

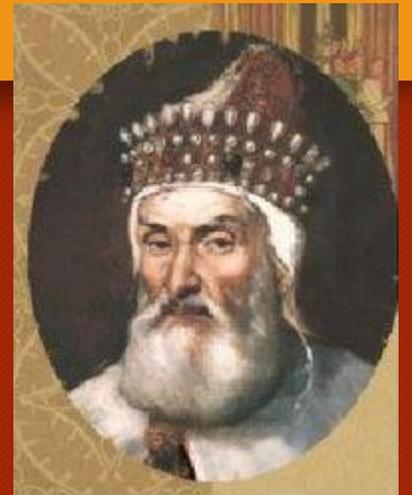
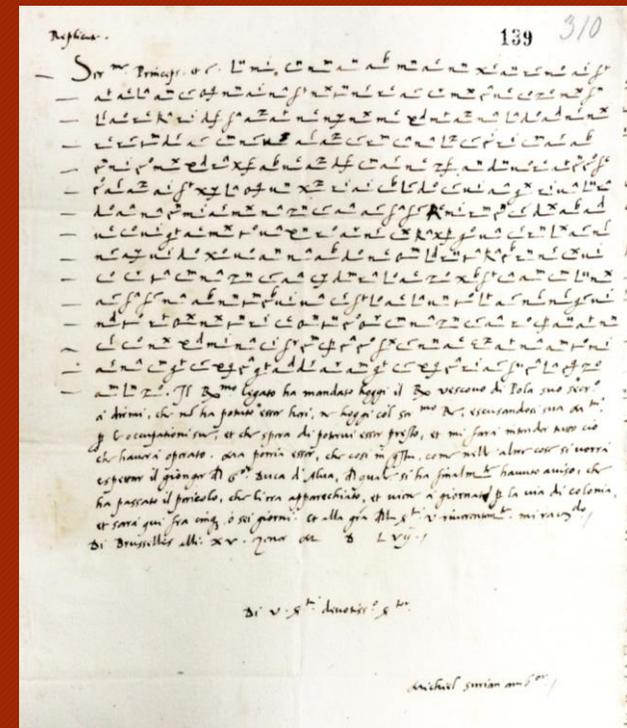
Convitto Nazionale  
Marco Foscarini  
Venezia

# Crittografia a Venezia tra matematica e storia

La Crittografia come matematica applicata

La Crittografia come strumento di ricerca storica

© Mathesis Venezia Paolo Bonavoglia  
26 nov 2018 aula magna Liceo Foscarini di Venezia  
© Archivio di stato di Venezia



# L'Archivio di Stato di Venezia

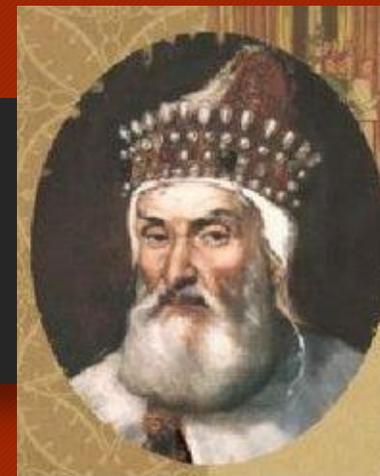
- Custodisce un numero enorme di:
- Dispacci cifrati di ambasciatori nelle capitali europee, per esempio Madrid, Parigi, ma anche Roma, Torino
- Dispacci di governatori di domini veneziani, per esempio Candia, Spalato ...
- Cifrari (chiavi o scontri di cifra) usati



[Archivio di Stato di Venezia](#)

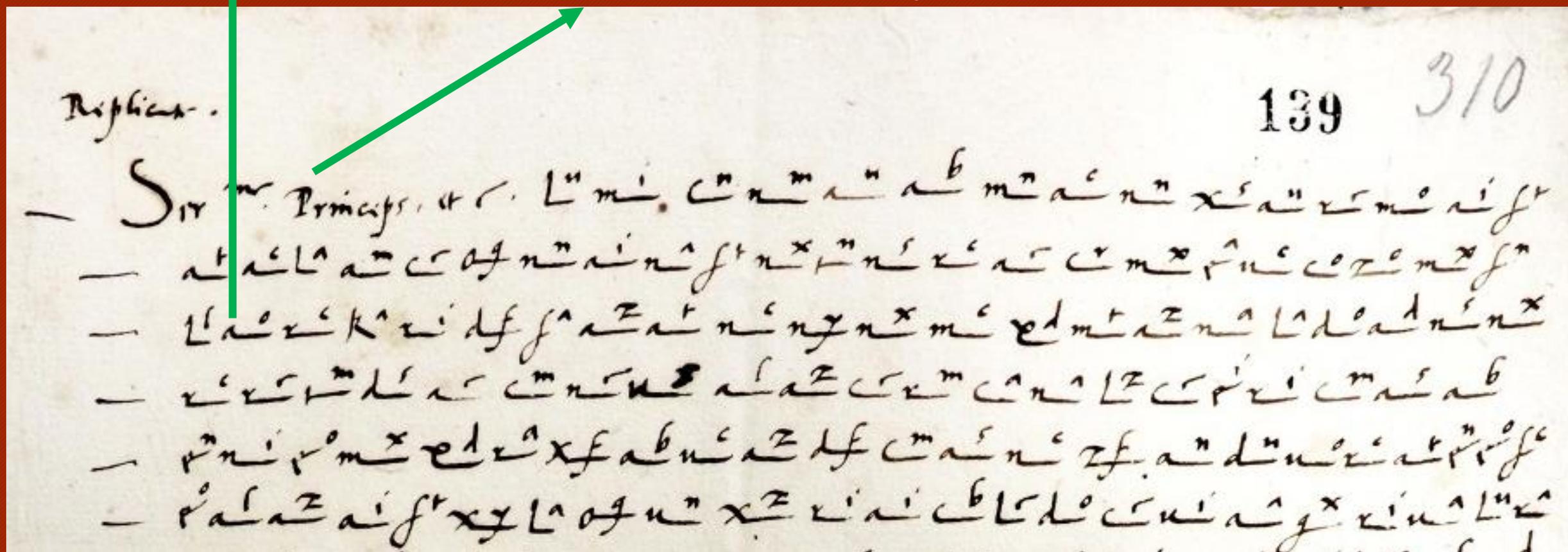


# Un dispaccio cifrato al Doge Lorenzo Priuli

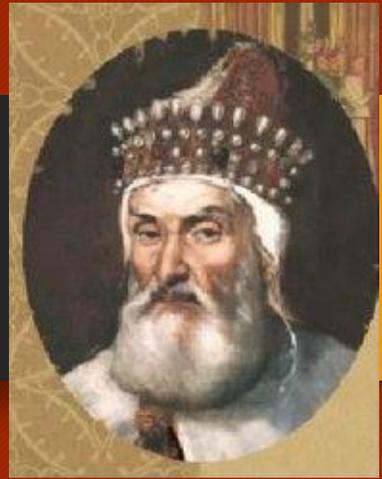


Il messaggio è in buona parte cifrato

Perché non cifrare anche questo?



# Un dispaccio da Bruxelles 15-1-1557 (o 1558?)



che hanno operato. Ora fanno esser, che così in q<sup>ta</sup>, come nell'altre cose si uorra  
esperare il giouorno di Co<sup>te</sup>. Duca d'Alua, di qual. si ha finalm<sup>te</sup> haunto auiso, che  
ha passato il periculo, che li era apparecchiato, et uien a giornata per la uia di Colonia,  
et sarà qui fra cinq. o sei giorni. et alla gra<sup>te</sup> d<sup>te</sup> v. riuocant<sup>te</sup>. miraco<sup>do</sup>.  
di Brusselles alli xv. g<sup>no</sup>. 1557.

Di v. s<sup>ta</sup>. duca d'Alua. s<sup>ta</sup>.

Michael surian amb<sup>or</sup>.

Di Bruxelles alli 15 gen 1557  
Che ci fa l'ambasciatore di  
Venezia in Spagna a Bruxelles??

Di Bruxelles alli 15 gen 1557  
Ma la presa di Calais fu nel  
gennaio 1558.  
Come si spiega??

# Un dispaccio decifrato

Responso.

139 310

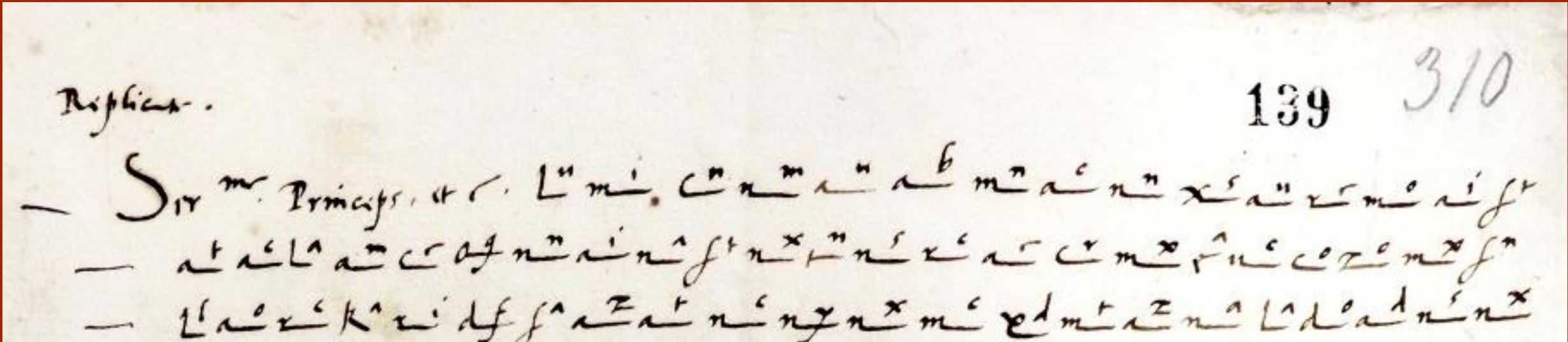
— Sir<sup>mo</sup> Principis, et c. L<sup>o</sup> mi. C<sup>o</sup> n<sup>o</sup> a<sup>o</sup> b<sup>o</sup> m<sup>o</sup> a<sup>o</sup> n<sup>o</sup> x<sup>o</sup> a<sup>o</sup> r<sup>o</sup> m<sup>o</sup> n<sup>o</sup> i<sup>o</sup> f<sup>o</sup>  
— a<sup>o</sup> t<sup>o</sup> a<sup>o</sup> l<sup>o</sup> a<sup>o</sup> c<sup>o</sup> a<sup>o</sup> g<sup>o</sup> n<sup>o</sup> a<sup>o</sup> i<sup>o</sup> n<sup>o</sup> f<sup>o</sup> n<sup>o</sup> x<sup>o</sup> n<sup>o</sup> r<sup>o</sup> a<sup>o</sup> c<sup>o</sup> m<sup>o</sup> f<sup>o</sup> u<sup>o</sup> c<sup>o</sup> o<sup>o</sup> r<sup>o</sup> m<sup>o</sup> f<sup>o</sup>  
— U<sup>o</sup> a<sup>o</sup> r<sup>o</sup> k<sup>o</sup> a<sup>o</sup> i<sup>o</sup> d<sup>o</sup> f<sup>o</sup> a<sup>o</sup> z<sup>o</sup> a<sup>o</sup> t<sup>o</sup> n<sup>o</sup> i<sup>o</sup> n<sup>o</sup> x<sup>o</sup> m<sup>o</sup> e<sup>o</sup> d<sup>o</sup> m<sup>o</sup> a<sup>o</sup> z<sup>o</sup> n<sup>o</sup> a<sup>o</sup> l<sup>o</sup> d<sup>o</sup> a<sup>o</sup> n<sup>o</sup> x<sup>o</sup>

**Archivio di Stato di Venezia**  
Senato, dispacci degli ambasciatori in Spagna,  
Decifrazioni di Luigi Pasini, Spagna 100

Di Bruselles XV Gennaio 1557.  
Ser<sup>mo</sup> Principis etc. [ Questa mattina  
è sparsa una voce per la Corte,  
senza saperse la origine, che fran-  
cesi sono andati sopra quines; et  
perche il loco è molto picciolo si

# Un dispaccio trascritto e decifrato

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  
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  
Questa mattina è sparsa una uoce per la corte senza sapersi la



# Sostituzione, i nomenclatori

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  
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

Questa mattina è sparsa una uoce per la corte senza sapersi la

## Nomenclatore

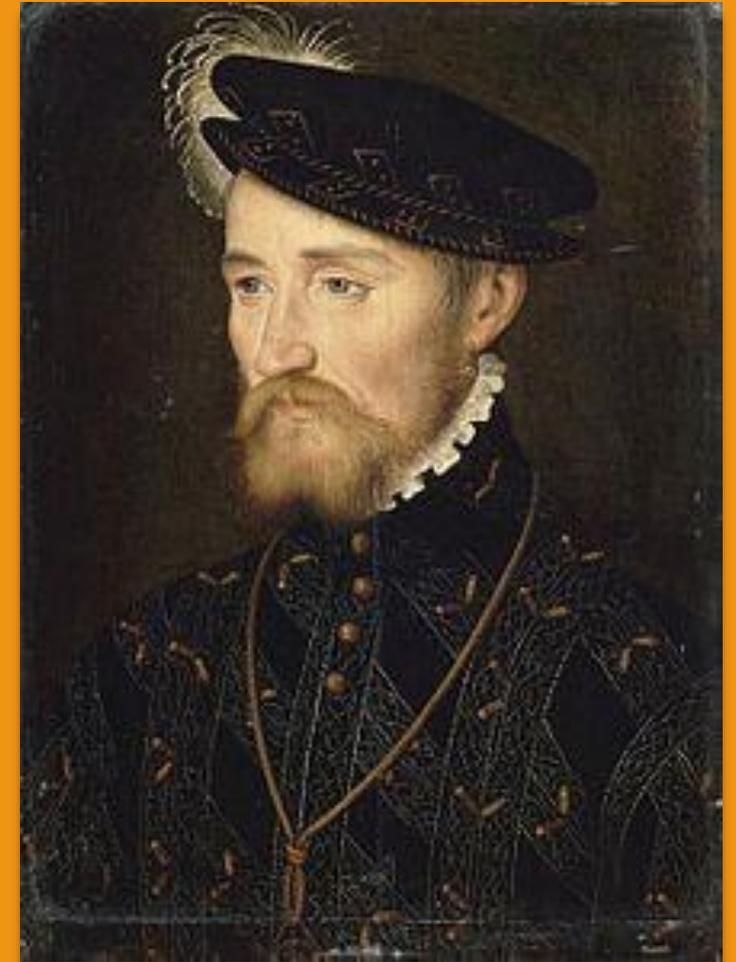
Cifrario per sostituzione: per lettera, per sillaba, per parole parziali o intere

Nella cancelleria del Doge i dispacci venivano decifrati da personale addestrato

# Il testo decifrato

- Questa mattina è sparsa una uoce per la corte senza sapersi la origine che Franzesi sono andati sopra Guines et perché il loco è molto picciolo si teme ragioneuolmente che non potrà far longa resistenza et non ui è modo di soccorrerlo perché non ui è essercito in esser ne comodita di farlo per la streteza del tempo et per mancamento de danari et con questo medesimo auiso si intende che il conte d Agamon il quale era andato uerso li confini come gia scrissi con quelle gente che ha potuto metter insieme e stato rotto et sualegiato da Franzesi et non si intende anchor altro particolare se non questo come il conte si e saluato con quella parte delli sui come ha hauuto caualli migliori et più presti di Anglia non si intende niuna cosa il che da occasione ad ogniuno di pensar mal cosi se li auisi non uengono ueramente come se uengono et che siano tenuti secreti

Perché auisi e non avisi?



Francesco I Duca di Guisa  
Comandante dell'esercito francese

# Alfabeto, sillabario, dizionario

## ALFABETO [Omofoni, massimo = 3]

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

## NUMERI

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>									

## SILLABARIO [30 sillabe]

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

Ricostruito da  
Luigi Pasini  
Intorno al 1870

DIZIONARIO									
accio	r <sup>f</sup>	del	u <sup>n</sup>	il quale	d <sup>x</sup>	one	c <sup>i</sup>	rispo	u <sup>e</sup>
ad	f <sup>r</sup>	deside	f <sup>b</sup>	ill.mo	d <sup>d</sup>	opera	u <sup>m</sup>	Roma	x <sup>i</sup>
al	n <sup>t</sup>	detta M.tà	E <sup>e</sup>	illustr	f <sup>h</sup>	or amb	a <sup>f</sup>	rr	x <sup>f</sup>
alcun	c <sup>t</sup>	ditt	z <sup>s</sup>	imp.Cesare	d <sup>e</sup>	ora	u <sup>f</sup>	S.Turco	E <sup>b</sup>
altr	d <sup>m</sup>	doue	o <sup>y</sup>	in	z <sup>b</sup>	ordin	E <sup>i</sup>	scrit	o <sup>t</sup>
an	u <sup>c</sup>	duca	R <sup>b</sup>	in	a <sup>n</sup>	pace	d <sup>l</sup>	scriue	z <sup>e</sup>
anchor	c <sup>y</sup>	duca di Sassonia	Z <sup>h</sup>	inte	z <sup>n</sup>	pare	t <sup>l</sup>	scudi	x <sup>x</sup>
inglesi	g <sup>l</sup>	esse	d <sup>u</sup>	Italia	d <sup>q</sup>	passat	o <sup>i</sup>	sempre	t <sup>d</sup>
Anglia	o <sup>r</sup>	essercito	z <sup>f</sup>	la qual	t <sup>e</sup>	per	a <sup>i</sup>	senato	E <sup>x</sup>
armata	n <sup>f</sup>	et	t <sup>a</sup>	langraui	c <sup>q</sup>	perché	d <sup>f</sup>	Ser.mo Principe	u <sup>z</sup>
bb	L <sup>h</sup>	et	r <sup>i</sup>	le qual	x <sup>t</sup>	Piasenza	R <sup>n</sup>	Serenissimo	c <sup>d</sup>
Capi del C.X	z <sup>a</sup>	ex	c <sup>z</sup>	lettere	u <sup>r</sup>	più	c <sup>c</sup>	sia	f <sup>u</sup>
capit	o <sup>o</sup>	exe	n <sup>p</sup>	li qual	d <sup>t</sup>	Pontefice	Z <sup>i</sup>	signor	z <sup>l</sup>
cardinal	e <sup>d</sup>	expedi	x <sup>c</sup>	liga	E <sup>h</sup>	pp	o <sup>h</sup>	spagnoli	a <sup>h</sup>
caual	n <sup>d</sup>	fant	L <sup>y</sup>	magnifico	t <sup>h</sup>	prefat	r <sup>l</sup>	ssim	t <sup>b</sup>
cc	Z <sup>d</sup>	far	a <sup>l</sup>	mai	c <sup>f</sup>	present	z <sup>t</sup>	stato	o <sup>m</sup>
che	a <sup>e</sup>	ff	z <sup>q</sup>	mal	E <sup>z</sup>	preterit	E <sup>a</sup>	sua	d <sup>l</sup>
chi	c <sup>u</sup>	Franza	a <sup>p</sup>	man	c <sup>b</sup>	princip	E <sup>y</sup>	sua Ces. M.à	t <sup>i</sup>
cla.mo	E <sup>t</sup>	franzi	c <sup>r</sup>	mente	d <sup>s</sup>	qual	e <sup>y</sup>	Sua Eccel.za	o <sup>s</sup>
come	a <sup>r</sup>	galee	o <sup>f</sup>	Milano	d <sup>z</sup>	qualche	r <sup>h</sup>	Sua Maestà	t <sup>c</sup>
commette	u <sup>d</sup>	gente	L <sup>x</sup>	mm	t <sup>q</sup>	quando	e <sup>e</sup>	sua Mag.a	n <sup>q</sup>
comunica	m <sup>e</sup>	Germania	E <sup>f</sup>	molt	n <sup>y</sup>	quant	r <sup>d</sup>	Sua Santità	d <sup>r</sup>
con	u <sup>a</sup>	gg	f <sup>l</sup>	Monsig.	t <sup>f</sup>	quel	c <sup>s</sup>	Sua Sig.ia	g <sup>c</sup>
conclu	o <sup>z</sup>	giom	Z <sup>u</sup>	Mor Granvella	x <sup>n</sup>	quella Mtà	d <sup>h</sup>	Sua X.M.tà	Z <sup>l</sup>
Cons. di X	E <sup>d</sup>	gli	o <sup>x</sup>	mr di Aras	c <sup>h</sup>	quest	L <sup>u</sup>	sue	x <sup>a</sup>
conside	u <sup>h</sup>	grand	n <sup>u</sup>	munition	a <sup>q</sup>	questa M.tà	E <sup>p</sup>	sue Sig.ie	t <sup>h</sup>
conte	f <sup>e</sup>	guerra	E <sup>c</sup>	necess	f <sup>z</sup>	re Christ.mo	z <sup>x</sup>	sui	L <sup>t</sup>
continuu	f <sup>p</sup>	habbia	d <sup>p</sup>	nn	Z <sup>c</sup>	Re dei Romani	g <sup>n</sup>	suizzeri	e <sup>f</sup>
Costantinopoli	x <sup>q</sup>	haue	f <sup>o</sup>	noi	d <sup>c</sup>	re di Portogallo	u <sup>u</sup>	suo	d <sup>b</sup>
dal	L <sup>c</sup>	hora	g <sup>u</sup>	non	c <sup>m</sup>	re di Scotia	u <sup>y</sup>	tal	z <sup>r</sup>
danari	g <sup>x</sup>	il	f <sup>a</sup>	noncio	g <sup>a</sup>	rece	Z <sup>p</sup>	tant	Z <sup>e</sup>
debbi	g <sup>m</sup>	il	r <sup>b</sup>	nostr	e <sup>x</sup>	reu.mo	e <sup>l</sup>	tempo	x <sup>z</sup>
del	R <sup>i</sup>	il che	c <sup>l</sup>	ogni	e <sup>m</sup>	reuerendo	g <sup>b</sup>	tia	e <sup>i</sup>

# Lista cifrante

# Lista decifrante

Per  
scrivere

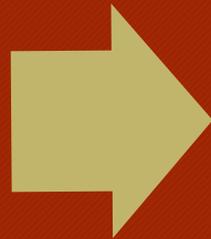
Per  
trazer

LISTA CIFRANTE												
0	g	co	a	fa	L	hi	z	y	mente	d	Pontefice	Z
0	z	come	a	fant	L	no	Z	mi	r	pp	o	h
0	u	x	commette	u	far	a	hora	g	u	Milano	d	pra
1	x	f	comunica	m	fe	t	zu	f	q	mm	t	pre
2	u	con	u	ff	z	a	o	mo	e	h	prefat	r
2	e	z	conclu	o	fi	n	o	molt	n	y	present	z
4	Z	Cons. di X	E	fo	m	ia	t	s	Monsig.	t	preterit	E
5	t	p	conside	u	fra	t	y	i	x	1	Mor Granv	na
6	o	conte	f	Francia	a	il	f	a	m	r	di Aras	C
7	E	U	continu	f	francesi	c	i	r	b	mu	r	pru
8	R	U	Costantino	poli	fre	z	a	che	c	i	munition	a
9	d	y	cre	L	fri	r	u	quale	d	x	n	c
?	f	f	cri	x	fro	E	il	mo	d	n	e	qual
a	m	i	cro	m	fru	x	d	alustr	f	h	a	u
a	c	x	ru	f	fu	g	imp. Cesare	d	e	ne	r	f
accio	r	f	cu	x	g	L	p	n	z	b	necess	f
ad	f	t	d	R	ga	r	n	a	n	i	r	o
al	n	t	da	c	o	galee	e	nte	z	n	n	Z
alcun	c	t	dal	L	ge	t	lo	m	no	e	qual	M
altr	d	m	danari	g	x	gente	L	x	Italia	d	q	no
an	u	c	de	a	Germania	E	i	t	m	on	c	quest
anchor	c	y	debbi	g	m	gg	f	ia	f	t	noncio	g
anglesi	g	i	del	R	gi	n	s	ia	qual	t	e	mostr
Anglia	o	t	del	u	glom	Z	u	angraui	c	q	u	e
armata	n	t	deside	f	u	gli	o	x	e	r	n	o
b	o	a	detta	M. t	E	gna	L	f	le	qual	x	t
ba	e	i	e	o	gne	m	lettere	u	i	ogni	e	h
bb	L	h	dit	z	gni	m	i	t	o	ne	c	i
be	Z	o	do	n	gno	r	u	qual	d	i	opera	u
bi	g	s	doue	o	gnu	hga	E	h	or	amb	a	f
bo	r	p	du	m	go	Z	a	la	d	u	ora	u
bu	r	p	duca	R	gra	t	z	le	n	ordin	E	i
c	o	p	duca di Saszo	grand	n	u	m	p	R	e	di Scotia	y
ca	L	e	e	a	gre	Z	y	no	L	b	pa	L
Capi del C. X	e	n	e	gri	r	lu	z	d	pace	d	i	reu. mo
capit	o	e	z	gro	m	ho	a	z	pare	t	i	reuerendo
cardinal	e	esse	d	gru	m	u	r	s	passat	o	n	i
caual	n	d	essercito	z	f	guerra	L	m	e	pe	f	z
cc	Z	e	t	a	guerra	E	c	ma	c	n	per	a
ce	m	o	et	r	i	h	g	magnifico	t	h	perché	d
che	a	e	x	c	ha	n	mai	c	f	pi	m	r
chi	c	i	u	e	x	habbia	d	p	mal	E	Plasenza	R
ci	n	t	expedi	x	haue	f	o	man	c	b	più	c
cla mo	E	f	m	he	o	me	d	po	n	e	S. Turco	E

LISTA DECIFRANTE												
a e de	d	c	noi	EP	questa	M	g	h	m	du	o	n
a b e	d	d	ill. mo	E	q	z	g	i	bo	m	m	gro
a c r	d	e	imp. Cesare	e	q	nu	g	i	anglesi	m	n	spa
a d fa	d	f	perché	E	r	pru	g	m	debbei	m	o	ce
a e che	d	h	quella	M	t	a	e	f	ba	g	n	Re dei Rom
a f or amb	d	i	sua	E	s	z	g	o	ssi	m	l	tro
a h spagnoli	d	i	pace	e	s	n	g	p	tru	m	f	lli
a i per	d	m	altr	E	c	la. mo	g	q	gnu	m	s	tta
a i far	d	n	lla	e	t	sso	g	i	quo	m	i	o
a m se	d	o	me	E	u	7	g	s	bi	m	l	gni
a n in	d	p	habbia	e	u	sta	g	t	ue	m	s	o
a o i	d	q	Italia	E	x	senato	g	u	hora	m	v	stu
a p Franza	d	i	Sua Santità	e	x	nostr	g	x	danari	m	f	
a q munition	d	s	mente	e	y	qual	g	y	su	n	a	si
a r come	d	t	li qual	E	y	princip	g	z	fu	n	b	pro
a s ui	d	u	esse	e	z	3	L	a	te	n	c	e
a u co	d	x	il quale	E	s	mal	L	b	llo	n	d	caual
a u na	d	y	9	f	a	il	L	c	dal	n	e	po
a x ssa	d	z	Milano	f	b	deside	L	d	ro	n	f	armata
a y tu	E	a	preterit	f	c	ta	L	e	ca	n	l	le
a z lo	e	a	no	f	d	ttu	L	f	gna	n	d	o
c a re	e	b	ua	f	e	conte	L	h	bb	n	l	ha
c b man	E	b	S. Turco	f	f	?	L	i	sca	n	m	tti
c c più	E	c	guerra	f	h	illustr	L	i	qua	n	n	sa
c d Serenissim	e	c	m	L	m	qua	n	o	i	r	i	prefat
c e n	e	d	cardinal	f	i	gg	L	n	cre	n	p	exe
c f mai	E	d	Cons. di X	f	m	x	L	o	pa	n	q	sua Mag. a
c h mr di Aras	E	e	detta	M. t	a	n	p	pra	L	p	g	r
c i one	e	e	quando	f	o	haue	L	q	zi	n	s	gi
c i l che	e	f	suetzeri	f	p	contin	L	f	ra	n	t	al
c m non	E	f	Germania	f	q	hu	L	s	tre	n	u	grand
c n ma	e	h	uittuaglie	f	r	ad	L	t	sui	n	x	o
c o da	E	h	liga	f	s	spo	L	u	quest	n	y	molt
c p u	e	i	ta	f	t	la	L	x	gente	n	z	spi
c q langraui	E	i	ordin	f	u	sia	L	y	fant	o	a	b
c r francesi	E	i	spu	f	x	pe	L	z	ste	o	b	pu
c s quel	e	i	reu. mo	f	y	cruc	m	a	sco	o	c	qu
c t alcun	E	m	fro	f	z	necess	m	b	fo	o	d	he
c u chi	e	m	ogni	g	a	noncio	m	c	pi	o	e	stro
c x a	e	n	mo	g	b	reuerendo	m	d	cro	o	f	galee
c y anchor	E	n	turchi	g	c	Sua Sig. ia	m	e	comunica	o	h	pp
c z ex	e	o	d	g	d	o	m	f	zu	o	i	passat
d a sse	E	o	uede	g	e	uu	m	h	gru	o	i	6
d b suo	e	p	zo	g	f	t	m	i	a	o	m	stato

# Cifra per sostituzione

Cifre per sostituzione sono cifre nelle quali ogni parte del testo **chiaro** viene **sostituita** da un testo **cifrato**.

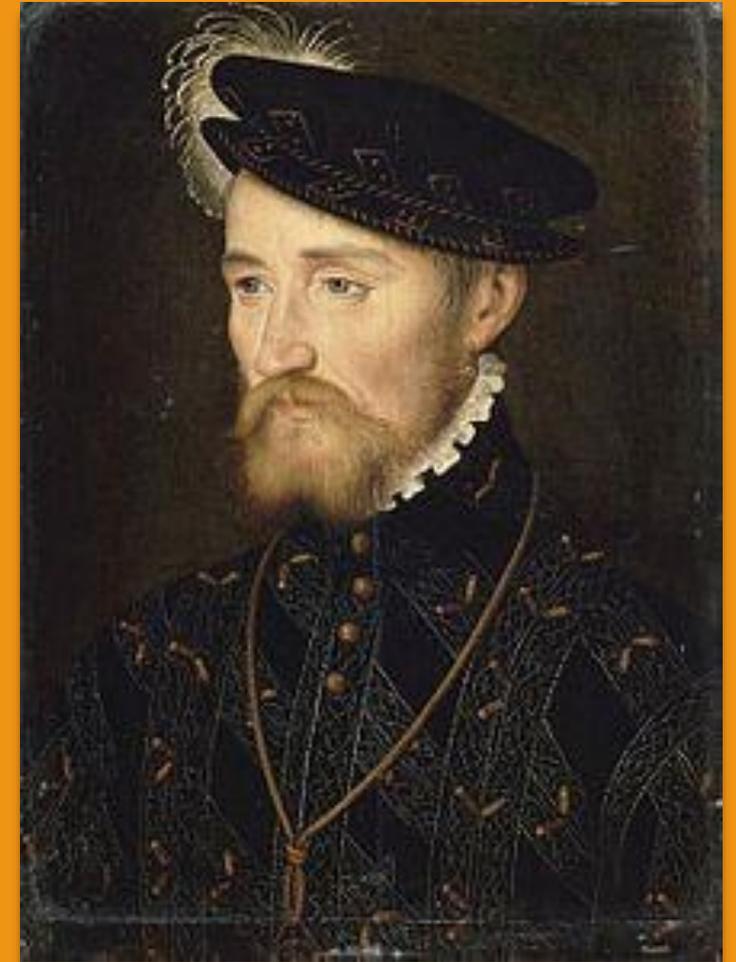


Sono possibili diverse sostituzioni:

- Sostituzione per lettera : **monografica**.
- Sostituzione per gruppi di lettere : **poligrafica**.
- Sostituzione per sillaba : **sillabario**.
- Sostituzione per parola : **dizionario**.
- Sostituzione per frase : **linguaggio convenuto**.

# Contesto storico

- Nel 1558 con la presa di Calais cadeva l'ultimo baluardo inglese in territorio francese.
- Francesco I duca di Guisa era un condottiero al servizio del Re di Francia; cattolicissimo combattè contro gli Ugonotti protestanti, al tempo delle guerre di religione.
- Morì durante l'assedio di Orleans nel 1563 a seguito di un colpo di pistola sparatogli da Jean de Poltrot de Méré, un *gentiluomo* protestante.



Francesco I Duca di Guisa  
Comandante dell'esercito francese

# Un dispaccio dell'ambasciatore veneziano in Savoia



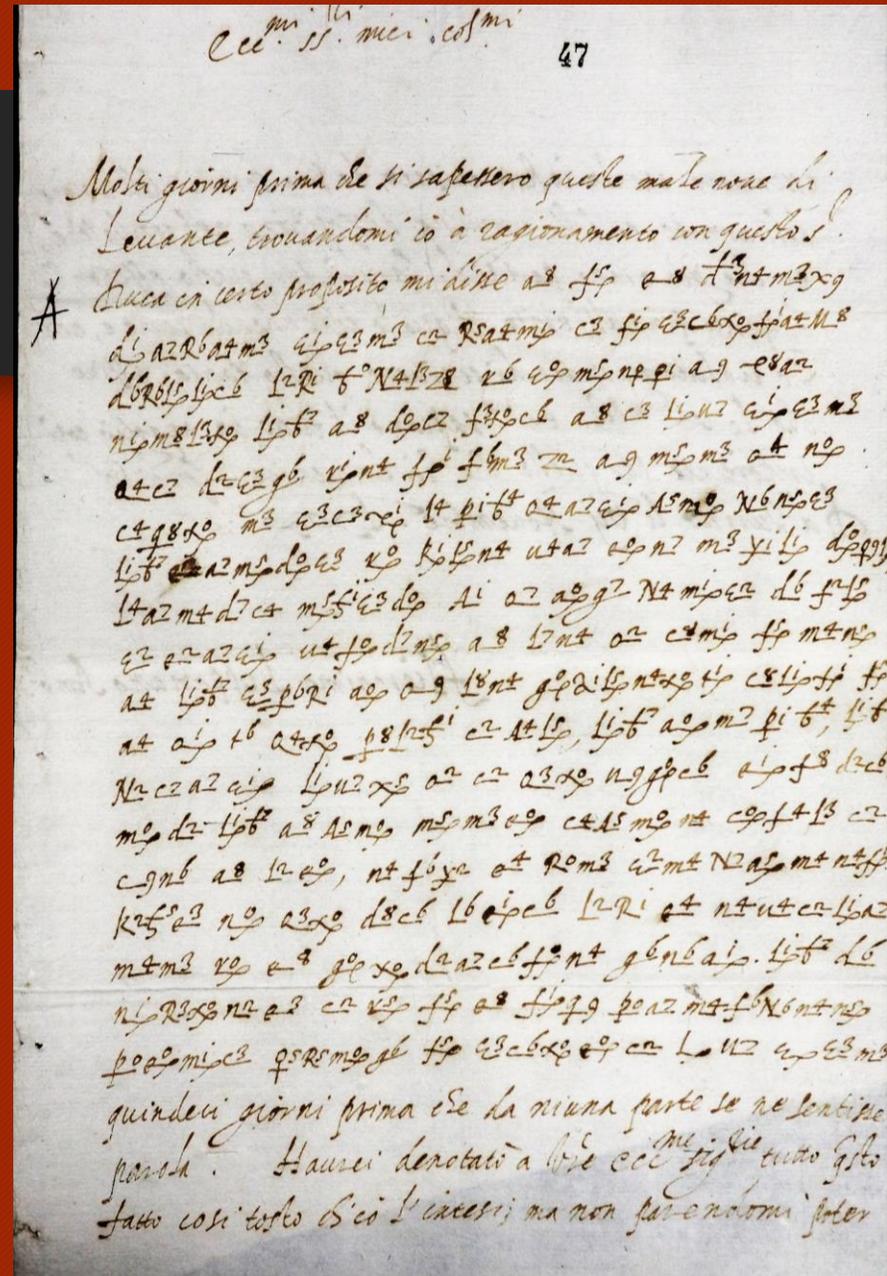
Emanuele Filiberto  
Duca di Savoia



Alvise I Mocenigo  
Doge di Venezia

Ambasciatore  
Veneziano in Savoia  
Hieronimo Lippomano

Torino 23 ott 1570



Archivio di Stato di Venezia

Senato, dispacci degli ambasciatori in Savoia, Filza 1, 47

# Un dispaccio dell'ambasciatore veneziano in Savoia

Molti giorni prima che si sapessero queste mate nuove di  
Leuance, trouandomi io à ragionamento con questo  
A Duca in certo proposito mi disse a<sup>8</sup> f<sup>5</sup> e<sup>8</sup> d<sup>3</sup> n<sup>4</sup> m<sup>3</sup> x<sup>9</sup>  
di a<sup>2</sup> r<sup>6</sup> a<sup>4</sup> m<sup>3</sup> a<sup>1</sup> e<sup>3</sup> m<sup>3</sup> ca R<sup>5</sup> a<sup>4</sup> m<sup>3</sup> e<sup>3</sup> f<sup>5</sup> e<sup>3</sup> e<sup>6</sup> x<sup>9</sup> f<sup>5</sup> a<sup>4</sup> m<sup>3</sup>  
d<sup>3</sup> r<sup>6</sup> b<sup>1</sup> s<sup>1</sup> p<sup>1</sup> e<sup>6</sup> l<sup>2</sup> r<sup>6</sup> t<sup>0</sup> N<sup>4</sup> l<sup>3</sup> z<sup>8</sup> v<sup>6</sup> e<sup>9</sup> m<sup>3</sup> n<sup>4</sup> e<sup>9</sup> i a<sup>9</sup> e<sup>8</sup> a<sup>2</sup>  
n<sup>4</sup> m<sup>3</sup> l<sup>3</sup> e<sup>9</sup> l<sup>1</sup> t<sup>2</sup> a<sup>8</sup> d<sup>0</sup> e<sup>2</sup> f<sup>3</sup> p<sup>0</sup> e<sup>6</sup> a<sup>8</sup> e<sup>3</sup> l<sup>1</sup> p<sup>1</sup> u<sup>2</sup> a<sup>1</sup> e<sup>3</sup> m<sup>3</sup>  
e<sup>4</sup> e<sup>2</sup> d<sup>2</sup> e<sup>3</sup> g<sup>6</sup> v<sup>1</sup> n<sup>4</sup> f<sup>5</sup> f<sup>6</sup> m<sup>3</sup> m a<sup>9</sup> m<sup>3</sup> m<sup>3</sup> a<sup>4</sup> n<sup>0</sup>  
i la bit<sup>4</sup> a<sup>4</sup> a<sup>7</sup> e<sup>1</sup> a<sup>5</sup> m<sup>0</sup> x<sup>1</sup> 6 n<sup>2</sup> e<sup>3</sup>

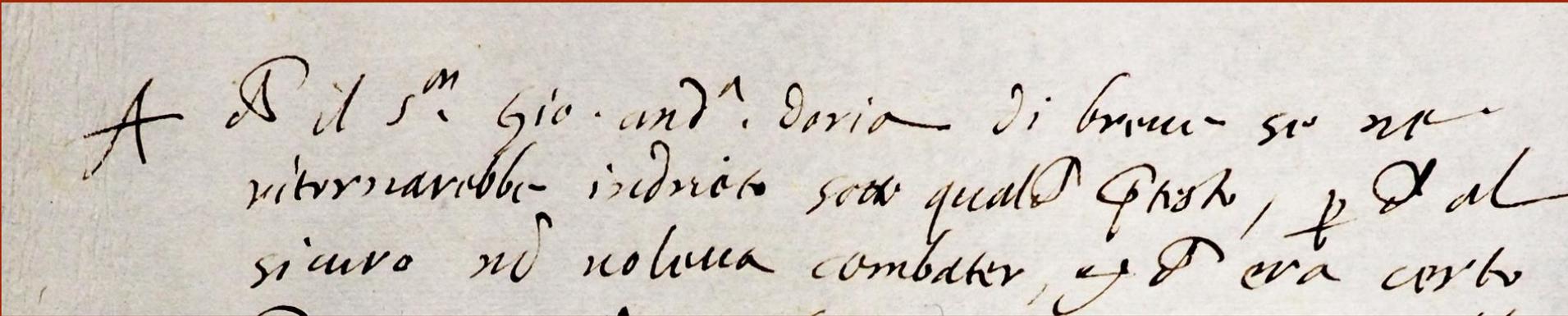
Novità:  
esponenti  
numerici

a<sup>8</sup> f<sup>5</sup> e<sup>8</sup> d<sup>3</sup> n<sup>4</sup> m<sup>3</sup> x<sup>9</sup>  
D1 a<sup>7</sup> R<sup>6</sup> a<sup>4</sup> m<sup>3</sup> E1 E3 m<sup>3</sup>

Marca di cancelleria

# La decifrazione di cancelleria

a8 f5 j8 d3 n4 m3 x9  
d1 a7 R6 a4 m3 E1 e3 m3



1570-11-07 Dispaccio dell'ambasciatore in Savoia 323																			
a8	f5	j8		d3	n4	m3	x9												
che	il	Signor		gi	o	a	n												
d1	a7	R6	a4	m3	E1	e3	m3	c2	R5	a4	m1	c3	f1	e3	c6	X0	f1	a4	M8
a	n	d	re	a	do	ri	a	di	b	re	ue	se	ne	ri	to	r	ne	re	?
d6	R6	L5	L1	c6	l2	R1	b0		N4	l3	z8	r6	E0	m5	nq	q1	a9	T8	a2
in	d	i	e	to	so	tto	qualche		pre	te	sto	?	al	si	cu	ro	non	?	?

ALFABETO [Omofoni, massimo = 3]

a	b	c	d	e	f	g	h	i	l	m	n	o	p	r	s	t	u
d <sup>1</sup>	R <sup>5</sup>	k <sup>1</sup>	R <sup>6</sup>	d <sup>0</sup>	K <sup>4</sup>	A <sup>5</sup>	p <sup>9</sup>	j <sup>5</sup>	f <sup>6</sup>	e <sup>6</sup>	a <sup>7</sup>	g <sup>5</sup>	L <sup>8</sup>	C <sup>5</sup>	N <sup>7</sup>	b <sup>7</sup>	n <sup>1</sup>
m <sup>3</sup>	s <sup>7</sup>	L <sup>1</sup>	Q <sup>1</sup>	L <sup>5</sup>	k <sup>5</sup>	S <sup>0</sup>	n <sup>4</sup>	X <sup>0</sup>	n <sup>7</sup>	u <sup>1</sup>							
											x <sup>9</sup>						

SILLABARIO [30 sillabe]

ba	be	bi	bo	bu	gra	gre	gri	gro	gru	pra	pre	pri	pro	pru	stra	stre	stri	stro	stru
m <sup>8</sup>	u <sup>4</sup>	p <sup>8</sup>	?	?	g <sup>0</sup>	o <sup>1</sup>	?	q <sup>9</sup>	?	?	N <sup>4</sup>	R <sup>4</sup>	b <sup>3</sup>	H <sup>0</sup>	?	?	?	?	?
ca	ce	ci	co	cu	ha	he	hi	ho	hu	qua	que	qui	quo	quu	ta	te	ti	to	tu
d <sup>2</sup>	f <sup>3</sup>	?	g <sup>6</sup>	n <sup>q</sup>	k <sup>2</sup>	?	?	S <sup>5</sup>	N <sup>6</sup>	?	N <sup>5</sup>	s <sup>4</sup>	?	?	j <sup>3</sup>	l <sup>3</sup>	m <sup>4</sup>	c <sup>6</sup>	k <sup>4</sup>
cra	cre	cri	cro	cru	ia	ie	ii	io	iu	ra	re	ri	ro	ru	tra	tre	tri	tro	tru
?	?	?	?	?	?	?	?	a <sup>6</sup>	?	c <sup>7</sup>	a <sup>4</sup>	e <sup>3</sup>	q <sup>1</sup>	?	?	y <sup>2</sup>	q <sup>0</sup>	?	?
da	de	di	do	du	la	le	li	lo	lu	sa	se	si	so	su	tta	tte	tti	tto	ttu
j <sup>1</sup>	a <sup>0</sup>	c <sup>2</sup>	E <sup>1</sup>	m <sup>6</sup>	j <sup>4</sup>	l <sup>4</sup>	m <sup>0</sup>	n <sup>6</sup>	A <sup>4</sup>	E <sup>2</sup>	c <sup>3</sup>	m <sup>5</sup>	l <sup>2</sup>	b <sup>2</sup>	A <sup>6</sup>	q <sup>8</sup>	?	R <sup>1</sup>	?
fa	fe	fi	fo	fu	lla	lle	lli	llo	llu	sca	sce	sci	sco	scu	ua	ue	ui	uo	uu
a <sup>5</sup>	T <sup>6</sup>	E <sup>8</sup>	R <sup>3</sup>	?	?	?	?	?	?	?	?	?	K <sup>3</sup>	?	?	m <sup>1</sup>	c <sup>8</sup>	L <sup>7</sup>	s <sup>5</sup>
fra	fre	fri	fro	fru	ma	me	mi	mo	mu	spa	spe	spi	spo	spu	za	ze	zi	zo	zu
?	?	?	?	?	G <sup>0</sup>	c <sup>4</sup>	n <sup>2</sup>	n <sup>5</sup>	?	?	p <sup>6</sup>	?	Q <sup>2</sup>	?	s <sup>8</sup>	?	?	?	?
ga	ge	gi	go	gu	na	ne	ni	no	nu	ssa	sse	ssi	sso	ssu					
f <sup>4</sup>	p <sup>0</sup>	d <sup>3</sup>	T <sup>1</sup>	?	a <sup>1</sup>	f <sup>1</sup>	f <sup>0</sup>	j <sup>0</sup>	?	a <sup>3</sup>	?	d <sup>7</sup>	u <sup>7</sup>	?					
gna	gne	gni	gno	gnu	pa	pe	pi	po	pu	sta	ste	sti	sto	stu					
?	?	?	g <sup>1</sup>	?	C <sup>0</sup>	j <sup>2</sup>	n <sup>8</sup>	f <sup>2</sup>	q <sup>5</sup>	d <sup>8</sup>	?	n <sup>9</sup>	z <sup>8</sup>	?					

DIZIONARIO									
accio	E4	del	r0	habbia	M1	mente	l1	quant	l7
ad	t6	deside	N2	haue	o4	Milano	K6	quel	c9
al	E0	detta Maestà	R8	il	f5	n1	n1	quest	r5
altr	t8	detto	r7	il quale	X1	non	a9	Re Christ.mo	g3
an	b5	dro	m9	in	d6	pace	M0	rra	y8
ancor	A7	esse	o3	inte	B7	per	n0	S. M.tà C.ma	y3
b3	pro	et	A9	Italia	k9	più	o2	sempre	X5
che	a8	far	t3	la qual	b6	princip	q4	Signor	j8
come	r2	galere	b4	Lega	Z2	qual	g2	Spagnoli	S4
con	ni	genti	R9	mai	o1	qualche	b0	sua	c5
con	U1	gli	x2	mal	R0	quando	H3	Sua Maestà	f8
dal	A1	guerra	H6	man	l6	quant	L2	sue	p1

# Il cifrario di Hieronimo Lippomano in Savoia

# Il cifrario di Hieronimo Lippomano in Savoia

LISTA DECIFRANTE

a0	de	E4	accio	I7	quant	p9	h	x7	un	
A1	dal	e6	m	L7	uo	pro	b3	x9	n	
a1	na	E8	fi	L8	p	q0	tri	y2	tre	
a3	ssa	f0	ni	I8	tant	q1	ro	y3	S. M. tà C. ma	
a4	re	f1	ne	m0	li	Q1	g	y8	rra	
A4	lu	f2	po	M0	pace	Q2	spo	Z0	ca	
a5	fa	f3	ce	m1	ue	q4	princip	Z2	Lega	
A5	g	f4	ga	M1	habbia	q5	pu	z7	uo	
a6	io	f5	il	m3	a	q8	tte	z8	sto	
A6	tta	f6	l	m4	ti	q9	gro			
A7	ancor	f8	Sua Maestà	m5	si	R0	mal			
a7	n	g0	gra	m6	du	r0	del			
a8	che	G0	ma	m8	ba	R1	tto			
A9	et	g1	gno	m9	dro	r2	come			
a9	non	g2	qual	n0	per	R2	ha			
b0	qualche	g3	Re Christo	n1	u	R3	fo			
b2	su	g5	o	N2	deside	R4	pri			
b3	pro	g6	co	n2	mi	r5	quest			
b4	galere	H0	pru	N4	pre	R5	b			
b5	an	H3	quando	n4	o	R6	d			
b6	la qual	H6	guerra	n5	mo	r7	detto			
B7	inte	I1	mente	N5	que	R8	detta Maestà			
b7	t	j0	no	N6	hu	R9	genti			
C0	pa	jl	da	m6	lo	S0	n			
c2	di	j2	pe	n7	t	s1	gno			
c3	se	j3	ta	N7	s	S4	Spagnoli			
c4	me	j4	la	n8	pi	s4	qui			
c5	sua	j5	i	n9	sti	S5	ho			
C5	r	j8	Signor	ni	con	s5	uu			
c6	to	k1	c	ni	n1	s7	c			
c7	ra	k2	ha	nq	cu	s8	za			
c8	ui	K3	sco	O1	suo	T1	go			
c9	quel	k4	tu	o1	mai	t3	far			
d0	e	K4	f	o2	più	t6	ad			
d1	a	k5	m	o3	esse	T6	fe			
d2	ca	K6	Milano	o4	haue	t8	altr			
d3	gi	k9	Italia	o6	pa	U1	con			
d6	in	L1	e	o7	tempo	u1	u			
d7	ssi	L2	quant	o9	Turco	u4	be			
d8	sta	L2	so	oi	gre	u7	sso			
E0	al	I3	te	p0	ge	X0	r			
E1	do	I4	le	p1	sue	X1	il quale			
E2	sa	L5	i	p6	spe	x2	gli			
e3	ri	I6	man	p8	bi	X5	sempre			

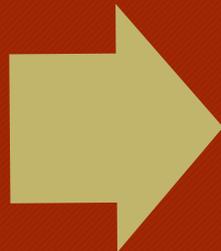
LISTA CIFRANTE

a	d1	fi	E8	mal	R0	ra	c7	u	n1	
a	m3	fo	R3	man	I6	re	a4	u	u1	
accio	E4	g	A5	me	c4	Re Christo	m1	ue	m1	
ad	t6	g	Q1	mente	I1	ri	e3	ui	c8	
al	E0	ga	f4	mi	n2	ro	q1	un	x7	
altr	t8	galere	b4	Milano	K6	rra	y8	uo	L7	
an	b5	ge	p0	mo	n5	s	N7	uo	z7	
ancor	A7	genti	R9	n	a7	S. M. tà C. ma	uu	s5		
b	R5	gi	d3	n	S0	sa	E2	za	s8	
b3	pro	gli	x2	n	x9	sco	K3			
ba	m8	gno	g1	n1	n1	se	c3			
be	u4	gno	s1	na	a1	sempre	X5			
bi	p8	go	T1	ne	f1	si	m5			
c	k1	gra	g0	ni	f0	Signor	j8			
c	s7	gre	oi	no	j0	so	I2			
ca	d2	gro	q9	non	a9	Spagnoli	E4			
ca	Z0	guerra	H6	o	g5	spe	p6			
ce	f3	h	p9	o	n4	spo	Q2			
che	a8	ha	k2	p	L8	ssa	a3			
co	g6	ha	R2	pa	C0	ssi	d7			
come	r2	habbia	M1	pa	o6	sso	u7			
con	ni	haue	o4	pace	M0	sta	d8			
con	U1	ho	S5	pe	j2	sti	n9			
cu	nq	hu	N6	per	n0	sto	z8			
d	R6	i	j5	pi	n8	su	b2			
da	jl	i	L5	più	o2	sua	c5			
dal	A1	il	f5	po	f2	Sua Maestà				
de	a0	il quale	X1	pre	N4	sue	p1			
del	r0	in	d6	pri	R4	suo	O1			
deside	N2	inte	B7	princip	q4	t	b7			
detta Maestà	io	a6	pro	b3	t	n7				
detto	r7	Italia	k9	pru	H0	ta	j3			
di	c2	l	f6	pu	q5	tant	I8			
do	E1	la	j4	qual	g2	te	o3			
dro	m9	la qual	b6	qualche	b0	tempo	o7			
du	m6	le	I4	quando	H3	ti	m4			
e	d0	Lega	Z2	quant	L2	to	c6			
e	L1	li	m0	quant	I7	tre	y2			
esse	o3	lo	n6	que	N5	tri	q0			
et	A9	lu	A4	quel	c9	tta	A6			
f	K4	m	e6	quest	r5	tte	q8			
fa	a5	m	k5	qui	s4	tto	R1			
far	t3	ma	G0	r	C5	tu	k4			
fe	T6	mai	o1	r	X0	Turco	o9			

# Nomenclatori e codici

## Nomenclatore

Consiste di alfabeto, sillabario, dizionario da usare a scelta.



## Codice

Come il nomenclatore ma molto più vasto, di solito richiede un fascicolo o volume

# Hieronimo Lippomano, una brutta fine

Hieronimo Lippomano fu uno dei più valenti ambasciatori veneziani del XVI secolo.

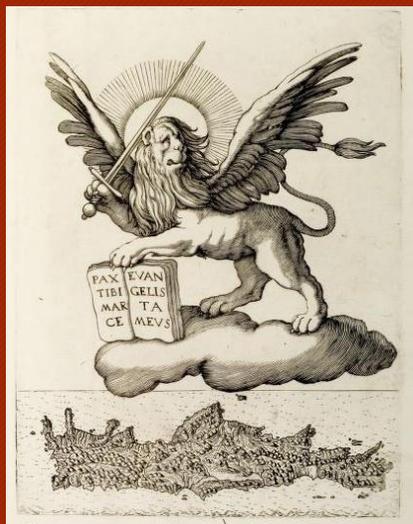
Ambasciatore a Ferrara, Firenze, Vienna, Torino, Madrid seppe stabilire relazioni amichevoli con i principali protagonisti dell'epoca: Emanuele Filiberto di Savoia, Filippo II di Spagna, don Giovanni d'Austria, e partecipò attivamente alla preparazione della lega per la battaglia di Lepanto.

Ottenuta la prestigiosa carica di bailo a Costantinopoli, all'apice della fortuna, fu accusato di alto tradimento per aver passato agli spagnoli segreti militari sulla costruzione di navi nell'Arsenale e richiamato a Venezia dal Consiglio di Dieci.

La nave che lo riportava a Venezia era giunta davanti al Lido, quando Lippomano si suicidò lanciandosi in mare.



# Un dispaccio del governatore militare di Candia



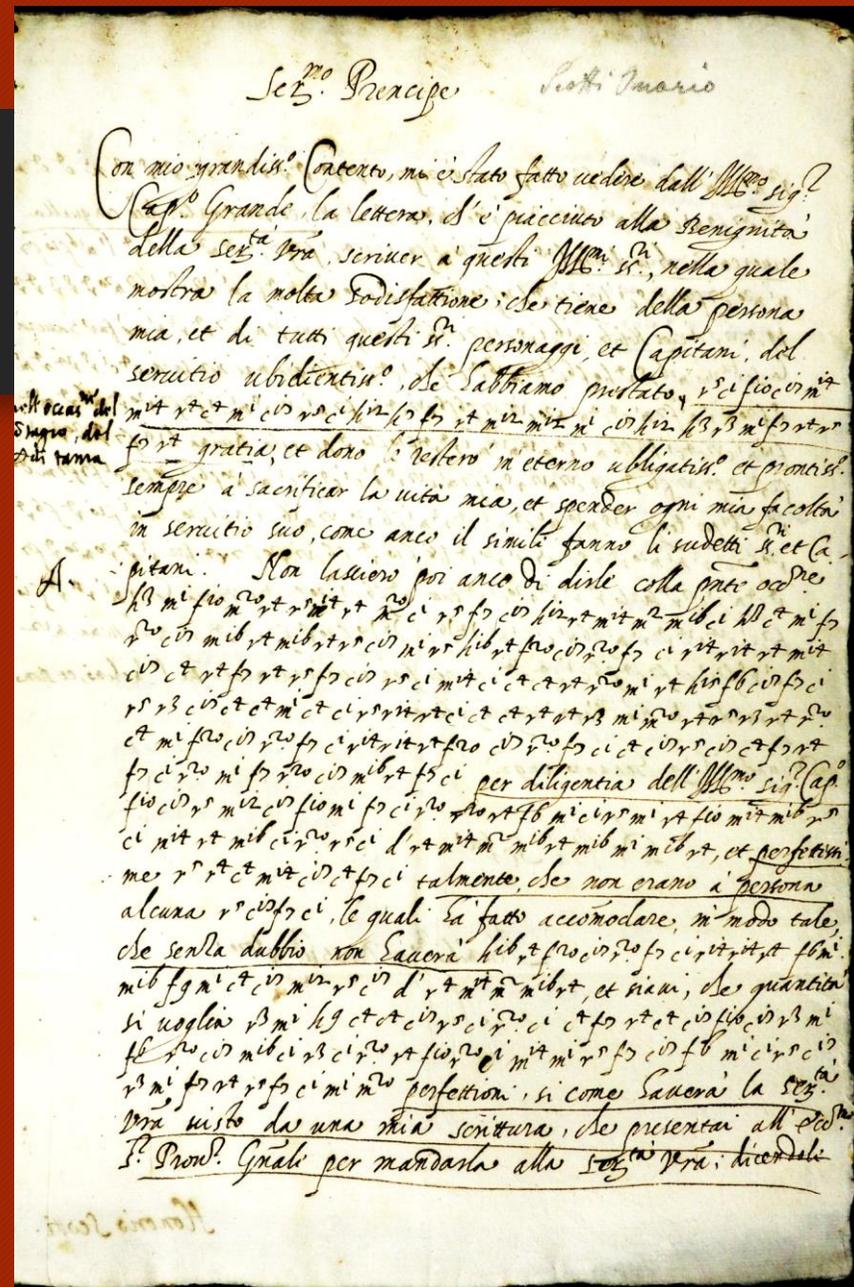
Governatore  
di Candia  
Honorio Scotti



Ser.mo et Ecc.mo  
Pasquale Cicogna  
Doge di Venezia



Candia 9 gen 1592 [1593]



Archivio di Stato di Venezia  
Capi da guerra, busta 8, Scotti Onorio

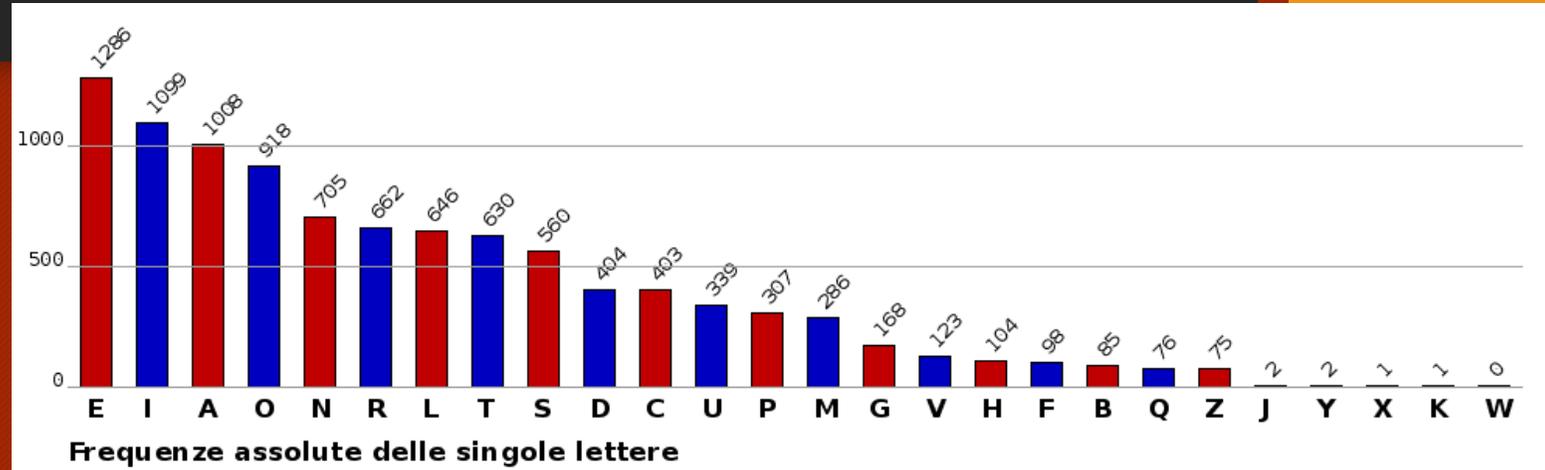


# Il dispaccio di Honorio Scotti

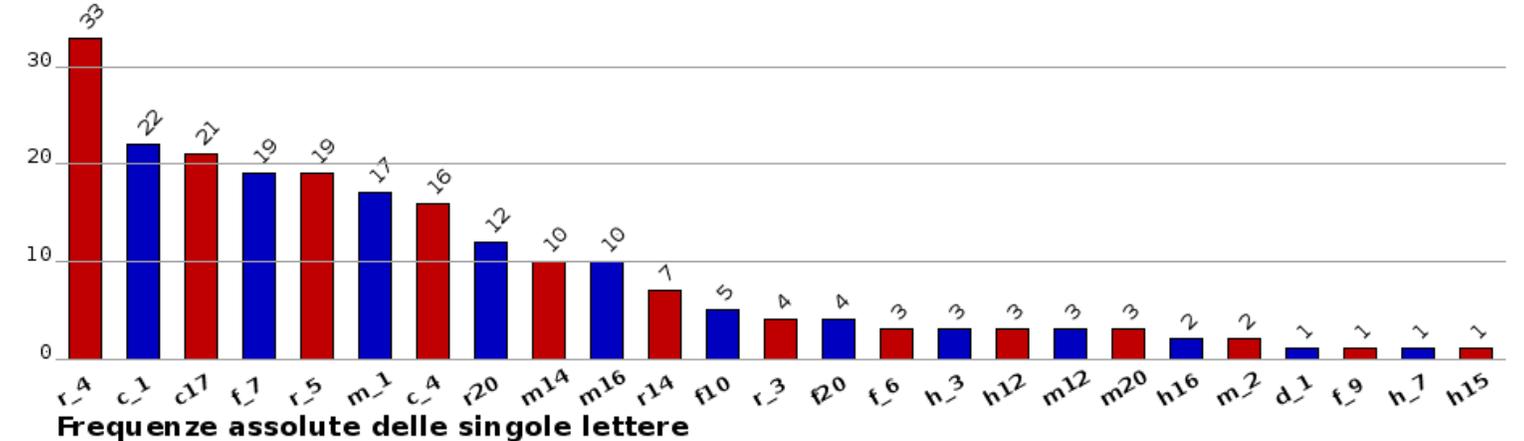
## Un confronto

Confrontando la statistica del dispaccio di H. Scotti con quello tipico della lingua italiana si osserva che l'andamento non è poi così diverso.

Quindi è valida l'ipotesi che si tratti di un ciframento lettera per lettera (monoalfabetico)



Presenze = 25 Moda = 33 Gruppi = 222 Segni cifranti = 25

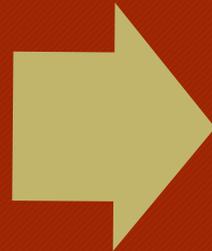




# Cifre monoalfabetiche

La cifra usata da Scotti sembra proprio un esempio di monoalfabetico.

**MASC**  
**Mono**  
**Alphabetic**  
**Substitution**  
**Cipher**



ALFABETO

a	b	c	d	e	f	g	i	l	m	n	o	p	q	r	s	t	u	z
r_4	f_9	m14	r_3	c_1	f20	m12	m_1	f10	m20	r_5	c17	f_6	m_2	r20	c_4	f_7	m16	r14

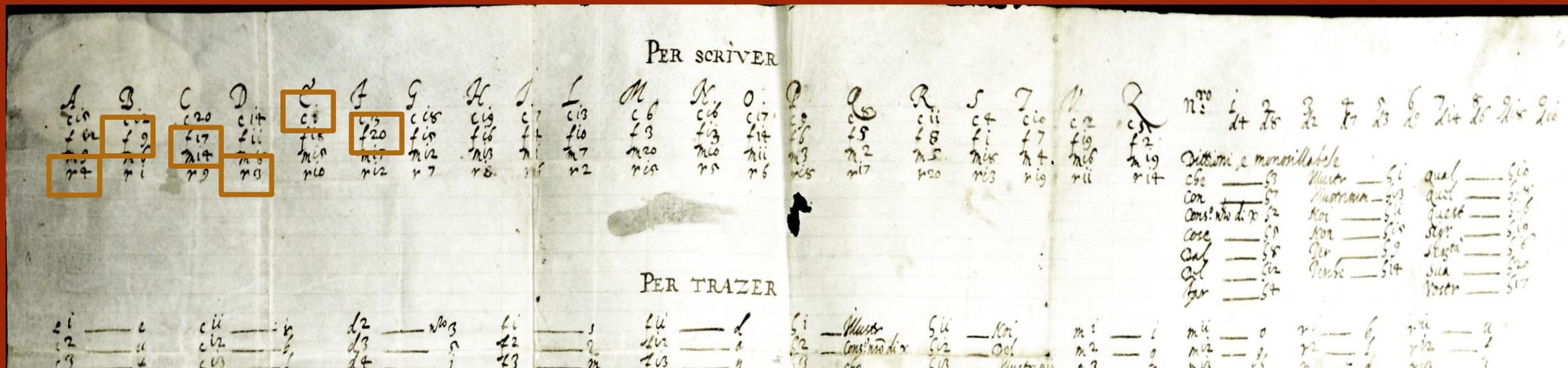
Ogni lettera del testo chiaro viene cifrata con un segno cifrante, lettera o gruppo di numeri in modo univoco,  
O anche con una scelta di caratteri  
*(omofoni)*

# Il cifrario originale, aveva 4 omofoni!

Perché l'addetto alla cifra usò solo una cifra per ogni lettera??

## ALFABETO

a	b	c	d	e	f	g	i	l	m	n	o	p	q	r	s	t	u	z
r_4	f_9	m14	r_3	c_1	f20	m12	m_1	f10	m20	r_5	c17	f_6	m_2	r20	c_4	f_7	m16	r14



Archivio di Stato di Venezia

Cifre, chiavi e scontri di cifra con studi successivi, busta 3



# 1412 Dogale di Michele Steno

Insuper scitis nos habere per omissionem & procurando & supplicando suz g...  
 c...  
 d...  
 b...  
 s...  
 Data in nostro ducali palatio die vigesimo mensis Junij Indis quarta / a Nullo ecce undecimo

bq p d d + 7 l + v x ÷ 7 3 0 f h y f g t y 0 v h ≡ ::

**quo D CLEMENTIASUASPERAMUS et**

Monografico (cifratura per lettere)  
 Monalfabetico (decifra univoca)  
 Con omofoni (cifratura univoca)

# Un dispaccio dell'ambasciatore veneziano in Francia

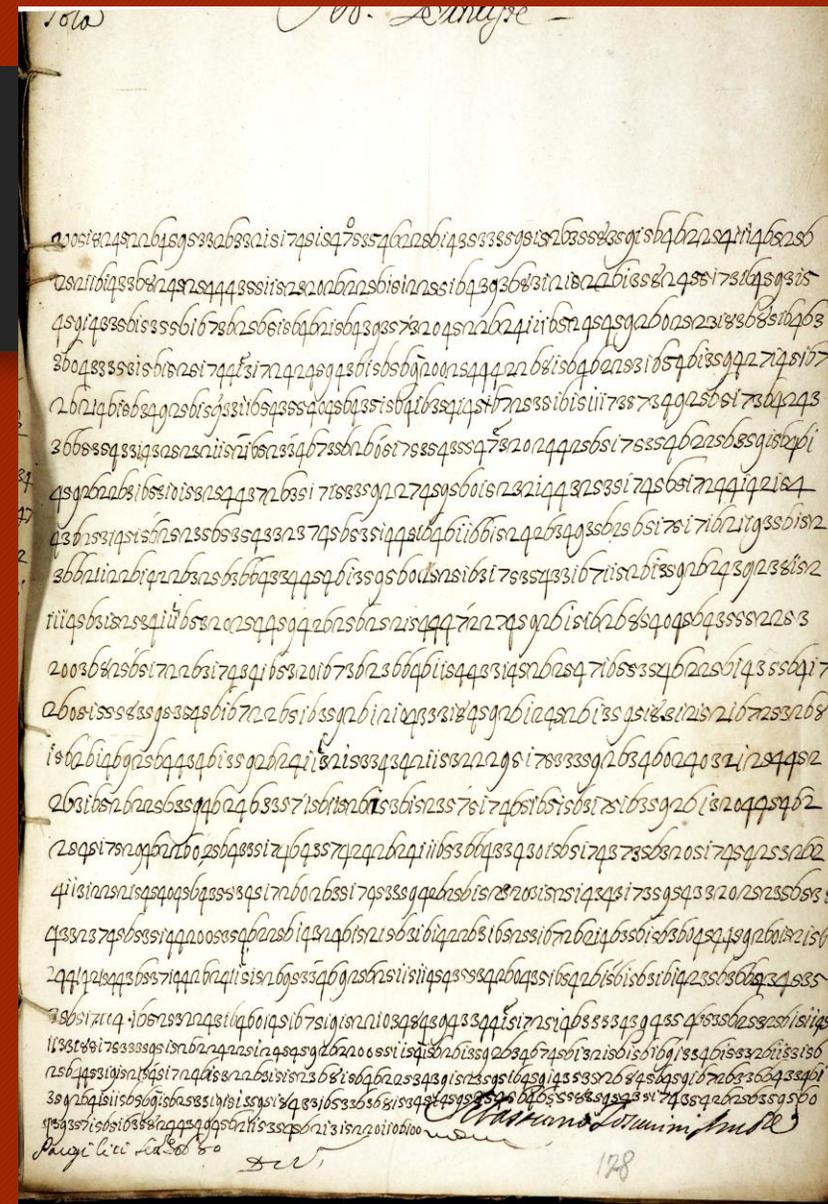


Louis XIV  
Il Re Sole

Ambasciatore  
Veneziano in Francia  
Sebastiano Foscari

Parigi 11 set 1680

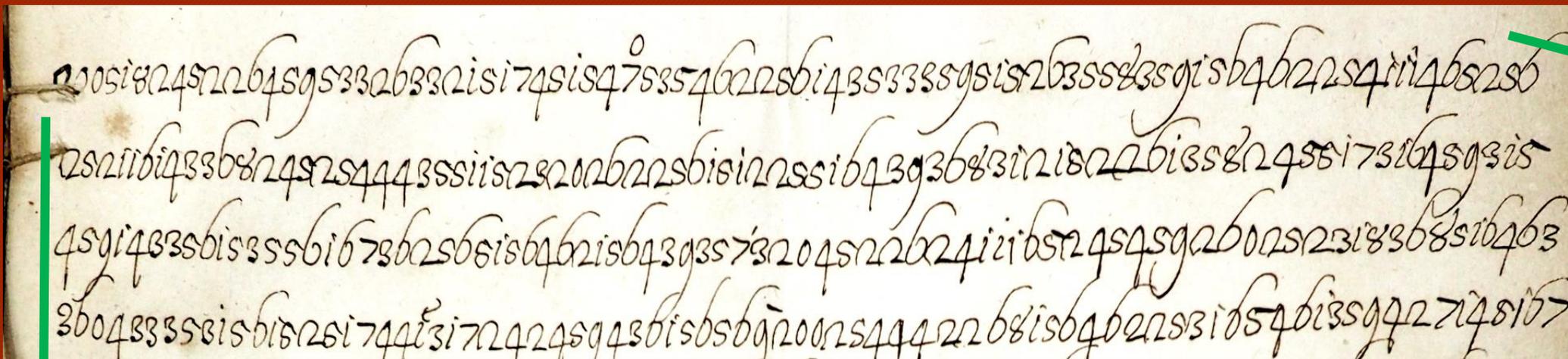
Ser.mo et Ecc.mo  
Alvise Contarini  
Doge di Venezia



Archivio di Stato di Venezia

Senato, dispacci degli ambasciatori in Francia, Filza 166, p.158

# Un dispaccio dell'ambasciatore in Francia



Novità:  
Solo numeri.  
Quali  
vantaggi?

Come si capisce che sono a gruppi di tre?

200 518 245 226 459 533 263 321 517 451 547 535 462 256 143 533 359 515 263 558 359 156 462 254 111 465 256  
252 116 143 368 245 254 443 551 152 320 262 256 151 225 516 439 368 312 152 261 358 245 517 316 459 315  
459 143 356 153 556 167 362 565 156 462 156 439 357 320 452 262 411 165 245 459 260 252 318 368 516 463  
360 433 353 156 152 517 441 317 242 459 436 156 569 200 254 442 268 156 462 253 165 461 359 427 145 167

# Il dispaccio decrittato di Sebastiano Foscarini

## 1680-09-11 Dispaccio dell'ambasciatore in Francia 606

200	518	245	226	459	533	263	321	517	451	547	535	462	256	143	533	359	515	263	558	359	156	462	254	111	465	256		
\n	do	po	fi	r	ma	to	il	di	spa	tia	mi	ui	e	ne	ma	n	da	to	u	n	a	ui	so	al	qual	e		
252	116	143	368	245	254	443	551	152	320	262	256	151	225	516	439	368	312	152	261	358	245	517	316	459	315			
se	be	ne	non	po	so	pre	sta	re	in	ti	e	ra	fe	de	per	non	haue	re	te	m	po	di	ce	r	ca			
459	143	356	153	556	167	362	565	156	462	156	439	357	320	452	262	411	165	245	459	260	252	318	368	516	463			
r	ne	i	ri	s	con	tri	tutt	a	ui	a	per	l	in	spe	ti	on	che	po	r	ta	se	co	non	de	uo			
360	433	353	156	152	517	441	317	242	459	436	156	569				200	254	442	268	156	462	253	165	461	359	427	145	167
tra	la	sci	a	re	di	parte	ci	pa	r	lo	a	Vostra_Serenit?			\n	so	pra	gli	a	ui	si	che	ue	n	go	no	con	
262	146	156	349	256	159	331	165	435	540	456	435	156	416	354	145	167	253	516	151	117	357	349	256	517	364	243		
ti	nu	a	ment	e	d	Italia	che	li	spagn	o	li	a	cre	sco	no	con	si	de	ra	bi	l	ment	e	di	tru	pe		
366	535	433	143	252	321	152	165	233	467	356	260	517	535	435	547	320	244	256	517	535	462	256	359	156	461			
nel	mi	la	ne	se	il	re	che	ha	quant	i	ta	di	mi	li	tia	in	pi	e	di	mi	ui	e	n	a	ue			

dopo firmato il dispaccio mi viene mandato un avviso al quale se bene non posso prestare intera fede per non hauere tempo di cercarne i riscontri tuttauia per l'inspektion che porta seco non deuo tralasciare di parteciparlo a Vostra\_Serenità sopra gli avvisi che uengono continuamente d'Italia che li spagnoli acrescono considerabilmente di trupe nel milanese il re che ha quantita di militia in piedi mi uien auertito che habbia risoluto di rinforzare il presidio di pinarolo sino a seimila huomini de uechi regimenti e di distribuire nel delfinato e nella prouenza seadecimila combatenti per essere al ocasion che insorgiesero piu forte degli spagnoli stesi ...

Luigi XIV  
Il Re Sole

Pinerolo

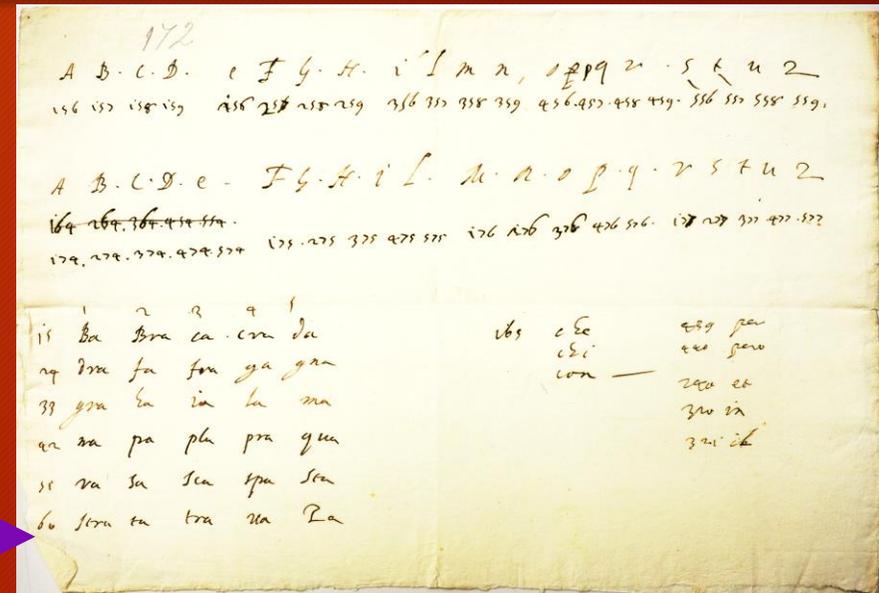
# Il cifrario di Sebastiano Foscari a Parigi 1680

DIZIONARIO									
al	111	così	169	hanno	311	on	411	quest	469
all	120	dal	210	haue	312	parte	441	signor	532
altr	112	del	211	hor	313	passat	430	spagn	540
an	113	doue	213	il	321	per	439	sua	529
bisogn	132	duca	229	in	320	però	440	tia	547
cardin	140	esse	238	Italia	331	piu	447	tutt	565
che	165	et	240	Mare	348	princip	431	Vostra_Serenità	569
chi	166	gli	268	ment	349	qual	465	\n	200
con	167	guerra	269	nel	366	quant	467		
cose	168	habbia	310	non	368	quel	468		

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	257	258	259	356	357	358	359	456	457	458	459	556	557	558	559						

SILLABARIO [30 sillabe]																									
ba	be	bi	bo	bu	ga	ge	gi	go	gu	pa	pe	pi	po	pu	sta	ste	sti	sto	stu						
115	116	117	118	119	424	425	426	427	428	242	243	244	245	246	551	552	553	554	555						
bra	bre	bri	bro	bru	gna	gne	gni	gno	gnu	pla	ple	pli	plo	plu	stra	stre	stri	stro	stru						
215	216	217	218	219	524	525	526	527	528	342	343	344	345	346	160	161	162	163	164						
ca	ce	ci	co	cu	gra	gre	gri	gro	gru	pra	pre	pri	pro	pru	ta	te	ti	to	tu						
315	316	317	318	319	133	134	135	136	137	442	443	444	445	446	260	261	262	263	264						
cra	cre	cri	cro	cru	ha	he	hi	ho	hu	qua	que	qui	quo	quu	tra	tre	tri	tro	tru						
415	416	417	418	419	233	234	235	236	237	542	543	544	545	546	360	361	362	363	364						
da	de	di	do	du	ia	ie	ii	io	iu	ra	re	ri	ro	ru	ua	ue	ui	uo	uu						
515	516	517	518	519	333	334	335	336	337	151	152	153	154	155	460	461	462	463	464						
dra	dre	dri	dro	dru	la	le	li	lo	lu	sa	se	si	so	su	za	ze	zi	zo	zu						
124	125	126	127	128	433	434	435	436	437	251	252	253	254	255	560	561	562	563	564						
fa	fe	fi	fo	fu	ma	me	mi	mo	mu	sca	sce	sci	sco	scu											
224	225	226	227	228	533	534	535	536	537	351	352	353	354	355											
fra	fre	fri	fro	fru	na	ne	ni	no	nu	spa	spe	spi	spo	spu											
324	325	326	327	328	142	143	144	145	146	451	452	453	454	455											



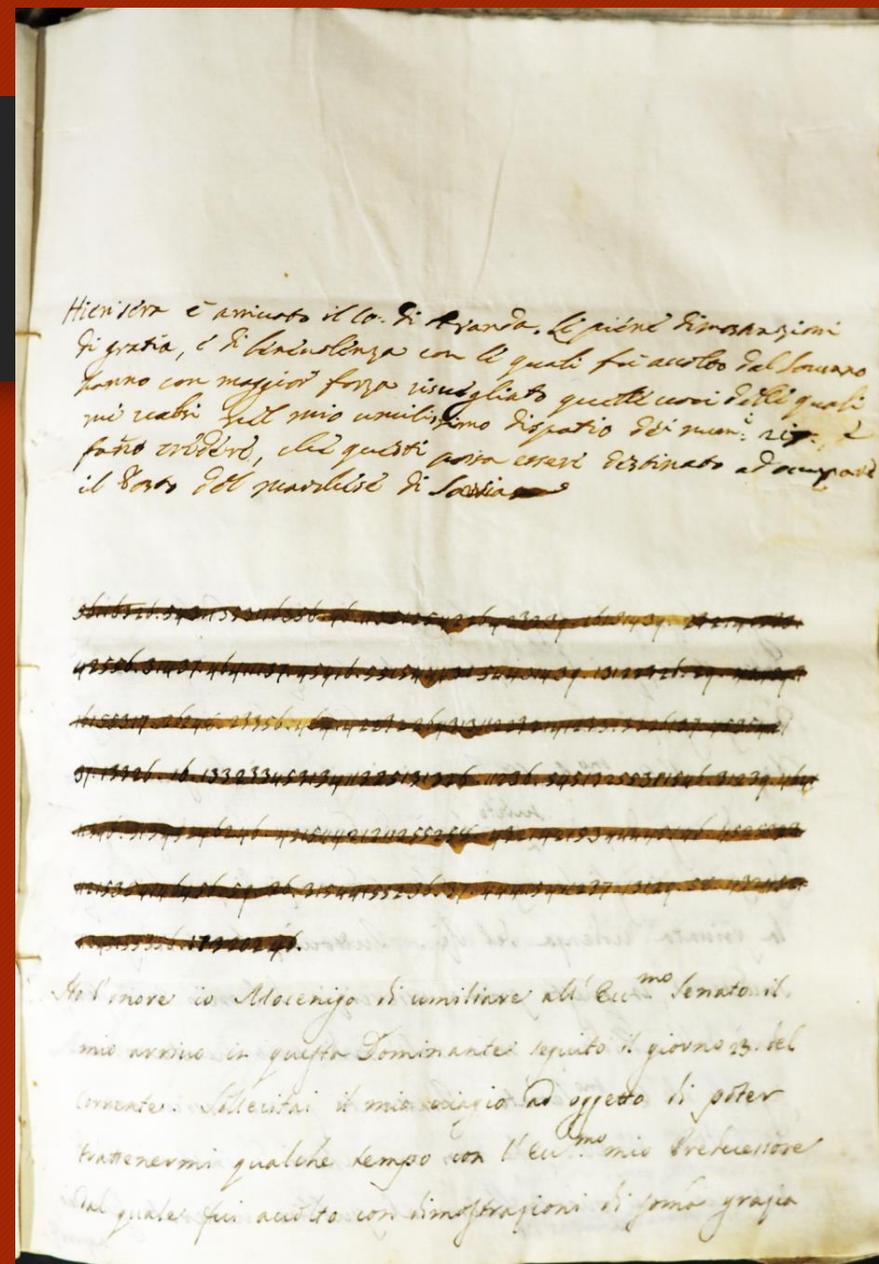
Cifrario ricostruito

Cifrario trovato tra le chiavi di cifra



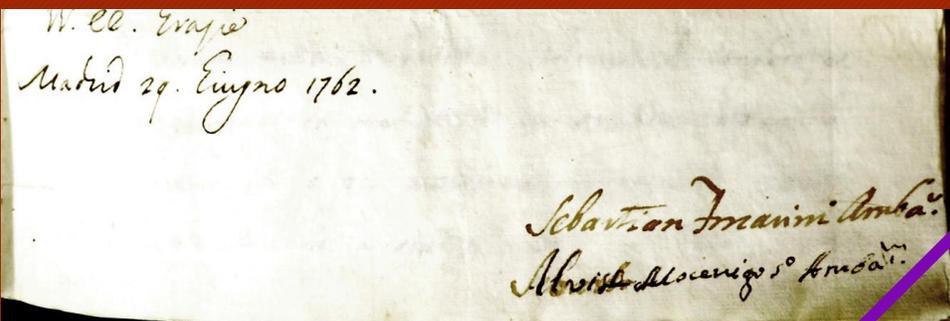
# Un dispaccio dell'ambasciatore veneziano in Spagna

Ser.mo et Ecc.mo  
Marco Foscarini  
Doge di Venezia



Archivio di Stato di Venezia

Senato, dispacci degli ambasciatori in Spagna, Filza 172, 221



Ambasciatore  
Veneziano in Spagna  
Sebastian Foscarini

Madrid 29 giu 1762

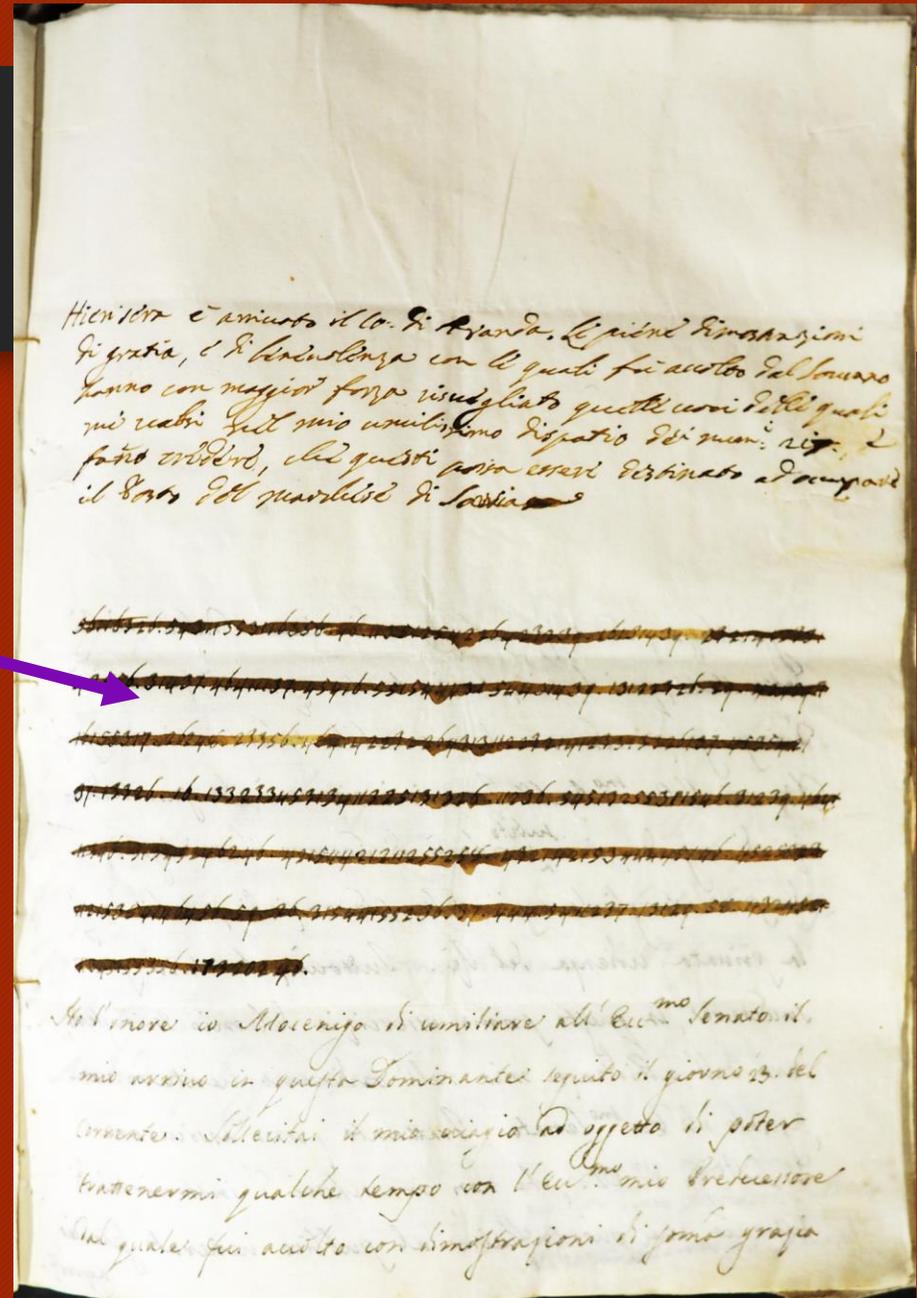


# Il dispaccio del nipote allo zio

Novità 1: il testo deciferato viene scritto direttamente sullo spazio in alto della pagina.

Novità 2: il cifrato viene cancellato dopo essere stato deciferato. Perché?

Peccato che l'inchiostro sia sbiadito lasciando leggere quasi alla perfezione il testo.



# Il cifrario di Sebastian Foscari

## ALFABETO [Omofoni, massimo = 2]

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	z
556	557	558	559	456	457	458	459	356	357	358	359	256	257	258	259	157	158	156	159
56.	57.	58.	59.	46.	47.	48.	49.	36.	37.	38.	39.	26.	27.	28.	29.	17.	18.	16.	19.

## NULLE

101 199 761 768 769 811

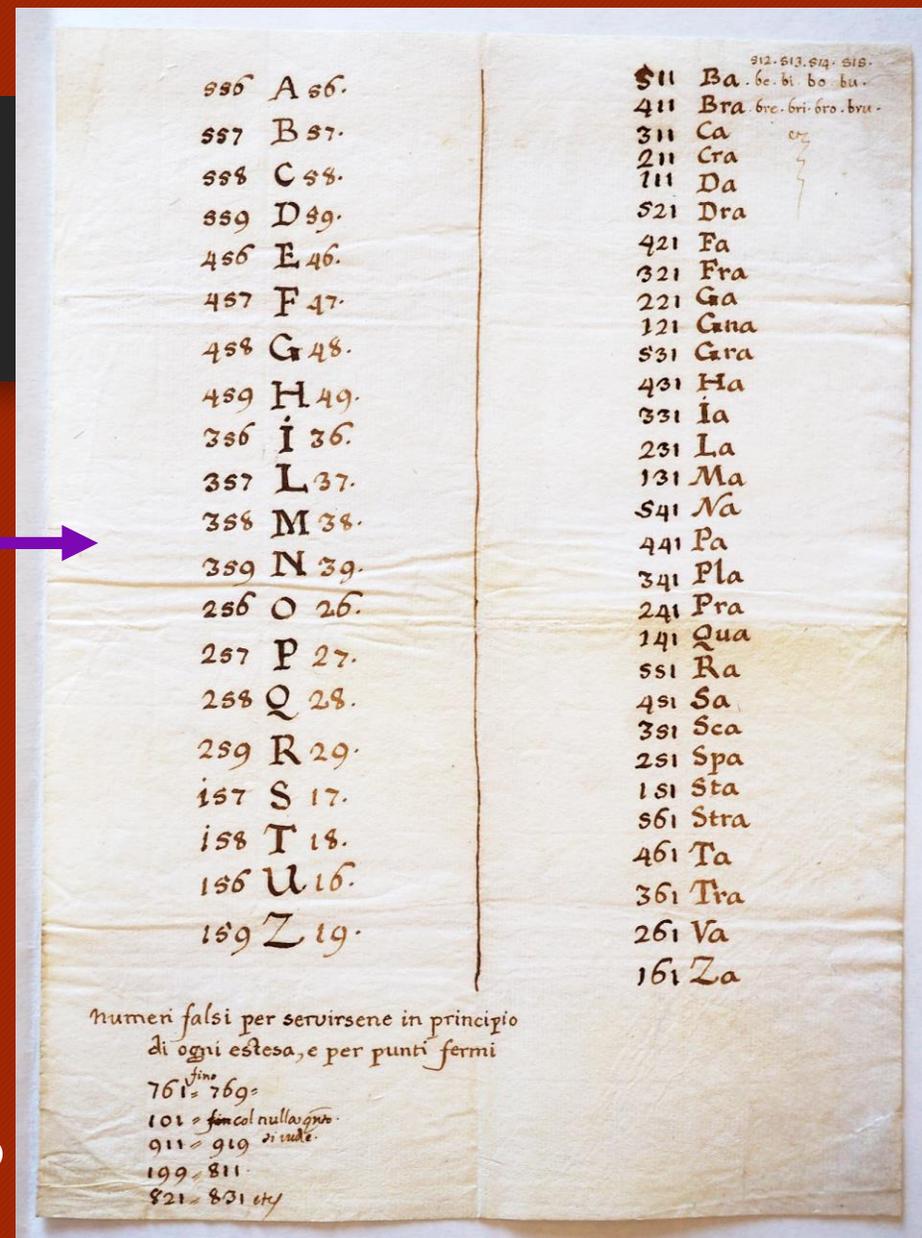
## SILLABARIO [30 sillabe]

ba	be	bi	bo	bu	ga	ge	gi	go	gu	pa	pe	pi	po	pu	sta	ste	sti	sto	stu
511	512	513	514	515	221	222	223	224	225	441	442	443	444	445	151	152	153	154	155
bra	bre	bri	bro	bru	gna	gne	gni	gno	gnu	pla	ple	pli	plo	plu	stra	stre	stri	stro	stru
411	412	413	414	415	121	122	123	124	125	341	342	343	344	345	561	562	563	564	565
ca	ce	ci	co	cu	gra	gre	gri	gro	gru	pra	pre	pri	pro	pru	ta	te	ti	to	tu
311	312	313	314	315	531	532	533	534	535	241	242	243	244	245	461	462	463	464	465
cra	cre	cri	cro	cru	ha	he	hi	ho	hu	qua	que	qui	quo	quu	tra	tre	tri	tro	tru
211	212	213	214	215	431	432	433	434	435	141	142	143	144	145	361	362	363	364	365
da	de	di	do	du	ia	ie	ii	io	iu	ra	re	ri	ro	ru	ua	ue	ui	uo	uu
111	112	113	114	115	331	332	333	334	335	551	552	553	554	555	261	262	263	264	265
dra	dre	dri	dro	dru	la	le	li	lo	lu	sa	se	si	so	su	za	ze	zi	zo	zu
521	522	523	524	525	231	232	233	234	235	451	452	453	454	455	161	162	163	164	165
fa	fe	fi	fo	fu	ma	me	mi	mo	mu	sca	sce	sci	sco	scu					
421	422	423	424	425	131	132	133	134	135	351	352	353	354	355					
fra	fre	fri	fro	fru	na	ne	ni	no	nu	spa	spe	spi	spo	spu					
321	322	323	324	325	541	542	543	544	545	251	252	253	254	255					

cifrario originale

Non c'è più dizionario,  
liste ordinate, la  
semplicità d'uso  
prevale sulla sicurezza.

cifrario ricostruito



Archivio di Stato di Venezia

Cifre, chiavi e scontri di cifra con studi successivi, busta 2

# Un cifrario originale: per scriuer (lista cifrante)

Per scriuer		decima grand										Numeri																			
A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	V	Z	1	2	3	4	5	6	7	8	9	0	0	
018	019	020	021	022	023	024	025	026	027	028	029	030	031	032	033	034	035	036	037	038	039	040	041	042	043	044	045	046	047	048	049
Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio
Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio	Accio

Ira	a	si
tre	a	si
tri	a	si
tro	a	si
tra	a	si
tia	a	si
tal	a	si
tant	a	si
tutt	a	si
tiene	a	si
tempo	a	si
treghe	a	si
treniso	a	si
tupesi	a	si
tuleschi	a	si
turcsi	a	si
Va	f	6i
ve	f	62
vi	f	63
no	f	64
nu	f	65

# Un cifrario originale: per trazer (lista decifrante)

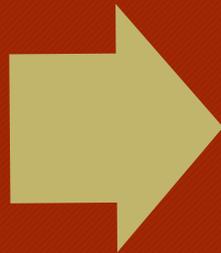
† trazer

A1	ba	120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520	521	522	523	524	525	526	527	528	529	530	531	532	533	534	535	536	537	538	539	540	541	542	543	544	545	546	547	548	549	550	551	552	553	554	555	556	557	558	559	560	561	562	563	564	565	566	567	568	569	570	571	572	573	574	575	576	577	578	579	580	581	582	583	584	585	586	587	588	589	590	591	592	593	594	595	596	597	598	599	600	601	602	603	604	605	606	607	608	609	610	611	612	613	614	615	616	617	618	619	620	621	622	623	624	625	626	627	628	629	630	631	632	633	634	635	636	637	638	639	640	641	642	643	644	645	646	647	648	649	650	651	652	653	654	655	656	657	658	659	660	661	662	663	664	665	666	667	668	669	670	671	672	673	674	675	676	677	678	679	680	681	682	683	684	685	686	687	688	689	690	691	692	693	694	695	696	697	698	699	700	701	702	703	704	705	706	707	708	709	710	711	712	713	714	715	716	717	718	719	720	721	722	723	724	725	726	727	728	729	730	731	732	733	734	735	736	737	738	739	740	741	742	743	744	745	746	747	748	749	750	751	752	753	754	755	756	757	758	759	760	761	762	763	764	765	766	767	768	769	770	771	772	773	774	775	776	777	778	779	780	781	782	783	784	785	786	787	788	789	790	791	792	793	794	795	796	797	798	799	800	801	802	803	804	805	806	807	808	809	810	811	812	813	814	815	816	817	818	819	820	821	822	823	824	825	826	827	828	829	830	831	832	833	834	835	836	837	838	839	840	841	842	843	844	845	846	847	848	849	850	851	852	853	854	855	856	857	858	859	860	861	862	863	864	865	866	867	868	869	870	871	872	873	874	875	876	877	878	879	880	881	882	883	884	885	886	887	888	889	890	891	892	893	894	895	896	897	898	899	900	901	902	903	904	905	906	907	908	909	910	911	912	913	914	915	916	917	918	919	920	921	922	923	924	925	926	927	928	929	930	931	932	933	934	935	936	937	938	939	940	941	942	943	944	945	946	947	948	949	950	951	952	953	954	955	956	957	958	959	960	961	962	963	964	965	966	967	968	969	970	971	972	973	974	975	976	977	978	979	980	981	982	983	984	985	986	987	988	989	990	991	992	993	994	995	996	997	998	999	1000
----	----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	------

psi - germania  
pr2 - grecia  
pr3 - genova  
pr4 - venetia  
pr5 - verona  
pr6 - vicenza  
pr7 - vallona  
pr8 - vdone  
pr9 - zara  
pr30 - zante

# E ora un balzo di un secolo e mezzo

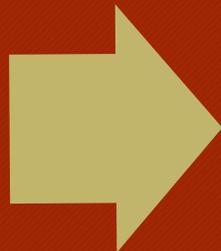
1762 la Repubblica  
di Venezia è ormai  
prossima alla fine



1918  
La Grande Guerra  
è al suo ultimo anno

# Inizio XX secolo

L'invenzione del telegrafo e poi della radio ha reso facile intercettare i messaggi.



Diventa essenziale cifrare tutti i messaggi trasmessi via radio

# Cifrario R, 1918, Grande Guerra

- Un cifrario della Grande Guerra, usato dall'esercito italiano dalla primavera del 1918, ricorda da vicino i nomenclatori veneziani.
- Per quattro secoli nomenclatori e codici sono stati i cifrari preferiti da diplomatici e militari.
- Quello a sinistra è il modello vuoto che deve poi essere compilato tirando a sorte le cifre in modo che siano assolutamente *imprevedibili*.

**TABELLA a. — Parole comuni di uso generale.**

1	2	3	4	5
al	caporal	fuoc	numer (N°)	riserv
artiglieri	che	general	occorre	richiest
aspirant	chi	ha, hanno	occupa	sergent
assieura	comunica	ho	osserva	servizi
attac	colonnell	il	partugli	settor
austria	comand	in	per	shrapnel
avanza	compagni	interdizion	perdit	telefon
battaglion	con	lanca-flamme	ploton	tenent
batteri	cotest	lanca-torpedine	prigionier	trince
bombard	dispo	maggior	possibil	trupp
brigat	division	mitragliatrice	quot	ufficial
calibr	fanteri	munizion	reggiment	uom
camminament	forit	nemio	repart	vigila
capitan	fonogramm	nostr	reticolat	zappator

**TABELLA b. (1) — Nomi propri di persona o località etc., di uso frequente e locale.**

1	2	3	4	5

(1) Questi 30 gruppi saranno scelti e incassellati dal Comando che distribuisce il Cifrario.

**TABELLA c. — Lettere semplici, (2) punteggiatura, desinenze, numeri.**

1	2	3	4	5	6	7	8	9	0
a	b	c	d	e	f	g	h	i	k
l	m	n	o	p	r	s	t	u	v
X	Y	Z	Stop (punto)	virgola (,)	due punti	Parentesi	-salm	-ment	-zion
1	2	3	4	5	6	7	8	9	0

Usare alternativamente i 2 o 3 gruppi cifranti corrispondenti alla stessa voce.  
(2) Il w e l si cifrano rispettivamente « v » e « i ».

**TABELLA d. — Sillabe.**

1	2	3	4	5	6	7	8	9	0
ba	co	fe	gu	mi	pa	quo	si	tta	vi
be	cu	fi	la	mo	pe	ra	so	tte	vo
bi	da	fo	le	mu	pi	re	sta	tti	vu
bo	de	fu	li	na	po	ri	su	tto	za
bu	di	ga	lo	ne	pu	ro	ta	ttu	ze
ca	do	ge	lu	ni	qua	ru	te	tu	zi
ce	du	gi	ma	no	que	sa	ti	va	zo
ci	fa	go	me	nu	qui	se	to	ve	zu

Usare alternativamente i 2 gruppi cifranti corrispondenti alla stessa sillaba.

**TABELLA e. (per gruppi di 3 cifre non terminanti né per 0, né per 1)**

**TABELLA f. (per decifrare tutti i gruppi di 2 cifre, nonché quelli di 3 cifre non terminanti né per 0, né per 1)**

1 <sup>a</sup> cifra del gruppo	2 <sup>a</sup> cifra									2 <sup>a</sup> cifra										
	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
1										6										
2										7										
3										8										
4										9										
5																				

**TABELLA g. (per decifrare i gruppi di 3 cifre terminanti per 0 e per 1)**

(2<sup>a</sup> e 3<sup>a</sup> cifra del gruppo)

1 <sup>a</sup> cifra del gruppo	00	01	10	11	20	21	30	31	40	41	50	51	60	61	70	71	80	81	90	91	
1																					
2																					
3																					
4																					
5																					
6																					
7																					
8																					
9																					

Le tabelle f e g danno il numero della colonna e l'indicazione della tabella in cui trovarsi il gruppo da decifrare (incrocio della linea e della colonna contrassegnate rispettivamente dalla 1<sup>a</sup> cifra e dalla 2<sup>a</sup> (o dalla 2<sup>a</sup> e 3<sup>a</sup>), del gruppo).

# Cifrario R 1918, compilato

TABELLA a. - Parole comuni di uso generale.

1	2	3	4	5
al 470	caporal 890	fuoc 990	numer (N°) 551	riserv 180
artiglieri 101	che 731	general 720	occorre 371	richiest 820
aspirant 540	chi 481	ha, hanno 891	occupa 981	sergent 911
assicura 140	comunica 661	ho 240	osserva 441	servizi 320
attac 690	colonnell 961	il 721	pattugli 131	settor 960
austria 870	comand 300	in 190	per 660	shrapnel 680
avanza 431	compagni 571	interdizion 261	perdit 871	telefon 541
battaglion 710	con 980	lancia-fiamme 460	ploton 630	tenent 881
batteri 880	cotest 461	lancia-torpedine 860	prigionier 350	trincee 450
bombard 801	dispo 761	maggior 730	possibil 740	trupp 741
brigat 381	division 550	mitragliatric 910	quot 850	ufficial 991
calibr 430	fanteri 130	munizion 391	reggiment 590	nom 831
camminament 200	ferit 280	nemie 580	repart 631	vigila 490
capitan 170	fonogramm 811	nostr 970	reticolat 941	zappator 780

TABELLA b. (1) - Nomi propri di persona o località etc., di uso frequente e locale.

1	2	3	4	5
aspirante Baldo 370	casello ferroviario 410	general Bahnan 100	mortuaria da 305 790	teleferica 851
camminamento Susegna 570	colonnello Costa 220	maggior Rondano 861	militaria del boschetto 301	tenente Gioberti 521
cannone da 102 210	carre assicuratore italiana 601	maggior Levi 610	obice da 149 800	tenente Loris 191
capitano Fabbris 361	dolina dei morti 471	maggior Siffa 151	osservatorio Debeli 231	ten. colonnello Dorino 411
capitano Petris 640	fortino Zagonola 711	Malga la Cava 360	quota 208 nord 290	trincea delle frasche sottotende De Andris 971
capitano Piazzi 270	gas assisiente 390	magazzino Genio Suga 611	quota 208 sud 421	

(1) Questi 26 gruppi saranno scelti e incollati dal Comando che distribuisce il Cifrario.

TABELLA c. - Lettere semplici, (2) punteggiatura, desinenze, numeri.

1	2	3	4	5	6	7	8	9	0
a 500	b 650	c 380	d 230	e 480	f 581	g 841	h 160	i 311	k 770
281	330	940	491	621	820	560		670	
310				120	840			251	
i 951	m 671	n 531	o 890	p 271	r 791	s 331	t 241	u 401	v 651
520	351	171	400	700	600	821	620	211	530
X 681	Y 451	z 501	Stop (punto) 201	virgola (,) 511	due punti 420	Parentesi 591	-esim 920	-ment 701	-zin 810
		221	781	901	161	110	181	341	561
1 260	2 760	3 751	4 931	5 340	6 691	7 900	8 930	9 340	0 440
950	141	150	321	121	921	510	291	250	771

Usare alternativamente i 2 o 3 gruppi cifranti corrispondenti alla stessa voce.

(1) H e P: il cifrario rispettivamente x y z e a e l i.

TABELLA d. - Silabe.

1	2	3	4	5	6	7	8	9	0
ba 50	co' 55	fe 68	gu 47	mi 46	pa 22	quo 11	si 85	tta 13	vi 67
	69								
be 35	cu 15	fi 12	la 90	mo 30	pe 82	ra' 44	so 87	tte 31	vo 78
						16			
bi 48	da 91	fo 54	le 51	mu 83	pi 60	re' 14	sta 36	tti 25	vu 86
						58			
bo 38	de' 19	fu 97	li 98	na 63	po 99	ri 53	su 40	tto 76	za 57
	43								
bu 23	di' 61	ga 26	lo 10	ne 64	pu 79	ro 95	ta' 74	ttu 20	ze 81
	29						33		
ca 80	do 66	ge 21	lu 34	ni 42	qua 17	ru 92	te' 77	tu 59	zi 96
							84		
ce 72	du 88	gi 71	ma 28	no' 41	que 52	sa 49	ti' 39	va 70	zo 75
				73			94		
ci 32	fa 62	go 27	me 45	nu 65	qui 24	se 56	to' 93	ve 89	zu 37
							18		

1 Usare alternativamente i 2 gruppi cifranti corrispondenti alla stessa sillaba.

TABELLA e. (per gruppi di 3 cifre non terminanti né per 0, né per 1)

TABELLA f. (per decifrare tutti i gruppi di 2 cifre, nonché quelli di 3 cifre non terminanti né per 0, né per 1)

3 <sup>a</sup> cifra del gruppo	Modificazione apportata alla sillaba corrispondente al gruppo della prima 2 cifre
4	SILLABA: preceduta da N
6	" " " S
2	frammentata " I
8	" " " R
5	seguita... " L
9	" " " N
3	" " " R
7	rovesciata

(1 <sup>a</sup> cifra del gruppo)	(2 <sup>a</sup> cifra)	(2 <sup>a</sup> cifra)
1	0 1 2 3 4 5 6 7 8 9	0 1 2 3 4 5 6 7 8 9
2	9 8 7 6 5 4 3 2 1 0	6 5 4 3 2 1 0 9 8 7
3	8 7 6 5 4 3 2 1 0 9	7 6 5 4 3 2 1 0 9 8
4	7 6 5 4 3 2 1 0 9 8	8 7 6 5 4 3 2 1 0 9
5	6 5 4 3 2 1 0 9 8 7	9 8 7 6 5 4 3 2 1 0

TABELLA g. (per decifrare i gruppi di 3 cifre terminanti per 0 e per 1)

(1 <sup>a</sup> cifra del gruppo)	(2 <sup>a</sup> e 3 <sup>a</sup> cifra del gruppo)
1	00 01 10 11 20 21 30 31 40 41 50 51 60 61 70 71 80 81 90 91
2	1 3 1 7 4 5 5 2 4 1 2 3 3 8 6 1 3 5 8 3 5
3	2 1 4 1 9 2 3 4 4 3 8 9 9 1 3 1 5 2 1 4 8
4	3 2 8 1 5 9 5 4 5 2 5 9 4 2 3 1 4 3 1 2 3
5	4 9 2 3 5 6 4 1 1 0 4 3 2 3 2 1 2 3 2 5 4
6	5 1 3 7 5 1 5 0 3 1 5 3 4 7 0 1 2 3 6 4 7
7	6 8 2 3 3 8 5 4 4 1 5 2 0 4 2 9 2 5 1 1 6
8	7 5 9 1 2 3 3 3 3 2 4 5 8 3 2 2 0 0 5 4 6
9	8 4 1 0 2 5 7 4 5 6 7 4 5 3 3 1 4 1 5 2 3
	9 7 5 3 5 8 6 6 4 3 4 1 5 2 3 5 2 4 3 5

Le tabelle f e g danno il numero della colonna e l'indicazione della tabella in cui trovarsi il gruppo da decifrare (incrocio della linea e della colonna contrassegnate rispettivamente dalla 1<sup>a</sup> cifra e dalla 2<sup>a</sup> o dalla 2<sup>a</sup> e 3<sup>a</sup> del gruppo).

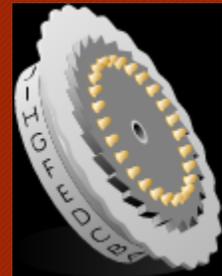
Un esempio di cifrario R compilato. I numeri sono estratti a sorte, quindi se anche il nemico venisse in possesso di questo particolare cifrario non potrà decifrare messaggi cifrati con un'altra compilazione del cifrario R.

Non risulta che il cifrario R sia stato decrittato dai crittoanalisti austriaci, nonostante si abbia notizia che almeno due copie del cifrario erano cadute nelle loro mani.

# Navigando in rete



[Archivio di Stato di Venezia](#)



<https://www.cryptomuseum.com/>

<https://www.cryptool.org/en/cryptool2>



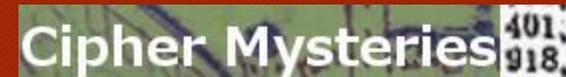
<https://bletchleypark.org.uk/>



Ufficio Storico SME



<http://scienceblogs.de/klausis-krypto-kolumne/>



<http://ciphermysteries.com/>

# Crittografia veneziana

Grazie per l'attenzione!