Venetian Cryptanalysis Treatises of the Renaissance

Paolo Bonavoglia
Mathesis Venezia c/o Convitto Liceo "Marco Foscarini"
Cannaregio 4941 I 30121 Venezia
paolo.bonavoglia@mathesisvenezia.it

Abstract

Cryptanalysis in Europe was born shortly after cryptography, during the age of the Renaissance; unlike the latter little is known about its early history; we know a few names of codebreakers, people practicing this art or writing about it: Soro, Marin, Argenti, Viète, but little about their methods and their achievements. This research is focused on the content of a few XVI century Venetian treatises on ciphers, particularly the collection of Zuan Francesco Marin.

1 Introduction

Historical cryptography, meaning the art of composing ciphers, is well known and documented, there are many treatises and books about it. Very different is the situation for cryptanalysis[1], meaning the art of decrypting encrypted messages without knowing the key, during the XV-XVIII centuries in Europe[2]: only a few names of codebreakers[3], notably two Venetians Giovanni (Zuan) Soro, Gianfrancesco Marin, and two French François Viète, Rossignol are known.

This is not surprising, cryptanalysis is maybe the only science that should hide rather than boast its successes, for obvious reasons.

To my knowledge the only Renaissance cryptanalist whose methods are known and have been studied, is François Viète the famous mathematician who was an aide to king Henry IV; an in-depth analysis about this is in the 1997 Pesic paper[4]. A few XV-XVI centuries books about deciphering cipher-texts without knowing the key are mentioned in the next section.

This research is a about the methods and treatises of Venetian cryptanalysts, based and centered on the collection of Zuan Francesco Marin, one of the best cryptanalysts of the XVI century.

2 Alberti, Simonetta, Argenti

A short mention has to be made about the older texts about cryptanalysis, to be kept as a different kind from texts proposing new cipher.

The well known and celebrated *De cyfris* by Leon Battista Alberti[5] is famous for the enciphering disk described at the end of the book. At the beginning Alberti gave some generic information about frequencies of the letters and how to use it to decrypt and to take steps to counter cryptanalysis, while writing in cipher; he also writes a few lines about transposition, but he simply concludes that "a shrewd and witty investigator" could solve this also. No examples are given.

Another old text about cryptanalysis is the 1474 "13 Rules for deciphering" of Cicco Simonetta, a diplomat and a politician that was then regent of the Duchy of Milan; the rules apply only to very simple ciphers, with spaces among words left visible, only one sign for each letter (today known as MASC); this is surprising[6] because the diplo-

[1] I will use the modern term of cryptanalysis for the art or science of deciphering encrypted messages without knowing the key, although this word is recent and, of course, does never appear in Renaissance texts, where it is called, in Italian, the art of *leuar le ziffre senza scontro* to raise ciphers without the key-sheet

[2] Outside Europe there was a golden age for cryptography and cryptanalysis in the IX century under the Arab Caliphate in Baghdad: Al-Kindi was a mathematician and a philologist that defined the analysis of frequencies as a codebreaking method. Did the first European cryptanalyst know the work of Al-Kindi? Maybe someone, like Fibonacci for the Arab numbers, discovered it and import it in Europe? As far as I know the question is open. In the Venetian Archives I didn't find any trace of such a possibility.

[3] Again, I will use the modern word codebreaker for a person able to break codes or ciphers, a term made popular by the monumental *Codebreakers* by David Kahn, the reference book about the history of cryptography. (Kahn, 1996)

[4] Cryptologia (Pesic, 1997)

[5] Alberti was a renown architect and theorist of the time, a typical Renaissance man with wide interests.

[6] Maybe not so surprising; it is possible and plausible that

matic ciphers used in Milan by the Sforzas, were much more advanced than that, making Simonetta's rules completely useless. Any way it is a first text of its kind published and quite lucky, being still remembered[7].

Much better, of course, the treatise of Matteo Argenti, secretary of the cipher of the Pope, but with Argenti we are at the end of the XVI century. Before that an advanced school of cryptanalists had developed in Venice.

3 The Founding Father: Zuan delle Ziffre alias Giovanni Soro and his Lost Book

At the beginning of the XVI century a Venetian secretary of the Council of Ten[8], Zuan Soro[9], the first known deputy of ciphers, gained great fame for his ability to decrypt every ciphertext; many princes of Italian states, even the Pope, asked his help to break intercepted messages they couldn't decipher[10]. Most news about his ability come from Marin Sanudo [11] in an anecdotal form [12].

It may sound strange that a valiant codebreaker like Soro allowed boasting of his achievements in such a way. As stated above, codebreakers should carefully hide their successes. But in this early times of this science, when very few people were able to break a cipher with homophones and nulls, it was convenient to boast, offering Soro's services to the princes who lacked secretaries able to break a cipher. And one can presume such services weren't for free.

On July 17, 1511 Zuan Soro wrote a *supplica* (supplication) to the Council of Ten asking for a chancellery in Noale[13] for his brother Andrea. He boasted his successes in decrypting ciphers, and announced he had began to write a book "*sopra el quale siano tute le rason et regule, mediante le qual lui interpreta le ziphre* (a book upon which are all the reasons and rules by which he interpreted the ciphers). He promised to leave the book to **CX** and to let it be seen only by secretaries eligible for such matters.

In 1543 Alvise Borghi, himself a deputy of ciphers, in a supplication to the **CX**, wrote that Soro had given the book to the **CX** and that he, Borghi, had long conversations with old Soro in 1537 and could read the book. Indeed a short receipt signed by Andrea di Franceschi, great chancellor, dated March 29, 1539 is found in the Archives [14] and these are the last news about the book, which is unfortunately lost: stolen? still in the archives?

4 The Follower: Zuan Baptista Lodouici, alias Giambattista Lodovici

Since 1518 Soro had an aid: Zuan Baptista Lodouici (or Zuan Batta; in modern Italian: Giambattista Ludovici); little is known about this secretary, but several papers with his name, are found in Marin's collection, a booklet in Latin, under his name, entitled *Quare*, see 6.3 for details, and an interesting narrow booklet about pattern finding in a sillabary, see 6.2.

5 The Polyglot: Aluise Borgi, alias Alvise Borghi

Aluise Borgi (modern Italian: Alvise Borghi[15]) is one of the best known deputies of ciphers after Soro. He was a polyglot, having served as secretary in a few embassies across Europe and this was an advantage when he got interested in the art of

Simonetta got from his secretaries of the ciphers an old set of rules used decades before, and now released just because they were outdated. Indeed the use of homophones and nulls is documented since the first 1400s, a clear sign that some elementary form of cryptanalysis like this, was already known.

[7] As a man and a politician Simonetta was not so lucky; in 1480 Ludovico il Moro, a Sforza, claimed the Duchy and occupied Milan. Simonetta was put to trial, sentenced to death, and beheaded in the Pavia castle the year after.

[8] The *Consiglio di Dieci*, Council of Ten, often abbreviated to *Consiglio di X* or **CX**, was a powerful tribunal and executive organ of the Republic of Venice, born to handle the security of the state. It was in charge of the ciphers also, naming a few secretaries as deputies of the ciphers, that is to cipher and decipher the messages sent from and to ambassadors, military chiefs and other representatives.

[9] See note above: *Zuan* is the name used in the documents in Italian, while in Latin documents it was *Ioannes*; later it was used the modern Italian Giovanni Soro, but in his life he was always Zuan.

[10] ASVe CX Parti miste reg. 34 c. 107-r, reg. 34 111.

[11] Marin Sanudo a Venetian politician and historian, author of a monumental "Diarij"(Sanudo, 1533) a day by day cronicle of the life in Venice; he was also a member of the **CX**, knew Soro and he wrote that Soro was able to decrypt every encrypted message, without exception.

[12] Here is an example: Sanudo notes in 1528 that the 20 years old Prince of Salerno Ferrante Sanseverino, visiting Venice, sent a servant to him, asking for a meeting with three renowned Venetian people: Pietro Bembo, Sanudo himself, and *Zuan Soro da le zifre*, but Sanudo let him know he had no time for that!

[13] Noale is a small historic village about 24 km NW of Venice.

[14] ASVe CX Cifre, chiavi e scontri di cifra ... busta 5,loose sheet.

[15] The surname was spelled Borgi until around 1550 thereafter it became Borghi; it is likely it was already pronounced like an hard **G** like in *Give* unlike soft **G** like in *John*; the writing rules had changed.

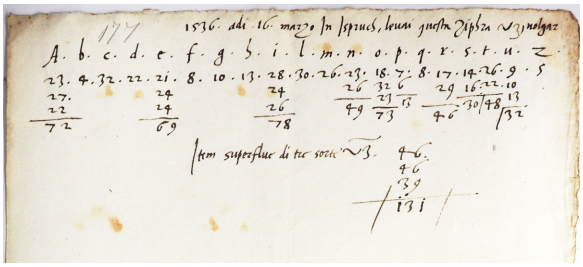

Figure 1: A decrypted cipher, alphabet, homophones, and nulls decrypted by *Alvise Borghi* with a table of frequencies (homophones are summed): the caption translated in English: 1536, the day 16th of March, I decrypted this cipher (23?) vernacular. *ASVe CX Cifre, chiavi e scontri di cifra ... b.3 c.177.*

decrypting ciphers. He boasted to have decrypted ciphers in French and Spanish that Soro was not able to decrypt[16] and that foreign Princes continued to ask for help to Venice to decrypt messages they could not read., The **CX** praised his great ability in this art.

In the inventory of the papers of Z.F. Marin, there are some items attributed to the hand of Borghi, but they are not been identified already,

Vice versa a sheet with a decrypted alphabet with homophones and nulls has been erroneously put among Venetian cipher keys in busta 3. The date, *1536, 16 marzo*, the place, Isbruch (Innsbrück), and the handwriting compared letter by letter to his supplication, indicate it is written by hand of Borghi, who was then secretary of the ambassador to the Emperor.

6 Zuan Francesco Marin and his Papers

The last great Venetian cryptanalyst after Soro, Zuan Francesco Marin[17] secretary since 1532, died in 1578, while he was still teaching the art of decrypting to Federico (or Ferigo) his only surviving son[18] who was designated to take the role of deputy of ciphers after his father.

On May 23, 1578 the Council of Ten (**CX**) met to find a way to continue the instruction of Ferigo and resolved to use the writings and books that Marino had in his office and at home, ordering the immediate requisition of all those papers, to be kept in the secret rooms of the **CX**.

6.1 The Inventory

Luckily an inventory of books and papers found in his office and home is still kept in the State Archive of Venice[19]; it was mentioned briefly by Meister [20] who writes he did not have the time to examine in-depth the content during his short stay in Venice.

It is a very long list of titles and descriptions, many of theses, but not all, are still in the busta 6 of the collection.

First, four printed books are listed: Trithemius's *Polygraphiae* book[21], then Porta's *de furtivis* ..[22], and a book by a G.B. Palatino about writing letters (apparently not about ciphers), and a book about *babuini*[23].

Then a long list of manuscripts and sheets, most of them were labeled with a capital letter, from A to X, or other sign, written on the cover of the first page.

The most interesting are:

[16] This claim is in contrast with Pasini who wrote the contrary in his book, (Pasini, 2019) cutting and pasting different parts of Borghi's supplication to attribute that success to Soro. Pasini was clearly writing a panegyric of Soro and this cut and paste was functional for this purpose. Anyway the matter of Soro's linguistic competences remains dubious.

[17] The name is variously spelled, Marin, Marino, Marini, the updated to modern Italian form should sound: Gianfrancesco Marino or Marini. I use Marin since it is the most used, for him and for other members of the family.

[18] Two other sons Aluise and Zuanne died in 1576 during the terrible plague of 1575-77 that killed about 50000 Venetians out of 150000.

[19] The inventory consists of a fascicle of three folded sheets, found in *ASVe CX Cifre, chiavi e scontri di cifra ... b.6.??*

[20] (Meister, 1902)

[21] Most likely is (Trithemius, 1613). The first book of Trithemius, *Steganographia* was banned by the Church, for supposed witchcraft contents.

[22] (Porta, 1606)

[23] See note above

4	*Quare* 1569, ex fragmentibus Ioh. Bapt. de Ludouicis.
K	*Babuini* in several languages, papers of Borghi. A booklet made of 8 fascicles written by the hand of Marin himself and at the end by his son. See the section below.
M	The treatise of cipher of Z.F. Marin; see below;
	It is one of the known manuscripts of the De Cyfris by Alberti[24]; but the compiler of the inventory doesn't seem to know Alberti.
P	Several booklets in print, loose sheets about the ciphers of G.B. Bellaso [25] [Among others] A long book with a parchment cover and several pieces of paper inside, marked as **ZL** Reg, see 6.2.

Many of these items are now kept in *busta 6* of the "*ASVe CX Cifre, chiavi e scontri di cifra ...* " collection. Alberti's manuscript is now digitized and visible with the computers in the scholar room of the Venetian Archives.

6.2 A Booklet about Pattern Finding

This is one of the items marked **P** in the inventory: a small and narrow booklet in bad condition, torn pages and loose sheets in dubious order[26] . The first page has a date: 1537, March 1, and a dedication to L.B. Alberti. On the second cover page you read a partially erased title:

"Primus
Z.L.Reg.
Liber Vocatus ????? IoanisFr
??? Venet?

The *Z.L.* initials may indicate Zuan Batta Lodouici[27] the successor of Soro, while the *IoanisFr* may refer to Ioan Franciscus Marin. A four hands, two authors work? The year is the one secretary Borghi met the old Soro and had a long conversation with him. Indeed the main deputy of ciphers in those years was already Lodouici, and Marin was still young; so the main author should be Lodouici. But since Soro was still alive, it is possible he had some influence on the book.

The following pages are mostly examples for breaking a syllable cipher, called *babuino*[28] by Venetian cryptographers (or syllabary) using the method today known as pattern finding, looking for some unusual disposition of syllables, the most simple: two identical signs (presumed to be syllables) consecutive. Under the signs there are several conjectures of words matching the pattern.

Other pages have identical signs not consecutive but at a distance of one or more places; and here too there are several conjectured words matching the pattern. A pair of pages is shown[29] in figure 2.

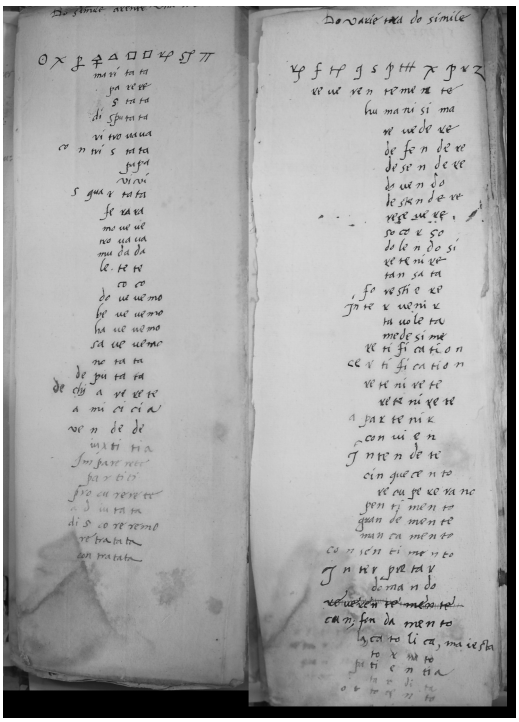

Figure 2: Two pages from booklet 1: conjectures matching a pattern of syllables. *ASVe Cifre, Chiavi e scontri di cifra ... busta 6.1.*

6.3 4 Quare

This booklet has a paperboard cover with a big title in capitals: **QUARE** at bottom a year: MDLXIX (1569) and, under it, // Maij // the month: May.

Under the title, barely legible a script in Latin.

Ex fragmentibus D. Io. Bap^{a} de
Ludouicis ??um delli mei nepta
post eius mortem,

So the author is the second deputy of ciphers,

[26] *ASVe CX Cifre, chiavi e scontri di cifra ... b.6.1*

[27] Updated to modern Italian should sound Giambattista Ludovici

[28] *Babuino* is sort of an acronym for the first syllables: ba-be-bi-bo-bu ...

[29] Figures, using a PDF reader, can be enlarged by zooming in, for better readability of small text.

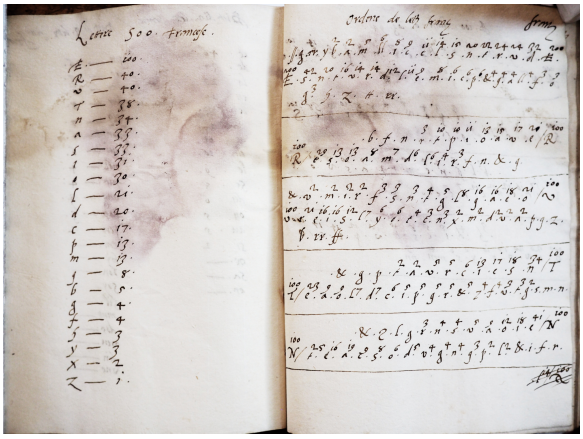

Figure 3: Pages about the French language. *ASVe CX Cifre, chiavi e scontri di cifra ... b.6.2 f.4.*

Zuan Baptista de Ludouicis, the successor of Soro, and this work is in Latin; the second page of the cover has an index, in Italian, listed at n.1 as Vulgar (people's language):

1. Vuulgar 2. Latino – 3. Todesco – 4. Spagnol – 5. Francese – 6. Schiauo[30]

At the top of page 1 one finds these rules:

Frequentiores multiplicent Orthographia negligat Vocalis Scribant dictiones sine uocalis aut sine consonantis aut

The first three pages are an introduction with a few general rules.

6.4 2 M IoFrancisci Marino - Del Modo di Extrazer le Ziffre

The best preserved and more complete book about cipher breaking is "*Del modo de extrazer le ziffre*" (About the mode of decrypting ciphers) by Zuan Francesco Marin. Marked with an **M** on the cover it is listed in the inventory under the same letter.

It is a bound book of 59 *carte*, that is 118 pages, *in quarto*[31] half format like the previous ones. The cover, in parchment, has only the capital letter **M**. The second face of the cover has a signature.

The handwriting is very similar to the one of a supplication of Marin to the **CX**, so it is almost certainly an autograph.

It is a practical handbook with instructions, rules and statistical tables, useful to decrypt simple ciphers (in modern language a MASC) but also particularly syllable ciphers. The language is a

[30] *Schiauo* is XVI cent. Italian for Slavonic language, likely the one used in Dalmatia, then under Venetian domain.

[31] roughly an A5 format; sheets of A3 format, folded twice.

Figure 4: Marin's book: A page about frequency of syllables. *ASVe CX Cifre, chiavi e scontri di cifra ... b.6.2 f.2 c.26.*

Venetian Italian, quite different from the Tuscan Florentine, that became the standard Italian.

The book has these sections:

c. 1	*Del modo di estrazer le ziffre* (about breaking ciphers)
c. 5	*Idioma italiano* (Italian language)
c.10	*Del fine delle ditioni* (about the end of words)
c.21	*Idioma italiano de sillabe* (Italian language)
c.31	*Francese* (French)
c.36	*Della ziffra de Babuini francese* (about the French cipher of Baboons
c.38	*Le più frequenti in ziffra francese de babuini* (the most frequent in the French cipher of baboons)
c.41	*In ziffra de Babuini vulgare Italiano* ()
c.46	*Ziffra latina de babuini* (Latin cipher of baboons)
c.47	*Spagnol* (Spanish)
c.57	*In lingua castellana de babuini*
c.59	*Spagnola de babuini*

As it may be clear from this summary the book is not a theoretical book, no theories or abstract models, it is rather a handbook with rules and councils and, above all, a lot of tables and statistics useful to decrypt syllable ciphers and something about dictionaries, the standard ciphers in the XV-XVIII centuries, with few exceptions. He focuses

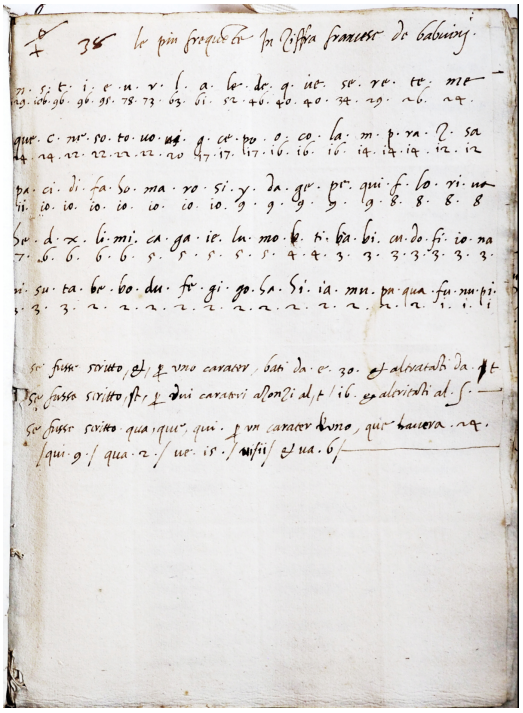

Figure 5: Marin's book: a statistics of frequencies of the French language, single letters and syllables. *ASVe CX Cifre, chiavi e scontri di cifra ... b.6.2 f.2 c.38v.*

on the syllable encryption that was the basis of Venetian ciphers (nomenclators); if one breaks and recovers many syllables, then other syllables and letters will follow, and the few dictions may be interpreted from the context. So, the cipher is broken. Many tables of Marin's book are about syllables; first of all statistics about frequencies of syllables and single letters in a text; thereafter tables about more common syllables following others.

A big question is: was this book useful to instruct new secretaries in the art of solving a cipher without the key? Some doubts emerge in this regard. Ferigo Marin, son of Zuan Francesco, was the main candidate to the role of his father, but looking among the papers of the archives no documents were found about cryptanalytic achievements of Ferigo, who was anyway deputy of ciphers together with Franceschi[32] ; the latter preferring the art of composing ciphers to the one of breaking them, just the contrary of the author of the booklet in the following section,

[32]Hieronimo (or Gerolamo) di Franceschi (1540?- 1600) father of the *cifra delle caselle* the most original cipher produced by the Venetian school of cryptography.

6.5 6 An Anonymous Booklet

This is the manuscript listed in folder **K** of the inventory of Marin papers; the compiler of the inventory attributes the writing of the first part to Marin himself and the last part to his son. Useful to avoid any doubt, he notes that the text ends with the words: "sa l'arte di compor."[33].

Today the book is found in folder N.6 of busta 6.2, and consists of a loose set of 8 folders each of them consisting of 2 folded sheets that give 8 pages, the total is 64 pages. Every page has at his bottom the first words of the following page, so there are no possible doubts about the order and the fact that they are part of a unique book; the last line of text is "sa l'arte di compore", confirming that it is the booklet mentioned by the inventory under letter **K**.

A comparison of the handwriting of this booklet with the one of Marin's main work (*Del modo di extrazer le ziffre*) and the one of a supplication to the **CX** confirms that this booklet was written by Marin himself until *carta* 13, where the handwriting suddenly changes, clearly written by another person, the son according to the compiler of the inventory; and near the end there is another change in the handwriting .

But this does not necessarily mean that Marin was the author of the work. Reading the text one has the immediate sensation that this one is a different author, different style, different language. Marin's main book is written in a Venetian idiom, while this manuscript is written in Tuscan idiom, more similar to modern Italian. And the text has the look of a transcription, several corrections look like oversights of the copyist having missed a word. The fact that the manuscript was written by different hands could reinforce the idea that it was a transcription.

The author writes in the first person, with frequent reminders of his activity as a codebreaker; he first declares he wouldn't boast to be the first to write about ciphers, many others did it, first of all L.B. Alberti, but he remarks most of them wrote about the art of composing ciphers, not the one of decrypting ciphers without knowing the key, the latter being a more demanding and more noble art. Only Alberti wrote something but too little and confusingly. It is clear that he believes to be the first to write about this second art, and particularly about difficult ciphers (i.e. homophonic ciphers

[33]In English: he knows the art of composing [ciphers]

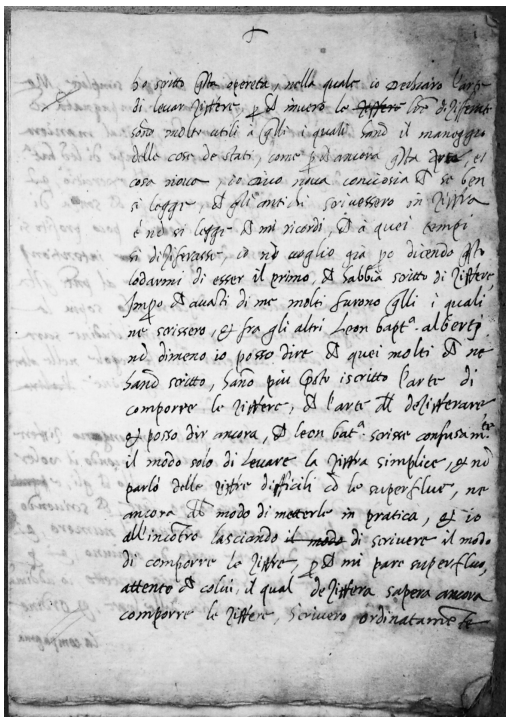

Figure 6: Anonymous work about cipher breaking, first page. *ASVe CX Cifre, chiavi e scontri di cifra ... b.6.2 f.6 c.1.*

with nulls). Page 1 is visible in figure 6.

After having analyzed the properties of the Italian language and of its letters, he gives some rules for breaking a cipher and an example of the cryptanalysis of a rather difficult cipher, one with homophones and nulls. The example cryptogram is visible in figure 7.

At the very end of the book he writes: *In conclusione chi sa l'arte di leuar zifre sa anche l'arte di compore*[34]

And so the anonymous author reiterates the superiority of cryptanalysis (knowing how to decrypt) over cryptography (knowing how to design a cipher).

But, finally, who is this author?

Surely an expert, having good practice in code breaking, knowing the work of L.B.Alberti, whose known manuscripts were in Rome, Florence, Venice and Paris, using as an example an homophonic cipher with signs closely resembling those used in Venice around year 1500. And a man asserting to be the first to write about cryptanalysis could make this statement early in the XVI century.

If one looks among Venetian *cifristi* of the XVI century, there is only one name that fits well with the above indentikit: Zuan Soro; he is a person with a long experience in cryptanalysis, the examples of ciphers closely match the ciphers used by Soro and only Soro could presume to be the first writing about cryptanalysis.

So, could this booklet be the famous lost treatise of Soro? maybe the first book, he promised in 1511, without the parts about the main languages? Maybe Marin made a copy of this book kept by the **CX** in a secret room, for his own use? Maybe was it left anonymous for this reason?

But this fascinating conjecture runs into a problem: the language is Italian, but a Tuscan Italian as seen above. Why should Soro or Marin have used, for a book to be kept secret, the Tuscan idiom, instead of the Venetian idiom he uses in other instances, his book and his supplication to the **CX**?

Marin understood this difference of idioms very well, and at page 29 of his book, after the statistics about syllables, he writes that he got the previous things from letters written in Venetian idiom, where many words end with an **.r.**, but in Tuscan the same will end in **.re.**. A few lines after, he adds that the same is true for words, in Venetian, ending with **n** that in Tuscan (Florentine) end rather in **ne** or **no**. And our anonymous writes e.g. *intentione* while a Venetian usually writes *intention*[35].

So, attributing the booklet to Soro requires him to have used Tuscan, something unusual but not impossible. To put in a nutshell, if the author was a Venetian secretary, it must be Zuan Soro, otherwise someone unrelated to the Venetian administration.

For now there are just conjectures. The whole question remains open.

7 Decrypted Messages

Of course it would of great interest to have a decrypted message as an example, like the one attributed to Borghi in figure 1; there are several papers in busta 3 and in busta 6 with Spanish and French ciphers, it is very difficult to understand whether they were recovered by cryptanalysis or by interception.

[34] English: In conclusion he who knows the art of decrypting ciphers, knows also the art of composing ciphers. It is interesting that the booklet has the verb "compore" with the final **e** as in Tuscan and modern Italian, while the inventory, written by a Venetian, has the Venetian form, without the final **e**.

[35] In modern Italian one writes *intenzione* like many other words ending with *-ione*.

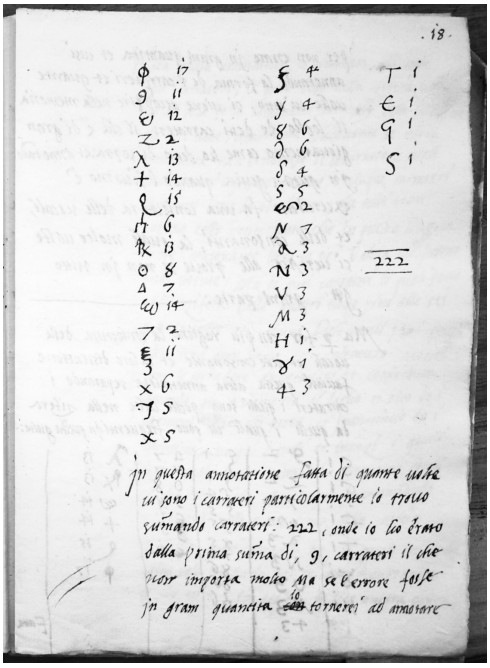

Figure 7: Anonymous: example of encrypted text. *ASVe CX Cifre, chiavi e scontri di cifra ... b.6.2 f.6 c.18-v.*

Maybe the best example is a fascicle containing a Spanish decrypted message row by row, letter (or syllable) by letter; but how this result was obtained remains in the realm of conjectures.

8 Agostino Amadi and his Treatise

The best known Venetian book about cryptography is the work of Agostin Amadi[36] a man with wide cultural interests, first of all for cryptography, although his name is not found among the **CX** deputies of ciphers[37]. maybe he acted as a teacher of ciphers for the future deputies.

Amadi wrote a 10 volume Treatise of ciphers,[38] indeed 5 volumes + 1 volume *Summa* and other 4 other volumes of examples, exercises; what is of interest here is volume 2, the one about cryptanalysis, so summarized in the *Summa*[39]

[36]The name is variously spelled: Agustin, Agostino, Amadi, Amai are the variants. Amadi was the most used by Agostino, while Amai was more use for his son: Piero Amai.

[37]His son Piero Amai was in contrast for decades a deputy of ciphers, the pupil of Hieronimo di Franceschi, but he did not write any book

[38]The treatise in a valuable parchment binding is not visible to the public, but has been digitized page by page in about seven hundreds jpeg files, visible on one of the eight workstations of the Scholar Room of the Venetian Archives

[39]English: The second volume is about mode of reading every kind of foreign ciphers even without knowledge, or cooperation or key, provided they are in the proper languages of the Italians, Gauls, Germans, and Spaniards.

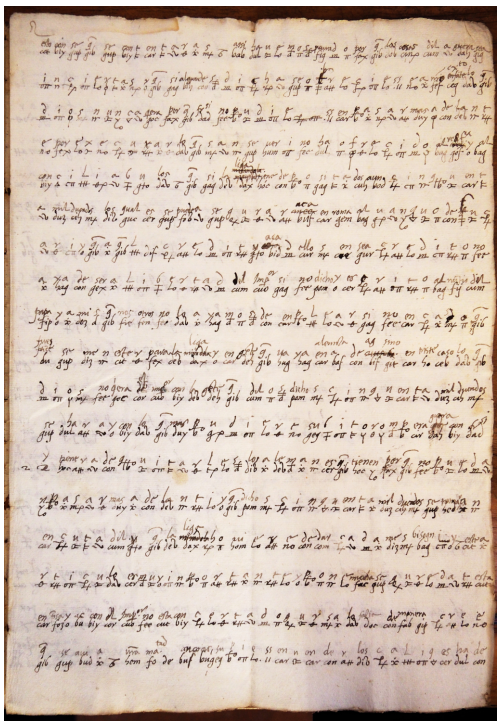

Figure 8: One of four sheets of a Spanish decrypted message.*ASVe CX Cifre, chiavi e scontri di cifra ... busta 6 cifre spagnole.*

> *Volumen secundum est de modo legendi omnia genera Zifrium alienarum absque intelligentiam, seu concursu, aut claue, dummodo sint Italorum, Gallorum, Theutonicorum, Hispanyarum in proprijs idiomatibus.*

Indeed it is a remarkable work, putting the methods used by Soro, Ludovici and Marin in a systematic and comprehensible form.

9 Conclusions

From this collection of books, booklets and various papers about decrypting ciphers, a double face situation arises: first, these works written by people that did all this in the real world of diplomatic and military ciphers, give an impressive view of the tools used for breaking foreign ciphers; second, there is no general theory or general method of cryptanalysis, only a set of tables of frequencies of all kind, useful tools, necessary for decrypting; but the last move, the breaking point, was left to the intuition and experience of the individual; and Amadi remembered that ”nothing should be done

without first invoking the help of God"[40].

Examining the papers in the Archives, the sensation is that the best was in the middle, Ludovici and Borghi were maybe the most successful codebreakers in many languages, while the book of Marin does not seem to progress forward after them. A confirmation can be this statement by H. di Franceschi, around 1587-88, found in a letter to the *Serenissimo Principe* of Venice[41] arguing against the use of weak ciphers:

> [42] *[...] la riducono con questo mezo à pericolo manifesto di esser leuata senza scontro, sì come dalle proue passate della B.M. di M. Z. Batta di Ludouici sec.^{o} di V.Ser^{ta} dalle regole che si trouano in esser et dal libro del .q. M. Agustino Amai ultimamente peruenuto in V.Ser^{ta} che tratta et insegna particolarmente a trazer di simile et di altra sorta di ziffre senza scontro, si può chiaramente certificare*

It is worth noting that Franceschi, perhaps the most original and brilliant mind in the history of Venetian cryptography, praises Ludovici and Amadi as the masters of *leuar le ziffre senza scontro*. Perhaps Soro's book had already been lost, or perhaps it was now considered outdated by Ludouici's rules and methods.

And the **CX** seems to have failed in its purpose to continue the cryptanalitic tradition after Zuan Fracnesco Marin's death in 1578; no other paper about the matter was found in the archives, no mentions of achievements in this field[43], that great tradition seems to have ended in 1578. As already stated above, Ferigo Marin, son of Zuan Francesco, and deputy of ciphers for decades left few traces of his work, and in 1601 was sent to Milan, that was under Spanish rule, as a secretary of the Venetian legacy.

It is likely that the Venetian *cifristi* were still able to decrypt more or less messages using Ludovici's and Marin's tools, but no meaningful step forward in this science was made.

And a remaining mystery is the one of the anonymous booklet. Who was the author? Maybe Soro? Who else?

[40] Original text in Italian: *Così come ho detto, che nissuna cosa si debe fare, se prima non si è invocato l'aiuto de Dio* (Amadi, 1586)

[41] *ASVe CX Cifre, chiavi e scontri di cifra ...busta 6. f. Carte del sec.o Franceschi*

[42] English: [...]in this way it is exposed to the manifest danger of being decrypted, as from the past tests of Messer Z. Batta of Ludouici, of blessed memory, secretary of Your Serenity, from the rules that are found there and in the recently received book of the late Agustino Amai which deals with and teaches methods to break similar and other types of ciphers, it can be clearly certified.

[43] This gap may be due also to a practical problem: paradoxically it is easier to search the CX decrees before 1600, because for some reason only CX decrees until 1600 were digitized and are now easily accessible in the study room of the archives. After 1600 a research requires much more time.

Acknowledgments

Special thanks to the archivists of the State Archives of Venice, for the helpfulness shown, and to Richard Bosch, Portland, Oregon for reviewing the English language.

References

Alberti, L. B. (1568). *Opuscoli Morali*. Francesco Franceschi, Venezia.

Amadi, A. (1586). *Il secondo volume delle zifre*. Archivio di Stato di Venezia, Venezia.

Bellaso, G. B. (1553). *La cifra del sig. Giouan Battista Bellaso, gentil'huomo bresciano ...* Venezia.

Bellaso, G. B. (1555). *Noui et singolari modi di cifrare de l'eccellente dottore di legge messer Giouan Battista Bellaso nobile bresciano, con le sue regole & essempi con somma & chiara breuità composti ..* L. Britannico, Brescia.

Kahn, D. (1967 - 1996). *The codebreakers*. Scribner, New York.

Meister, A. (1902). *Die Anfänge der modernen diplomatischen Geheimschrift*. Ferdinand Schöningh, Paderbord.

Pasini, L. (1872 - 2019). *Delle scritture in cifra usate nella Repubblica di Venezia*. Aracne, Venezia.

Pesic, P. (1997). François viète, father of modern cryptanalysis. *Cryptologia*.

Porta, G. D. (1563 - 1606). *De Furtivis Literarum Notis, Vulgo de Ziferis ...* Napoli.

Sanudo, M. (1533). *Diarii*. Venezia.

Trithemius, I. (1507 - 1613). *Libri Polygraphiae*. Lazari Zetzneri, Argentorati (Strasbourg).

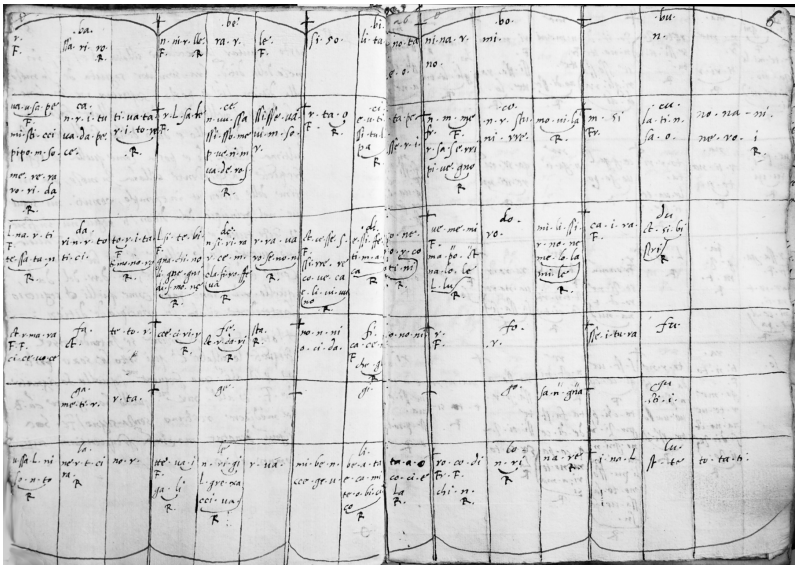

Figure 9: A large and complex table showing for every syllable the most frequent syllables or letters following it. Very useful to decrypt a cipher with syllabaries and single letters. *ASVe CX Cifre, chiavi e scontri di cifra ... b.6.2 f.2.*

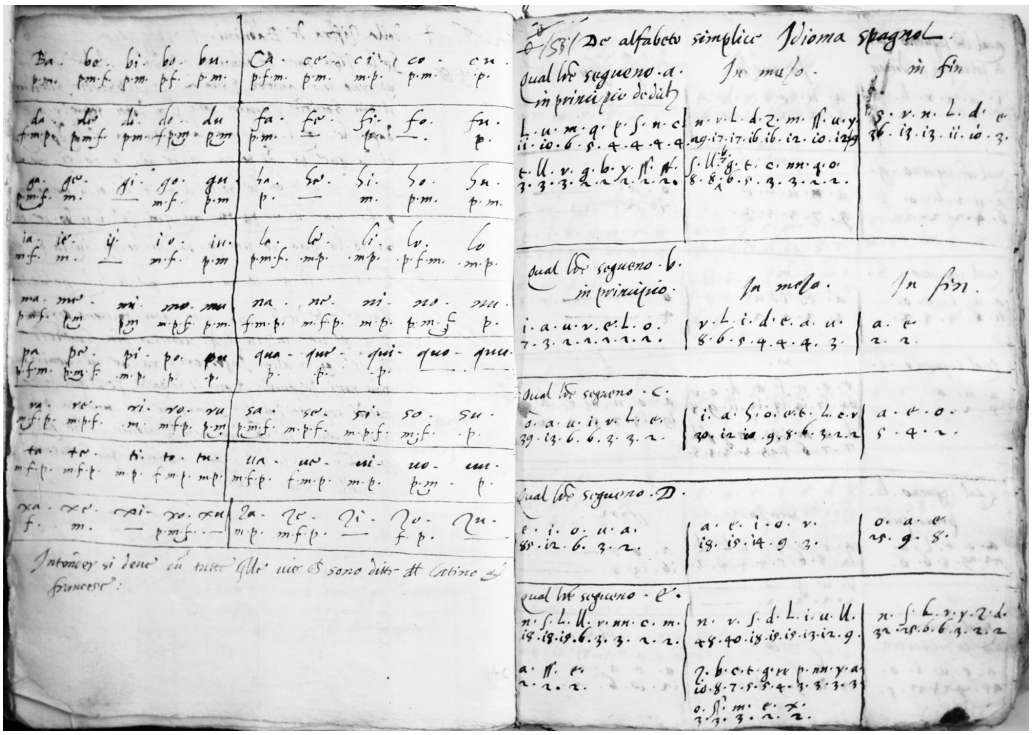

Figure 10: Tables of frequencies for the Spanish language; on the left of syllables, on the right for the simple alphabet and for digraphs: letter following another. *ASVe CX Cifre, chiavi e scontri di cifra ... b.6.2 f.2 c.15.*