Hieronimo di Franceschi and Pietro Partenio: Two Unknown Venetian Cryptologists

Paolo Bonavoglia
Former teacher of Mathematics and Computer Science
Mathesis Venezia c/o Convitto "Marco Foscarini" Venezia
paolo.bonavoglia@liceofoscarini.it

Abstract

In 1596 the powerful Council of Ten, the secret service of the Republic of Venice, sent a message to the new Baylo in Constantinople, warning him to use, for ordinary messages which needed to be encrypted, Pietro Partenio's cipher, but for questions of extraordinary importance to use the *Zifra delle caselle*[1] cipher invented by Hieronimo di Franceschi. But who were Partenio and Franceschi?
This paper is the report of the first results of a research in the State Archive of Venice about these two unknown cryptologists, still in progress.

1 Two unknown cryptologists

Hieronimo[2] di Franceschi, Pietro Partenio, who were they?

If one searches the web with Google[3] for these names the result is a long list of results having nothing to do with cryptology.

And still the State Archive of Venice has plenty of documents about them, dispersed in several funds and envelopes. And there is plenty of documents having to do with Franceschi and Partenio.

Let us start with a 1596 letter.

[1]The word *zifra* or *ziffra* is used in the XVI century for cipher; beginning at the end of that century, *cifra* replaces more and more *zifra*

[2]*Hieronimo* is a very common name in the XVI century; towards the end of the century the Italian form *Gerolamo* or *Girolamo* takes over.

[3]Google is today the most powerful tool for fast searches, very useful also for serious researches, most notably Google Books gives access to a huge library of old books otherwise hard to find; so a Google negative result is meaningful. Of course I had searched also the indexes of the most authoritative cryptology books like (Kahn, 1967), (Bauer, 1997), and the archives of Cryptologia, with the same negative result. As far as I know Franceschi's and Partenio's names are mentioned in passing and without details only in (Pasini, 1872), and (Preto, 1994). So the use of the adjective *unknown* seems appropriate.

2 Two statements of the Council of Ten

Inside the archive there is an interesting letter. dated 30 August 1596, written by the Chiefs of the Council of Ten, [4] to the new baylo of Constantinople.

The text translated into English is:

> We recommend with the Chiefs of the Council of X, that when it is necessary to write in cipher you continue using the ordinary cipher, but, when treating affairs of extraordinary importance, you will use the [*Ziffra delle caselle*] of the cautious and most loyal secretary of the Senate Hieronimo di Franceschi, abstaining from using those of the most loyal Pietro Partenio, up to our new order.

The message is signed by Piero Lando, and two of the chiefs of CCX. Here Franceschi's cipher is seen ad better than Partenio's.

But, as we will see in the following, in 1593 another document of CCX had stated just the contrary.

Now we will examine some of these ciphers of Franceschi and Partenio. The most surprising aspect is that both of them used super-encryption as a method to enforce security. But first I will give a short description of a typical Venetian code.

3 A XVI century Venetian nomenclator

So to begin let us see a typical Venetian nomenclator[5] used in the second half of the XVI cen-

[4]The Council of Ten was the secret service of the Republic of Venice, and was in charge for ciphers; in the following I will use the two short forms used in the archive: CX for Council of Ten; CCX for Chiefs of the Council of Ten; and ASVE is the common acronym for *Archivio di Stato di Venezia*.

[5]The words "nomenclator" and "code" are in some way synonyms in the cryptographic lexicon; usually a nomencla-

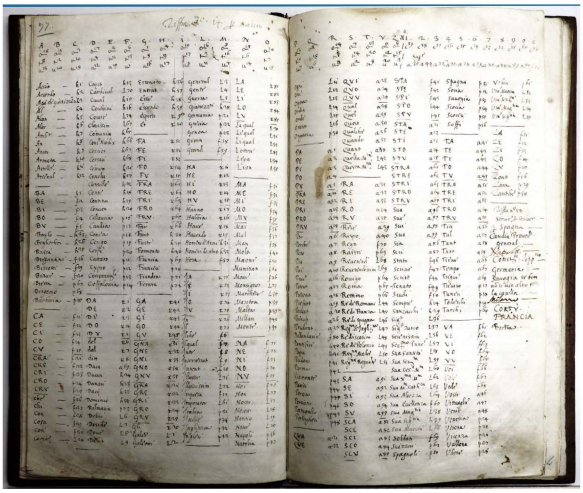


Figure 1: The *zifra granda* in the book of ciphers 1578-1587. *ASVE Cifre, chiavi e scontri di cifra ... b.4, r.16. For no profit use only*

tury. Hundreds of diplomatic messages encoded this way are stored in the Venetian archives.

A good source is a book of ciphers[6] having at the first page a decree of the CX dated August 18, 1578 and at the last page another CX decree dated August 26, 1587.

Both decree mention Hieronimo de Franceschi as the reference person of the CX for ciphers. The last page mentions a *falso scontro* (fake key) cipher proposed by Franceschi, to be given to the baylo of Constantinople for saving the keys even in the case the Turks should seize the baylo and his secretary and force them to handle the key. No technical details are given about this cipher.

At the date of this paper, I couldn't find any other trace of this cipher; as we will see below, ciphers of the like were designed by Pietro Partenio in the following years.

The book has many nomenclators approved by the CX, among them is the *Ziffra n. 14*[7] found at *carta* 77 of In the following figure we see the *lista per scriuer* i.e. the encrypting list: As we see the nomenclator has different parts:

- An alphabet, here with three homophones for each letter.

tor is small, typically one or two sheets, while a code is larger, a booklet at least; for obvious reasons in this paper I will use the word nomenclator.

[6]ASVE, CX Cifra, chiavi e scontri di cifra con studi successivi, busta 4, reg. 16. Calligraphy is very similar to that of Franceschi, so it is very likely that the book was written by his own hand .

[7]Copies of this cipher known also as *Ziffra Granda*, the big cipher, are found on loose sheets in the Venetian archive

SYLLABARY [27 syllables]

ba	be	bi	bo	bu	gra	gre	gri	gro	gru	qua	que	qui	quo	quu	tra	tre	tri	tro	tru					
f_1	f_2	f_3	f_4	f_5	r21	r22	r23	r24	r25	a21	a22	a23	a24	a25	a51	a52	a53	a54	a55					
ca	ce	ci	co	cu	ha	he	hi	ho	hu	ra	re	ri	ro	ru	ua	ue	ui	uo	uu					
f11	f12	f13	f14	f15	r11	r12	r13	r14	r15	a31	a32	a33	a34	a35	f61	f62	f63	f64	f65					
cra	cre	cri	cro	cru	ia	ie	ii	io	iu	sa	se	si	so	su	za	ze	zi	zo	zu					
f21	f22	f23	f24	f25	r71	r72	r73	r74	r75	a91	a92	a93	a94	a95	f51	f52	f53	f54	f55					
da	de	di	do	du	la	le	li	lo	lu	sca	sce	sci	sco	scu										
r_1	r_2	r_3	r_4	r_5	r81	r82	r83	r84	r85	a81	a82	a83	a84	a85										
fa	fe	fi	fo	fu	ma	me	mi	mo	mu	spa	spe	spi	spo	spu										
r51	r52	r53	r54	r55	f31	f32	f33	f34	f35	f41	f42	f43	f44	f45										
fra	fre	fri	fro	fru	na	ne	ni	no	nu	sta	ste	sti	sto	stu										
r61	r62	r63	r64	r65	f71	f72	f73	f74	f75	a71	a72	a73	a74	a75										
ga	ge	gi	go	gu	pa	pe	pi	po	pu	stra	stre	stri	stro	stru										
r41	r42	r43	r44	r45	a_1	a_2	a_3	a_4	a_5	a61	a62	a63	a64	a65										
gna	gne	gni	gno	gnu	pra	pre	pri	pro	pru	ta	te	ti	to	tu										
r31	r32	r33	r34	r35	a11	a12	a13	a14	a15	a41	a42	a43	a44	a45										

Figure 2: The syllabary of the *ziffra granda* the ordered lists are clearly visible.

- An abacus, the ten digits encrypted with one or more groups.
- A syllabary in group of 5, each with a different vowel at the end, for instance **ba, be, bi, bo, bu**.
- A dictionary with common words.

Every letter or group is encrypted with a cipher made of one letter followed by a number of one or two digits, often written like exponents, for instance letter **A** is encrypted with three ciphers (homophones): $o^{18}t^{8}u^{15}$ the syllable **FA** is encrypted with r^{51}, the word *Guerra* is encrypted with L^{54} and so on, for about five hundred ciphers. The heart of this cipher is the syllabary, these signs are the most used. Here is a more readable table; it appears a strong regularity, syllable ending with **A** always end with **1**, syllable in B always end with 2 and so on. This is an obvious weakness, the enemy will get great help in rebuilding the syllabary. This cipher was also known as *ziffra granda* and it was widely used by ambassadors in European capitals. For not so important matters a smaller cipher was used a *ziffra piccola* (small cipher). An example in the same book is in figure 2.

This cipher has an alphabet with two homophones for each letter, with the exception of **H** who has only a cipher the number 20; the **A** has two homophones 16 and 36, **B** has 13 and 33, **C** has 1 and 21, strangely all homophones have a difference of 20. There is also a small dictionary of 60 words, all with two digits ciphers, from 40 to 99, for instance **con** encrypted with 50, **Re di Spagna** with 73 and so on.

According to Pasini classification[8] this cipher is

[8]Luigi Pasini, see also footnote 1, was the last archivist to reorder the papers having to do with cryptography, and classified ciphers using the cipher for the first letter: A

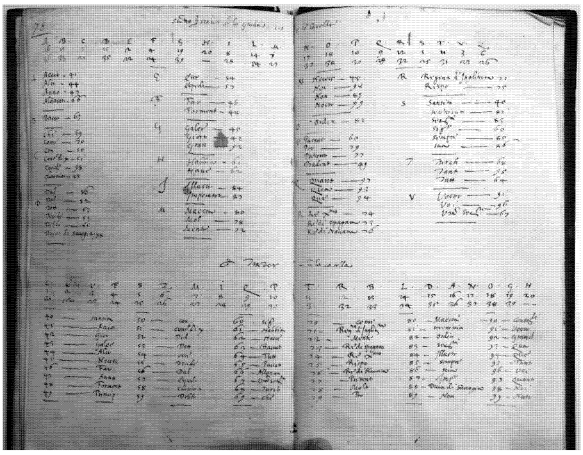


Figure 3: The *cifra piccola* used as the base cipher by the *cifra delle caselle*. *ASVE CX Cifre, chiavi e scontri di cifra ... b.4, r.16. For no profit use only*

named **A 16-36**. Many copies of this cipher are found inside the folders where Pasini collected the ciphers and key sheets.

But the real importance of this small cipher, will be seen in the next paragraph; a hint can be read in the headline of the page. *Sono per scriuer su la grada cioè le caselle* = They are for writing on the grid, that is the boxes.

4 Hieronimo di Franceschi

Very little is known about this cryptologist; his name is frequently mentioned in the CX papers, in 1578 he is mentioned in a CX book of ciphers[9] as a notary at the Doge's chancellery; in 1587 he is mentioned as a secretary of the Venetian Senate. His name appears in many deeds of the notary Pietro Partenio between 1577 and 1596, acting as an attorney for other people, or as a landlord renting flats. He was the reference person of the CX for cryptography in those years, known above all for his *cifra delle caselle*.
In the first page of the book there are these Franceschi's rules for *scriuer ben la zifra* (to write well the cipher):

1. Use signs that mean words or syllables as much as possible.

2. Having to use simple letters, the signs meaning these letters must be changed, and especially the vowels.

3. When using the superfluous (nulls) put these nulls in the middle between words, between consonants, and the vowels, and especially behind the Q, behind the S, the T, L, P and so on

5 The cifra delle caselle

Now let's talk about this *cifra delle caselle* one of the most interesting ciphers found in the State Archives of Venice. A cipher which was used in the real world for many years.[10]

First of all let us see a real message from the archives, encrypted with the *caselle*.[11]

It is well visible the ordered and regular way the two digits numbers were written down. This immediately recalls the grids contained in one of the book of ciphers found in the CCX envelope, were four different grids are present.

Three grids have 24 columns, while the fourth, the one for France, for some reason, is thinner having only 21 columns.

But what is important is the perfect correspondence between a grid and an encrypted text.

Above each window in the grid there are three numbers in the range 0..19. What's the purpose of these numbers? The answer is in the *ziffra piccola* seen in the previous chapter, which used numbers in the range 1..20 as ciphers. The reason for those strange homophones differing by 20 is now clear; it is just an *escamotage* to realize a modulo 20 arithmetic.[12]

The plaintext was first encrypted with this small nomenclator, then the resulting encrypted text was written inside the dedicated grids, and the grid number were subtracted to the single ciphers giving the final cryptogram to be transmitted.

The reverse process of deciphering was just the opposite, one had to add numbers of the cryptogram to those of the grid to recover the nomenclator ciphers.

This method of encrypting twice is best known, as **superencryption**, a method which came in

[9] See footnote 6, page 2.

[10] As previously stated, this cipher is mentioned in (Preto, 1994); Preto says only that Franceschi was known as the inventor of this cipher, in fact he is just reporting news found in the deeds of the CX and CCX archives.

[11] The complete method was recovered by the author in December 2018 and a detailed report about the matter will be published on Cryptologia; *The "Cifra delle Caselle", a XVI century superencrypted cipher* (ID: 1609132 DOI:10.1080/01611194.2019.1609132). An updated report is on the web, starting from page: http://www.crittologia.eu/storia/cifraCaselle.html [in Italian]

[12] Modular arithmetic was formalized by Gauss in the XIX century, so both Franceschi and Partenio had to invent complicate procedures for this purpose,

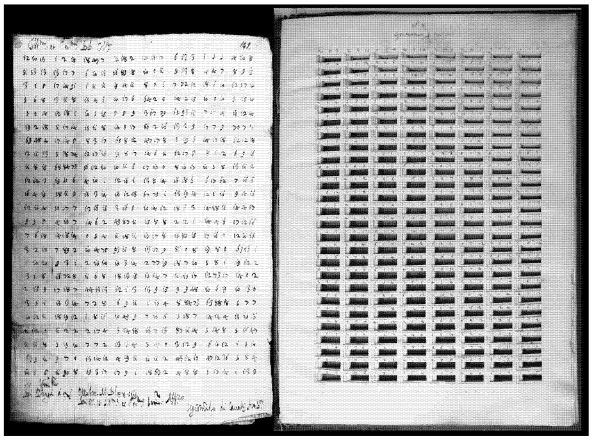


Figure 4: On the left a diplomatic message from the Venetian ambassador in Prague dated 1578-10-11, encrypted with the *cifra delle caselle*. On the right one of the grids used for super-encrypting a message; this is the one used by the ambassador in Germany (Holy Roman Empire). *ASVE Senato, dispacci ambasciatori in Germania, f13, c142 and ASVE CX Cifre, chiavi e scontri di cifra ... b.4. For no profit use only*

common use in the XIX century or immediately before. So a superencryprion cipher is something in advance of two centuries! As far as I know is the oldest of this kind[13] .

6 Pietro Partenio

Pietro Partenio was a notary active from 1563 to 1618 according to the register of notary deeds stored in the Venetian archive.

As stated above there are several Partenio's deeds since the 1570s where Hieronimo de Franceschi is named, a proof that Partenio and Franceschi knew each other and had professional links. Partenio is never mentioned in the book of ciphers 1578-1587, so we can guess he became interested in ciphers in the following years and designed several interesting ones.

We find detailed descriptions of six ciphers in a fine CCX parchment book (1592-93)[14], other ciphers on loose sheets and finally a book of ciphers

[13] Update: the idea of combining two ciphers is rather simple and goes back to the beginnings of cryptography, if it is true that the well known Arab cryptologist Al-Kindi in his IX century book wrote about something like super-encryption, but gave no details or examples. As far as I know, Franceschi's cipher is the first super-encrypted cipher well documented and used in the diplomatic messages of the real world.

[14] ASVE CCX Raccordi 1 1593

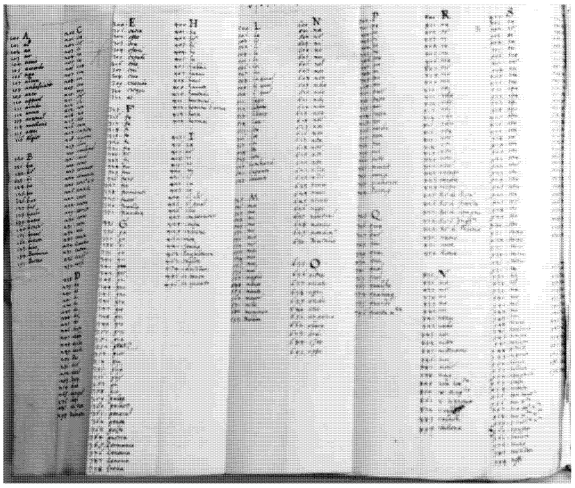


Figure 5: The nomenclator of the second cipher. *ASVE CX Cifre, chiavi e scontri di cifra ... b.2, f.23. For no profit use only*

dated 1606 with six ciphers, some of them already described in the CCX book.

Partenio divides his ciphers into two categories: 1) *cifre sospette* (suspicious ciphers): the suspicious enemy easily recognizes them as encrypted messages; 2) *cifre di senso corrente* (ciphers of current sense) that is ciphers that produce messages of common language, a sort of steganography. This paper is about the first kind, the second deserves further research.

7 Partenio's ciphers

Now we will describe and examine some of these ciphers, from the 1592/93 CCX book and from the 1606 booklet. Let's begin with a cipher of the latter, because it is the most similar to Franceschi's *caselle*.

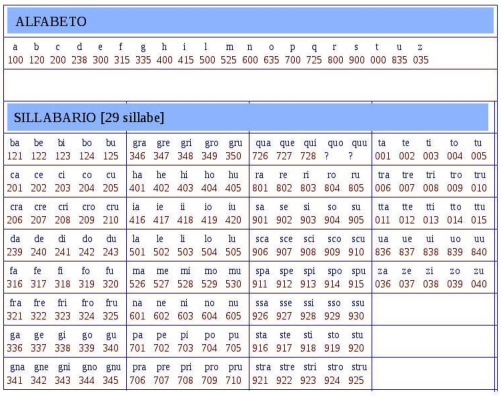
7.1 Second cipher (1606)

This second cipher of the 1606 booklet is interesting because Partenio explicitly mentions the Franceschi's *cifra delle caselle* boasting the superiority of his own.

The base cipher is a 3-digit nomenclator shown in the following figure.

The nomenclator is almost totally ordered; there are exception, the syllables are ordered separately, as seen in the alphabet and syllabary shown here.

But, of course, the most interesting part is super-encryption: indeed the method is similar to Franceschi's cipher; one had to do a subtraction to encrypt and an addition to decipher, here using a



ALFABETO

a	b	c	d	e	f	g	h	i	l	m	n	o	p	q	r	s	t	u	z
100	120	200	238	300	315	335	400	415	500	525	600	635	700	725	800	900	000	835	035

SILLABARIO [29 sillabe]

ba	be	bi	bo	bu	gra	gre	gri	gro	gru	qua	que	qui	quo	quu	ta	te	ti	to	tu
121	122	123	124	125	346	347	348	349	350	726	727	728	?	?	001	002	003	004	005
ca	ce	ci	co	cu	ha	he	hi	ho	hu	ra	re	ri	ro	ru	tra	tre	tri	tro	tru
201	202	203	204	205	401	402	403	404	405	801	802	803	804	805	006	007	008	009	010
cra	cre	cri	cro	cru	ia	ie	ii	io	iu	sa	se	si	so	su	tta	tte	tti	tto	ttu
206	207	208	209	210	416	417	418	419	420	901	902	903	904	905	011	012	013	014	015
da	de	di	do	du	la	le	li	lo	lu	sca	sce	sci	sco	scu	ua	ue	ui	uo	uu
239	240	241	242	243	501	502	503	504	505	906	907	908	909	910	836	837	838	839	840
fa	fe	fi	fo	fu	ma	me	mi	mo	mu	spa	spe	spi	spo	spu	za	ze	zi	zo	zu
316	317	318	319	320	526	527	528	529	530	911	912	913	914	915	036	037	038	039	040
fra	fre	fri	fro	fru	na	ne	ni	no	nu	ssa	sse	ssi	sso	ssu					
321	322	323	324	325	601	602	603	604	605	926	927	928	929	930					
ga	ge	gi	go	gu	pa	pe	pi	po	pu	sta	ste	sti	sto	stu					
336	337	338	339	340	701	702	703	704	705	916	917	918	919	920					
gna	gne	gni	gno	gnu	pra	pre	pri	pro	pru	stra	stre	stri	stro	stru					
341	342	343	344	345	706	707	708	709	710	921	922	923	924	925					

Figure 6: Alphabet and syllabary of the second cipher.

modulo 10 arithmetic, instead of the modulo 20 of Franceschi.

Partenio, seeking as usual a key that could be memorized without writing, uses a different method to generate the obscuring sequence of numbers.

He starts with a verse, from a poetry or other text, and writes it on three rows. Let's use his own example, the verse is:

"*Iam in me sperauit liber abacum protega me um quontam c*," where the final *c* is a null, used to fill the three rows schema. The verse has to be written on three rows, and will be read per columns:

```
iaminmesperauit
liberabacumprot
egameumquontamc
```

Now let us transform these letters in numbers using this table:

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

Now every letter of the verse is converted into the number above, and the numbers are read per columns forming group of three number to match the ciphers of the nomenclator.

In this example the sequence is:

ile	aig	mba	iem	nre	mau	ebm	...
905	197	121	931	265	119	521	...

The super-encrypting procedure is similar to the *caselle*. The numbers of the single digits of the nomenclator's ciphers are subtracted modulo ten by the numbers of the key.

For deciphering just do a sum instead of a subtraction.

Let us see the example of Partenio:

Ha questa Maestà intendimento con alcuni de capitani in Corfù.

The following table shows the procedure; the first row has nomenclator ciphers, the second has:

ha	questa maestà	inte	ndi	mento	con ...	
401	796	430	611	559	213	...
905	197	121	951	265	119	...
506	609	319	760	394	104	...

So the cryptogram to send is:

506609319760394104 ...

To decipher just do an addition modulo 10.

Of course Partenio does not use the "modulo 10" arithmetic, introduced by Gauss in the XIX century, and has to write two pages of instructions explaining how to subtract and sum this way.

7.2 A comparison with the caselle

At the end of the instructions Partenio makes a comparison between his cipher, defined *fortissima* (very strong) and *quella del Franceschi* (the one of Franceschi), remarking his nomenclator may reach 1000 among words, syllables and single letters, while Franceschi's nomenclator had only two digits and only "40 or 50 among syllables and words"[15]

Partenio makes also an important remark: he is afraid that secretaries may use his ciphers in a simplified and easier manner, using only the nomenclator without the super encrypting tools.

This is exactly what did happen; in the XVII century the most used ciphers were similar to Partenio's, 3-digit ciphers, ordered lists but superencryption was forgotten.

7.3 The false sense

Finally Partenio describes a complicate device to give the cryptogram a false meaning to disguise the enemy. For this he uses this Latin square of numbers[16] (On the left the original[17], on the right a more readable view):

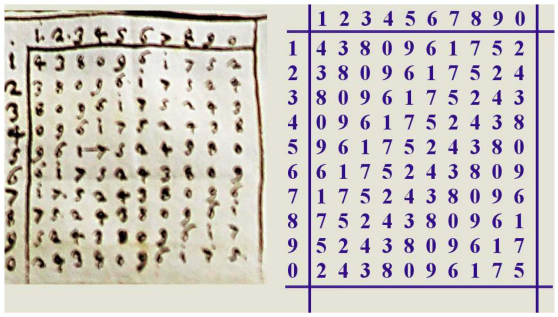
Suppose you want to add this fake message:

Sarà guerra tra questa m.tà et Re di Polonia

[15] Indeed Franceschi's small cipher has 20 letters and 60 words; it does not have syllables.

[16] Latin square is a square of $n \times n$ objects where every object appears once and only once on each row and on each column. Mathematically this the Pythagorean table of a binary operation that is invertible; the associated algebraic structure is called quasi-group. For this reason the Latin squares have been widely used in cryptography beginning with Trithemio, Vigenère and so on. This one is peculiar being disordered.

[17] ASVE Cifre, chiavi, scontri di cifra ... busta 3



	1	2	3	4	5	6	7	8	9	0
1	4	3	8	0	9	6	1	7	5	2
2	3	8	0	9	6	1	7	5	2	4
3	8	0	9	6	1	7	5	2	4	3
4	0	9	6	1	7	5	2	4	3	8
5	9	6	1	7	5	2	4	3	8	0
6	6	1	7	5	2	4	3	8	0	9
7	1	7	5	2	4	3	8	0	9	6
8	7	5	2	4	3	8	0	9	6	1
9	5	2	4	3	8	0	9	6	1	7
0	2	4	3	8	0	9	6	1	7	5

Figure 7: The latin square, original on the left, more readable on the right. *ASVE CX Cifre, chiavi e scontri di cifra ... b.2, libro Partenio. For no profit use only*

The first syllable of the fake message is ***sa***; the nomenclator has 901 as the cipher of it. Now you apply the binary operation defined by the Latin square to the digit of the fake text and the corresponding digit of the cryptogram, as in the following table,

sa	Ra	guerra	tra	questa m.tà	et	...
901	801	364	006	796	311	...
506	609	319	760	394	104	...
856	855	963	699	515	820	...

Finally we intercollegiate the numbers of the true cryptogram with the fake one, so obtaining the following fake cryptogram:

58056668059539169376690935984518044

Now the secretary receiving this cryptogram knows that only the odd placed numbers are good and will easily recover the plaintext.

But, to use Partenio's example, if the Baylo of Constantinople or his secretary are forced by the Turks to deliver ciphers and keys, they will give them the nomenclator and the Latin square and these false instructions: take the numbers in pairs, follow the first number row until you find the second and write the column number, group the numbers obtained by three and use the nomenclator to retrieve the normal text. Due to the property of the Latin square, the Turks will get the false message. Try it and believe it.[18]

7.4 Remarks

This is an amazing cipher, undoubtedly. It has also a pair of weakness: 1) violation of Knockoff's rule; if the enemy discovers the method, the fake effect is lost. 2) the nomenclator is too regular, it is almost a ordered list.

[18] Hint: take the first two numbers 5 and 8, look the 5 row and find 8 under 9, 9 is the first digit; take 0 and 5 and in the 0 row find 5 under 0, the second digit is 0; take 6 and 6, look 6 row and find 6 under 1, the third digit is 1, so the first cipher is 901, from the nomenclator you get "sa". And so on ...

Figure 8: The nomenclator of Partenio's third cipher. *ASVE Cifre, chiavi e scontri di cifra ... b.2, f. Partenio. For no profit use only*

7.5 Third cipher (1592)

The following cipher is the third one of the 1592 CCX register[19], and may be considered another Partenio's reply to Franceschi's *caselle*. Instead of a grid, we have a paperboard slider as a poly alphabetic tool.

The base cipher, a nomenclator has about a thousand signs formed by a letter from a 24 letters alphabet (Italian with K X Y &) followed bay a two digits number in the range 1..24. For instance **a** is encrypted with **A**, **DA** with **E12**, **Il Signor Turco** with **K12**, **Galee** with **I15**.

Let's see the cipher procedure with the example used by Partenio: the message to be encrypted is. "*Il Signor Turco arma galee*"[20] . We find **k12** as the cipher of "**Il Signor Turco**"; now we have to use a paperboard slider (see following figure) made of a fixed part (top and bottom in the figure) and a sliding part (middle in the figure).

We find copies of this strip with instructions in several parts of the Venetian archive. The one shown below is pasted on an instruction sheet found in the Venetian Archives.

here is a more readable presentation:

We start with the slider in the aligned position, as in the following figure:

[19] ASVE CCX Raccordi 1, 1592 p.28

[20] English: The Turkish Master is arming galleys

Figure 9: Partenio's strip pasted on a cipher sheet. *ASVE CX Cifre, chiavi e scontri di cifra ... b.2, f.23. For no profit use only.*

a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	&																
y	i	r	k	z	a	s	b	t	g	q	f	x	u	n	m	d	h	c	k	e	p	o	l	y	i	r	k	z	a	s	b	t	g	q	f	x	u	n	m
18	2	19	7	16	6	21	20	13	12	4	8	3	11	5	15	14	11	22	9	17	24	23	1	18	2	19	7	16	6	21	20	13	12	4	8	3	11	5	15
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24																

Now under **k** in the top row we find **g**, while above **12** there is **8**, so **k12** becomes **g8**.

We find **Arma** has cipher **b4**; under the letter **b** we find **i**, while above **4** there is **7**. So, **b4** is with **i7**. In a similar way the cipher of Galee, i15 becomes t5. So the cryptogram for "*Il Signor Turco arma galee*" is:

g8 i7 t5

Partenio does not give detailed rules to when and how to move the slider, changing the alphabet. He writes this is something to be agreed between the two parts. As an example he proposes to move the slider one step to the left, every one or two lines.

The deciphering procedure is just the inverse of the previous. In the above example to decrypt **g8 i7 t5** we just look for g and 8 using the slider from bottom to top, and finding **k12**. And so on with the rest.

7.6 Remarks

Again, the weakness of this cipher is the base cipher, too regular. A super-encryption with a mono-alphabetic substitution could be enough to overcome this weakness; the poly-alphabetic substitution is a plus giving a good level of safety for the XVI century.

7.7 Sixth cipher

The sixth cipher of the book is basically a transposition cipher based on a long key. Partenio uses this example: as a key-phrase take the Latin "*En lex tua meditatio mea in corde meo*"phrase as a message to send: *Vi sono in Brescia capi ribelli.*

One writes down the key-phrase on a row, finds the first letter, in the alphabetic order, here as in most cases **a**, and writes **1** exactly under this **a**; then find the second letter, another **a** and under it writes **2** and so on until the end of the message.

	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
X	12	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11
Z	13	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12
A	14	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13
B	15	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14
C	16	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
D	17	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
E	18	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
F	19	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
G	20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
H	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Figure 10: The square of the sixth cipher.

Next, the plain text is written on a third row following the numbers order; when the text is over, the remaining places are filled with random letters.

Then text resulting on the third row is the cryptogram to dispatch. Here is the example, step by step:

E	n	l	e	x	t	u	a	m	e	d	i	t	a	t	i	o	m	e	a	i	n	c	o	r	d	e	m	e	o
7	20	16	8	30	26	29	1	17	9	5	13	27	2	28	14	22	18	10	3	15	21	4	23	25	6	11	19	12	24
i	r	c	n	o	i	d	u	a	b	n	c	l	i	b	i	b	p	r	s	a	i	o	e	l	o	e	i	s	l

So we have a cipher that does not require a written sheet, may be taken by heart, that's the main goal of Partenio's ciphers[21].

7.8 The fake key

This is a device similar to the one seen in cipher 2, for the same purpose; it is somehow easier to use.

Partenio's idea is to add a fake cipher key (in Italian a *falso scontro*) that the ambassador could give to the enemy.

In the previous example, we could add this fake message: *Dalle sue parole io spero buona pace* of the same length, in a way the enemy, using the fake key would get this fake meaning.

u	i	s	o	n	o	i	n	b	r	e	s	c	i	a	c	a	p	i	r	i	b	e	l	l	i				
e	n	l	e	x	t	u	a	m	e	d	i	t	a	t	i	o	m	e	a	i	n	c	o	r	d	e	m	e	o
6	19	15	7	29	25	28	0	16	8	4	12	26	1	27	13	21	17	9	2	14	20	3	22	24	5	10	18	11	23
i	r	c	n	g	i	d	u	a	b	n	c	c	i	a	i	b	p	r	s	a	i	o	e	l	o	e	i	s	l

For this purpose Partenio proposes another Latin square table, this time 20×20. The square is regular but row labels are shifted and the column labels scrambled according to a keyword.

The first letter of the encrypted message is **i**, the first of the fake message is **d**, so we look on the first column of the square for the **i** and look on this

[21]Three centuries after Auguste Kerckhoffs included a similar principle as his rule number 3, see (Kerckhoffs, 1883).

row until below the letter **d**. The number found is 10, and we write i^{10}. The following letter of the encrypted text is **r**, to get the second letter of the fake message **a** we need to reach number **15**, so we write r^{15}, and so on; finally the encrypted text looks so:

$i^{10}r^{15}c^{8}n^{17}b^{17}i^{1}z^{13}u^{28}a^{14}b^{1}n^{7}c^{6}s^{22}...$

a cryptogram who has the typical look of a Venetian nomenclator encrypted message, a perfect fake.

So, in case of capture, the ambassador should give up to the enemy the table square, with instructions leading to recover the fake messages instead of the true ones.

7.9 Is this fake perfect?

Indeed the true cryptogram here is the sequence of the letters, the numbers being only a fake leading to the fake meaning. Only half of the cryptogram is good, like in cipher 2. Indeed, the cipher is just a transposition disguised as a nomenclator.

An enemy examining such a cryptogram could at glance observe that the statistical distribution of the letters resembles a plausible language distribution: many vowels, e, i, a the most frequent, and could guess a transposition is the real cipher.

So far, the fake looks weaker than the one seen in the second cipher.

And like cipher 2, this cipher does not satisfy Kerckoffs principle; if the enemy discovers the method, the whole contraption is unmasked.

On the other hand, a transposition for 30-40 letters message is not so easy to break.

8 Were Partenio's ciphers used in the real world?

A difficult question; the 1596 CCX letter shown at the beginning of this paper, explicitly refers to Partenio's ciphers as used before 1596 by the Baylo; and still at the current date not a single such message was found in the archives, of the Baylo or other ambassador, to the Doge or to the Council of Ten.[22]

[22]Last update: two paragraphs encrypted with a cipher similar to Partenio's n.2 were found at the beginning of two messages of Piero Duodo, Venetian ambassador in France, dated August 1595; in June 1595 the CX had recommended the use of Partenio's cipher, after learning from Giovanni Mocenigo, the previous ambassador in France, that Francois Viète, the well known French mathematician, boasted to be able to decrypt Venetian ciphers. The cipher seems to have been used for a very short period of time

9 Conclusion

From the above examples Franceschi and Partenio have in common the use of super-encryption, but have different priorities: Franceschi cares more about safety, while Partenio, as already stated, cares more about ease of use, and keys easy to memorize.

Ease of use is important: a procedure too complicated may induce bad behaviors of the cipher operators; a classical example is a monoalphabetic cipher with homophones; the operator should change homophone very often, as recommended by Franceschi's rules, but this is annoying and demanding, so an operator may memorize only one cipher for letter going back to a simple monoalphabetic cipher; a secret letter by the CCX to the governor of Candia, has reprimands about bad ciphering habits, and at the end tells: "to use only one alphabet would be like not writing in cipher at all."[23]. The reprimand had little effect and reducing an homophonic cipher to a trivial monoalphabetic remained a common practice.

On the other hand safety is important too: an easy to use cipher may be also an easy to decrypt one. A typical example: the use of an ordered list in a nomenclator, a step in the direction of ease, one just needs a single list, but also a big help for the enemy, an ordered list nomenclator is much easier to break than a disordered one. And yet in the XVII century Venetian cryptography used more and more ordered lists instead of the disordered of the XV and XVI century.

Franceschi used a small but disordered list with super-encryption; Partenio used ordered lists also with super-encryption.

The followers used similar ordered lists but without the burden of superencryption! Precisely the fear expressed by Partenio in his postscript to the second cipher. The golden age of Venetian cryptography had come to an end.

10 Acknowledgments

I wish to thank Elio Canestrelli, former professor of mathematics at the Ca 'Foscari University of Venice, for providing me with the starting point and information about the encrypted dispatches of Alberto Badoer. Special thanks also to the archivists Giovanni Caniato, Marilena Bonato and many others for the assistance provided at the

[23]CCX Lettere Secrete 10, 25-08-1583

State Archives of Venice.

References

Ibrahim Al-Kadi. 1992. *Origins of Cryptology: the Arab Contributions*. Cryptologia, 16:2, 97-126, Philadelphia, Pa. DOI: 10.1080/0161-119291866801

Friedrich Ludwig Bauer, 1997. *Decrypted Secrets*. Springer, Berlin. ISBN: 3-540-24502-2

Paolo Bonavoglia. 2019. *The Cifra delle Caselle, a superencrypted XVI Century Cipher*. Cryptologia, Philadelphia, Pa. DOI:10.1080/01611194.2019.1609132

David Kahn. 1967. *Codebreakers*. Scribner, New York, NY. ISBN: 978-0-684-83130-5

Auguste Kerckhoffs. 1883. *La cryptographie militaire*. Paris.

Luigi Pasini 1872, 2019. *Delle scritture in cifra usate nella Repubblica di Venezia*. Aracne, Roma ISBN: 978-88-255-1926-6

Luigi Pasini. 1885. *Archivio di Stato di Venezia. Consiglio di Dieci - Cifre, Chiavi e Scontri di cifra, a cura di L. Pasini e G. Giomo*.

Paolo Preto 1994. *I servizi segreti di Venezia*. EST, Milano

Luigi Sacco. 1958, 2012. *Un primato italiano, la crittografia nei secoli XV e XVI*. Ist.Poligrafico dello Stato, Roma, Italy.