Venetian Cryptanalysis Treatises of the Renaissance

Posters on show on June 21, 2022

by Paolo Bonavoglia

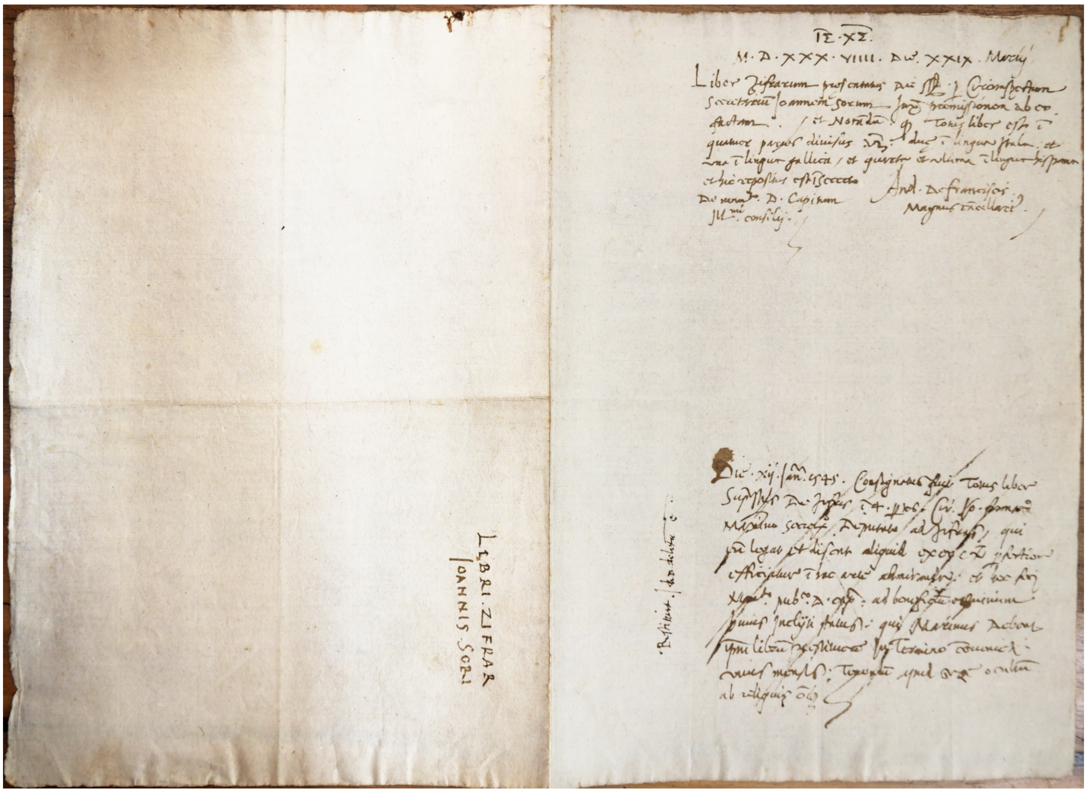
HistoCrypt2022

Amsterdam

Het Trippenhuis

Zuan Soro Citadin et Servitor Zuan Soro

The founding father and his lost book



IE·XI.

M·D·XXX·VIIII· Die XXIX· Martij

Liber Ziffrarum presentatus per Sp. circumspectum Secretarium Ioannem Sorum iuxta promissionem ab eo factam. / et Notandum quod totus liber est in quatuor partes divisus videlicet duae in lingua Itala, et una in lingua gallica / et quarta et ultima in lingua hispana et hic repositus est in secreto Dominorum D. Capitum Ill.mi consilij.

And. De franciscis Magnus Cancellarius

~~Die xij Jan. 1545. Consignatus fuit totus liber suprascriptus De Ziphris in 4. partes Cir. Io. Franc.o Marino secretario Deputato ad Ziffras, qui [illegible] legat et discat aliquid ex eo [illegible] [illegible] [illegible] [illegible] et [illegible] [illegible] pub.co D. [illegible] ad beneficium [illegible] [illegible] [illegible] qui Marinus debeat ipsum librum restituere sub termino unius mensis, tenendo apud se occulte ab aliquo [illegible]~~

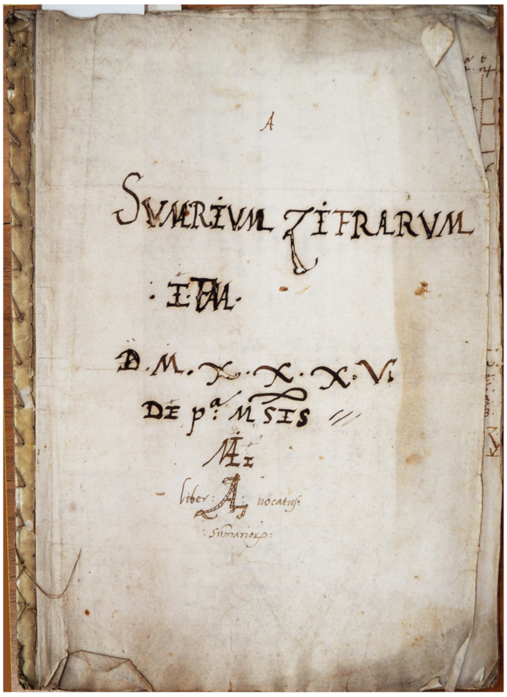
Restituit [illegible]

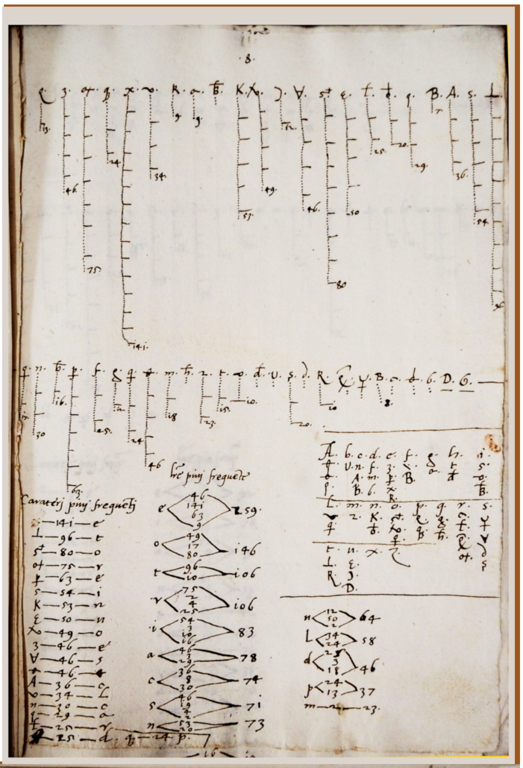
LIBRI ZIFRAR IOANNIS SORI

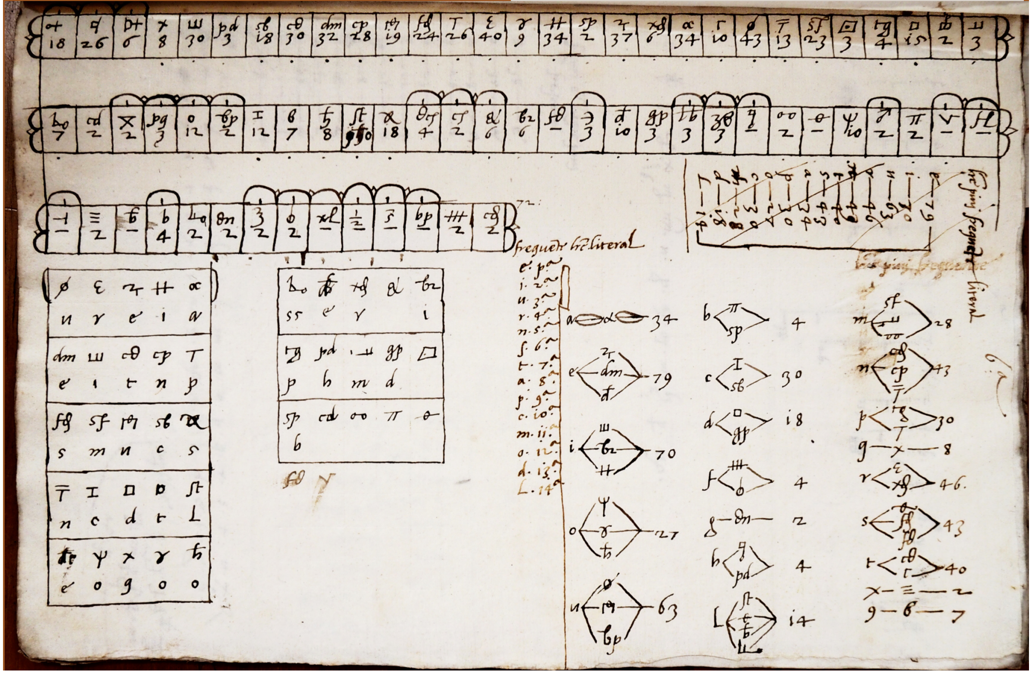
Zuan Soro, alias Giovanni Soro, was elected secretary of the **CX** (Council of Ten) in 1505, and became soon a master code breaker; he is the first secretary officially named as ”Deputy of ciphers”. In 1511 he announced his purpose to write a treatise about code breaking. 28 years after, on 29 March 1539, he delivered the book to the great chancellor Andrea di Franceschi, as one can see in the receipt her on the top of this sheet. Below another writing dated 12 January 1545 (1546 modern style) telling us the book had the title *De Ziphris* and was lent to the circ. Io. Franc.^{o} Marino secretary and deputy of ciphers, under the condition to give back it within a month, and do not show the book to anyone else. Marino later returned the book, the receipt was crossed out, and no other information was found about the book, that in 1871 was mentioned as lost by Pasini. *ASVe, Consiglio di Dieci (shortly* ***CX****), Cifre, chiavi e scontri di cifra ... b.5.2 loose sheet.*

Soro or Ludouici?

Cryptanalysis of a homophonic cipher



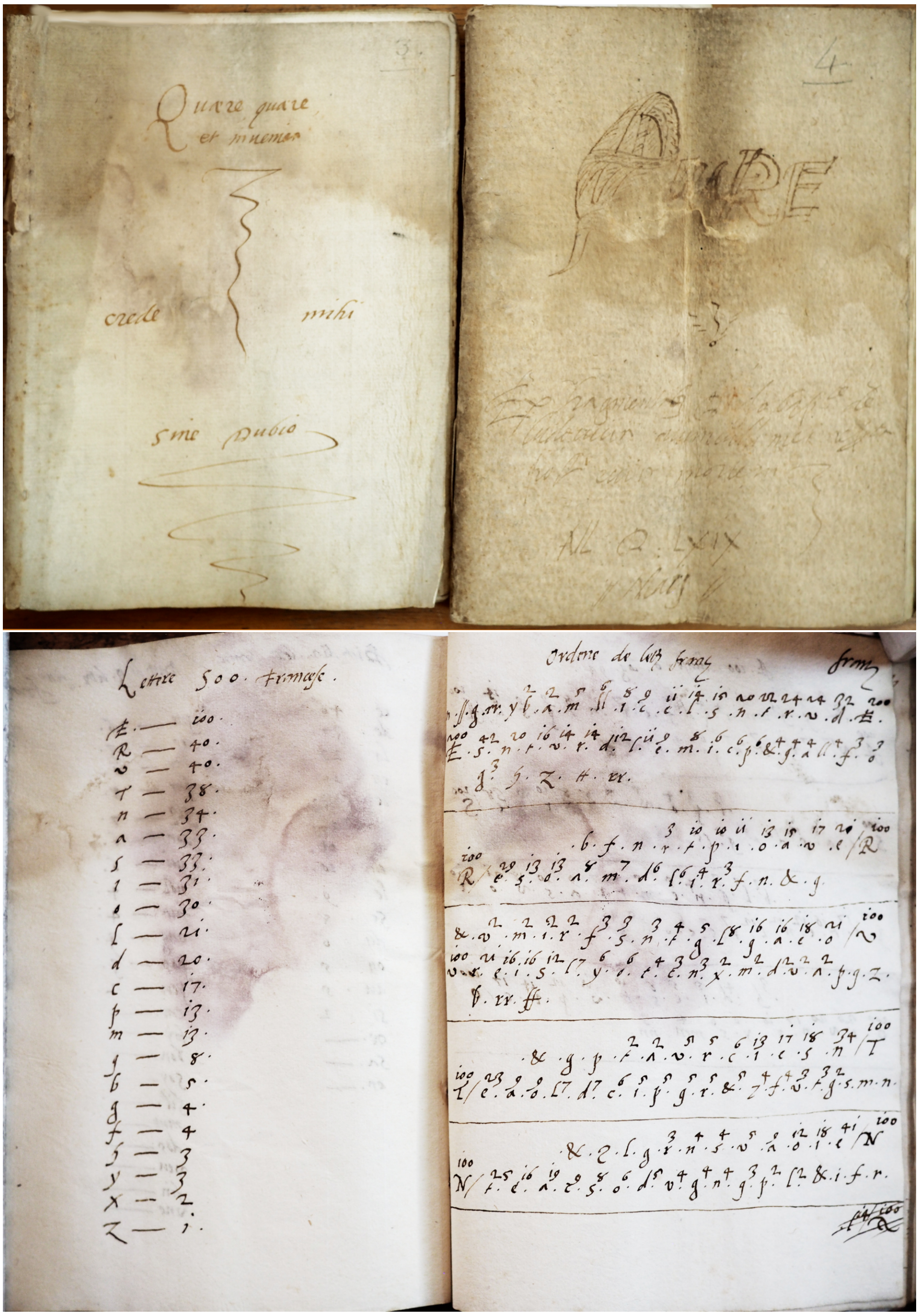

Caratterj piu frequenti
le piu frequente


frequente biliteral
le piu frequente

Cover page of the *Summarium Ziphrarum* a 1535 booklet having pages written in a fair style, clearly a summary of a decryption. Here it is evident the decryption of a cipher with homophones and nulls. Soro was still in office but Ludovici was on the rise. But how could this solution be reached? Likely examining digraphs; vowels make digraph with most letters, consonants with a few other letters. And one can guess much trial and error work. *ASVe, CX: cifre, chiavi e scontri di cifra ... b.4.5*

Zuan Batta Ludouici di me Zuanb.ta di Lodouici,

The pupil who surpassed his teacher


Quere quare et invenies
crede mihi
sine dubio
M D LXIX
Ordene de lre francese

Lettere 500 francese.

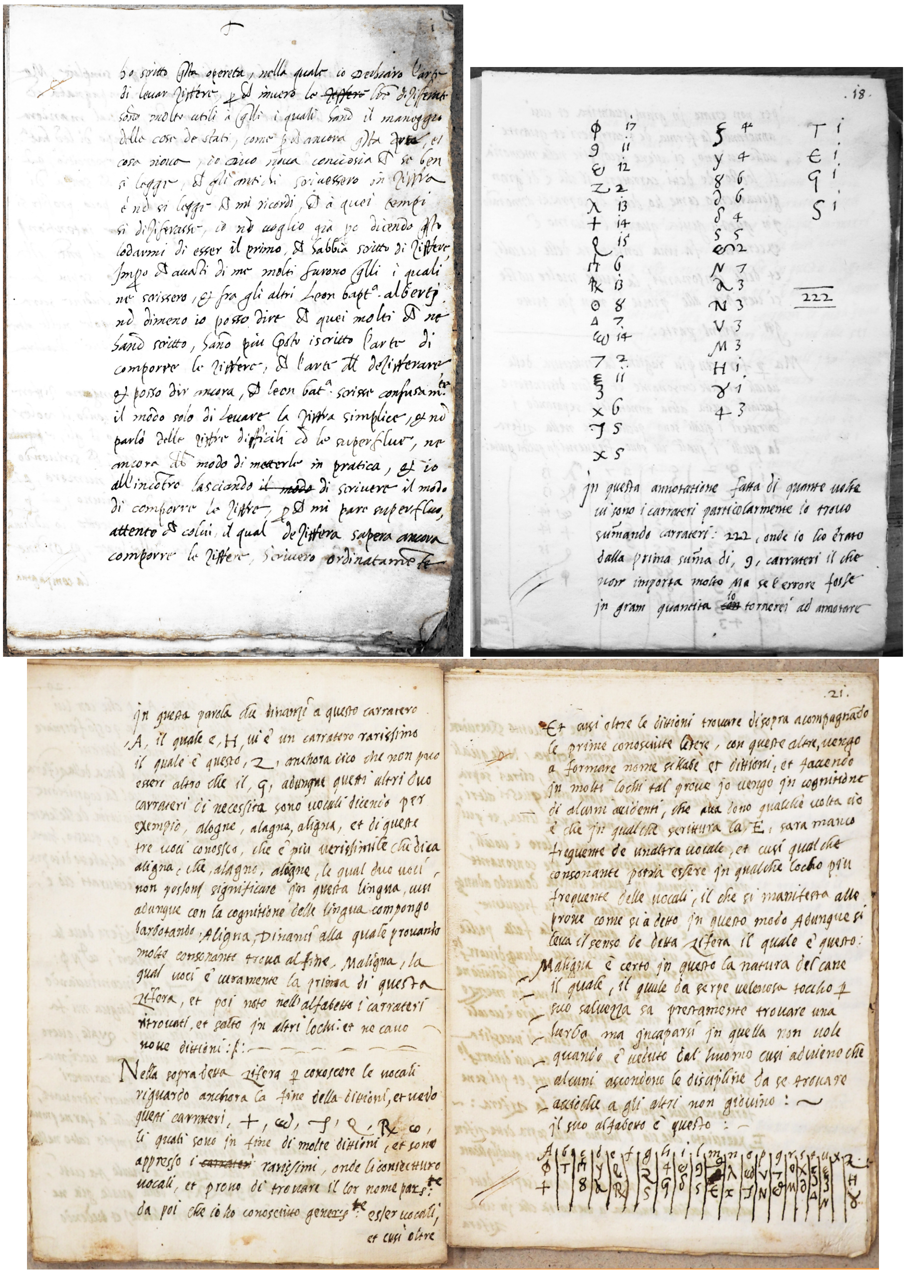
E	100
R	40
v	40
T	38
n	34
a	33
s	33
i	31
o	30
l	21
d	20
c	17
p	13
m	13
q	8
b	5
g	4
f	4
h	3
y	3
x	2
z	1

Zuanbatta Ludouici (Latin de Lodouicis), alias Giambattista Ludovici became deputy of ciphers in 1518, the second after Soro. He and later Alvise Borghi surpassed Soro, being able to decrypt not only homophonic ciphers, but also syllables and nomenclators, in many languages. By GB Ludovici we have only fragments bound in two booklets, dated 1569; page with tables of frequency for the French language: on the left frequencies of single letters; on the right the first page of the tables for digraphs, beginning with the most frequent that is **E**; the first row gives frequencies of digraphs ending with **E**, the second for digraphs beginning with **E**; and so on for other letters R V T N ... *ASVe, CX, Cifre, chiavi e scontri di cifra ... b.6.2 f...*

Anonymous

Soro or Borghi? Or who else?

An anonymous treatise about code breaking



ho scritto questa operetta, nella quale io declararò l'arte di leuar ziffere, perche inuero le ~~ziffere~~ arte di ziffera sono molto utili à quelli i quali hanno il maneggio delle cose de stati, come per ancora questa ~~arte~~, et cosa nuoua, io dico nuoua conciosia che se ben si legge, che gli antichi scriuessero in ziffra e non si legge che mi ricordi, che à quei tempi si diziferasse, io non voglio già per dicendo questo lodarmi di esser il primo, che habbia scritto di ziffere, imperò che auanti di me molti furono quelli i quali ne scrissero, et fra gli altri Leon bapt.a alberti, non dimeno io posso dire che quei molti che ne hanno scritto, hanno più presto iscritto l'arte di comporre le ziffere, che l'arte del deziferare, et posso dir ancora, che leon bat.a scrisse confusam.te il modo solo di leuare la ziffra simplice, et non parlò delle ziffre difficili co le superflue, ne ancora del modo di metterle in pratica, et io all'incontro lasciando ~~il modo~~ di scriuere il modo di comporre le ziffre, perche mi pare superfluo, attento che colui, il qual de ziffera sapera ancora comporre le ziffere, scriuero ordinatamente ~~le~~

.18.

ϕ	17	ʃ	4	T	1
9	11	y	4	Є	1
ʊ	12	8	6	ᑫ	1
Z	2	∂	6	S	1
λ	13	δ	4		
+	14	s	5		
ℓ	15	ɷ	2		
ɦ	6	N	7		
℞	13	ɑ	3	222	
⊖	8	N	3		
Δ	7	V	3		
ω	14	M	3		
7	2	H	1		
ɛ 3	11	ɣ	1		
x	6	4	3		
ℸ	5				
x	5				

jn questa annotatione fatta di quante uolte ui sono i carrateri particolarmente io trouo sumando carrateri: 222, onde io ho errato dalla prima suma di, 9, carrateri il che non importa molto Ma se l'errore fosse jn gram quantita ~~seu~~ io tornerei ad annotare

jn questa parola che tirarsi a questo carratero A, il quale e, H, ui è un carratero rarissimo il quale è questo, Z, anchora dico che non puo essere altro che il, q, adunque questi altri duo carrateri di necessita sono uocali dicendo per exempio, alogne, alagna, aligna, et di queste tre uoci conosco, che è piu uerisimile che dica aligna, che, alagno, alogne, le qual duo uoci non posson significare jn questa lingua, uisi adunque con la cognitione delle lingua compongo barbotando, Aligna, Dinanzi alla quale prouando molte consonante troua al fine, Maligna, la qual uoce è ueramente la prima di questa zifera, et poi noto nell'alfabeto i carrateri ritrouati, et salto jn altri lochi: et ne cauo noue dittioni: f:

Nella sopradetta zifera per conoscere le uocali riguardo anchora la fine della dittioni, et uedo questi carrateri, +, ω, ℸ, ℓ, ℞, ω, li quali sono jn fine di molte dittioni, et sono appresso i ~~carrateri~~ rarissimi, onde li consietturo uocali, et prouo di trouare il lor nome particolarmente: da poi che io ho conosciuto generalmente esser uocali, et cusi oltre

.21.

Et cusi oltre le dittioni trouate di sopra acompagnado le prime conosciute letere, con queste altre, uengo a formare nome sillabe et dittioni, et facendo jn molti lochi tal proue jo uengo jn cognitione di alcuni accidenti, che ~~aua~~ sono qualche uolta cio è che jn qualche scrittura la, E, sara manco frequente de unaltra uocale, et cusi qualche consonante potria essere jn qualche locho piu frequente delle uocali, il che si manifesta alle proue come gia detto jn questo modo Adunque si leua il senso de detta zifera il quale è questo:

Maligna è certo jn questo la natura del cane il quale, il quale da serpe uelenoso tocho per suo saluezza sa prestamente trouare una herba ma jncaparsi jn quella non uole quando è ueduto dal huomo cusi adiuiene che alcuni ascondono le discipline da se trouare acciochè a gli altri non giouino: ~

il suo alfabeto è questo: ~

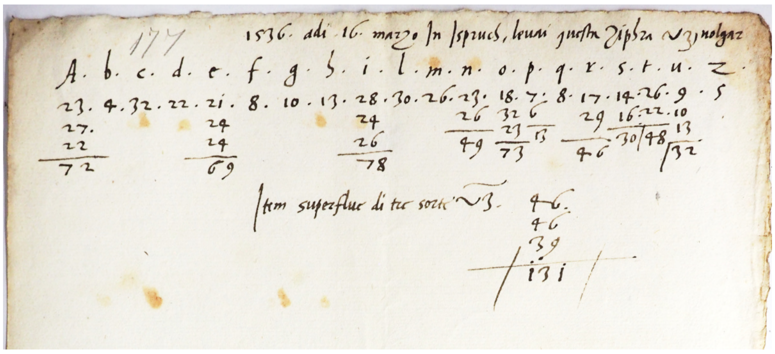
A	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	x	z
ϕ +	T	ɱ 8	y ɑ	ℓ ℞		Z S	4 9	ʊ δ	9 s	ϴ Є	λ x	ω ℸ	V N	T ɷ	ϴ M	X ∂	ʃ 3 Δ	ɛ 3 N		H ɣ

Sample of pages of an anonymous booklet about the art of leuar *le ziffere senza scontro* using today's language, cryptanalysis. The author says he is not the first to write about ciphers, but, as far as he knows, the first to write about this art. Below, two pages of this *operetta*, about difficult ciphers, those with homophones and nulls.The manuscript is listed in the inventory of Z.F. Marin, as written by hand of Marin himself in the first part, of his son Ferigo for the rest. The transcription of the work of someone else, someone writing in the first half of the 1500's, someone believing to be the first to write about codecreaking, someone knowing Alberti's *De Zifris*, someone having to do with homophonic ciphers of signs. Who is the author? A first hypothesis was Soro, his lost book, fascinating but without any evidence. Reading Borghi's supplications to the CX, strong analogies, even identical locutions suggest Borghi as a plausible author of this nice *operetta*, but one must presume he didn't know already the secret book of Soro, when he wrote it. An open question. *ASVe, CX, Cifre, chiavi e scontri di cifra ... b.6.2 f.6*

Aluise Borgi

Jo Aluise Borgi

The Polyglot



177 1536. adi 16. marzo In Ispruch, levai questa ziphra ∽3 volgar

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

23. 4. 32. 22. 21. 8. 10. 13. 28. 30. 26. 23. 18. 7. 8. 17. 14. 26. 9. 5

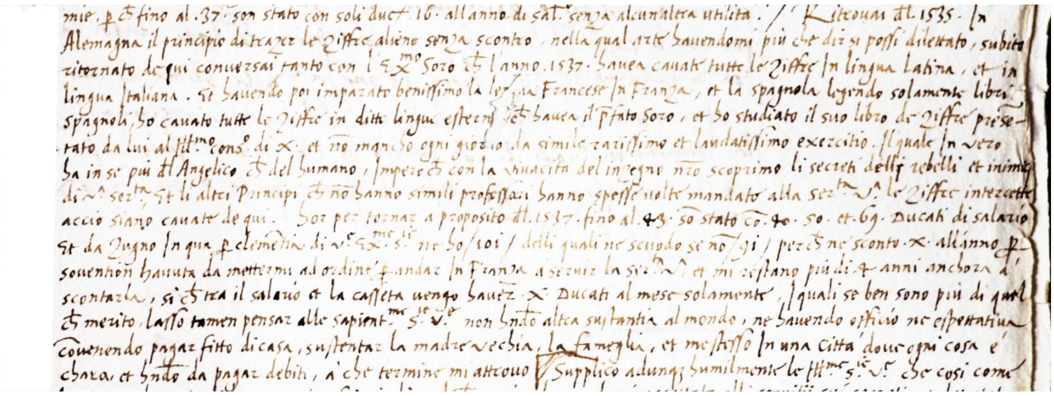
27. 24 24 26 32 6 29 16. 22. 10

22 24 26 49 23 13 46 30 48 13

72 69 78 73 32

Item superflue di tre sorte ∽3. 46. 46 39 131

Aluise Borgi, alias Alvise Borghi. A master of codebreaking, learned it in Germany while he was secretary of the ambassador to the Emperor. He left no writings with his name except for a few supplications to the Council of Ten, like the following, and this leaflet. A homophonic cipher decrypted in Innsbruck, 1536, March 16, only a diagram of frequencies is given. The codebreaker was almost surely Alvise Borghi, that those years worked as a secretary of the Venetian embassy to the Holy Roman Empire. It was mistakenly archived as a cipher key, so it is, among other cipher keys, in *ASVe, CX Cifre, chiavi e scontri di cifra ... b.3 c. 177.*

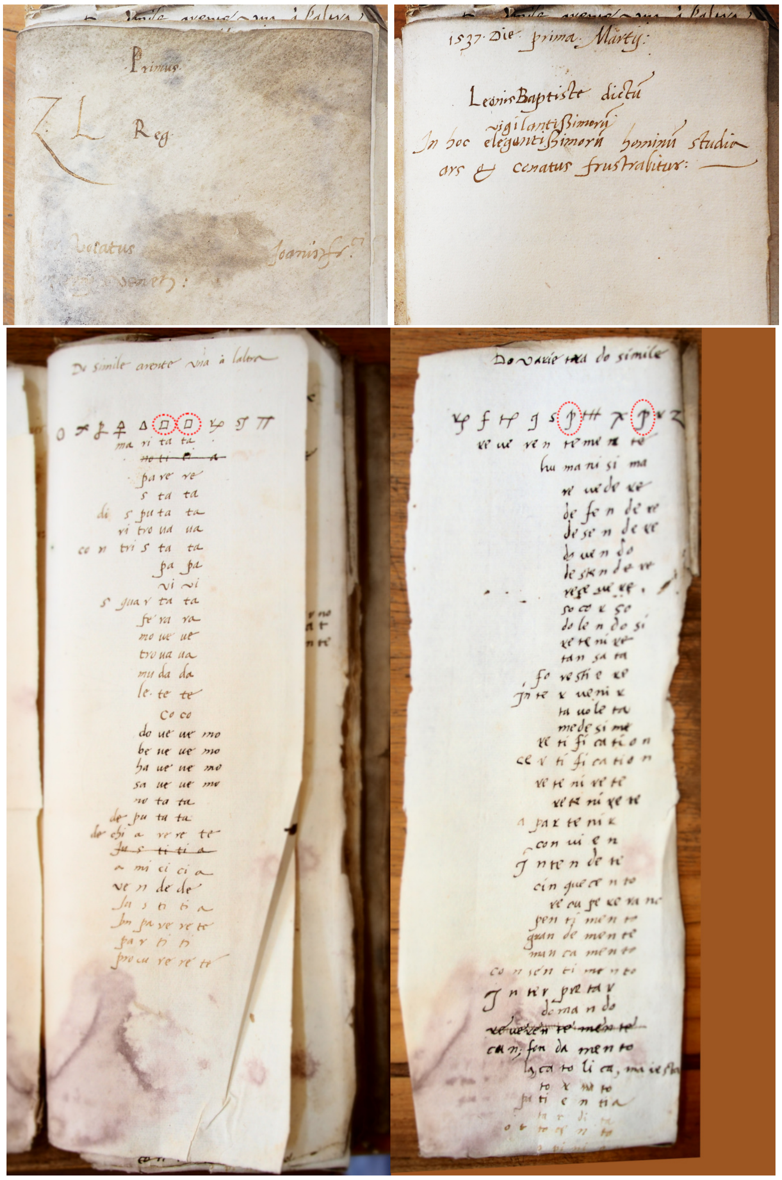


mie, per che fino al .37. son stato con soli duc.ti 16. all'anno di sal.o senza alcun'altra utilita. // Ritrovai del .1535. In
Alemagna il principio di trazer le ziffre aliene senza sconto, nella qual arte havendomi piu che dir si possi dilettato, subito
ritornato de qui conversai tanto con l'Ecc.mo Zoro che l'anno .1537. havea cavate tutte le ziffre In lingua latina, et in
lingua Italiana. Et havendo poi imparato benissimo la lengua Francese In Franza, et la spagnola legendo solamente libri
spagnoli, ho cavato tutte le ziffre in ditte lingue estrane che havea il p.fato Zoro, et ho studiato il suo libro de ziffre prese-
tato da lui al Ill.mo Cons.o di X. et non mancho ogni giorno da simile rarissimo et laudatissimo exercitio. Il quale In vero
ha in se piu del Angelico che del humano, Impero che con la vivacita del ingegno nro scoprimo li secreti delli rebelli et inimici
di V.a Ser.tà Et li altri Principi che non hanno simili professori hanno spesse volte mandato alla Ser.tà V.a le ziffre interzette
accio siano cavate de qui. Hor per tornar a proposito del .1537. fino al .43. so stato con .40. 50. et .69. Ducati di salario
Et da Zugno In qua per clementia di V.e Ecc.me S.rie ne ho /101/ delli quali ne scuodo se no /91/ per che ne sconto .X. all'anno per
souention havuta da mettermi ad ordine per andar In Franza a servir la Ser.tà V.a et mi restano piu di .4. anni anchora a
scontarla, si che tra il salario et la casseta vengo haver .X. Ducati al mese solamente, I quali se ben sono piu di quel
che merito, lasso tamen pensar alle sapient.me S.rie V.e non havendo altra sustantia al mondo, ne havendo officio ne espettativa
convenendo pagar fitto di casa, sustentar la madre vecchia, la fameglia, et me stesso In una Citta dove ogni cosa e'
chara, et havendo da pagar debiti, a che termine mi attrovo. Supplico adunque humilmente le Ill.me S.rie V.e che cosi come

An extract from the 1548 supplication to the **CX** where he asks for a salary increase, in a city where everything is so expensive ... he also tells of his career first as an embassy secretary and then as a skilled codebreaker. *ASVe, CX parti secrete f7 1547-52.*

Zuan Francesco Marin

the last Venetian code breaker

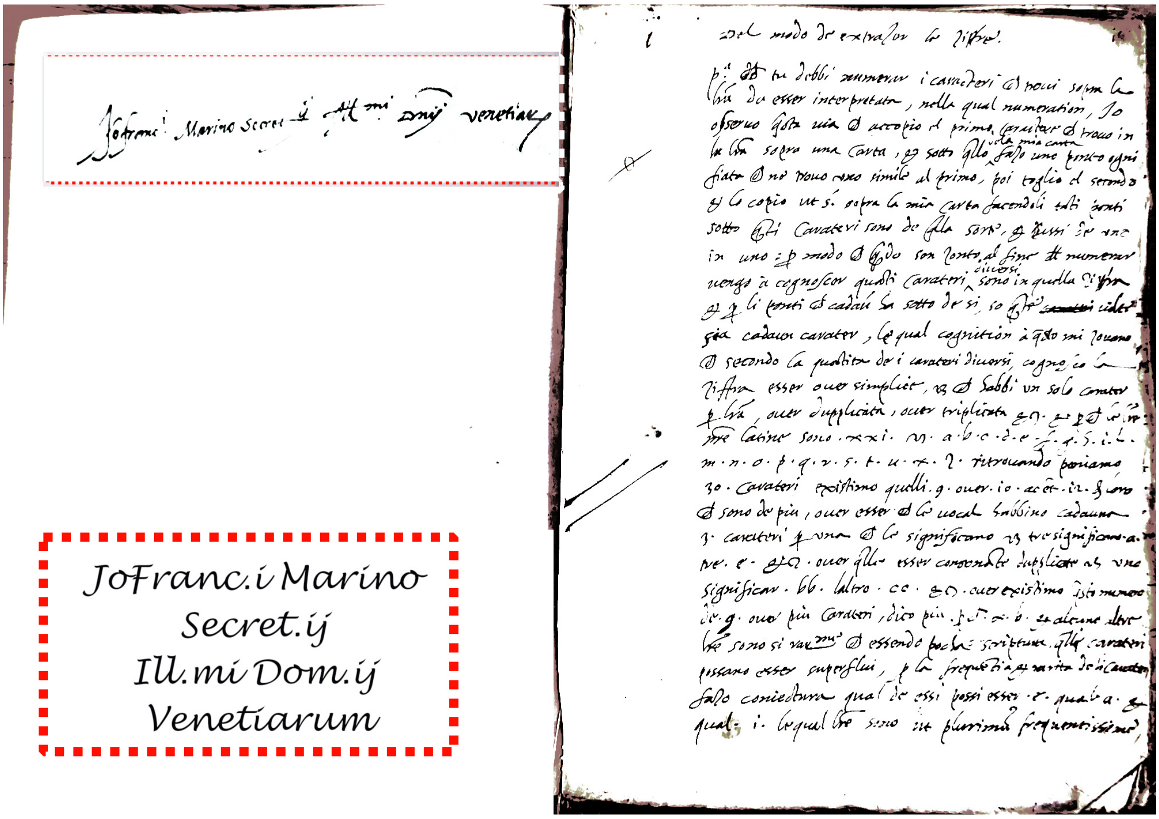


Zuan Francesco Marin, Gianfrancesco Marino, the last great Venetian code breaker. A booklet about decryption of syllabaries dated 1537, March 1.

The name Joanis Fr^{ci} refers surely to the one of Zuan Francesco Marin, the last great codebreaker of Venice. On the right the dedication to Leon Battista Alberti. Bottom: A pair of pages showing some pattern matching trials. *ASVe, CX Cifre, chiavi e scontri di cifra ... b.6.1 f.1*

Zuan Francesco Marin

Del modo di estrazer le ziffre



Jofranc.i Marino Secret.ij Ill.mi Dom.ij Venetiarum

JoFranc.i Marino
Secret.ij
Ill.mi Dom.ij
Venetiarum

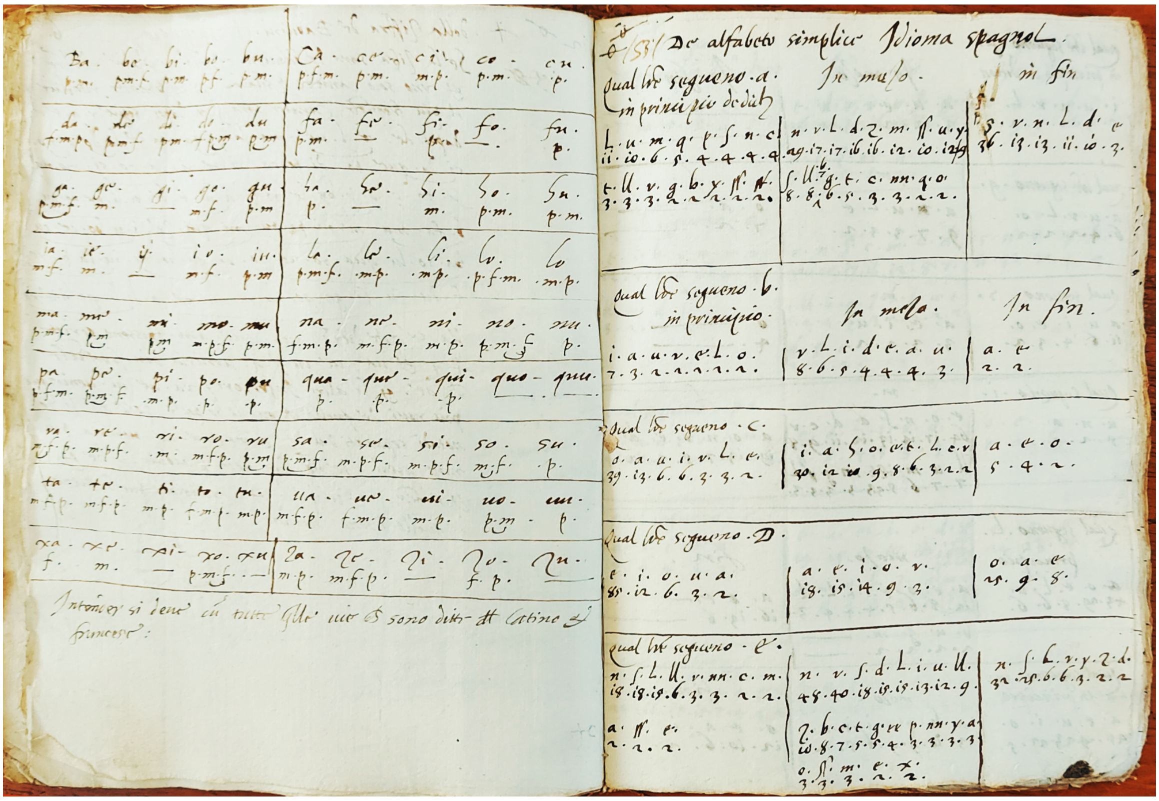
Del modo de extrazer le ziffre.

P.a che tu debbi numerar i caratteri che voci sopra la
lra da esser interpretata, nella qual numeration, Io
osservo questa via che accopio el primo caratter che trovo in
la lra sopra una carta, et sotto quello sulla mia carta fazo uno ponto ogni
fiata che ne trovo uno simile al primo, poi toglio el secondo
et lo copio ut s. sopra la mia carta facendoli tali ponti
sotto quanti caratteri sono de quella sorte, et cussi de uno
in uno per modo che quando son zonto al fine de numerar
vengo a cognoscer quanti caratteri diversi sono in quella ziffra
et per li ponti che cadaun ha sotto de si, so quante ~~[illegible]~~ volte
gia cadaun carater, la qual cognition a questo mi zouano
che secondo la qualita de i caratteri diversi, cognosco la
ziffra esser over simplice, videlicet che habbi un solo carater
per lra, over dupplicata, over triplicata etc. et per che le le-
tre latine sono .xxi. videlicet a.b.c.d.e.f.g.h.i.l.
m.n.o.p.q.r.s.t.u.x.z. ritrovando poniamo
30. caratteri existimo quelli .9. over .10. accenti .12. [illegible]
che sono de piu, over esser che le vocal habbino cadauna
3. caratteri per una che le significano, videlicet tre significano .a.
tre .e. etc. over quelle esser consonante dupplicate ad una
significar .bb. laltro .cc. etc. over existimo questi manco
de .9. over piu caratteri, dico piu per che .x. h. et alcune altre
lre sono si varissime che essendo poche scritture quelli caratteri
possano esser superflui, per la frequentia et rarita de i caratteri
fazo coniectura qual de essi possi esser .e. qual .a. et
qual .i. le qual lre sono in plurimo frequentissime,

Z.F. Marin's book, "*Del modo di estrazer le ziffre*" "About the mode to decrypt the ciphers", a treatise about the methods used by Marin and his predecessors. The book is rich of frequency tables of many kinds, relative to Latin, Vulgar(Italian), French and Spanish languages. Apparently nothing really new compared to Ludovici's fragments. *ASVe, CX: cifre, chiavi e scontri di cifra ... b. 6.2 f.2.*

Zuan Francesco Marin

Pages by Marin inside *Del modo di estrazer le ziffre*



Ba. p.m.	be. p.m.f.	bi. p.m.	bo. p.f.	bu. p.m.	Ca. p.f.m.	ce. p.m.	ci. m.p.	co. p.m.	cu. p.
da. f.m.p.	de. p.m.f.	di. p.m.	do. f.p.m.	du p.m.	fa. p.m.	fe. —	fi. [illegible]	fo. —	fu. p.
ga. p.m.f.	ge. m.	gi. —	go. m.f.	gu p.m	ha. p.	he. —	hi. m.	ho. p.m.	hu. p.m.
ia. m.f.	ie. m.	ij. —	io. m.f.	iu. p.m	la. p.m.f.	le. m.p.	li. m.p.	lo. p.f.m.	lu m.p.
ma. p.m.f.	me. p.m.	mi. p.m.	mo. m.p.f.	mu p.m.	na. f.m.p.	ne. m.f.p.	ni. m.p.	no. p.m.f.	nu. p.
pa p.f.m.	pe. p.m.f.	pi. m.p.	po. p.	pu p.	qua. p.	que. p.	qui. p.	quo. —	quu. —
ra. m.f.p.	re. m.p.f.	ri. m.	ro. m.f.p.	ru p.m	sa. p.m.f.	se. m.p.f.	si. m.p.f.	so. m.f.	su. p.
ta. m.f.p.	te. m.f.p.	ti. m.p.	to. f.m.p.	tu. m.p.	ua. m.f.p.	ue. f.m.p.	ui. m.p.	uo. p.m.	uu. p.
xa. f.	xe. m.	xi. —	xo. p.m.f.	xu —	za. m.p.	ze. m.f.p.	zi. —	zo. f.p.	zu. —

Intonces si deue cu tutte qlle uie che sono ditte dt Latino et francese:

(58) De alfabeto simplice Idioma spagnol.

Qual lre segueno .a. in principio de dicti	In mezo.	in fin
L. u. m. q. t. s. n. c 11. 10. 6. 5. 4. 4. 4. 4	n. r. L. d. z. m. ss. u. y. 29. 17. 17. 16. 16. 12. 10. 12	s. r. n. L. d. e 36. 13. 13. 11. 10. 3.
t. ll. v. g. b. y. ss. ff. 3. 3. 3. 2. 2. 2. 2. 2.	s. ll. g. t. c. nn. q. o. 8. 8. 6. 5. 3. 3. 2. 2.	

Qual lre segueno .b. in principio.	In mezo.	In fin.
i. a. u. r. e. L. o. 7. 3. 2. 2. 2. 2. 2.	r. L. i. d. e. a. u. 8. 6. 5. 4. 4. 4. 3.	a. e 2. 2.

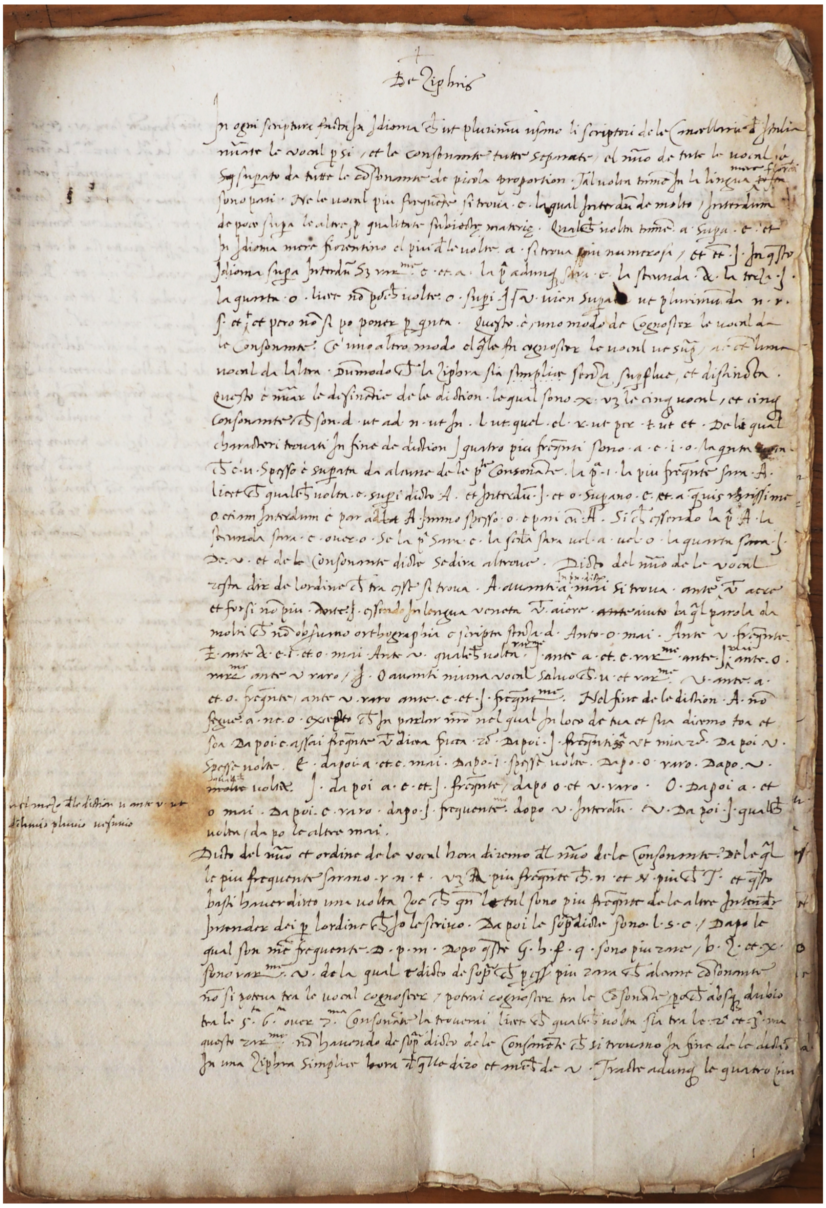
Qual lre segueno .c.		
o. a. u. i. r. L. e. 39. 13. 6. 6. 3. 3. 2.	i. a. h. o. ct. L. e. r 30. 12. 10. 9. 8. 6. 3. 2. 2	a. e. o. 5. 4. 2.

Qual lre segueno .D.		
e. i. o. u. a. 85. 12. 6. 3. 2.	a. e. i. o. r. 18. 15. 14. 9. 3.	o. a. e 25. 9. 8.

Qual lre segueno .e.		
n. s. L. ll. r. nn. c. m. 18. 18. 15. 6. 3. 3. 2. 2.	n. r. s. d. L. i. u. ll. 48. 40. 18. 15. 15. 13. 12. 9.	n. s. L. r. y. z. d. 32. 25. 6. 6. 3. 2. 2
a. ff. e. 2. 2. 2.	z. b. c. t. g. rr. p. nn. y. a 10. 8. 7. 5. 5. 4. 3. 3. 3. 3	
	o. ss. m. e. x. 3. 3. 3. 2. 2.	

A couple of pages of Marin's treatise, with frequencies of pair of letters near a given letter, starting with **A**: groups like a*, *a*, *a that is as a first letter (*in principio*), as a letter in the middle *In mezo*, as the second letter (*in fin*). Very useful for decrypting homophonic ciphers also. *ASVe, CX: cifre, chiavi e scontri di cifra ... b. 6.2 f.2.*

Yet another anonymous De Zyphris



De Ziphris

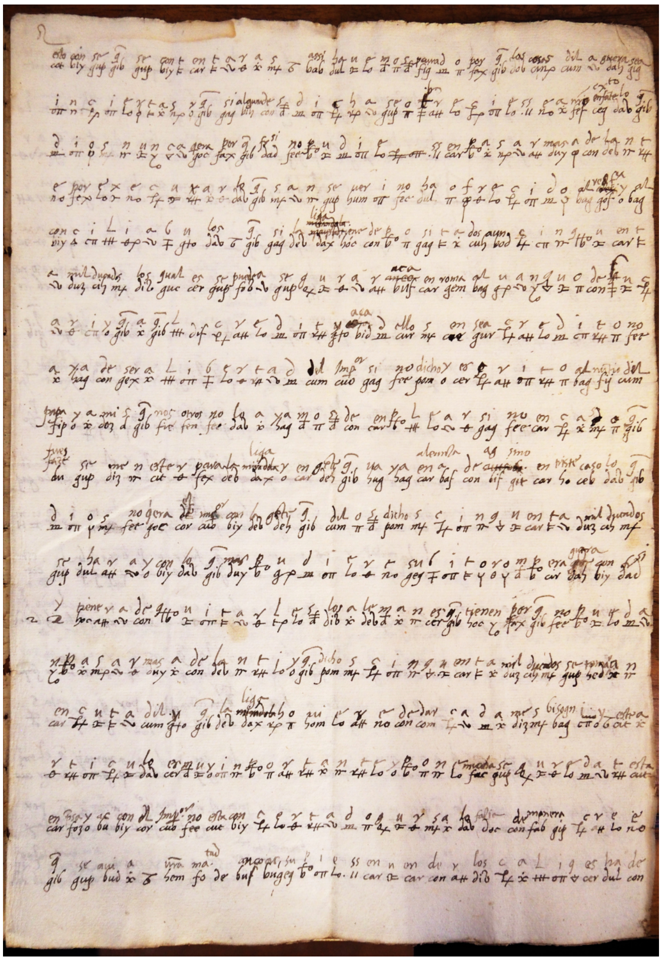
In ogni scriptura fatta in idioma che ut plurimum usamo li scriptori de la Cancelleria de Italia numero le vocal per si, et le consonante tutte separate, el numero de tute le vocal io sempre supera de tutte le consonante de picola proportion. Tal volta trovemo in la lingua maxime fiorentina tosca sono pari. Ne le vocal piu frequente si trova .e. la qual intervien de molte, intervenium de poco supera le altre per qualitate subiecte materie. Qualche volta trovemo .a. supera .e. et in idioma maxime fiorentino el piu de le volte .a. si trova piu numerosa, et et .i. in questo idioma supera intervenendo zoe raramente .e. et .a. la prima adunque sera .e. la seconda .a. la terza .i. la quarta .o. licet non poche volte .o. supera .i. et .u. vien superato ut plurimum da .n. .r. .s. et .t. et pero non si po ponere per quinta. Questo è uno modo de cognoscere le vocal da le consonante. E' uno altro modo el quale fa cognoscere le vocal ut supra, ac et l'una vocal da l'altra. Dummodo che la ziphra sia simplice senza superflue, et disiuncta. Questo è mirar le desinentie de le diction. le qual sono .x. vz le cinq vocal, et cinq consonante che son .d. ut ad .n. ut in. l. ut quel. el. r. ut per. t. ut et. De le qual charatheri trovati in fine de diction i quatro piu frequenti sono .a. e. i. o. la quinta che è .u. spesso è superata da alcune de le predicte consonante. la prima .i. la piu frequente sera .A. licet che qualche volta .e. supi dicto .A. et intervenir .i. et .o. superano .e. et .a. quis rarissime o etiam intervenium e per adeta A. sono spesso .o. e piu cha A. Sichè essendo la prima .A. la secunda sera .e. over .o. Se la prima sara .e. la sesta sara vel .a. vel .o. la quarta sera .i. De .u. et de le consonante dicto se dira altrove. Dicto del numero de le vocal resta dir de l'ordine che tra queste si trova. A. avanti a in predicto mai si trova. ante .u. acco et forsi non piu. ante .i. essendo in lengua veneta .u. aiere. ~~ante~~ aiuto la qual parola da molti che non observano orthographia e scripta senza .d. Ante .o. mai. Ante .u. frequente E ante de .e. i. et .o. mai Ante .u. qualche volta. I ante .a. et .e. raramente ante .i. ante .o. rare ante .u. raro, .i. .O avanti niuna vocal salvo che .u. et raramente. .U. ante .a. et .o. frequente, ante .u. raro ante .e. et .i. frequentemente. Nel fine de le diction .A. non segue .a. ne .o. excepto che in parlar vero nel qual in loco de tua et sua diremo toa et soa. Da poi .e. assai frequente .u. dicea fiera ed. Da poi .i. frequentissime et mia ed. Da poi .u. spesse volte. E. dapoi .a. et .e. mai. Dapo .i. spesse volte. Dapo .o. raro. Dapo .u. ~~molte~~ qualche volte. I. da poi .a. e. et .i. frequente, dapo .o. et .u. raro. O. dapoi .a. et .o. mai. Da poi .e. raro. dapo .i. frequentemente. dopo .u. intervien. U. Da poi .i. qualche volta, da po le altre mai.

nel mezo de le diction u ante u et [illegible]

Dicto del numero et ordine de le vocal hora diremo del numero de le consonante. De le quali le piu frequente serano .r. n. t. vz la piu frequente che .n. et .r. piu che .t. et questo basti haver dicto una volta che qui le tal sono piu frequente de le altre intendar intendere dei per l'ordine che io le scrivo. Da poi le sopradicte sono l. s. c. Dapo le qual son mio frequente .d. p. m. Dapo queste .g. h. f. q. sono piu rare, .b. z. et .x. sono rarissime. .u. de la qual è dicto de sopra che possa piu rara che alcune consonante non si potria tra le vocal cognoscere, potrai cognoscere tra le consonante, perche absque dubio tra le 5a 6a over 7a consonante la trovarai licet che qualche volta sia tra le 2a et 3a ma questo raramente. Non havendo de sopra dicto de le consonante che si trovano in fine de le diction in una ziphra simplice hora de quello dico et meto de .u. Tratte adunque le quatro piu

This anonymous booklet has a title "De Zifris" borrowed by Alberti, but no name of the author. Could it be Soro's De Zifris? It looks very unlikely. *ASVe, CX: cifre, chiavi e scontri di cifra ... b.7.1 f.1*

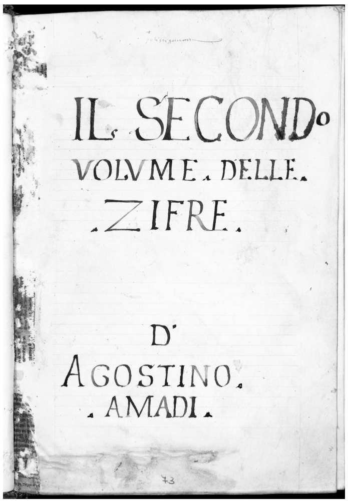
Lot of Spanish ciphers decrypted



Among the archive papers Spanish decrypted messages outnumber a few French ones and the fewer German ones. Was Spanish cryptography weak? Maybe, but one must remember that since 1535, the duchy of Milan was under Spanish rule, and Spain plotted to size Venice too, so Spain was the nearest menace for Venice. *ASVe, CX: cifre, chiavi e scontri di cifra ... b.6.misc.*

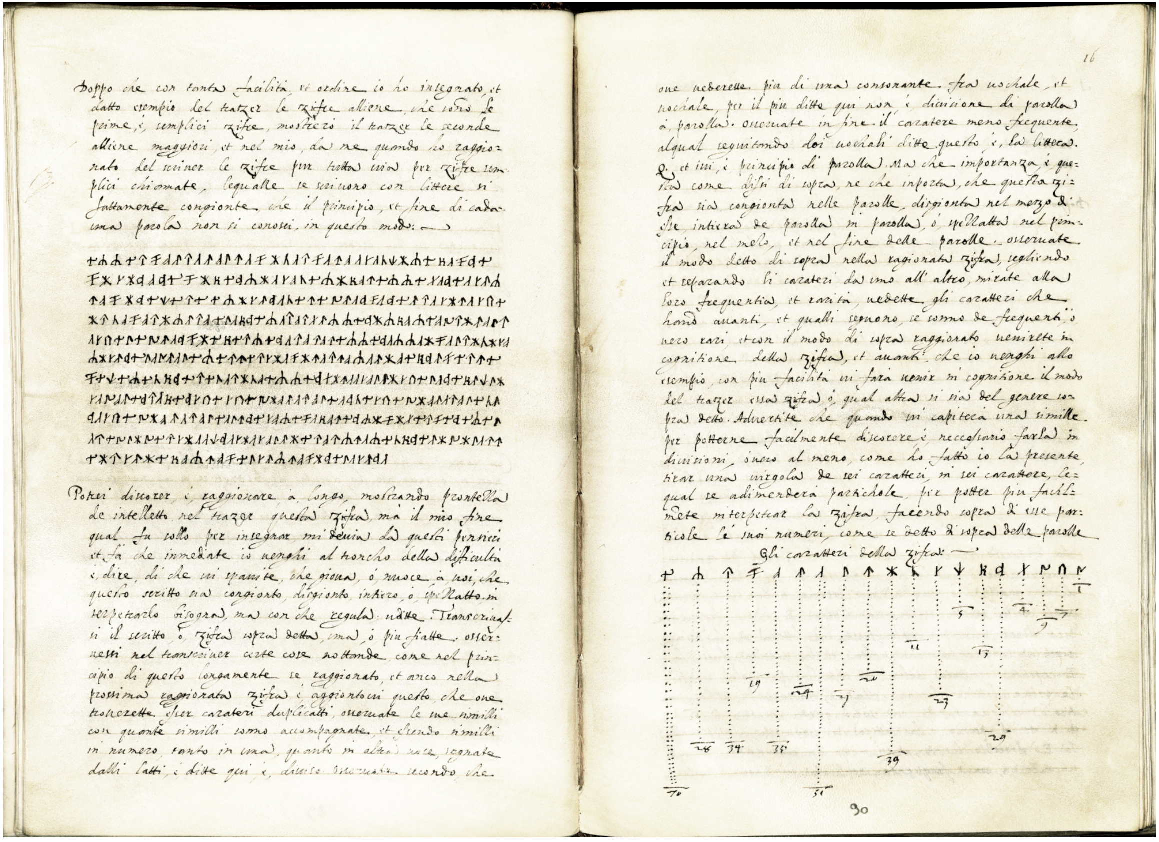
Agostino Amadi

Il Secondo Volume de le zifre



IL SECONDo
VOLVME. DELLE.
.ZIFRE.

D'
AGOSTINO.
. AMADI.



Doppo che con tanta facilità, et ordine io ho integrato, et datto esempio del trazer le zifre alliene, che sono le prime, et semplici zifre, mostrerò il trazer le seconde alliene maggiori, et nel mio, da ne quando ho raggionato del scriver le zifre per tutta via per zifre semplici chiamate, lequalle se scriveno con littere si fattamente congionte, che il principio, et fine di cadauna parola non si conosce, in questo modo: —

Poteri discorer, et raggionare a longo, mostrando prontezza de intelletto nel trazer questa zifra, ma il mio fine qual fu sollo per integrar mi devia da questi pensieri et fa che immediate io venghi al tocho della difficultà et dire, di che vi spaurite, che giova, o nuoce a voi, che questo scritto sia congionto, disgionto, intiero, o spezzatto in interpretarlo bisogna, ma con che regula: udite. Transcrivasi il scritto o zifra sopra detta, una, o più fiatte. osservesti nel transcriver certe cose notande come nel principio di questo longamente se raggionato, et anco nella prossima raggionata zifra et aggiontovi questo, che ove trovarete esser carateri duplicatti, osservate le sue simili con quante simili sono accompagnate, et essendo simili in numero, tanto in una, quanto in altra vece, segnate dalli latti et ditte qui è divisio. osservate secondo che

16

ove vederette più di una consonante fra vochale, et vochale, per il più ditte qui non è divisione di parolla a parolla. osservate in fine il caratere meno frequente, alqual seguitando doi vochali ditte questo è, la littera. Q. et ivi è principio di parolla. Ma che importanza è questa come dissi di sopra, ne che importa, che questa zifra sia congionta nelle parolle, disgionta nel mezzo di esse, intiera de parolla in parolla, o spezzatta nel principio, nel mezo, et nel fine delle parolle. osservate il modo detto di sopra nella ragionata zifra, segliendo et separando li carateri da uno all'altro, mirate alla loro frequentia, et rarità, vedette gli caratteri che hanno avanti, et qualli seguono, se sonno de frequenti, o vero rari, et con il modo di sopra raggionato venirete in cognitione della zifra, et avanti che io venghi allo esempio, con più facilità vi farà venir in cognitione il modo del trazer essa zifra o qual altra si sia del genere sopra detto. Advertite che quando vi capiterà una simille per potterne facilmente discorere è neccessario farla in divisioni, over al meno, come ho fatto io la presente, tirar una virgola de sei caratteri, in sei carattere, le qual se adimenderà partichole, per potter più facilmente interpretar la zifra, facendo sopra di esse particole li suoi numeri, come se detto di sopra delle parolle

Gli carateri della zifra: —

The last and best known Venetian book about cryptography is the one of Agostin Amadi, handled to the CX in 1588, after his death, and ten years after the death of Marin. Sort of a swan song of the Venetian cryptanalysis. It has ten parts (called volumes), here the interesting one is the second about the art of *leuar le ziffre senza scontro* that is cryptanalysis. Here two pages about decrypting a cipher with fancy signs homophones... The book is more conversational and less technical than those of Marin and Ludovici. The role of Amadi inside the Ducal Palace and the Council of Ten is not clear, maybe an external councilor like later Partenio. The educational style of the book, may suggest he acted as a teacher for aspiring deputies of ciphers, but no evidence was found about this conjecture. The treatise has been digitized and can be read on the workstations in the Venice Archive scholar room. file `Inquisitori-Stato-Codice-Amadi-reg-1269_0147_073-r.jpg`