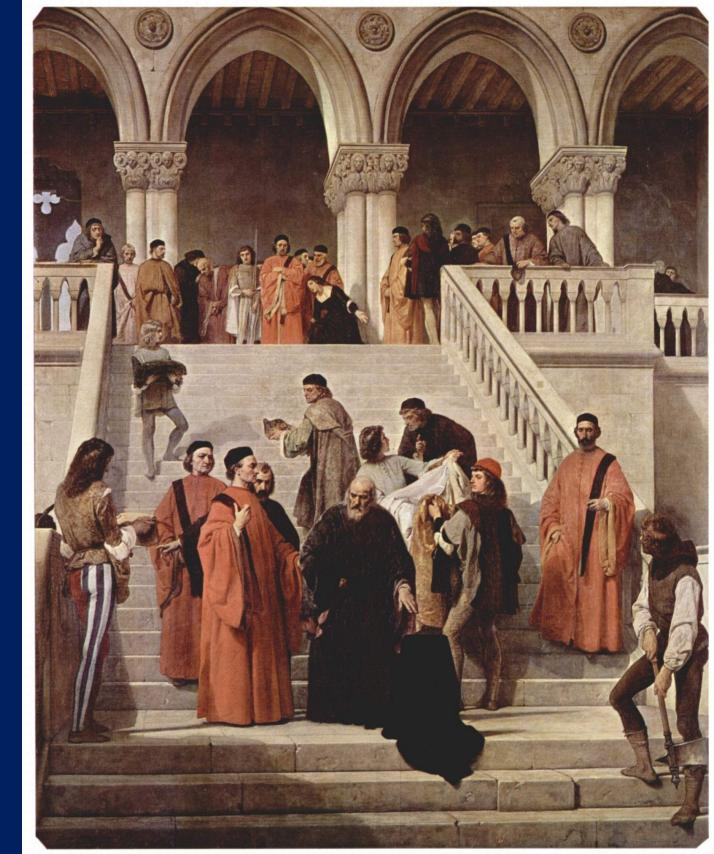
# Una ricerca su fonti primarie (Archivio di Stato di Venezia)

Questa ricerca sulla storia della crittografia veneziana è iniziata nel febbraio 2018 ed è ripresa nel 2021 dopo la pandemia, presso l'Archivio di Stato di Venezia.

The screenshot shows the official website of the Archivio di Stato di Venezia. At the top left is the logo of the Ministry of Culture (MC) with the text "MINISTERO DELLA CULTURA". Below it is the specific logo for the Archivio di Stato di Venezia. The main navigation menu includes "Home", "Chi siamo", "Servizi al pubblico", "Patrimonio", "Scuola APD", "Notizie", and "Come fare per". A large image of a long, narrow room filled with floor-to-ceiling wooden bookshelves is displayed. In the bottom left corner of the image, there is a caption in white text: "Deposito monumentale (cosiddetto Braccio dei Dieci savi)".



# Il Consiglio di Dieci (CX)



I Dieci in un dipinto ottocentesco di F. Hayez

Il Consiglio di Dieci (Cons<sup>o</sup> di X o CX) era il tribunale della Serenissima Repubblica che si occupava della sicurezza, dello spionaggio e della crittografia: nominava, previa prova di ammissione, i segretari deputati alle cifre (*Ziffre*), incaricati di cifrare e decifrare i dispacci diplomatici e militari; alcuni poi progettavano cifre e decrittavano dispacci cifrati alieni intercettati.

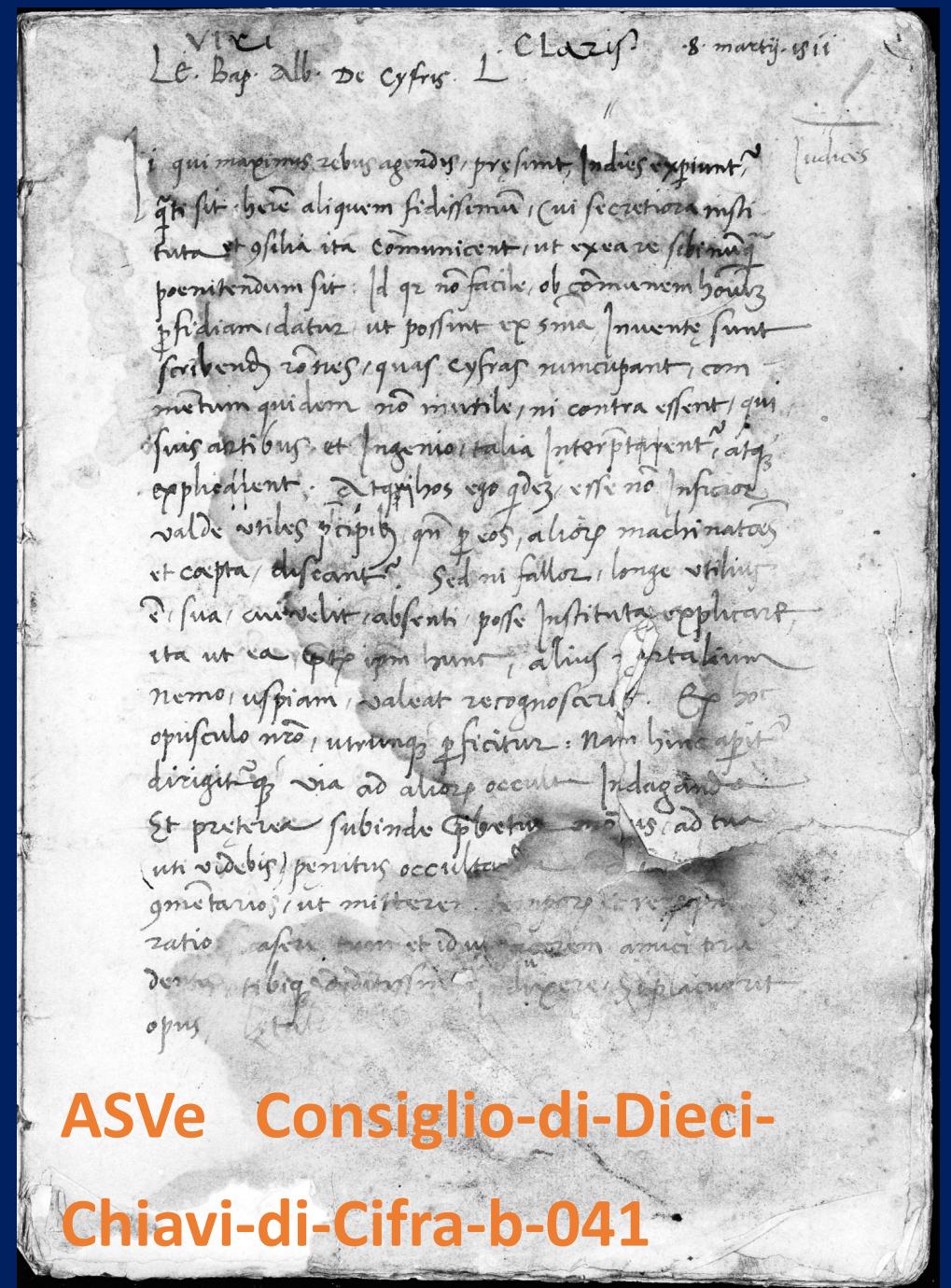
Era formato di dieci membri effettivi eletti dal Maggior Consiglio.

Ai dieci si aggiungevano di diritto il Doge e i sei consiglieri ducali, portando il totale a 17 come i posti visibili nella sala di riunione ancor oggi visitabile all'interno del Palazzo Ducale. Gli scranni furono razziati dalle truppe francesi nel 1797 anno della fine della Serenissima Repubblica.

# Il *De Cifris* di Leon Battista Alberti

Leon Battista Alberti, architetto e umanista nella letteratura crittografica viene citato soprattutto per il disco cifrante introdotto alla fine del suo opuscolo *De Cyfris*, e si legge che quest'opera rimase sconosciuta fino al 1568, quando fu pubblicata a stampa a Venezia.

Ma esistevano diversi manoscritti tre dei quali a Venezia ... e i cifristi veneziani lo conoscevano bene fin dal 1511 almeno.



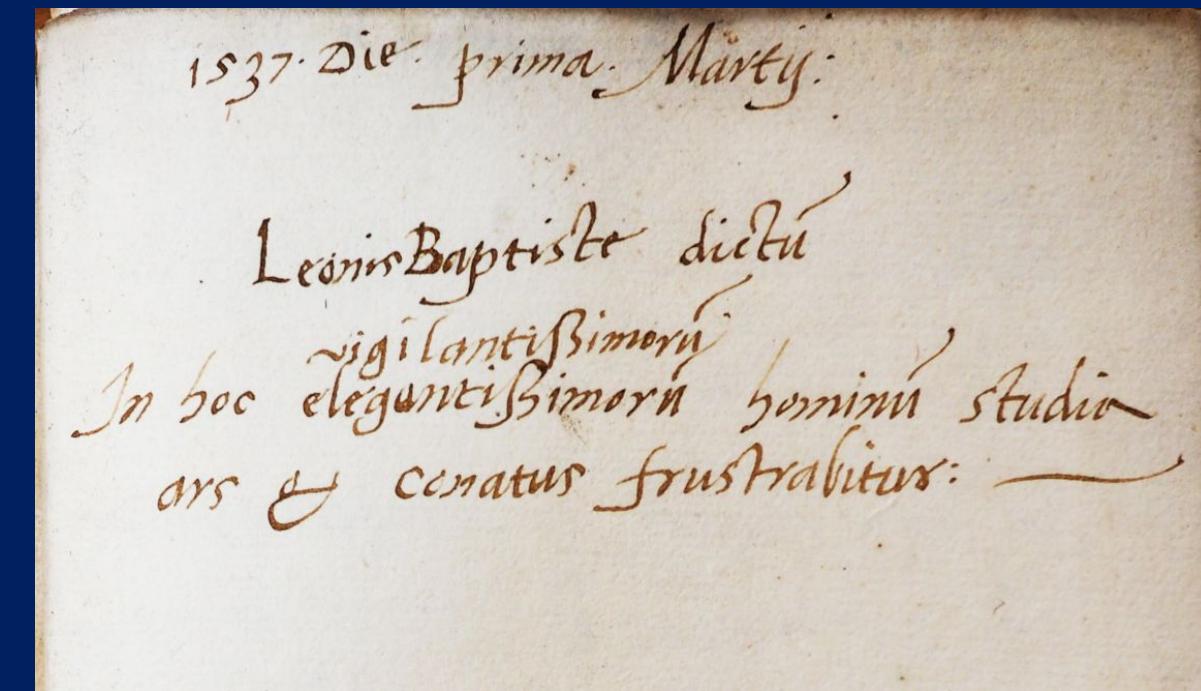
ASVe Consiglio-di-Dieci-  
Chiavi-di-Cifra-b-041

# Leon Battista Alberti e i cifristi veneziani

... e i cifristi veneziani lo conoscevano bene fin dal 1511 almeno, quando Zuan Soro annunciò il suo proposito di scrivere un trattato delle cifre.

Non per il disco ma per la crittanalisi!

I successori di Soro, Z. Ludovici, A. Borghi, Z.F. Marin lo menzionano spesso e sviluppano le sue idee portandole molto avanti fino al trattato delle cifre “*Del modo de extrazer le ziffre*” di Z. F. Marin molto ampio e molto tecnico.



ASVe Consiglio-di-Dieci-  
Chiavi-di-Cifra-b.6

# Finita l'era dei grandi crittanalisti si cercano nuovi più sicuri sistemi

Già il Borghi a metà del secolo si vantava, lui e gli altri crittanalisti Ludovici e Marin di essere in grado di decrittare qualsiasi messaggio cifrato in qualsiasi lingua.  
Era un'esagerazione o no?

Nasceva la domanda “Se a Venezia siamo in grado di farlo è verosimile che anche altri principi dispongano o disporranno presto di persone in grado di fare lo stesso”.  
(in effetti in Francia il re Enrico IV lo troverà in Francois Viète)

E quindi bisognerà inventarsi nuovi più sicuri metodi. Ovvero nuove cifre.

Franceschi e Partenio partono da questo stesso dubbio ma giungono a conclusioni diametralmente opposte.

# XVI secolo Cinquecento

In effetti già Alberti, Tritemio, Bellaso, Porta avevano presentato cifre **polialfabetiche** dette anche **cifre con chiave**, come cifre fortissime impossibili da decrittare ...

eppure le cancellerie italiane ed europee ...

I continuaron ad usare il vecchio e collaudato **nomenclatore** (detto anche **repertorio**, o se molto grande **codice**) ,

Come mai?

# Polialfabetico vs Nomenclatore

[...] Questo spiega l'elogio di Matteo: "**La cifra con chiave** è la più nobile e la più grande del mondo, la più sicura e fedele che mai vi fu uomo che potesse scoprirla".

*Perché, allora, il nomenclatore ha regnato sovrano per 300 anni dopo Porta?  
Perché i crittografi non hanno utilizzato questo cifrario "più nobile" e "più sicuro"?*

A quanto pare, perché non apprezzavano la sua lentezza e diffidavano della sua accuratezza. La cifratura in un sistema polialfabetico, con la necessità di tenere traccia di quale alfabeto fosse in uso in ogni momento e di assicurarsi che la lettera del testo cifrato fosse presa da quell'alfabeto, non poteva essere paragonata in velocità a una cifratura con nomenclatore..

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

# Franceschi vs Partenio un caso a ruoli invertiti

[...] Il caso che esamineremo è quello di Venezia dove si svolse un simile dibattito, ma a ruoli invertiti:

- Hieronimo di Franceschi, un professionista, segretario della Cancelleria Ducale e del Senato, era il sostenitore del cifrario polialfabetico che chiamava *ziffra uera* e accanito avversario dei vecchi cifrari, i nomenclatori, dove ogni segno ha una decifrazione unica.
- Pietro Partenio era viceversa un dilettante delle cifre, un notaio privato, che a 52 anni si presentò al CX come paladino dei nomenclatori, disprezzando la codifica lettera per lettera come nelle cifre del Tritemio, vecchie di 90 anni.

Entrambi erano peraltro d'accordo nel considerare non sicuri i cifrari utilizzati in quegli anni e nel promuoverne di nuovi.

# La lingua italiana del XVI secolo

- Uno dei grossi problemi è che l'italiano (qui idioma veneto) del Cinquecento presenta differenze sia a livello ortografico, sia a livello semantico; alcuni esempi che è qui importante ricordare:

## Ortografia:

- **V u** c'era una sola lettera V maiuscola e u minuscola che si pronunciava a volte come vocale, a volte come consonante: *uenire Venetia*
- **H** il verbo avere si scrive sempre, come in latino, con la H iniziale, e così molte altre parole: *hauendo, hauere, hoggi, hora ...*
- **T** invece di **Z** *institution, constitution ...*
- **Z** invece di **G o C**: *zente, zennaro, zugno; ziffra, Franzia*

## Semantica:

- **scontro**: non è un incidente stradale, ma il foglio di *riscontro* di una cifra: scontro di cifra
- **esso**: è usato nel senso di questo, quello: *esso Partenio*
- **parte**: delibera, le parti del Cons<sup>o</sup> di X sono ordinanze esecutive.

# Ma che cosa è un nomenclatore?

Bruxelles dispaccio cifrato dell'ambasciatore veneziano in Spagna sulla imminente presa di Calais, ancora sotto dominio inglese, da parte dei francesi.

Raphias.

139

310

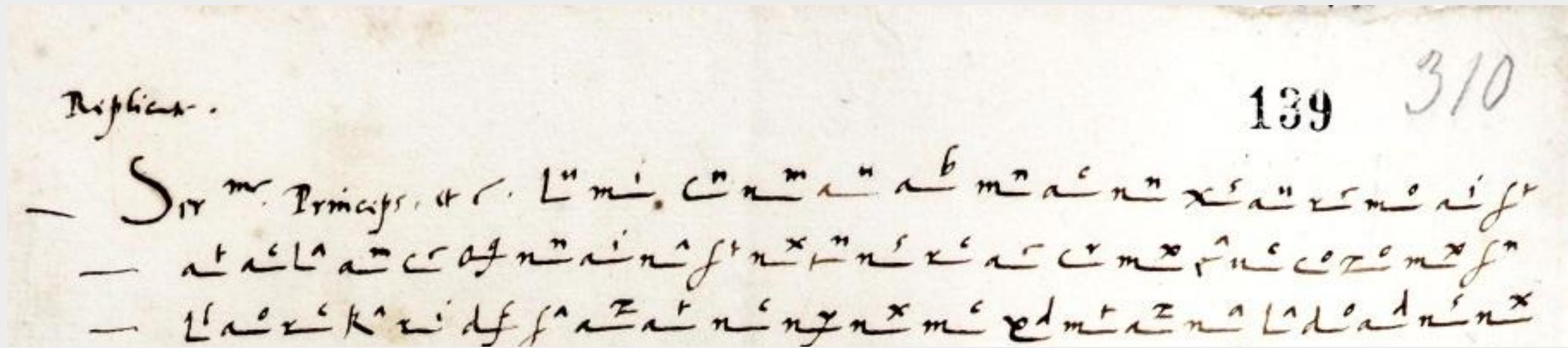
— سریں پرنسپلز اور لائیٹنگ کمپنیز کے مالکوں کے تھے۔  
— اس کی بحث کے لئے اس کے مالکوں کے تھے۔  
— اس کی بحث کے لئے اس کے مالکوں کے تھے۔  
— اس کی بحث کے لئے اس کے مالکوں کے تھے۔  
— اس کی بحث کے لئے اس کے مالکوں کے تھے۔  
— اس کی بحث کے لئے اس کے مالکوں کے تھے۔

# Ma che cosa è un nomenclatore?

Si cifra lettera per **lettera**, ma anche per **sillaba**, per **gruppo** di lettere e per **parola**

**Lu mi cn nm au ab mn ac nn xs au re mo ai ft at ac La am ce oq nn ai na ft nx tn**  
**quest a ma tti na e spa r sa u na uo ce per la co r te se n za sa per si la o ri**

Questa mattina è sparsa una uoce per la corte senza sapersi la ori[gine]



Ma che cosa è un nomenclatore?

# *La cifra usata nel 1557 pag.1*

Omofoni



Alfabeto																									
a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	z						
a <sup>a</sup>	o <sup>a</sup>	o <sup>p</sup>	R <sup>c</sup>	a <sup>b</sup>	m <sup>z</sup>	L <sup>p</sup>	g <sup>h</sup>	a <sup>o</sup>	t <sup>m</sup>	e <sup>c</sup>	c <sup>e</sup>	r <sup>a</sup>	R <sup>e</sup>	a <sup>c</sup>	R <sup>a</sup>	g <sup>f</sup>	c <sup>p</sup>	E <sup>s</sup>							
m <sup>i</sup>				n <sup>c</sup>				n <sup>o</sup>		e <sup>s</sup>	n <sup>x</sup>		u <sup>o</sup>						x <sup>s</sup>						
c <sup>x</sup>				z <sup>z</sup>																					

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	fra	fre	fri	fro	fru
e <sup>r</sup>	Z <sup>o</sup>	g <sup>s</sup>	g <sup>i</sup>	r <sup>p</sup>	L <sup>e</sup>	m <sup>o</sup>	n <sup>r</sup>	a <sup>t</sup>	x <sup>b</sup>	...	L <sup>n</sup>	x <sup>p</sup>	m <sup>d</sup>	f <sup>y</sup>	c <sup>o</sup>	a <sup>a</sup>	e <sup>o</sup>	n <sup>i</sup>	m <sup>l</sup>	L <sup>r</sup>	t <sup>x</sup>	Z <sup>n</sup>	m <sup>b</sup>	g <sup>z</sup>	t <sup>y</sup>	z <sup>m</sup>	r <sup>z</sup>	E <sup>m</sup>	x <sup>d</sup>
ga	ge	gi	go	gu	gna	gne	gni	gno	gnu	gra	gre	gri	gro	gru	ha	he	hi	ho	hu	ia	ie	ii	io	iu	la	le	li	lo	lu
r <sup>m</sup>	t <sup>r</sup>	n <sup>s</sup>	Z <sup>q</sup>	L <sup>I</sup>	L <sup>f</sup>	m <sup>p</sup>	m <sup>u</sup>	r <sup>q</sup>	g <sup>q</sup>	t <sup>z</sup>	Z <sup>y</sup>	r <sup>r</sup>	m <sup>m</sup>	m <sup>h</sup>	n <sup>l</sup>	o <sup>d</sup>	z <sup>y</sup>	Z <sup>a</sup>	f <sup>q</sup>	t <sup>s</sup>	...	x <sup>l</sup>	m <sup>t</sup>	...	f <sup>t</sup>	r <sup>n</sup>	t <sup>o</sup>	a <sup>z</sup>	r <sup>s</sup>
lla	lle	lli	llo	llu	ma	me	mi	mo	mu	na	ne	ni	no	nu	pa	pe	pi	po	pu	pra	pre	pri	pro	pru	qua	que	qui	quo	quu
d <sup>n</sup>	n <sup>h</sup>	m <sup>r</sup>	L <sup>b</sup>	z <sup>d</sup>	c <sup>n</sup>	d <sup>o</sup>	r <sup>t</sup>	e <sup>n</sup>	r <sup>x</sup>	a <sup>u</sup>	r <sup>c</sup>	r <sup>o</sup>	e <sup>a</sup>	e <sup>q</sup>	L <sup>o</sup>	f <sup>x</sup>	m <sup>c</sup>	n <sup>e</sup>	o <sup>b</sup>	f <sup>n</sup>	o <sup>n</sup>	...	n <sup>b</sup>	E <sup>r</sup>	L <sup>m</sup>	Z <sup>b</sup>	u <sup>t</sup>	g <sup>r</sup>	o <sup>c</sup>
ra	re	ri	ro	ru	sa	se	si	so	su	sca	sce	sci	sco	scu	spa	spe	spi	spo	spu	ssa	sse	ssi	sso	ssu	sta	ste	sti	sto	stu
a <sup>d</sup>	c <sup>a</sup>	t <sup>n</sup>	L <sup>d</sup>	R <sup>o</sup>	n <sup>n</sup>	a <sup>m</sup>	n <sup>a</sup>	m <sup>x</sup>	g <sup>y</sup>	L <sup>i</sup>	u <sup>b</sup>	t <sup>t</sup>	m <sup>a</sup>	Z <sup>z</sup>	m <sup>n</sup>	Z <sup>t</sup>	n <sup>z</sup>	f <sup>s</sup>	E <sup>l</sup>	a <sup>x</sup>	d <sup>a</sup>	g <sup>o</sup>	e <sup>t</sup>	r <sup>y</sup>	e <sup>u</sup>	L <sup>z</sup>	t <sup>u</sup>	f <sup>i</sup>	my
stra	stre	stri	stro	stru	ta	te	ti	to	tu	tra	tre	tri	tro	tru	tta	tte	tti	tto	ttu	ua	ue	ui	uo	uu	za	ze	zi	zo	zu
z <sup>p</sup>	x <sup>y</sup>	u <sup>p</sup>	o <sup>e</sup>	Z <sup>x</sup>	f <sup>c</sup>	L <sup>a</sup>	z <sup>o</sup>	u <sup>i</sup>	a <sup>y</sup>	u <sup>s</sup>	L <sup>s</sup>	Z <sup>s</sup>	m <sup>q</sup>	g <sup>p</sup>	m <sup>s</sup>	x <sup>o</sup>	n <sup>m</sup>	r <sup>u</sup>	f <sup>d</sup>	e <sup>b</sup>	g <sup>t</sup>	a <sup>s</sup>	r <sup>e</sup>	g <sup>e</sup>	o <sup>q</sup>	Z <sup>f</sup>	L <sup>q</sup>	e <sup>p</sup>	m <sup>f</sup>

**Ma che cosa è un nomenclatore?**

# *La cifra usata nel 1557 pag.2*

<b>Numeri</b>									
0	1	2	3	4	5	6	7	8	9
g <sup>d</sup>	x <sup>r</sup>	u <sup>l</sup>	e <sup>z</sup>	Z <sup>r</sup>	t <sup>p</sup>	o <sup>l</sup>	E <sup>u</sup>	R <sup>u</sup>	d <sup>y</sup>
z <sup>l</sup>									
u <sup>x</sup>									

<b>Doppie</b>									
bb	cc	ff	gg	ii	mm	nn	pp	rr	uu
L <sup>h</sup>	Z <sup>d</sup>	z <sup>q</sup>	f <sup>l</sup>	f <sup>l</sup>	t <sup>q</sup>	Z <sup>c</sup>	o <sup>h</sup>	x <sup>f</sup>	x <sup>f</sup>

<b>Dizionario</b>														
Anglia	o <sup>r</sup>	Capi del C.X	z <sup>a</sup>	Cons. di X	E <sup>d</sup>	Costantinopoli	x <sup>q</sup>	Franza	a <sup>p</sup>	Germania	E <sup>f</sup>	Italia	d <sup>q</sup>	
Milano	d <sup>z</sup>	Monsig.	t <sup>f</sup>	Mor Granvella	x <sup>n</sup>	Piasenza	R <sup>n</sup>	Pontefice	Z <sup>i</sup>	Re dei Romani	g <sup>n</sup>	Roma	x <sup>i</sup>	
S. Turco	E <sup>b</sup>	Ser.mo Principe	u <sup>z</sup>	Serenissimo	c <sup>d</sup>	Sua Eccel.za	o <sup>s</sup>	Sua Maestà	t <sup>c</sup>	Sua Mag.a	n <sup>q</sup>	Sua Santità	d <sup>r</sup>	
Sua Sig.ia	g <sup>c</sup>	Sua X M.tà	Z <sup>l</sup>	V. Serenità	Z <sup>m</sup>	accio	r <sup>f</sup>	ad	f <sup>r</sup>	al	n <sup>t</sup>	alcun	c <sup>t</sup>	
altr	d <sup>m</sup>	an	u <sup>c</sup>	anchor	c <sup>y</sup>	anglesi	g <sup>l</sup>	armata	n <sup>f</sup>	bassa	e <sup>g</sup>	capit	o <sup>o</sup>	
cardinal	e <sup>d</sup>	caual	n <sup>d</sup>	che	a <sup>e</sup>	chi	c <sup>u</sup>	cla.mo	E <sup>t</sup>	come	a <sup>r</sup>	commette	u <sup>d</sup>	
comunica	m <sup>e</sup>	con	u <sup>a</sup>	conclu	o <sup>z</sup>	conside	u <sup>h</sup>	conte	f <sup>e</sup>	continu	f <sup>p</sup>	dal	L <sup>c</sup>	
danari	g <sup>x</sup>	debbi	g <sup>m</sup>	del	R <sup>i</sup>	deside	f <sup>b</sup>	detta M.tà	E <sup>e</sup>	ditt	z <sup>s</sup>	doue	o <sup>y</sup>	
duca	R <sup>b</sup>	duca di Sassonia	Z <sup>h</sup>	esse	d <sup>u</sup>	essercito	z <sup>f</sup>	et	t <sup>a</sup>	ex	c <sup>z</sup>	exe	n <sup>p</sup>	
expedi	x <sup>c</sup>	fant	L <sup>y</sup>	far	a <sup>l</sup>	franzesi	c <sup>r</sup>	galee	o <sup>f</sup>	gente	L <sup>x</sup>	giorn	Z <sup>u</sup>	
gli	o <sup>x</sup>	grand	n <sup>u</sup>	guerra	E <sup>c</sup>	habbia	d <sup>p</sup>	haue	f <sup>o</sup>	hora	g <sup>u</sup>	il	f <sup>a</sup>	
il che	c <sup>l</sup>	il quale	d <sup>x</sup>	ill.mo	d <sup>d</sup>	illustr	f <sup>h</sup>	imp.Cesare	d <sup>e</sup>	in	z <sup>b</sup>	inte	z <sup>n</sup>	
la qual	t <sup>e</sup>	langraui	c <sup>q</sup>	le qual	x <sup>t</sup>	lettere	u <sup>r</sup>	li qual	d <sup>t</sup>	liga	E <sup>h</sup>	magnifico	t <sup>g</sup>	
mai	c <sup>f</sup>	mal	E <sup>z</sup>	man	c <sup>b</sup>	mente	d <sup>s</sup>	molt	n <sup>y</sup>	mr di Aras	c <sup>h</sup>	munition	a <sup>q</sup>	
necess	f <sup>z</sup>	noi	d <sup>c</sup>	non	c <sup>m</sup>	noncio	g <sup>a</sup>	nostr	e <sup>x</sup>	ogni	e <sup>m</sup>	one	c <sup>i</sup>	
opera	u <sup>m</sup>	or amb	a <sup>f</sup>	ora	u <sup>f</sup>	ordin	E <sup>i</sup>	pace	d <sup>l</sup>	pare	t <sup>l</sup>	passat	o <sup>i</sup>	
per	a <sup>i</sup>	perche	d <sup>f</sup>	più	c <sup>c</sup>	prefat	r <sup>l</sup>	present	z <sup>t</sup>	preterit	E <sup>a</sup>	princip	E <sup>y</sup>	
qual	e <sup>y</sup>	qualche	r <sup>h</sup>	quando	e <sup>e</sup>	quant	r <sup>d</sup>	quel	c <sup>s</sup>	quella Mtà	d <sup>h</sup>	quest	L <sup>u</sup>	
questa M.tà	E <sup>p</sup>	re Christ.mo	Z <sup>x</sup>	re d'Anglia	x <sup>u</sup>	re di Portogallo	u <sup>u</sup>	re di Scotia	u <sup>y</sup>	rece	Z <sup>p</sup>	reu.mo	e <sup>l</sup>	
reuerendo	g <sup>b</sup>	rispo	u <sup>e</sup>	scrit	o <sup>t</sup>	scriue	z <sup>e</sup>	scudi	x <sup>x</sup>	sempre	t <sup>d</sup>	senato	E <sup>x</sup>	
sia	f <sup>u</sup>	signor	z <sup>i</sup>	spagnoli	a <sup>h</sup>	ssim	t <sup>b</sup>	stato	o <sup>m</sup>	sua	d <sup>i</sup>	sua Ces. M.à	t <sup>i</sup>	
sue	x <sup>a</sup>	sue Sig.ie	t <sup>h</sup>	sui	L <sup>t</sup>	suizzeri	e <sup>f</sup>	suo	d <sup>b</sup>	tal	z <sup>r</sup>	tant	Z <sup>e</sup>	
tempo	x <sup>z</sup>	tia	e <sup>i</sup>	tregue	z <sup>h</sup>	turchi	E <sup>n</sup>	tutt	z <sup>u</sup>	uede	E <sup>o</sup>	uittuaglie	e <sup>h</sup>	
uogli	z <sup>c</sup>	uoи	x <sup>e</sup>	uole	u <sup>q</sup>	uostr	o <sup>u</sup>	zont	x <sup>h</sup>					

## Domande

- Che ci faceva l'ambasciatore veneziano in Spagna a Bruxelles?
  - La resa di Calais è datata gennaio 1558, Perché la lettera è datata 1557?
  - Perché la lettera inizia con un "Serenissimo Principe" in chiaro? Non andrebbe cifrato?
- 
- What was the Venetian ambassador in Spain doing in Brussels?
  - The surrender of Calais is dated Jan 1558, Why is the letter dated 1557?
  - Why does the letter begin with "Most Serene Prince" in plain text? Should it not be ciphered?

# *Pregi e difetti del nomenclatore*

## **Pregi:**

- E' facile da scrivere e da decifrare avendo a portata di mano lo scontro, che alla lunga può essere imparato a memoria.
- E' relativamente poco ingombrante se come era fortemente raccomandato qui si usano di preferenza il sillabario e il dizionario
- E' molto sicuro, se usato correttamente

## **Difetti:**

- E' esposto al pericolo del furto o della copia dello scontro da parte del nemico.
- Il cambio dello scontro (cifrario) richiede spedizione per Corriere sicuro e tempi piuttosto lunghi, mesi, per l'addestramento dei segretari costretti a reimparare a memoria molti segni.
- Segretari pigri o frettolosi possono essere indotti a cifrare per singole lettere più facili da ritenere a memoria.

# Una cifra polialfabetica

detta anche

## Cifra con chiave

Si sceglie come contrassegno (o chiave) un versetto facile da ritenere a memoria, Bellaso usa questo versetto:

**"Virtuti omnia parent"**

L'addetto alla cifra dovrà scrivere il testo chiaro e sotto il verme ripetuto a sufficienza; per ogni lettera del chiaro e del verme, cercare nella tavola la riga con la lettera del verme, e quindi la lettera del chiaro nella riga; come cifra userà la lettera accoppiata, sotto o sopra.

Se il messaggio è **"L'armata turchesca partira a cinque di luglio"** la prima del contrassegno è V, cerchiamo nella riga VX la prima lettera del chiaro L e sotto la L troviamo S; la cifra quindi è S. Continuando si ottiene:

contrassegno	VIRTV TIOMN IAPAR ENTVI RTVTI OMNIA PAREN TVIRT VTIO
testo chiaro	LARMA TAYTV RCHES CAYPA RTIRA YAYCI NQVEY DIYLV GLIO
testo cifrato	SYOHV XYBQO GPGRN OBSGY OXRZY BAZNX VDYQZ DRAGV PITE

Il crittogramma da trasmettere è quindi:

SYOHV XYBQO GPGRN OBSGY OXRZY BAZNX VDYQZ DRAGV PITE

# Cifra Bellaso 1552



A a b c d e f g h i l m n o p q r s t u v x y z  
E a b c d e f g h i l m n o p q r s t u v x y z  
**I** a b c d e f g h i l m n o p q r s t u v x y z  
**O** a b c d e f g h i l m n o p q r s t u v x y z  
**V** a b c d e f g h i l m n o p q r s t u v x y z  
B a b c d e f g h i l m n o p q r s t u v x y z  
C a b c d e f g h i l m n o p q r s t u v x y z  
D a b c d e f g h i l m n o p q r s t u v x y z  
F a b c d e f g h i l m n o p q r s t u v x y z  
G a b c d e f g h i l m n o p q r s t u v x y z  
H a b c d e f g h i l m n o p q r s t u v x y z  
L a b c d e f g h i l m n o p q r s t u v x y z  
M a b c d e f g h i l m n o p q r s t u v x y z  
N a b c d e f g h i l m n o p q r s t u v x y z  
P a b c d e f g h i l m n o p q r s t u v x y z  
Q a b c d e f g h i l m n o p q r s t u v x y z  
R a b c d e f g h i l m n o p q r s t u v x y z  
S a b c d e f g h i l m n o p q r s t u v x y z  
T a b c d e f g h i l m n o p q r s t u v x y z  
X a b c d e f g h i l m n o p q r s t u v x y z  
Y a b c d e f g h i l m n o p q r s t u v x y z  
Z a b c d e f g h i l m n o p q r s t u v x y z  
Nobilis. Virti. D. lo. Baptiste Bellaso. Juris. Confut. Brixienis.  
M. D. LII.

# *La cifra polialfabetica*

## *Pregi e difetti*

### **Pregi:**

- E' facile da scrivere e da decifrare avendo a portata di mano la tabella e la chiave.
- Si usano solo le lettere dell'alfabeto nessuna necessità di imparare altri segni o gruppi di lettere o numeri.
- Una lettera del crittogramma non corrisponde sempre alla stessa lettera del chiaro, anzi può corrispondere a una qualsiasi lettera. Quindi il cifrario è indecifrabile! O no?

### **Difetti:**

- Cifrare lettera per lettera richiede più tempo e occupa più posto.
- Il dover ad ogni lettera fare una ricerca nella tabella richiede tempo e attenzione con rischio di errori
- Se il segretario **perde il segno** saltando una lettera della chiave o del testo chiaro **tutto il resto del crittogramma risulta errato e indecifrabile**
- Tanto più breve la chiave, tanto più facile da ricordare, ma anche tanto meno sicuro il sistema, solo con una chiave illimitata, il cifrario è realmente, anche teoricamente, indecifrabile.

# *La cifra polialfabetica*

## *Il rischio di perdere l'allineamento*

### Difetti:

- Se il segretario **perde il segno** saltando una lettera della chiave o del testo chiaro **tutto il resto del crittogramma risulta errato e indecifrabile.**

contrasegno	VIRTV TIOMN IA <b>VIR TVTIO MNIAV IRTVT</b>
testo chiaro	LARMA TAYTV RCHEs CAYPA RTIRA YAYCI
testo cifrato	SYBOV EYBCD GP <b>QPC RVHEX ACTEV AQHYZ</b>
contrasegno	VIRTV TIOMN IA <b>IRT VTIOM NIAVI RVTI</b>
testo chiaro	LARMA TAYTV RCHEs CAYPA RTIRA YAYCI
testo cifrato	SYBOV EYBCD GP <b>SVD YPAFR AIXIY GPCRT</b>

Esempio : usiamo come *contrasegno* (chiave) VIRTVTIOMNIA e vediamo cosa succede se il segretario distrattamente perde la V iniziale: tutto il resto del cifrato cambia e al momento della decifra produrrà testo incomprensibile

Il male non è irreparabile, ma in un testo lungo può comportare inaccettabili perdite di tempo

# DIANA, ovvero Bellaso alla guerra del Vietnam?

Durante la guerra del Vietnam (1965-1975) i soldati nella giungla senza disponibilità di macchine cifranti usarono un cifrario carta e penna: la tabella ricorda quella del Bellaso, ei la relazione tra gli ordinali della lettera chiara o palese, **P**, della lettera della chiave **K**, e della cifrata, **C**, è:

$$p + k + c = (25 \text{ mod } 26)$$

Ma la forza della cifra non dipende da questa relazione ma dalla chiave che deve essere disordinata, scritta su un libretto da rinnovare quando finisce.

chiave da OTP	<b>MFNIQ PAEYT VVIUF LRLSK XMXIX RGTOT PBZCJ PSJUR</b>
CP	
testo chiaro	----- IVIET CONGA TTACC HERAN NOQUE STASE
RA	
testo cifrato	MFNIQ PAEYT WJJBB MUBBP JUCPA BPPLT XKKDM SOQNE
GK	
One Time Pad	Blocco indicatore a pos. 245 KFKWR TJPWF HZCHF JOBWV KXSAP VENCR MMXWI PPSEM XMMAT RKHTG DEEVF URKIU BUGZR POHHS TFFFG YXRGR YJVDF AXXKG RMAYL SNZZV STBXZ HWWYD OWNJA TKXQV DHIEG TWTTW PMPQK OXGLW KZTYJ TRURH PVPXZ VRWPL TEXJU HXSOJ PYJJW TDONU VDPLB PHTMW EFABO VJMOX WDWFN TZQHM LDQAO RQVKC SOITQ XOZJD WGHTL UMKKU XVXNW <b>MFNIQ</b> <b>PAEYT</b> VVIUF LRLSK XMXIX RGTOT PBZCJ PSJUR CPMKK SVCDO NBAKJ XCPRR JGSIJ BYCKS TNHGX SZTUC HHEIS NGUDX LNEDV NETQP MJCUQ AMPTG SBOWK GKQAN NLARP WFTQV ICFLW VLIKF PCGEZ RKJHL XVWXN LUTFK OONTZ JPKSA PIDWM CNWLV IIQEG EQAXW LLKYF KIVUB VKJYH WAUTM QBVGG BLXCI TNTEM ZOUUJ WQTGO ACPVW BLXWS DYEAA MUNGY AFNVA WRRPX FQAUM WWXTT QXRUY RHTFN RFTEA UARLQ PQGPL SLIQF BHDS CJJVO XMTQR TKSLW JAMQP YJBGZ GHHKZ KMJUH XRUQI MKTFV POVCE LANMH NTPVD OFQXA XVSRM AEWTJ SJXOL CAMPM TDGIZ KXFV FYQXQ DYUAS DSBBH NDHZA UTWAC WKABL VGJME ZQCUQ VXIWY QKCKX VRDSS GODGP PCWYP BYFDS VZQEW OVGRS QMKUE DBTGI IVLFU AGSGK LCJBG FQBMH UCTFX YIYSP GAKRG ESNXY XIBHK HMAJZ IEBCJ YASXS

Tavola nel formato originale, simile a Bellaso 1552

A	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Z Y X N W U T S R Q P O N M L K J I H G F E D C B A
B	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Y X W V U T S R Q P O N M L K J I H G F E D C B A Z
C	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z X W V U T S R Q P O N M L K J I H G F E D C B A Z Y
D	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z W V U T S R Q P O N M L K J I H G F E D C B A Z Y X
E	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z V U T S R Q P O N M L K J I H G F E D C B A Z Y X W
F	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z U T S R Q P O N M L K J I H G F E D C B A Z Y X W V
G	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z T S R Q P O N M L K J I H G F E D C B A Z Y X W V U
H	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z S R Q P O N M L K J I H G F E D C B A Z Y X W V U T
I	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z R Q P O N M L K J I H G F E D C B A Z Y X W V U T S
J	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Q P O N M L K J I H G F E D C B A Z Y X W V U T S R
K	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z P O N M L K J I H G F E D C B A Z Y X W V U T S R Q
L	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z O N M L K J I H G F E D C B A Z Y X W V U T S R Q P
M	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z N M L K J I H G F E D C B A Z Y X W V U T S R Q P O
N	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z M L K J I H G F E D C B A Z Y X W V U T S R Q P O N
O	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z L K J I H G F E D C B A Z Y X W V U T S R Q P O N M
P	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z K J I H G F E D C B A Z Y X W V U T S R Q P O N M L
Q	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z J I H G F E D C B A Z Y X W V U T S R Q P O N M L K
R	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z I H G F E D C B A Z Y X W V U T S R Q P O N M L K J
S	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z H G F E D C B A Z Y X W V U T S R Q P O N M L K J I
T	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z G F E D C B A Z Y X W V U T S R Q P O N M L K J I H
U	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z F E D C B A Z Y X W V U T S R Q P O N M L K J I H G
V	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z E D C B A Z Y X W V U T S R Q P O N M L K J I H G F
W	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z D C B A Z Y X W V U T S R Q P O N M L K J I H G F E
X	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z C B A Z Y X W V U T S R Q P O N M L K J I H G F E D
Y	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z B A Z Y X W V U T S R Q P O N M L K J I H G F E D C
Z	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A Z Y X W V U T S R Q P O N M L K J I H G F E D C B

# *Matematicamente*

*Gruppo chiaro*



**Cifra**

*Segno cifrante*

*Segno cifrante*



**Decifra**

*Gruppo chiaro*

*Nomenclatore*

*lettera*

*chiara*



*lettera chiave*

**Cifra**

*Segno cifrante*

*Segno cifrante*



**Decifra**

*lettera chiave*

*Polialfabetico*

**1573**

. Hieronimo (Girolamo)  
. di Franceschi  
1540-1600

Franceschi :- Antica famiglia di cittadini, per lo più segretari del Senato o della cancelleria ducale.

# 1572: Irrompe sulla scena Hieronimo di Franceschi

Nel settembre 1572 irrompe sulla scena della crittografia veneziana un giovane di 32 anni che propone un nuovo tipo di cifra, a suo dire indecifrabile.

Di personaggi che giravano per le corti italiane ed europee presentando cifre assolutamente indecifrabili se ne contano a decine.

Quella di Franceschi si distingue per diversi aspetti, primo tra tutti il fondamento teorico esposto in modo un po' ossessivo ma comunque basato su alcune idee molto interessanti:

Franceschi distingue le cifre in due grandi famiglie, che sono poi in sostanza sempre quelle due :

1. Le vere cifre (*uerere ziffre*) sono **cifre assolutamente impossibili da decifrare senza lo scontro**. Nel senso che un testo cifrato con una cifra vera deve essere del tutto indipendente dal testo chiaro, e quindi deve poter essere decifrato in un qualsiasi altro prefissato testo chiaro in una qualsiasi lingua semplicemente usando un'altra chiave costruita ad hoc, detta **falso scontro**.
2. Le cifre vecchie (*ziffra ueccchia*) ovverosia i nomenclatori, consistendo di segni cifranti che si decifrano in modo univoco in una sola lettera, sillaba o parola questo non è possibile e quindi almeno in teoria possono essere decrittate. Se ben progettate e ben messe in pratica, può essere difficile o molto difficile decrittarle, ma mai impossibile. Non sono quindi vere cifre, ma andrebbero chiamate *Modi oscuri di scrivere*

# Cosa aveva in mente Franceschi per uera ziffra?

- Nient'altro che una cifra polialfabetica? È possibile, ma la cifra proposta utilizzando addizione, sottrazione e chiavi lunghe quanto il messaggio, come un Vernam, fa un passo avanti.
- Il crittosistema perfetto di Shannon? Certo che no, Franceschi non ha dato una definizione rigorosa, anzi non aveva gli strumenti matematici e il formalismo per farlo. Cose come i logaritmi, l'aritmetica modulare, la logica formale... dovevano ancora arrivare. Ma l'idea di base e il cifrario proposto accennano a qualcosa di molto simile.
- Un'altra cifra assolutamente indecifrabile, come quelle proposte da tanti nel XVI secolo? Forse qualcosa di più, per capire di che si tratta è utile un foglio con due modi descritti in modo non troppo dettagliato.
  -

# Condizioni della cifra nel primo modo

• Ha la ziffera mia queste condizioni di grandissimo comodo e utile.

1. Leuar da questa palese si puo un significato finto come si uuole, falso et uerisimile . Sopra l'istessi caracteri, poi si manifesta l'auiso uero seguro et in tutto nascosto ad ognuno.

2. E facil a componer in qual ci uoglia lingua, et impossibile che s'intenda mai se non da colui che da me prima conoscenza la chiaue, o contrasegno con il quale s'apre l'interior mio rinchiuso.

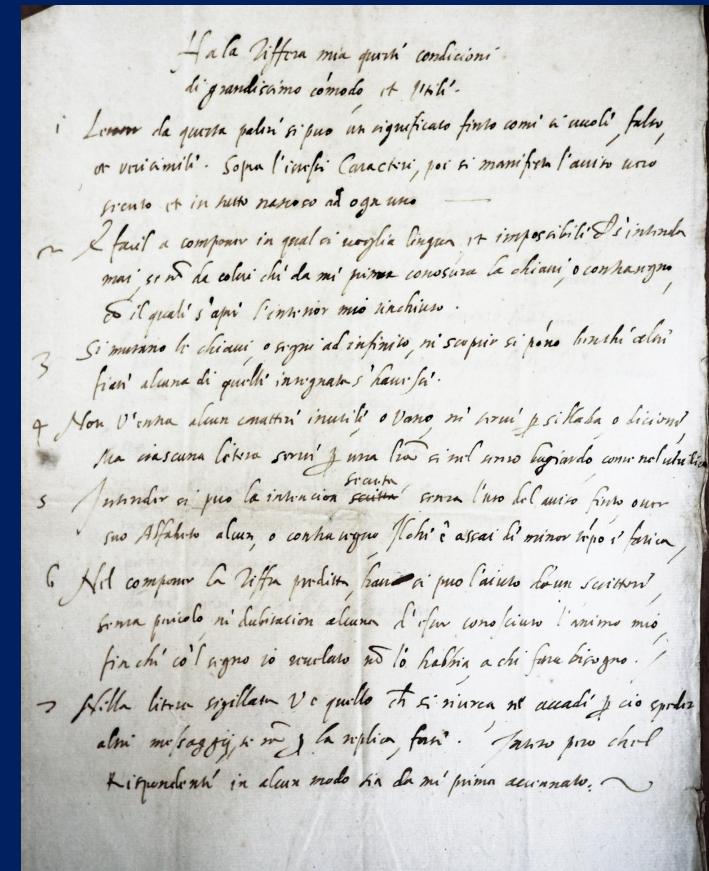
3. Si mutano le chiaui o segni ad infinito, ne scoprir si possono benché altre fiate alcuna di quelle insegnata s'hauesse

4. Non u'entra alcun carattere inutile o uano, né scriue per sillaba, o dizione, ma ciascuna lettera scriui per una lettera sì nel senso bugiardo, come nel utile

5. Intender si può la intencion secura senza l'uso del auiso finto ouer suo alfabeto alcun, o contrasegno, il che `e assai di minor tempo e fatica.

6. Nel componer la ziffra predetta, hauer si può l'aiuto d'un scrittore, senza pericolo n'e dubitacion alcuna d'esser conosciuto l'animo mio, finché col segno io reuelato non lo habbia a chi farà bisogno.

7. Nella **litera sigillata** u'è quello che si ricerca ne accadi per ciò spedir altri messaggij se non per la replica, Inteso però che'l rispondente in alcun modo sia da me prima accennato.

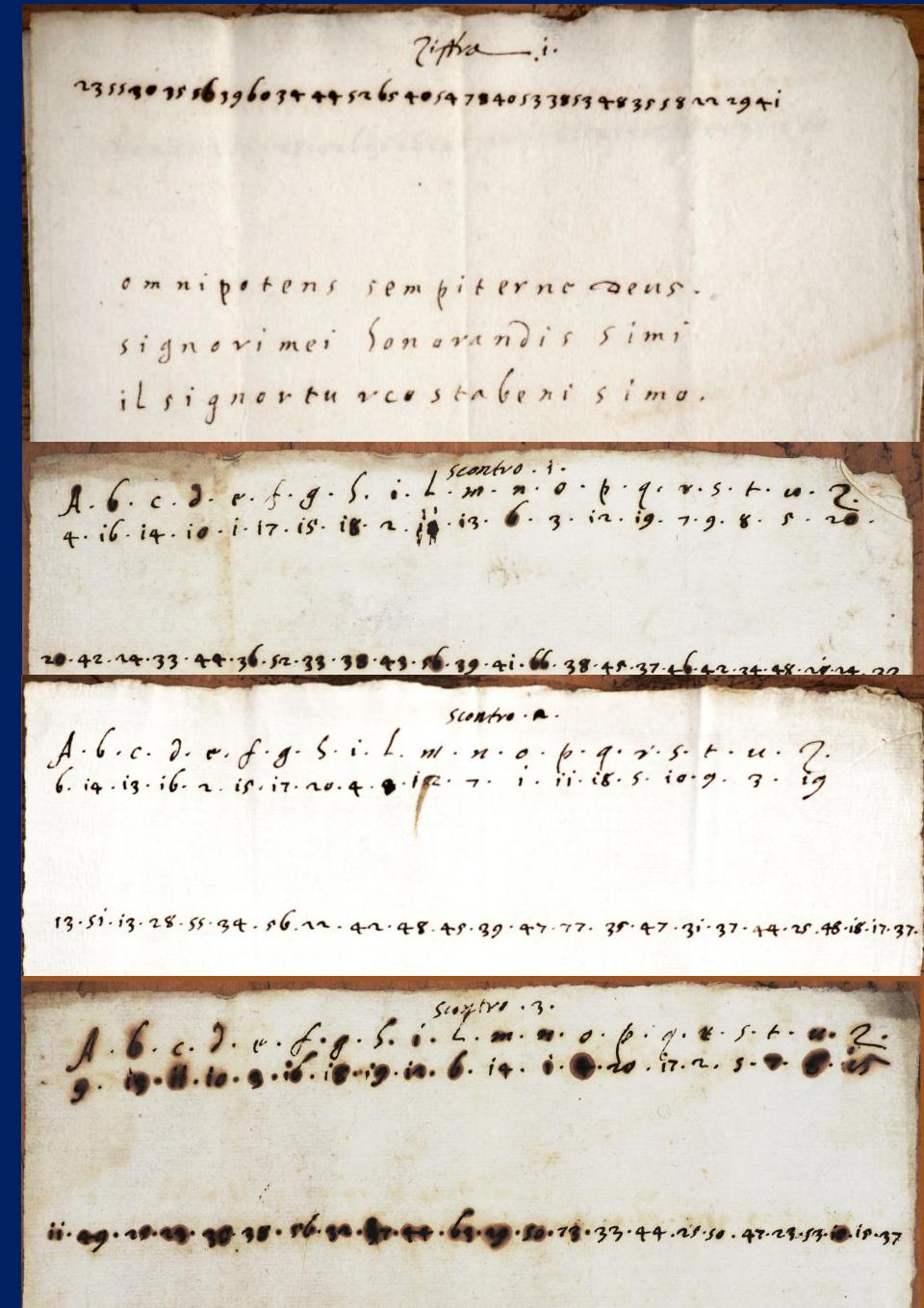


# Cifra del falso scontro di Franceschi: 3 esempi in 1

Per comprendere il funzionamento di questa cifra del falso scontro è stato fondamentale il ritrovamento di una serie di fogli scolti con esempi/esercizi, basati su questi tre possibili messaggi ognuno di 24 lettere:

Omnipotens semperne deus  
Signorimei honorandissimi  
Il signor turco stabenissimo

Nei tre fogli in basso vediamo tre differenti alfabeti chiamati *scontri* 1, 2, 3 che servono a convertire le lettere in numeri.

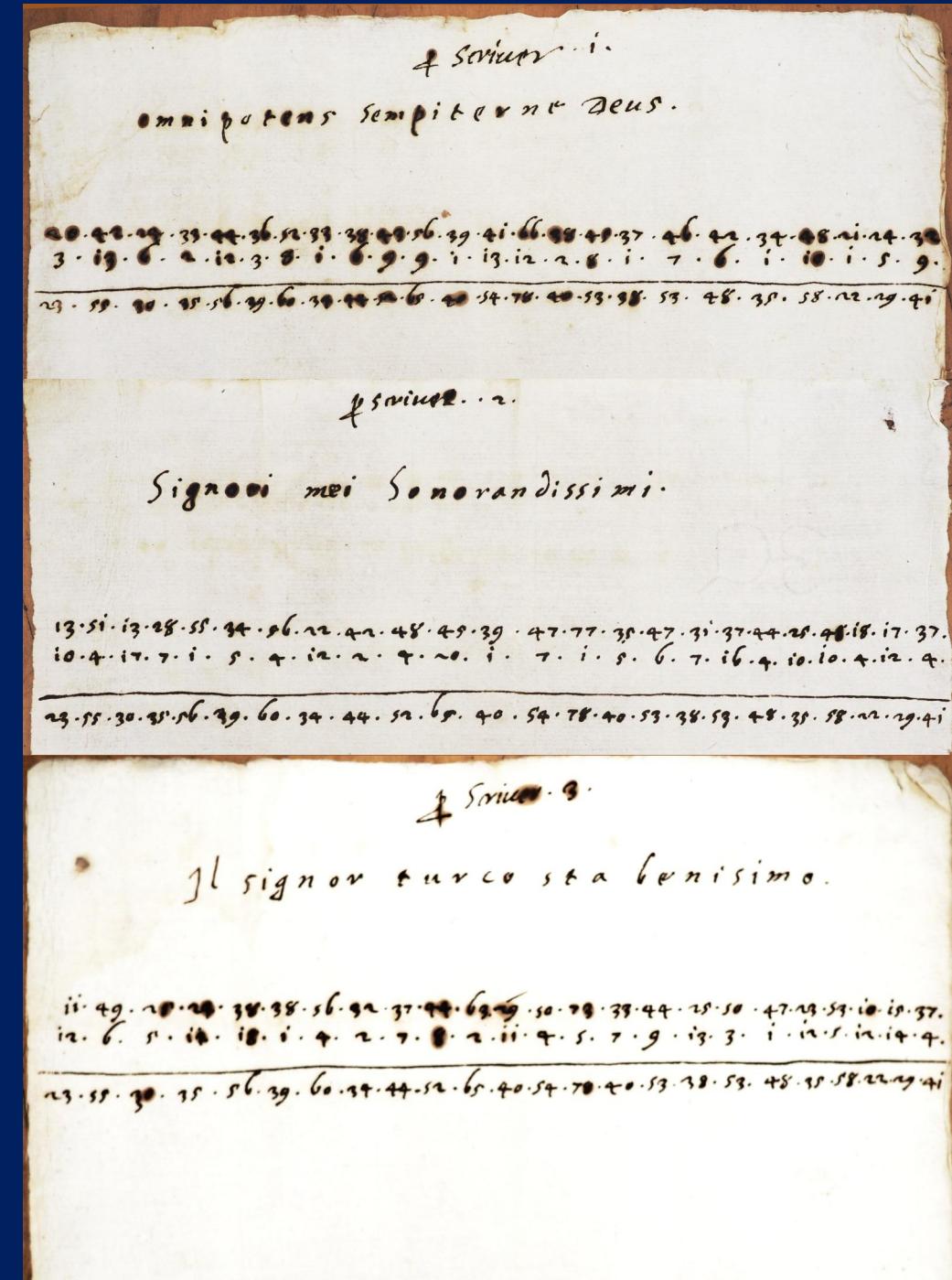


# Primo modo di Franceschi Cifrare sommando

Per scrivere in cifra (*scriuer*), occorre prima sostituire ogni lettera con il numero dato dallo scontro, quindi sommarlo al corrispondente numero della chiave.

Tutto qui una banale addizione.  
E la decifra consiste ovviamente in una sottrazione.

Ma doverne farne a centinaia, per ogni lettera, il pericolo che ci scappi l'errore o peggio ancora che si perda il segno è consistente, anche per segretari abituati a tenere i conti di cassa.



# Primo modo di Franceschi Decifrare sottraendo

Finalmente la procedura per decifrare (*trazer*) il messaggio ricevuto.

E' semplicemente l'inverso della precedente: sottrarre il singolo numero del cifrato dal corrispondente della chiave, quindi sostituire il risultato con la corrispondente lettera dello *scontro*.

Tutto qui, una semplice sottrazione.

In verità la sottrazione è un po' più difficile della somma e doverne fare a decine in breve tempo è un problema.



# Franceschi e Bellaso

*Et per poter più facilmente conquisir questo beneficio, ho giudicato necessario informarmi in modo che  
abbiano qualche similitudine, o conformità con quelle del Belaso, del Tritomio, del Posta, et di  
altri simili scrittori; in questa profusione, accio che quello di Belaso ordinano suol tener ogni Principe,*

Da dove aveva preso l'idea di *uera ziffra*?

Franceschi cita diverse volte Bellaso e mostra di conoscerne le opere e la sua *uera ziffra* ricorda il *Vero modo di scriuere in cifra* di Bellaso.

E la lista di *condizioni* di Franceschi ha molti punti in comune con le *singular qualità* delle cifre dell'opuscolo di Bellaso del 1564.

Ma la cifra di Franceschi introduce una novità che lui stesso evita di nominare esplicitamente: l'uso dell'aritmetica, addizioni e sottrazioni invece di sostituzioni.

IL VERO MODO DI  
SCRIVERE IN CIFRA  
CON FACILITÀ, PRESTEZZA,  
ET SECUREZZA,



DI MISER GIOVAN BATTISTA BELLASO,  
GENTILHOMO BRESCIANO.

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

LE SINGOLAR QVALITA  
DELLE CIFRE, SONO QUESTE,

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

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

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

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

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

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

# Una congettura sul metodo

*Si mutano le chiaui o segni ad infinito,  
ne scoprir si possono benché altre fiate  
alcuna di quelle insegnata s'hauesse*

Messaggio cifrato da inviare

*Nella litera sigillata u'è  
quello che si ricerca ne  
accadi per ciò spedir  
altri messaggij se non  
per la replica, ...*

Messaggio falso  
Chiave falsa  
(falso scontro)

Il segretario che riceve il tutto decifra il  
dispaccio con la chiave che aveva  
ricevuto in precedenza e usa la chiave  
falsa arrivata intatta nella lettera, per  
cifrare

Dentro la lettera sigillata, una nuova chiave



i	l	s	i	g	n	o	r	t	u	r	c	o	s	t	a	b	e	n	i	s	i	m	o
12	6	5	12	18	1	4	2	7	8	2	11	4	5	7	9	13	3	1	12	5	12	14	4
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	
11	49	25	23	38	38	56	32	37	44	63	29	50	73	33	44	25	50	47	23	53	10	15	37
—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
23	55	30	35	56	39	60	34	44	52	65	40	54	78	40	53	38	53	48	35	58	22	29	41

23	55	30	35	56	39	60	34	44	52	65	40	54	78	40	53	38	53	48	35	58	22	29	41
-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
s	i	g	n	o	r	i	m	e	i	h	o	n	o	r	a	n	d	i	s	s	i	m	i
10	4	17	7	1	5	4	12	2	4	20	1	7	1	5	6	7	16	4	10	10	4	12	4
—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
13	51	13	28	55	34	56	22	42	48	45	39	47	77	35	47	31	37	44	25	48	18	17	37

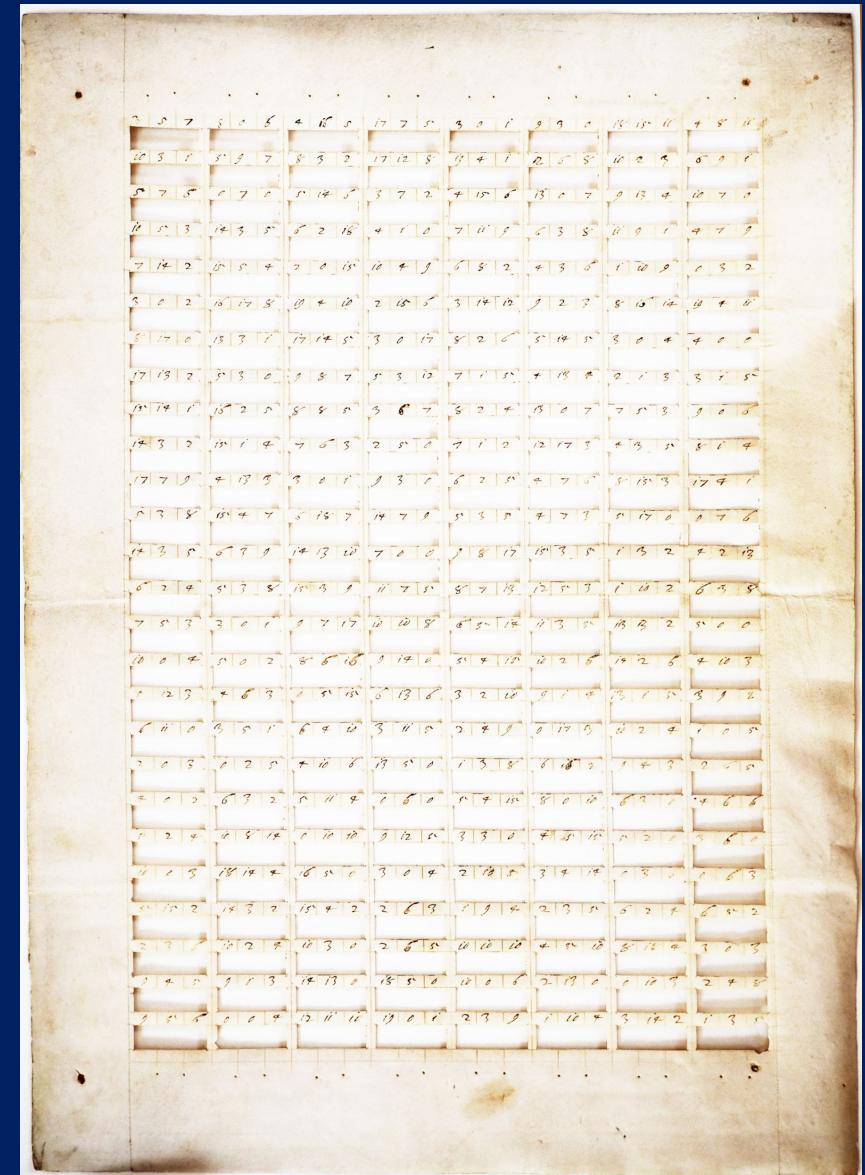
Dentro la busta sigillata



# The Cifra delle Caselle

Zuan Francesco Marin, il principale deputato alle cifre di quegli anni, si oppose fermamente alla cifra di Franceschi, sostenendo che era troppo lento, troppo difficile e soggetto a errori, insomma le classiche obiezioni viste sopra.

Franceschi giunse infine a un compromesso, non sappiamo se concordato con il Marin o no, revisionando la cifra; il risultato fu la Cifra delle Caselle, ovvero delle finestrelle, dalla principale innovazione, l'uso di una griglia per facilitare il lavoro. Questo cifrario fu approvato e utilizzato dalle ambasciate veneziane a partire dal 1577.



Grata per il bailo a Costantinopoli. ASVe  
CX Cifre, chiavi ... b. 6.3

[Cifra delle Caselle - Esempio interattivo](#)

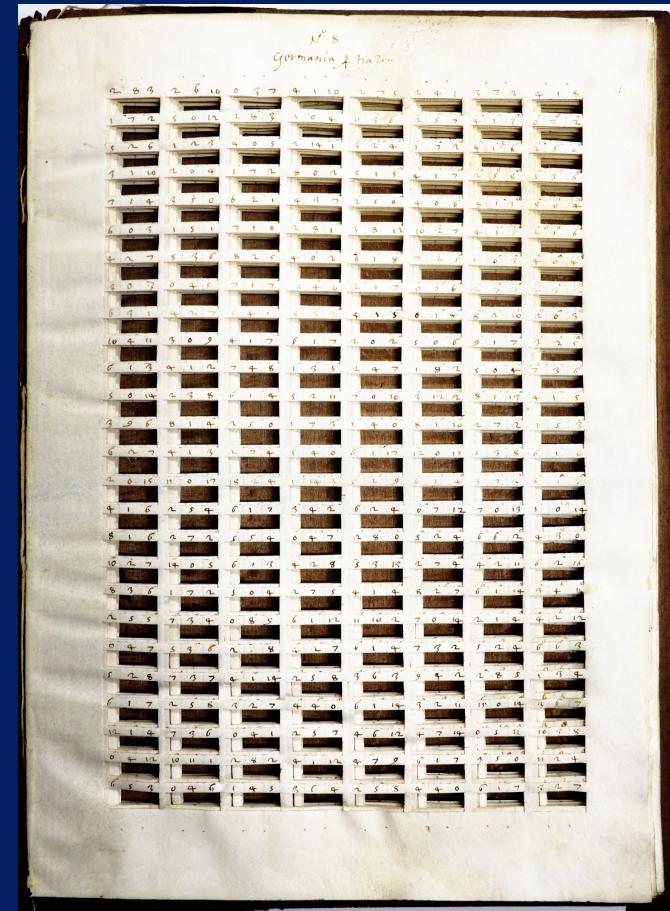
E quindi ci fu nel Cinquecento almeno un caso di uso professionale del sistema polialfabetico:

## **La cifra delle caselle di Hieronimo di Franceschi**

# Che c'è di nuovo?

Quali erano le novità di questa nuova cifra?

1. La chiave è scritta su una griglia di cartoncino o pergamena, con tante piccole finestre (le caselle che hanno dato il nome al cifrario). Il segretario metterà un foglio bianco sotto la griglia per fare la sottrazione e scrivere il numero risultante all'interno della finestra, sotto il numero corrispondente della chiave), in modo **che sia impossibile perdere l'allineamento**.
2. La chiave può essere al massimo di  $26 \times 24 = 624$  numeri di 2 cifrari, per griglie di 8 colonne, meno per griglie più piccole di 7 colonne. Se un testo ha più di 624 lettere, si deve inserire un nuovo foglio sotto la stessa griglia. Quindi, il principio della chiave lunga come il messaggio e della chiave falsa è abbandonato, almeno per i messaggi lunghi.
3. La cifra alfabetica ha ora due omofoni per ogni lettera, A ha 16 36 realizzando una rudimentale aritmetica modulo 20; numeri nell'intervallo 1..40
4. I restanti 60 numeri nell'intervallo 40-99 sono utilizzati per un piccolo dizionario, con un vantaggio minimo o nullo e in contraddizione con il principio della singola lettera. Un compromesso?
- 5.



[Cifra delle Caselle - Esempio interattivo](#)

# La cifra delle Caselle

per Scrivere

A.	B.	C.	D.	E.	F.	G.	H.	I.	L.	M.	N.	O.	P.	Q.	R.	S.	T.	V.	Z.
16.	17.	18.	19.	20.	21.	22.	23.	24.	25.	26.	27.	28.	29.	30.	31.	32.	33.	34.	35.
i.	i.	i.	i.	i.	i.	i.	i.	i.	i.	i.	i.	i.	i.	i.	i.	i.	i.	i.	i.
16.	17.	18.	19.	20.	21.	22.	23.	24.	25.	26.	27.	28.	29.	30.	31.	32.	33.	34.	35.
36.	37.	38.	39.	40.	41.	42.	43.	44.	45.	46.	47.	48.	49.	50.	51.	52.	53.	54.	55.
36.	37.	38.	39.	40.	41.	42.	43.	44.	45.	46.	47.	48.	49.	50.	51.	52.	53.	54.	55.
<u>Accio</u> — 41	<u>dal</u> — 56	<u>G.</u> <u>Lion</u> — 42	<u>Necess</u> — 49	<u>Re</u> <u>X:</u> — 74	<u>Turch</u> — 68														
<u>A.</u> <u>Alcy</u> — 44	<u>del</u> — 52	<u>Grand</u> — 92	<u>Koi</u> — 98	<u>Re</u> <u>di</u> <u>spagn</u> — 73	<u>Tant</u> — 95														
<u>Anno</u> — 47	<u>det</u> — 53	<u>Habbia</u> — 61	<u>Nostr</u> — 99	<u>R. Re</u> <u>di</u> <u>Nauren</u> — 76	<u>Tut</u> — 64														
<u>Atanson</u> — 66	<u>desile</u> — 59	<u>Haur</u> — 64	<u>Reg</u> <u>o</u> <u>ngli</u> — 71	<u>Rispo</u> — 75	<u>V. Basar</u> — 91														
<u>B.</u> <u>Bafia</u> — 65	<u>est</u> — 55	<u>taua di Sangiari</u> — 88	<u>J. Illustr</u> — 84	<u>o. ordm</u> — 82	<u>V. Noi</u> — 96														
<u>Che</u> — 69	<u>Ebe</u> — 54	<u>Imperator</u> — 62	<u>Papat</u> — 65	<u>Santita'</u> — 40															
<u>Come</u> — 70	<u>Espedi</u> — 57	<u>La Reg</u> <u>Madre</u> — 62	<u>P. Per</u> — 79	<u>sexmo</u> — 81															
<u>Con</u> — 50	<u>Fav</u> — 46	<u>Maestri</u> — 40	<u>Princip</u> — 49	<u>sexin</u> — 83															
<u>Cors</u> <u>di</u> <u>ri</u> — 51	<u>Forment</u> — 48	<u>M. Molt</u> — 78	<u>Recant</u> — 97	<u>signor</u> — 60															
<u>Constanti</u> — 90	<u>Galee</u> — 43	<u>Mente</u> — 72	<u>Qua</u> — 93	<u>sempre</u> — 85															
<u>Clarissim</u> — 58			<u>Que</u> — 94	<u>sua</u> — 86															

Per scrivere

$$\text{Grata} \rightarrow 8 \quad A \rightarrow 16 \quad 16 - 8 = 8$$

La cifra di A è 8

$$\text{Grata} \rightarrow 19 \quad A \rightarrow 36 \quad 36 - 19 = 17$$

La cifra di A è 17

$$\text{Grata} \rightarrow 19 \quad A \rightarrow 16 \quad 16 - 19 = 17 \pmod{20} \quad \text{La cifra di A è 17}$$

N° 8  
Germania & Parigi

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

[Cifra delle Caselle - Esempio interattivo](#)

# Cifrare usando le Caselle

Lo maggior corno de la fiamma antica

I	o	m	a	g	g	i	o	r	c	o	r	n	o	d	e	l	a	f	i	a	m	m	a
14	18	7	16	19	19	8	18	12	1	18	12	17	18	15	2	14	16	4	8	16	7	7	16
2	8	3	2	6	10	0	3	7	4	1	10	2	7	5	2	4	1	3	7	2	4	1	8
12	10	4	14	13	9	8	15	5	17	17	2	15	11	10	0	10	15	1	1	14	3	6	8
a	n	t	i	c	a																		
16	17	11	8	1	16																		
1	7	2	5	0	12																		
15	10	9	3	1	4																		

Crittogramma da trasmettere:

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

12+	10+	4+	14+	13+	9+	8+	15+	5+	17+	17+	2+	15+	11+	10+	0+	10+	15+	1+	1+	14+	3+	6+	8+	
2	8	3	2	6	10	0	3	7	4	1	10	2	7	5	2	4	1	3	7	2	4	1	8	
14	18	7	16	19	19	8	18	12	21	18	12	17	18	15	2	14	16	4	8	16	7	7	16	
1	o	m	a	g	g	i	o	r	c	o	r	n	o	d	e	l	a	f	i	a	m	m	a	
15+	10+	9+	3+	1+	4+																			
1	7	2	5	0	12																			
16	17	11	8	1	16																			
a	n	t	i	c	a																			

Plain text

Cifra A16-36

Grata Germania

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

Cifra delle Caselle - Esempio interattivo

# Cifrare usando le Caselle

Le istruzioni originali non sono state ritrovate in archivio, ma, comparando testi cifrati con gli originali in chiaro, ne ho fatto una ricostruzione software che funziona, nel senso che produce risultati corretti sia cifrando sia decifrando.

Nei primi versi dall'Amleto «*to be or not to be*» la prima lettera **T**, consultanto lo scontro della cifra piccola può cifrarsi con 11 o 31, qui il software ha scelto 11, la prima cifra della grata è 2, e quindi  $11 - 2 = 9$ ; il primo segno cifrante è quindi 9.

E così via ...

t	o	b	e	o	r	n	o	t
11	18	13	2	18	12	17	18	11
2	8	3	2	6	10	0	3	7
9	10	10	0	12	2	17	15	4

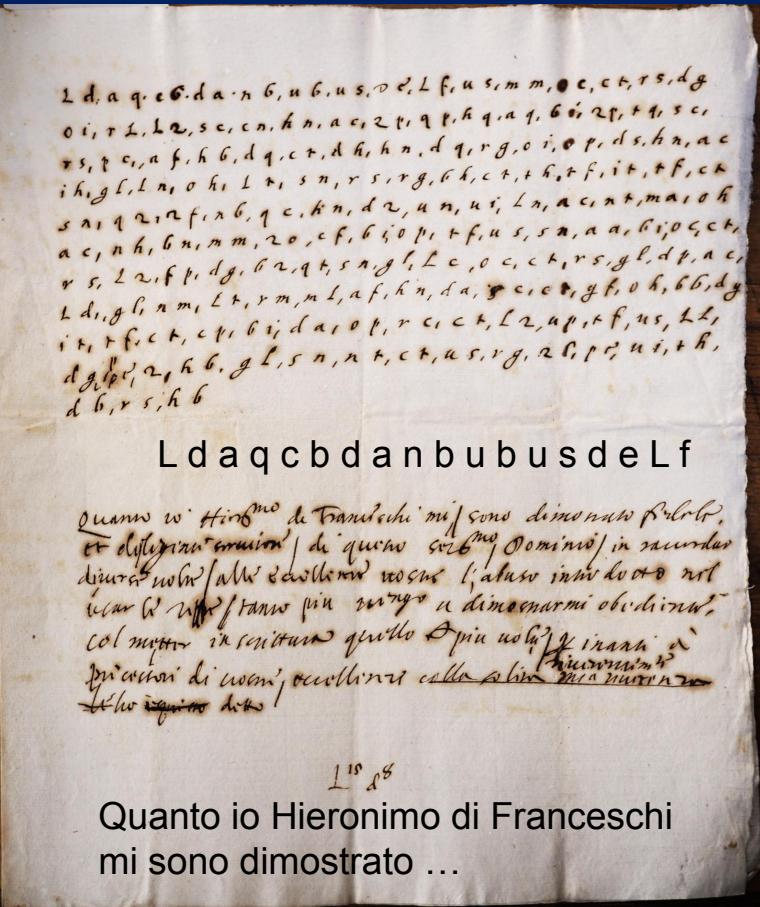
Un problema che potrebbe insorgere è quello dei numeri negativi che possono presentarsi per le lettere dell'alfabeto che hanno le cifra minore di 20. Per esempio se la prima cifra della chiave qui accanto fosse 16 si avrebbe  $11 - 16 = ??$ , ma nel Cinquecento una tale differenza era impossibile.

Ovvio rimedio usare l'omofono alto in questo caso 31 e  $31 - 16 = 15$ . Come già osservato è una sorta di aritmetica modulare, qui modulo 20.

E quindi era probabilmente questa la regola per cifrare, usare sempre l'omofono più alto.

# Secondo modo

Resta in dubbio il funzionamento del secondo modo che Franceschi descrive come cifra non sospetta, cioè steganografia. Consisterebbe in un sistema che trasforma un qualsiasi testo chiaro in un qualsiasi altro testo chiaro, usando la matrice quadrata qui sotto.



L'esempio a sinistra mostra un testo chiaro e una sequenza di lettere sopra.

Cercando nella colonna **Q** il numero sulla riga **L** si trova 15 ecc.ecc.

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

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

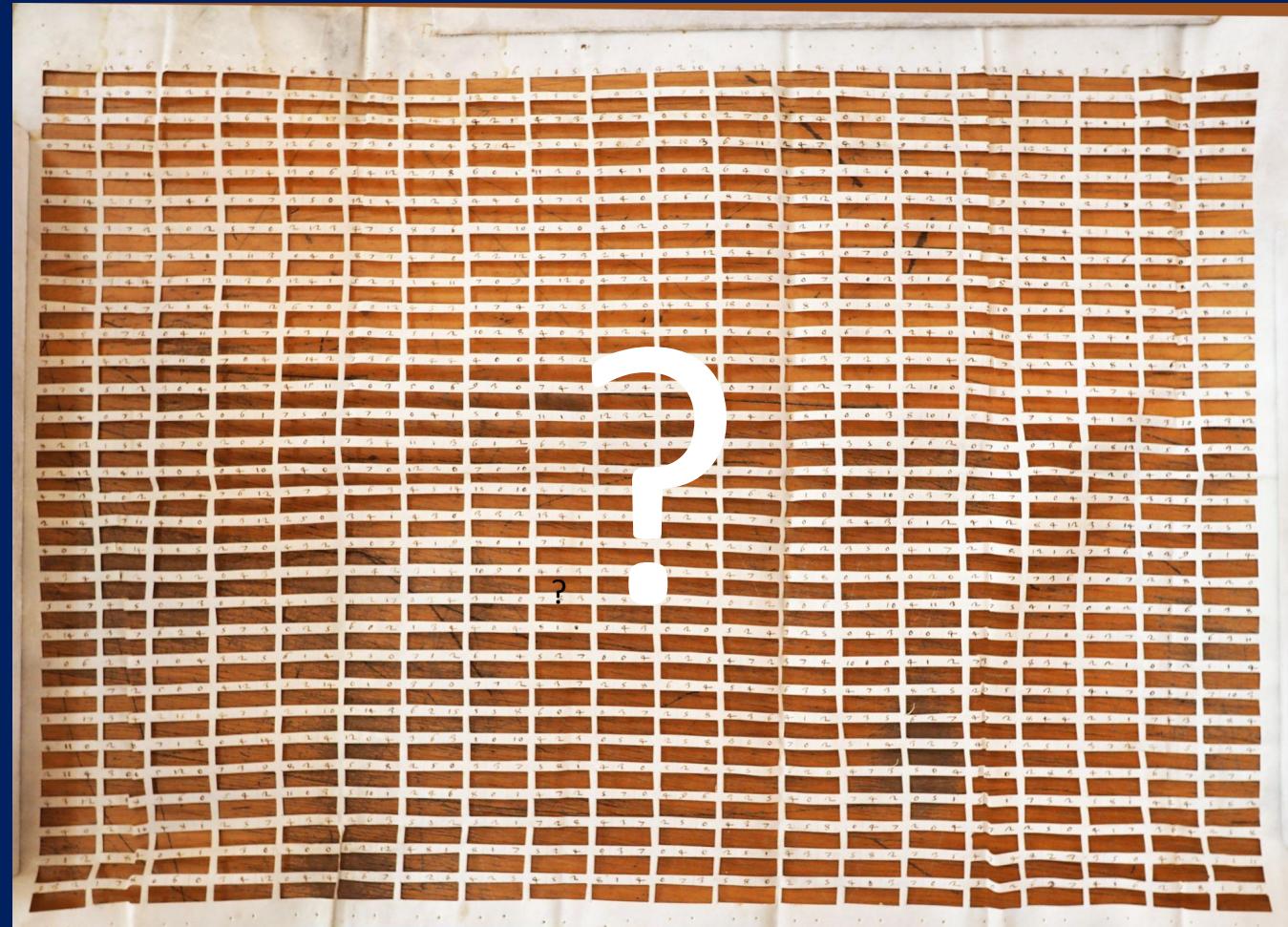
# **Secondo modo e altri**

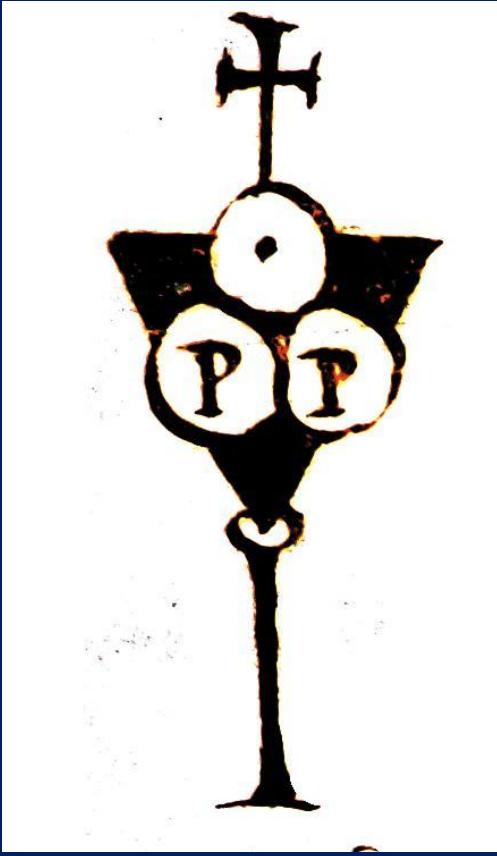
Tra le carte di Franceschi si trovano molti abbozzi, tra l'altro due grate di dimensioni enormi, come questa di 30 colonne con tre numeri e 31 righe, in totale :

$$30 \times 3 \times 31 = 2790$$

Insomma una cifra delle caselle con chiave di 2790 numeri, sufficiente per messaggi lunghi al massimo 2790 lettere.

Per rendere possibile di nuovo il falso scontro?





# Pietro Partenio

## 1538-1620

Partenio :- originario di Spilimbergo, il cognome è diffuso in Friuli, apre uno studio notarile a Venezia nel 1563, e ottiene la cittadinanza veneziana nel 1576 .

# 1590 Pietro Partenio

Nel 1590 Pietro Partenio un affermato notaio, titolare di uno studio dal 1563, si presenta al CX con queste parole:

*....Applicai già anni vinti et più lo Pietro Partenio servitor di V.S. l'animo mio al studio delle cifre con grandissima mia delezzazione, et con speranza e desiderio di ritrouarne con la grazia di Dio qualcheduna, che potesse essere di comodo a V.S. [...]*

Il CX come è consuetudine nomina una commissione di 5 nobili per valutare la cifra, e l'opinione dei cinque è ampiamente positiva.

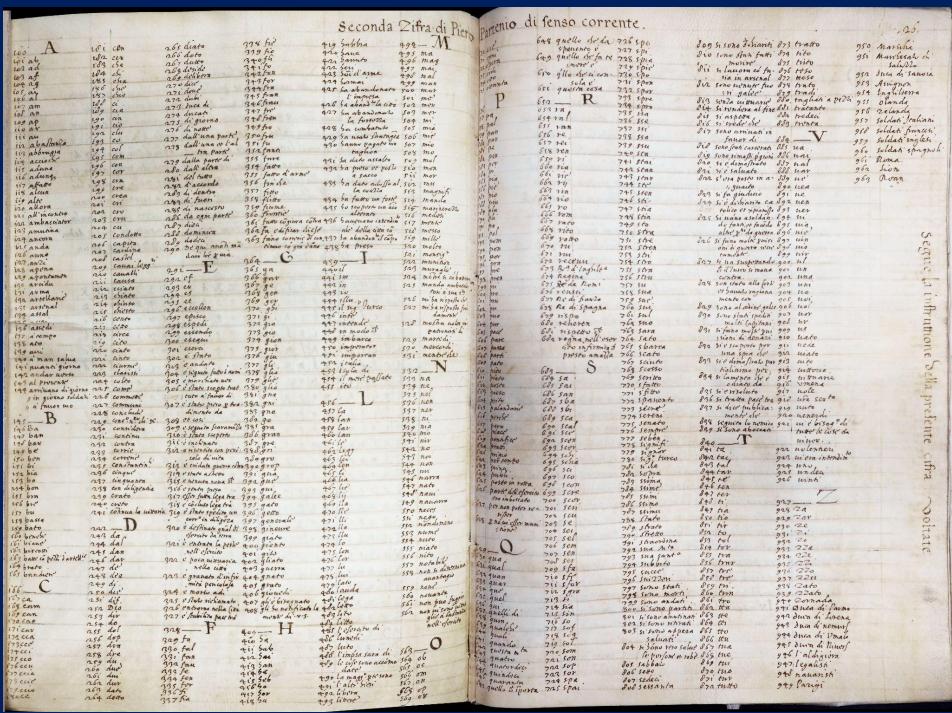
# Le sette cifre di Pietro Partenio

Tra il 1592 e 1593, Partenio dona al CX sette cifre che vengono lodate moltissimo dal CX, ricompensate con un piccolo vitalizio, e trascritte in bella forma su un pregiato volume in pergamena.

Le cifre donate sono molto varie, c'è anche una cifra steganografica che ricorda le Ave Marie del Tritemio: il messaggio viene camuffato da preghiera o altro messaggio sensato e quindi non sospetto.

Più interessanti i nomenclatori come quello della cifra 2 con segni cifranti consistenti in numeri di tre cifre che permettono uno scontro di un migliaio di voci tra lettere,, sillabe, parole ... il tutto accompagnato da una tabellina che Partenio chiama *auertimento* una forma di sovraccifratura utile in caso di furti o smarrimento dello scontro.

Non risulta peraltro che vengano usate da diplomatici o militari, fino al 1595



i Ser <sup>mo</sup> Principe	i No si maraugha v ser <sup>4</sup>	i se non gli scriuo	i Perche son certo	i che quando
2 Ser <sup>no</sup> P. sig colendis <sup>o</sup>	2 Non si ha maraugha	2 se no la rauaglihi	2 perbe son sicuro	2 che quando io
3 Ser <sup>o</sup> P. s <sup>o</sup> mio col <sup>mo</sup>	3 Non resti maraughita	3 se no ha aviso da me	3 perbe tengo certo	3 che ogni fiata d
4 Principe ser <sup>mo</sup>	4 No restira maraughita	4 se ro gli do rauaglihi	4 perbe tengo perto	4 e ogni uolta de
5 Principe ser <sup>mo</sup> sig <sup>o</sup> colmo	5 Non si altera	5 se non ha mie lettere	5 perbe credo	5 che ogni fiata de io
6 Ser <sup>o</sup> P. et sig <sup>o</sup> colmo	6 Nd Sabbia amiratione	6 se no ha letete mie	6 perbe credo certo	6 e ogni uolta che io
7 Principe ser <sup>o</sup> s <sup>o</sup> colmo	7 No prenda amiratione	7 se no riceve mie be'	7 perbe e cosa certa	7 che se
8 P. ser <sup>mo</sup> s <sup>o</sup> mio col <sup>mo</sup>	8 Non prendi maraughi	8 se no e auisata da me	8 perbe tengo perto	8 che se io
9 Ser <sup>o</sup> Piet mu s <sup>o</sup> col <sup>mo</sup>	9 No sabbia alciamirante	9 se no riceve be' mie	9 perbi son sicuriss	9 che merite
o Principe s <sup>o</sup> s <sup>o</sup> mio col <sup>mo</sup>	o No babbia alc'marua <sup>4</sup>	o se no e da me auisata	o perbe tengo perto	o che mortreio
gli seniussi	i con le' in cifra	i sarebbe tutto squarciato	i con dispiacer suo	
2 La rauaglihi	2 con le' cifrate	2 sarebbe tutto abrigiato	2 con dignitudo suo	
3 la auifasa	3 con le' suspece	3 sarebbe tutto malmentato	3 con mala satisfact <sup>o</sup> sua	
4 gli dessi rauaglihi	4 con le' scrite in cifra	4 sarebbe tutto dissipato	4 con assai dispiacer suo	
5 Volesse seniughi	5 co' carattere suspecto	5 andarebbe tutto a male	5 co' poca satisfact <sup>o</sup> sua	
6 uoleffe auisarla	6 co' carat <sup>o</sup> di cifra	6 capitarebbe tutto male	6 co' non poco dispiacer suo	
7 uolesse rauagliharsi	7 in carat <sup>o</sup> di cifra	7 tutto sarebbe squarciato	7 con assai dispiacer suo	
8 uoloffi darli rauaghi	8 in carat <sup>o</sup> e no' nicio	8 tutto sarebbe abrigiato	8 co' molto dispiacer suo	
9 uoloffi darli auiso	9 in carat <sup>o</sup> suspecto	9 tutto sarebbe malmentato	9 con alteratione sua	
o gli seniussi cosa ab <sup>o</sup>	o co' le' non intese	o tutto sarebbe dissipato	o co' qual <sup>o</sup> alteratio sua	

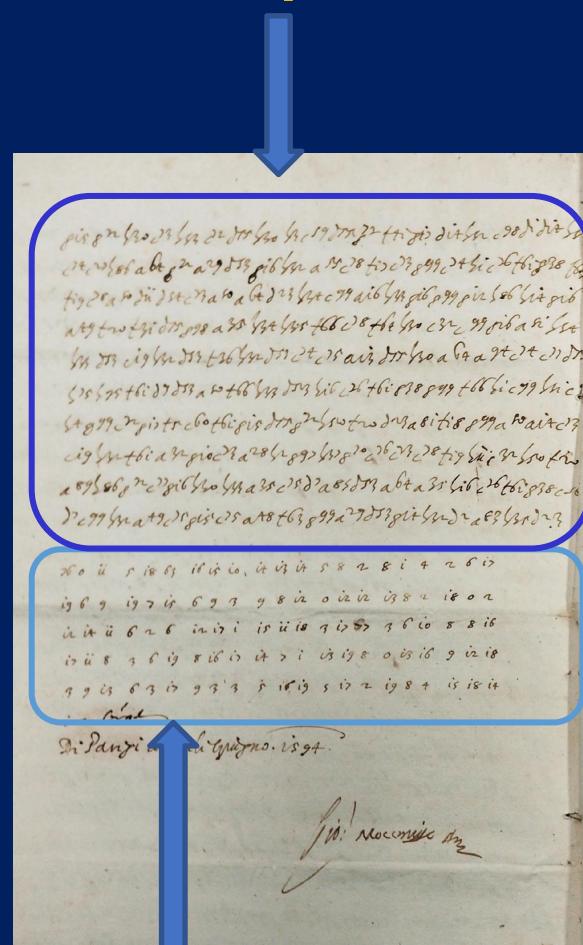
# Giovanni Mocenigo ambasciatore veneziano a Tours e poi a Parigi

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» che gli consegnò come omaggio di Enrico IV 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 **Francois Viète**, il famoso matematico alla corte di Enrico IV.

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.

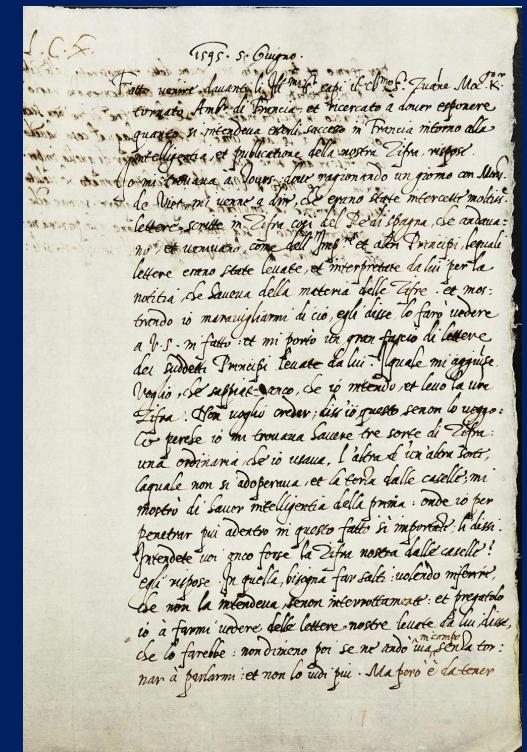
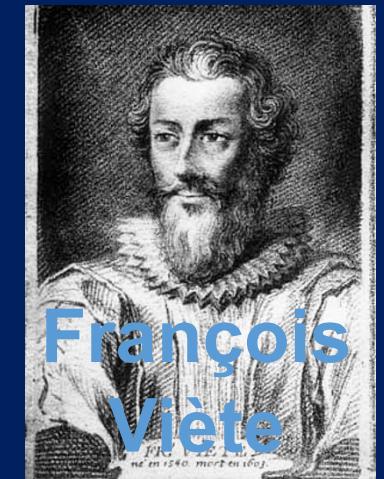
Ziffra prima



Caselle

# 5 giugno 1595 - l'ambasciatore Zuane Mocenigo compare davanti al CX

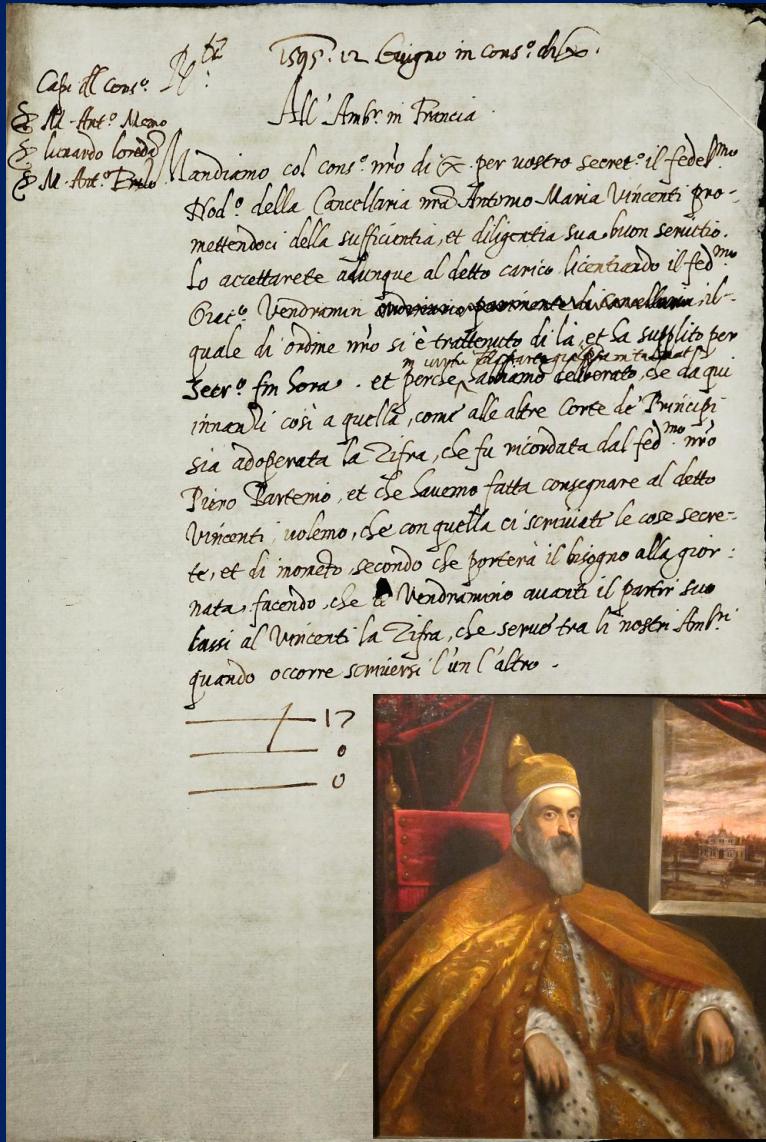
Io lo mi trouaua a Tours doue ragionando un giorno con Mons. de Viet mi uenne a dire che erano intercette moltissime lettere scritte in zifra così del Re di Spagna, che andauano et ueniuano, così come dell'Imperatore et altri Principi, le quali lettere erano state leuate et interpretate da lui per la 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[osta] 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.



## *Domande rimaste aperte*

- 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 viceversa accettò l'ordine del CX di usare la cifra delle caselle negli ultimi anni prima del rientro a Venezia?
- Oppure vi fu un secondo incontro con Viète?
- Perché Viète viola il consolidato principio di non far sapere al nemico i propri successi crittanalitici?

# Una settimana dopo il CX decreta ...



Una settimana dopo, il 12 giugno 1595, il CX decretò all'unanimità, 17 su 17 compreso quindi il Doge Marin Grimani che presiedeva, 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.

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. **FALSO**
- Le cifre del Partenio divennero quelle correnti per le ambasciate veneziane. **FALSO**

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

# <La cifra 5 del Partenio

La cifra approvata dal CX in sostituzione delle caselle era la n.5 di quelle donate al CX.

Quello accanto è lo scontro approvato dal CX per sostituire le caselle per i messaggi o le parti di esso più riservate.

Fu ricavato da quello presentato nel 1592 come cifra 2, ma riducendo il numero di segni cifranti a circa 500, la metà di quella della cifra 2

Si trattava di un nomenclatore con segni cifranti di tre numeri, per esempio A si cifrava con 100, Papa con 401 ...

<i>Partenio..</i>	100 A	150 cam	200 ruzza	250 gno	300 inde'	350 onto'	400 lorenzino'	450 sca	500 sua magia'	550 venona
	101 ad	151 car	201 ducu	251 gruu	301 inghettora	351 abt	401 papa	451 sca'	501 sua signa'	551 vicenda
	102 an	152 cor	202 doran	252 gruu	302 inghettora	352 abt	402 padon	452 sa	502 sua vita'	552 valona
	103 arca	153 ddt	203 doran	253 gruu	303 abt	353 abt	403 porma	453 sca	503 soldati'	553 videro'
	104 accia	154 col	204 domino	254 gruu	304 abt	354 abt	404 plamant'	454 sca	504 sue suzari'	554 uelen'
	105 accia	155 col	205 domino	255 gruu	305 abt	355 abt	405 portogallo	455 sca	505 spagna'	555 uela de la
	106 accia	156 cor	206 dudu	256 gruu	306 abt	356 abt	406 portogallo	456 sca	506 spagnoli'	556 uela de la
	107 accia	157 cor	207 dudu	257 gruu	307 abt	357 abt	407 portogallo	457 sca	507 sua magna'	557 uela magna'
	108 accia	158 cor	208 dudu	258 gruu	308 abt	358 abt	408 portogallo	458 sca	508 sua magna'	558 uela magna'
	109 ambo	159 cor	209 dudu	259 gruu	309 abt	359 abt	409 portogallo	459 sca	509 sua magna'	559 uela magna'
	110 ambo	160 cor	210 dudu	260 gruu	310 abt	360 abt	410 portogallo	460 sca	510 sua magna'	560 uela magna'
	111 ambo	161 cor	211 dudu	261 gruu	311 abt	361 abt	411 portogallo	461 sca	511 sua magna'	561 uela magna'
	112 ambo	162 cor	212 dudu	262 gruu	312 abt	362 abt	412 portogallo	462 sca	512 sua magna'	562 uela magna'
	113 ambo	163 cor	213 dudu	263 gruu	313 abt	363 abt	413 portogallo	463 sca	513 sua magna'	563 uela magna'
	114 ambo	164 cor	214 dudu	264 gruu	314 abt	364 abt	414 portogallo	464 sca	514 sua magna'	564 uela magna'
	115 ambo	165 cor	215 dudu	265 gruu	315 abt	365 abt	415 portogallo	465 sca	515 sua magna'	565 uela magna'
	116 ambo	166 cor	216 dudu	266 gruu	316 abt	366 abt	416 portogallo	466 sca	516 sua magna'	566 uela magna'
	117 ambo	167 cor	217 dudu	267 gruu	317 abt	367 abt	417 portogallo	467 sca	517 sua magna'	567 uela magna'
	118 ambo	168 cor	218 dudu	268 gruu	318 abt	368 abt	418 portogallo	468 sca	518 sua magna'	568 uela magna'
	119 ambo	169 cor	219 dudu	269 gruu	319 abt	369 abt	419 portogallo	469 sca	519 sua magna'	569 uela magna'
	120 ambo	170 cor	220 dudu	270 gruu	320 abt	370 abt	420 portogallo	470 sca	520 sua magna'	570 uela magna'
	121 ambo	171 cor	221 dudu	271 gruu	321 abt	371 abt	421 portogallo	471 sca	521 sua magna'	571 uela magna'
	122 ambo	172 cor	222 dudu	272 gruu	322 abt	372 abt	422 portogallo	472 sca	522 sua magna'	572 uela magna'
	123 ambo	173 cor	223 dudu	273 gruu	323 abt	373 abt	423 portogallo	473 sca	523 sua magna'	573 uela magna'
	124 ambo	174 cor	224 dudu	274 gruu	324 abt	374 abt	424 portogallo	474 sca	524 sua magna'	574 uela magna'
	125 ambo	175 cor	225 dudu	275 gruu	325 abt	375 abt	425 portogallo	475 sca	525 sua magna'	575 uela magna'
	126 ambo	176 cor	226 dudu	276 gruu	326 abt	376 abt	426 portogallo	476 sca	526 sua magna'	576 uela magna'
	127 ambo	177 cor	227 dudu	277 gruu	327 abt	377 abt	427 portogallo	477 sca	527 sua magna'	577 uela magna'
	128 ambo	178 cor	228 dudu	278 gruu	328 abt	378 abt	428 portogallo	478 sca	528 sua magna'	578 uela magna'
	129 ambo	179 cor	229 dudu	279 gruu	329 abt	379 abt	429 portogallo	479 sca	529 sua magna'	579 uela magna'
	130 ambo	180 cor	230 dudu	280 gruu	330 abt	380 abt	430 portogallo	480 sca	530 sua magna'	580 uela magna'
	131 ambo	181 cor	231 dudu	281 gruu	331 abt	381 abt	431 portogallo	481 sca	531 sua magna'	581 uela magna'
	132 ambo	182 cor	232 dudu	282 gruu	332 abt	382 abt	432 portogallo	482 sca	532 sua magna'	582 uela magna'
	133 ambo	183 cor	233 dudu	283 gruu	333 abt	383 abt	433 portogallo	483 sca	533 sua magna'	583 uela magna'
	134 ambo	184 cor	234 dudu	284 gruu	334 abt	384 abt	434 portogallo	484 sca	534 sua magna'	584 uela magna'
	135 ambo	185 cor	235 dudu	285 gruu	335 abt	385 abt	435 portogallo	485 sca	535 sua magna'	585 uela magna'
	136 ambo	186 cor	236 dudu	286 gruu	336 abt	386 abt	436 portogallo	486 sca	536 sua magna'	586 uela magna'
	137 ambo	187 cor	237 dudu	287 gruu	337 abt	387 abt	437 portogallo	487 sca	537 sua magna'	587 uela magna'
	138 ambo	188 cor	238 dudu	288 gruu	338 abt	388 abt	438 portogallo	488 sca	538 sua magna'	588 uela magna'
	139 ambo	189 cor	239 dudu	289 gruu	339 abt	389 abt	439 portogallo	489 sca	539 sua magna'	589 uela magna'
	140 ambo	190 cor	240 dudu	290 gruu	340 abt	390 abt	440 portogallo	490 sca	540 sua magna'	590 uela magna'
	141 ambo	191 cor	241 dudu	291 gruu	341 abt	391 abt	441 portogallo	491 sca	541 sua magna'	591 uela magna'
	142 ambo	192 cor	242 dudu	292 gruu	342 abt	392 abt	442 portogallo	492 sca	542 sua magna'	592 uela magna'
	143 ambo	193 cor	243 dudu	293 gruu	343 abt	393 abt	443 portogallo	493 sca	543 sua magna'	593 uela magna'
	144 ambo	194 cor	244 dudu	294 gruu	344 abt	394 abt	444 portogallo	494 sca	544 sua magna'	594 uela magna'
	145 ambo	195 cor	245 dudu	295 gruu	345 abt	395 abt	445 portogallo	495 sca	545 sua magna'	595 uela magna'
	146 ambo	196 cor	246 dudu	296 gruu	346 abt	396 abt	446 portogallo	496 sca	546 sua magna'	596 uela magna'
	147 ambo	197 cor	247 dudu	297 gruu	347 abt	397 abt	447 portogallo	497 sca	547 sua magna'	597 uela magna'
	148 ambo	198 cor	248 dudu	298 gruu	348 abt	398 abt	448 portogallo	498 sca	548 sua magna'	598 uela magna'
	149 ambo	199 cor	249 dudu	299 gruu	349 abt	399 abt	449 portogallo	499 sca	549 sua magna'	599 uela magna'
	150 ambo	200 cor	250 dudu	300 gruu	350 abt	390 abt	450 portogallo	500 sca	550 sua magna'	600 uela magna'
	151 ambo	201 cor	251 dudu	301 gruu	351 abt	391 abt	451 portogallo	501 sca	551 sua magna'	601 uela magna'
	152 ambo	202 cor	252 dudu	302 gruu	352 abt	392 abt	452 portogallo	502 sca	552 sua magna'	602 uela magna'
	153 ambo	203 cor	253 dudu	303 gruu	353 abt	393 abt	453 portogallo	503 sca	553 sua magna'	603 uela magna'
	154 ambo	204 cor	254 dudu	304 gruu	354 abt	394 abt	454 portogallo	504 sca	554 sua magna'	604 uela magna'
	155 ambo	205 cor	255 dudu	305 gruu	355 abt	395 abt	455 portogallo	505 sca	555 sua magna'	605 uela magna'
	156 ambo	206 cor	256 dudu	306 gruu	356 abt	396 abt	456 portogallo	506 sca	556 sua magna'	606 uela magna'
	157 ambo	207 cor	257 dudu	307 gruu	357 abt	397 abt	457 portogallo	507 sca	557 sua magna'	607 uela magna'
	158 ambo	208 cor	258 dudu	308 gruu	358 abt	398 abt	458 portogallo	508 sca	558 sua magna'	608 uela magna'
	159 ambo	209 cor	259 dudu	309 gruu	359 abt	399 abt	459 portogallo	509 sca	559 sua magna'	609 uela magna'
	160 ambo	210 cor	260 dudu	310 gruu	360 abt	400 abt	460 portogallo	510 sca	560 sua magna'	610 uela magna'
	161 ambo	211 cor	261 dudu	311 gruu	361 abt	401 abt	461 portogallo	511 sca	561 sua magna'	611 uela magna'
	162 ambo	212 cor	262 dudu	312 gruu	362 abt	402 abt	462 portogallo	512 sca	562 sua magna'	612 uela magna'
	163 ambo	213 cor	263 dudu	313 gruu	363 abt	403 abt	463 portogallo	513 sca	563 sua magna'	613 uela magna'
	164 ambo	214 cor	264 dudu	314 gruu	364 abt	404 abt	464 portogallo	514 sca	564 sua magna'	614 uela magna'
	165 ambo	215 cor	265 dudu	315 gruu	365 abt	405 abt	465 portogallo	515 sca	565 sua magna'	615 uela magna'
	166 ambo	216 cor	266 dudu	316 gruu	366 abt	406 abt	466 portogallo	516 sca	566 sua magna'	616 uela magna'
	167 ambo	217 cor	267 dudu	317 gruu	367 abt	407 abt	467 portogallo	517 sca	567 sua magna'	617 uela magna'
	168 ambo	218 cor	268 dudu	318 gruu	368 abt	408 abt	468 portogallo	518 sca	568 sua magna'	618 uela magna'
	169 ambo	219 cor	269 dudu	319 gruu	369 abt	409 abt	469 portogallo	519 sca	569 sua magna'	619 uela magna'
	170 ambo	220 cor	270 dudu	320 gruu	370 abt	410 abt	470 portogallo	520 sca	570 sua magna'	620 uela magna'
	171 ambo	221 cor	271 dudu	321 gruu	371 abt	411 abt	471 portogallo	521 sca	571 sua magna'	621 uela magna'
	172 ambo	222 cor	272 dudu	322 gruu	372 abt	412 abt	472 portogallo	522 sca	572 sua magna'	622 uela magna'
	173 ambo	223 cor	273 dudu	323 gruu	373 abt	413 abt	473 portogallo	523 sca	573 sua magna'	623 uela magna'
	174 ambo	224 cor	274 dudu	324 gruu	374 abt	414 abt	474 portogallo	524 sca	574 sua magna'	624 uela magna'
	175 ambo	225 cor	275 dudu	325 gruu	375 abt	415 abt	475 portogallo	525 sca	575 sua magna'	625 uela magna'
	176 ambo	226 cor	276 dudu	326 gruu	376 abt	416 abt	476 portogallo	526 sca	576 sua magna'	626 uela magna'
	177 ambo	227 cor	277 dudu	327 gruu	377 abt	417 abt	477 portogallo	527 sca	577 sua magna'	627 uela magna'
	178 ambo	228 cor	278 dudu	328 gruu	378 abt	418 abt	478 portogallo	528 sca	578 sua magna'	628 uela magna'
	179 ambo	229 cor	279 dudu	329 gruu	379 abt	419 abt	479 portogallo	529 sca	579 sua magna'	629 uela magna'
	180 ambo	230 cor	280 dudu	330 gruu	380 abt	420 abt	480 portogallo	530 sca	580 sua magna'	630 uela magna'
	181 ambo	231 cor	281 dudu	331 gruu	381 abt	421 abt	481 portogallo	531 sca	581 sua magna'	631 uela magna'
	182 ambo	232 cor	282 dudu	332 gruu	382 abt	422 abt	482 portogallo	532 sca	582 sua magna'	632 uela magna'
	183 ambo	233 cor	283 dudu	333 gruu	383 abt	423 abt	483 portogallo	533 sca	583 sua magna'	633 uela magna'
	184 ambo	234 cor	284 dudu	334 gruu	384 abt	424 abt	484 portogallo	534 sca	584 sua magna'	634 uela magna'
	185 ambo	235 cor	285 dudu	335 gruu	385 abt	425 abt	485 portogallo	535 sca	585 sua magna'	635 uela magna'
	186 ambo	236 cor	286 dudu	336 gruu	386 abt	426 abt	486 portogallo	536 sca	586 sua magna'	636 uela magna'
	187 ambo	237 cor	287 dudu	337 gruu	387 abt	427 abt	487 portogallo	537 sca	587 sua magna'	637 uela magna'
	188 ambo	238 cor	288 dudu	338 gruu	388 abt	428 abt	488 portogallo	538 sca	588 sua magna'	638 uela magna'
	189 ambo	239 cor	289 dudu	339 gruu	389 abt	429 abt	489 portogallo	539 sca	589 sua magna'	639 uela magna'
	190 ambo	240 cor	290 dudu	340 gruu	390 abt	430 abt	490 portogallo	540 sca	590 sua magna'	640 uela magna'
	191 ambo	241 cor	291 dudu	341 gruu	391 abt	431 abt	491 portogallo	541 sca	591 sua magna'	641 uela magna'
	192 ambo	242 cor	292 dudu	342 gruu	392 abt	432 abt	492 portogallo	542 sca	592 sua magna'	642 uela magna'
	193 ambo	243 cor	293 dudu	343 gruu	393 abt	433 abt	493 portogallo	543 sca	593 sua magna'	643 uela magna'
	194 ambo	244 cor	294 dudu	344 gruu	394 abt	434 abt	494 portogallo	544 sca	594 sua magna'	644 uela magna'
	195 ambo	245 cor	295 dudu	345 gruu	395 abt	435 abt	495 portogallo	545 sca	595 sua magna'	645 uela magna'
	196 ambo	246 cor	296 dudu	346 gruu						

# La cifra 5 del Partenio

- La cifra approvata dal CX in sostituzione delle caselle era la n.5 di quelle donate al CX.
- Si trattava di un nomenclatore con segni cifranti di tre numeri, per esempio A si cifrava con 100, Papa con 401 ...
- La novità è l'aggiunta di una tabellina di sovraccifratura, accanto due esempi uno banale e ordinato, l'altro quello usato a Parigi nel 1595.  
L'esempio a lato mostra come cifrare, per decifrare si fa il percorso inverso.
- L'operazione di cifra **non** è univoca.
- L'operazione di decifra è univoca.

Semplice 1593

Chiave ordinata semplice dal volume ASVe CX Raccordi 1 1593

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

Francia 1595

Chiave usata dall'ambasciata di Francia nell'estate 1595

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

**Esempio:** per cifrare *Papa* si cerca la parola nello scontro e si trova 401.

401 va sovraccifrato cifra per cifra usando la tabellina che fa da chiave:

sotto 4 si trovano **f** ed **l**, se ne sceglie una a caso, diciamo **f**  
sotto **0** ci sono **p** ed **h**,

scegliamo **p**

sotto **1** ci sono **c** e **t**, scegliamo **t** e quindi *Papa* si cifra con **fpt**

Papa

4	0	1
f	p	t

A

1	0	0
c	p	h
t	h	p

# **1596 la sfida di Franceschi**

*Comparso li giorni passati dauanti gli Ecc.<sup>mi</sup>. S<sup>ri</sup> Capi dell'III.<sup>mo</sup> Cons.<sup>o</sup> di X il circ. et fd.<sup>mo</sup> sect.<sup>o</sup> del Senato Hieronimo di Franceschi espose a SS. Ecc.<sup>me</sup> che hauendo il fed.<sup>mo</sup> Piero Partenio data la sua zifra con una particolare expressa conditione che senza un suo auertimento col quale si scriue, ella è intrazibile quando ben il scontro con la cosa scritta secondo quello capitasse in mano d'altri ,*

*egli per il zelo et obbligo che ha di anteporre ad ogni altro rispetto il seruitio del suo Principe,*

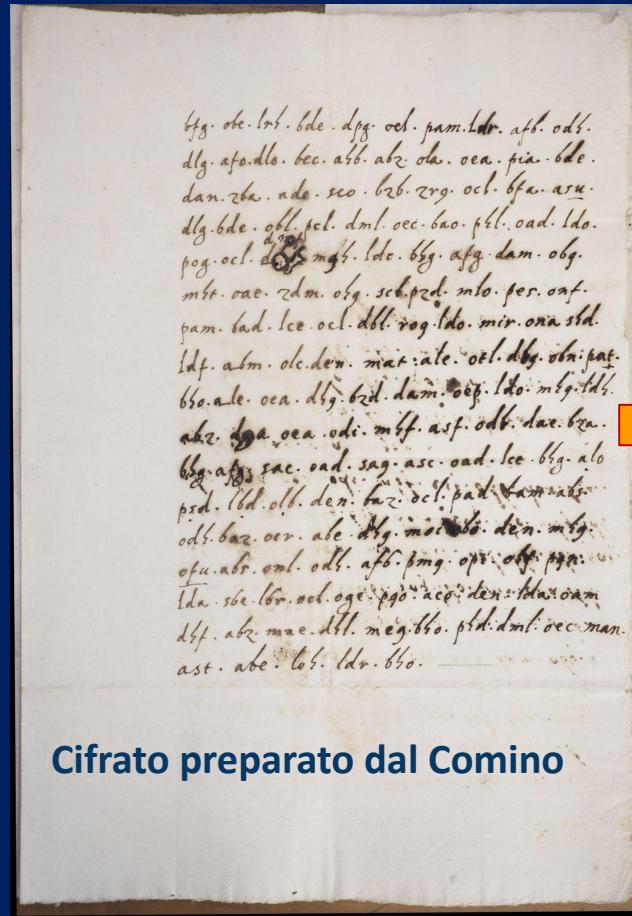
*si obligasse di far conoscer il fatto che la zifra del d.<sup>o</sup> Partenio è trazibile, et che egli senza sapere alcun suo particolare auertimento la trazerà*

....

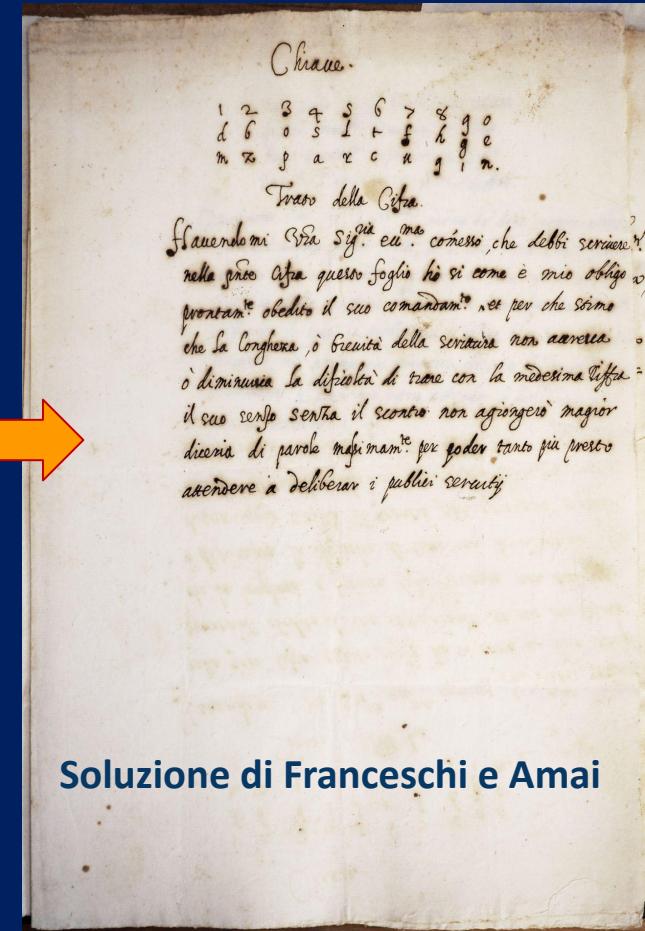
- ASVe - Parti secrete del CX data 8 agosto 1596

# Agosto 1596 Franceschi forza la cifra 5!

[...] uenne il Franceschi pochi giorni dapoi insieme col fed<sup>mo</sup> Piero Amai giouene deputato alle zifre, et allieuo di esso Franceschi, et presentò scritto il senso della zifra data cauata il qual senso confrontato col primo originale si trouò esser l'istesso di parola in parola.



Cifrato preparato dal Comino



Soluzione di Franceschi e Amai

Comino 1596

Chiave usata dal segretario Comino per la sfida di Franceschi del 1596

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

# **30 agosto 1596**

## **Partenio si giustifica**

*Et essendo di poi stato chiamato al tribunale di SS.SS. Ecc.<sup>me</sup> il Partenio con dirli che la sua zifra era stata cauata dal Franceschi, come di sopra, et che douesse anch'egli dire quanto li pareua per suo interesse, confessò che la zifra sua non era compitamente perfetta, perché ella non arriuaua al n<sup>o</sup> di mille ma di 500 soli numeri, il quale non era suo difetto, perché egli da principio offerse et diede la sua zifra perfetta mostrando il uero modo da usarla intrazibile che era di arriuar a mille numeri, ma che poi era stata fatta in quest'altra maniera con numeri fino a 500.*

# **... settembre 1596**

## **ma il CX non è convinto**

*Secondo il parere et ordine del medesimo Franceschi et altre sue simili ragioni et escusationi, le quali udite et maturam<sup>te</sup> considerato il tutto SS.SS.Ecc<sup>me</sup> per l'autorità dalle leggi a quelle concessa in tal materia hanno terminato che sia quanto prima scritto così la nouo Bailo che ua à Const<sup>li</sup> come in tutti i luoghi, doue farà bisogno, che nelle occasioni di scriuer in zifra debba continuar à scriuer con la zifra ordinaria; ma occorrendo cose di estraordinaria importanza adoperino la **zifra delle caselle** del detto Franceschi, soprasedendo dal scriuer nella zifra del Partenio fino ad altro ordine del predetto Conso*

## ***Settembre 1596 – virulenta reazione del Partenio***

Pochi giorni dopo arriva la reazione del Partenio, una lunghissima lettera, nella quale sostiene che lui per *avvertimento* intendeva non solo la tabellina ma anche le istruzioni d'uso della medesima, lamenta il fatto che sia stato chiamato a preparare la sfida un segretario che non conosceva bene la cifra e che avrebbero dovuto chiamare l'autore della cifra, e aggiunge:

- *Protesto (siami lecito così dire con buona gratia di V.S. III.<sup>me</sup>) che la proua da loro et tra loro fatta è nulla et un ordimento fabricato dal sud<sup>o</sup> Franc<sup>i</sup> per leuarmi l'onore, la riputatione et la gratia del mio Principe non ingannato da me per malitia [...]*
- Partenio concludeva poi riconoscendo che la *cifra delle caselle* era fortissima, ma sottoposta al rischio del furto e finiva paragonandola, per il fatto di cifrare lettera per lettera, alla cifra del Tritemio vecchia ormai di 90 anni.

# *16 settembre 1596 – il CX si spacca e si affida a una commissione di 5 nobili*

- Letta questa lettera del Partenio il CX si spaccò in due opposte fazioni e come già fatto in passato decise di affidarsi a una commissione di 5 nobili.
- Furono eletti:
- Leonardo Donà, il futuro doge protagonista di un famoso scontro con il papato e patrocinatore di Galileo e del suo cannocchiale.
- Giacomo Foscarini
- Niccolò Gussoni
- Paolo Peruta
- Giacomo Soranzo



## *Gennaio 1598 (1597 m.v.) – la commissione è sollecitata a decidere qualcosa*

All'inizio la commissione se la prese comoda tanto che dopo 18 mesi nel febbraio 1598 (1597 more veneto, capodanno il 1 marzo), il CX preso atto che la delibera del 16 set 1596 non era stata eseguita, sollecitava i cinque a concludere qualcosa al più presto.

Cercando tra le delibere del CX non si trova poi più nulla, la commissione sembra svanita nel nulla, ma ...

# *1599 1600 (?) ma la commissione dei 5 nobili avea concluso qualcosa?*

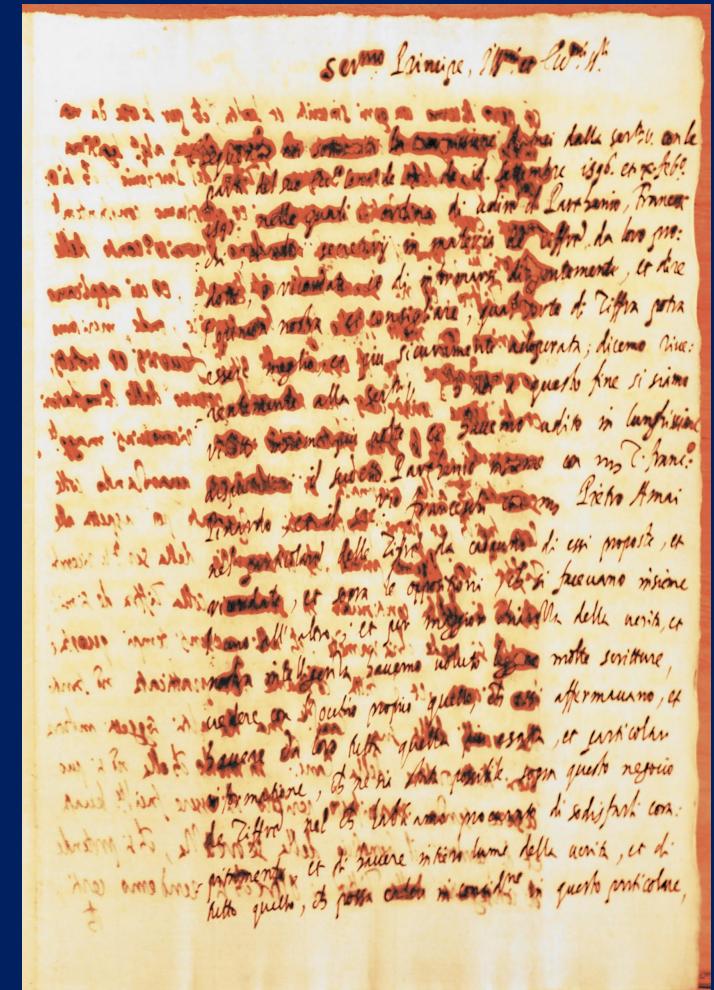
Cosa aveva concluso la commissione? Aveva poi concluso qualcosa?

Solo all'inizio di quest'anno 2022 sono emerse da una busta 6 due fascicoli di fogli a mala pena leggibili per il trasudare degli inchiostri attraverso le pagine.

Ma fotografando, ingrandendo, osservando di traverso, all'inizio della prima pagina finalmente si leggeva:

*Eseguendo noi sottoscritti la commissione dataci dalla Ser<sup>tà</sup> V. con le parti del suo Eccelso Consiglio de X de 16 Settembre 1596 et X Feb 1597 ...*

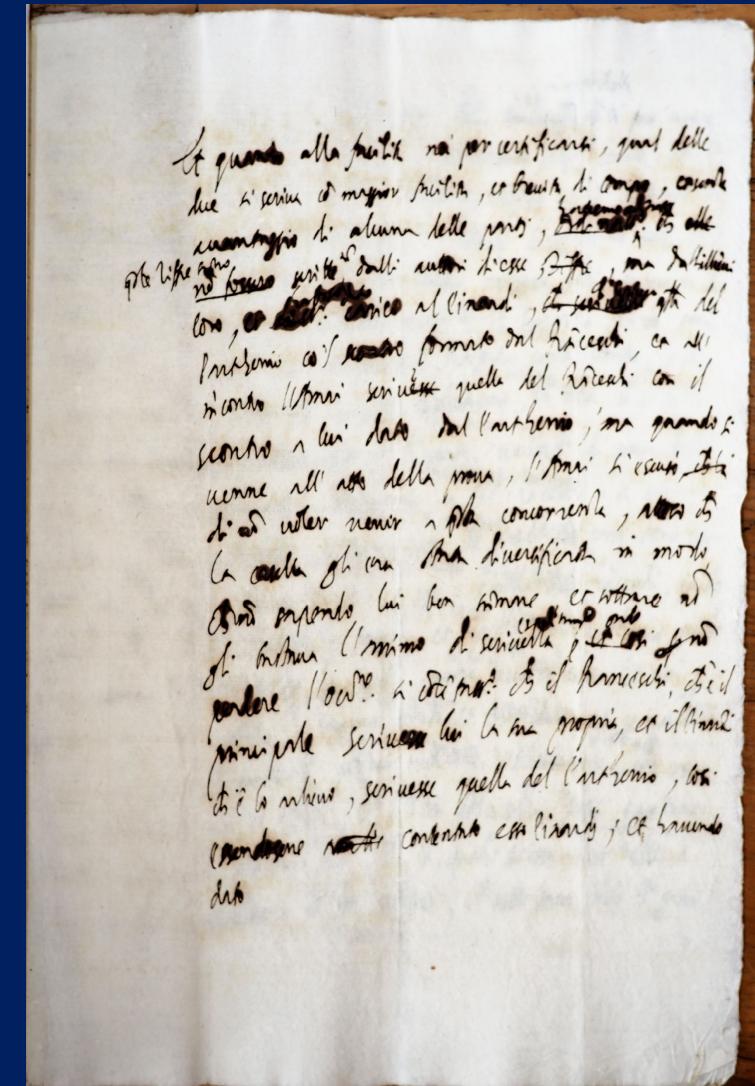
Erano le due minute della relazione finale , mai consegnata!



# **1599 1600 (?) la commissione dei 5 organizza la finalissima Franceschi vs Partenio, ma ...**

- Dopo numerose e lunghe discussioni con i due antagonisti, la commissione decise di organizzare una prova per confrontare le due cifre in termini di velocità e facilità d'uso.

[...] 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 che non sapendo lui ben summare et sottrarre non gli bastaua l'animo di scriuerla per quel tramite, donde non perdere l'occasione si continuerà con il Franceschi, che è il principale scriuesse lui la sua propria, et il Pinardi che è lo alieuo scriuesse quella del Parthenio, così essendosene contentato esso Pinardi, et hauendo dato a tutte doi le parti l'istessa cosa da scriuere, trouiamo per esperienza di molta [importantia?], et che pregiudicheria troppo al publico seruitio che per le difficoltà della ziffra douessero trattenersi lungamente, non essendo alcuno che non conosca quanto [giudi..uoli] la [lentezza] o la perda di un auiso; et però quanto alla facilità diremo che quella del [Franceschi] adoperarsi più facilmente dell'altra, Eseguendo noi sottoscritti la commissione [...]



# Exit Franceschi

Ma la relazione dei 5 nobili non fu mai consegnata.

Motivo più probabile la morte del Franceschi che dovette avvenire nella prima metà del 1600, dato che nel giugno 1600 il CX deliberò una sanatoria dei debiti che i due nipoti avevano ereditato dal loro nonno H. di Franceschi.

Per parte sua Partenio scompare per cinque anni da carte e delibere per ritornare in scena all'inizio del 1606.

# L'ultima cifra del Partenio

Nel 1605, cinque anni dopo la triste conclusione della disputa con Franceschi e la sua morte, Pietro Partenio scrisse una lunga lettera al CX deprecando la scarsa qualità delle cifre utilizzate in quegli anni, in effetti una cifra chiamata z10, che era un normalissimo nomenclatore con segni cifranti fatti di lettere e numeri.

E si offrì anche di scrivere un nuovo libretto di cifrari più sicuri. L'ultima cifra del libretto (ancora presente negli Archivi veneziani), utilizza un quadrato che richiama da vicino quello di Franceschi, ma con una trasposizione della chiave come il primo cifrario, e con questo quadrato per generare un altro testo.

Qui Partenio sembra il verso a Franceschi

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

E N L E X T V A M E D I T A T I O M E A I N C O R D E M E O  
06 19 15 07 25 28 00 16 08 04 12 26 01 27 13 21 17 09 02 14 20 03 22 24 05 10 18 11 23  
I R C N I A V A B N C A I A I B P R S A I O E L O E I S L

# Exit Partenio

*Dalla relazione finale, aprile 1621, dei tre nobili incaricati dal CX nel 1619 di riformare le cifre veneziane*

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

Pietro Partenio peraltro non seppe mai di questa liquidazione finale delle sue cifre.

Era morto nel 1620, alla bella età di 82 anni, secondo le genealogie del Tassini non aveva nè moglie nè figli. Ma considerava “quale mio figliolo” il giovanissimo aspirante cifrista Ottavian Medici

# Una cifra di Ottavian Medici

Alla fine insomma sia le cifre di Franceschi, sia quelle di Partenio furono abbandonate e per sempre, paradossalmente con motivazioni simili: troppo complicate e lente da usare nel mondo reale

La commissione dei 3 nobili sancì la svolta con una nuova cifra progettata da due giovani cifristi Ottavian Medici, il pupillo di Partenio e destinato a divenire la figura dominante della crittografia veneziana, in effetti l'ultimo cifrista veneziano di qualche spessore, e Giambattista Lionello del quale invece si perdono poi le tracce,

La cifra è un nomenclatore normale con alfabeto duplice (con due omofoni per lettera), sillabario, nulle, e dizionario, l'parziale novità è che i segni cifranti sono fatti di soli numeri di tre cifre decimali. Medici aggiunse l'espeditivo tratto dal trattato di Matteo Argenti, segretario alle cifre papali, di scrivere tutte le cifre decimali attaccate in modo che non si vedesse la separazione tra segni cifranti.

Alfabeto																										
a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	z							
156	157	158	159	256	175	258	259	356	357	176	276	376	457	458	177	277	377	477	559							
174	274	374	474	574	257	275	375	475	575	358	359	456	476	576	459	556	557	558	577							
Numeri																										
0	1	2	3	4	5	6	7	8	9																	
579	178	179	278	279	378	379	478	479	578																	
41 Nulle																										
86	87	88	89	96	97	98	99	100	101	102	103	104	105	106	114	123	132	141	150							
180	214	223	232	241	250	314	323	332	341	350	414	423	432	441	450	514	523	532	541							
550																										
Sillabario																										
ba	be	bi	bo	bu	bra	bre	bri	bro	bru	ca	ce	ci	co	cu	cra	cre	cri	cro	cru	da	de	di	do	du		
115	116	117	118	119	215	216	217	218	219	315	316	317	318	319	415	416	417	418	419	515	516	517	518	519		
dra	dre	dri	dro	dru	fa	fe	fi	fo	fu	fra	fre	fri	fro	fru	ga	ge	gi	go	gu	gna	gne	gni	gno	gnu		
124	125	126	127	128	224	225	226	227	228	324	325	326	327	328	424	425	426	427	428	524	525	526	527	528		
gra	gre	gri	gro	gru	ha	he	hi	ho	hu	ia	ie	ii	io	iu	la	le	li	lo	lu	ma	me	mi	mo	mu		
133	134	135	136	137	233	234	235	236	237	333	334	335	336	337	433	434	435	436	437	533	534	535	536	537		
na	ne	ni	no	nu	pa	pe	pi	po	pu	pla	ple	pli	pio	plu	pra	pre	pri	pro	pru	qua	que	qui	quo	quu		
142	143	144	145	146	242	243	244	245	246	342	343	344	345	346	442	443	444	445	446	542	543	544	545	546		
ra	re	ri	ro	ru	sa	se	si	so	su	sca	sce	sci	sco	scu	spa	spe	spi	spo	spu	sta	ste	sti	sto	stu		
151	152	153	154	155	251	252	253	254	255	351	352	353	354	355	451	452	453	454	455	551	552	553	554	555		
stra	stre	stri	stro	stru	ta	te	ti	to	tu	tra	tre	tri	tro	tru	ua	ue	ui	uo	uu	za	ze	zi	zo	zu		
160	161	162	163	164	260	261	262	263	264	360	361	362	363	364	460	461	462	463	464	560	561	562	563	564		

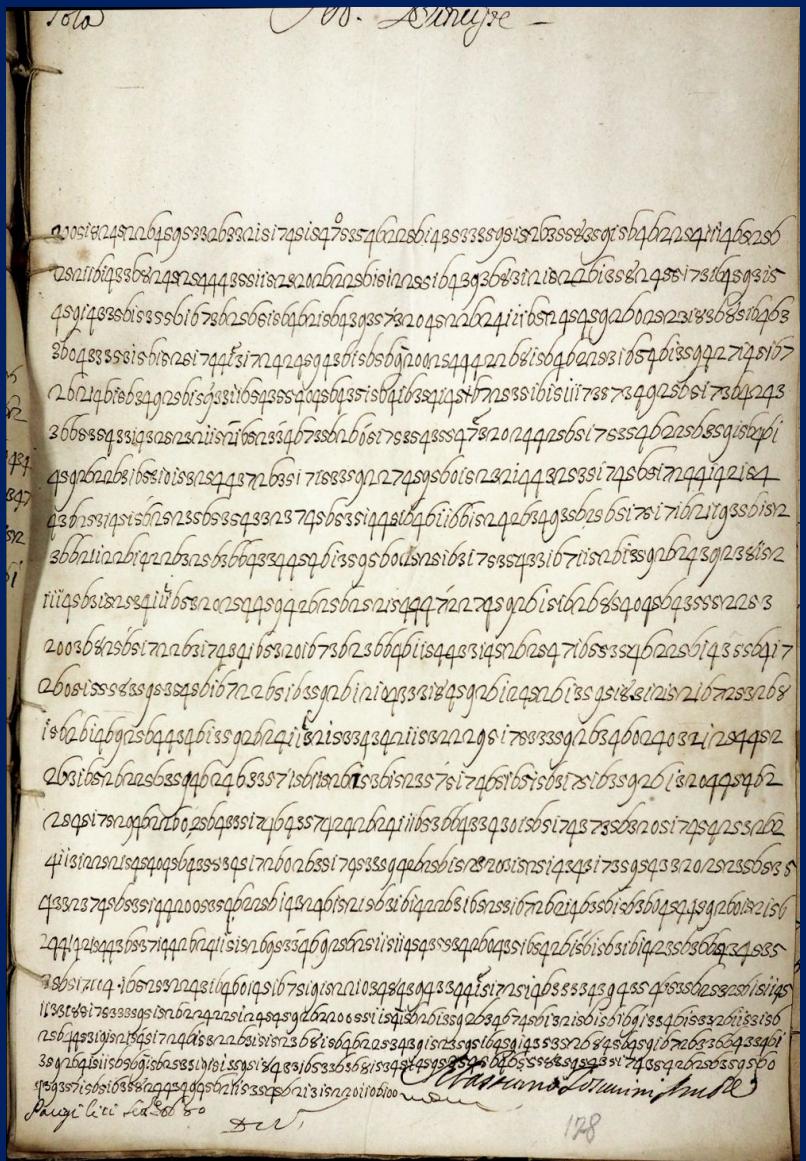
# Conclusion?

Dopo Medici ... il nulla; i suoi successori si limitarono a riciclare le cifre del Medici fino alla fine della repubblica; alla fine del Seicento torna in uso tale e quale la cifra del 1621,

Il dispaccio accanto, totalmente cifrato, firmato dall'ambasciatore a Parigi Sebastiano Foscarini, datato 2 settembre 1680, usa ancora la cifra del 1621, quasi sessant'anni dopo.

nel 1715 viene ripescata una cifra del Medici del 1630.

...ed è proprio la fine!

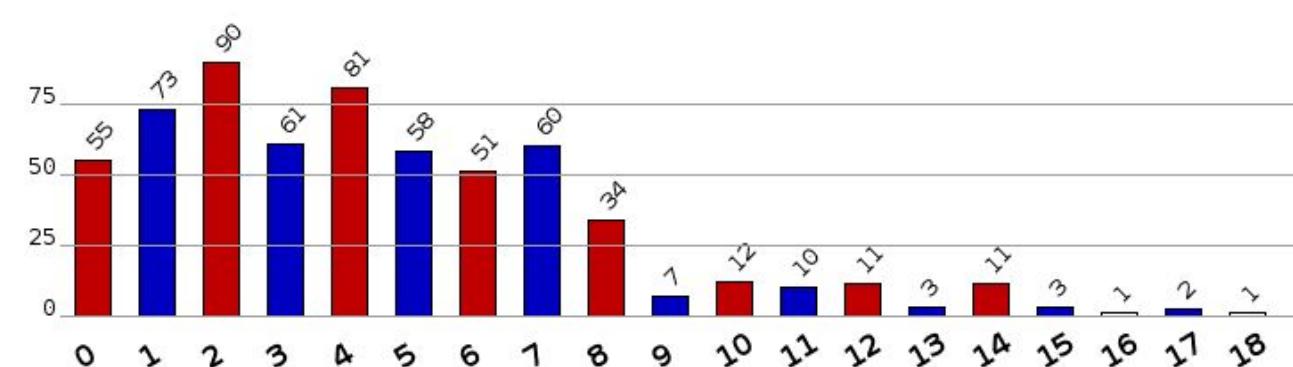


**Grazie per l'attenzione!**

# Grata Germania

(Holy Roman Empire, Prag, Vienna)

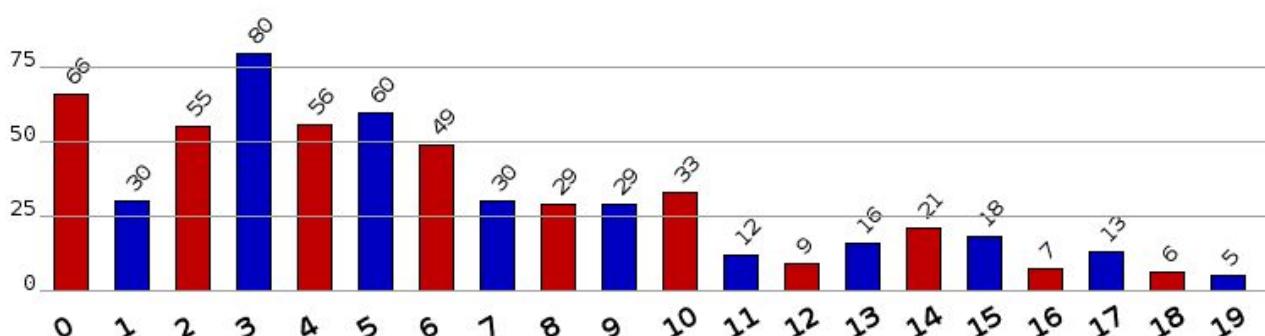
Is it really disordered?



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

# Grata Costantinopoli (Impero Ottomano)

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