How mathematics spread and transformed cryptographic activities

Marie-José Durand-Richard, Philippe Guillot

How mathematics spread and transformed cryptographic activities

Marie-José Durand-Richard[1]
Philippe Guillot[2]

Cryptographic glossary

• Plaintext : is the name of the message before cyphering.
• Cryptogram : is the name of the message after ciphering.
• to Cypher : is the generic name of the practice of the cryptograph, transforming a plaintext into a cryptogram.
• to Decypher : is the generic name of the practice of the receiver of the cryptogram, working to recover the plaintext from the known key.
• to Break the code : is the name of practice of the cryptanalyst, often considered as an enemy or an opponent, working to recover the plaintext without knowing the key.
• to Encrypt : means to cipher since the use of computers.
• Decryption : is the practice of the cryptanalyst since the use of computers.

INTRODUCTION

People tend to be unaware of what cryptography is. Because it is usually invisible, it is consequently not thought about. Yet its use has become widespread in many aspects of everyday life, from credit cards to mobile phones. Since computer networks exist, transmission of information has thus been regulated by procedures of secrecy, whose hidden use is not without questioning the exercise of democracy.

This paper intends to clarify the practices of cryptology, and their progressive entanglement with mathematics. It includes two parts. The first is related to the period when the main tools for cyphering and code breaking came from the analysis of language.

[1] Honorary lecturer, University Paris 8 Vincennes Saint-Denis. Associates researcher, SPHERE Laboratory, UMR 7219 CNRS-Université Paris Diderot. marie-jo.durand-richard@orange.fr
[2] Assistant professor, University Paris 8 Vincennes-Saint-Denis. philippe.guillot@univ-paris8.fr

Nevertheless, since the Arabic scholars, mathematics has been locally introduced for breaking codes, but the various techniques evolved slowly because of the secret around these practices. Simultaneously, new cyphering practices were also produced to counter attempts to break the codes. The second part begins with the military use of telegraph and the claim by Auguste Kerckhoffs to focus on cryptographic systems rather than on individual secret messages. Step by step, dealing with cryptographic systems opened the way to mechanical devices and also to the mathematical analysis of their running, both to overcome the subsequent modes of cyphering and to define them. A somewhat confidential *savoir-faire,* focused on cyphering and deciphering messages, has become an academic discipline taught at University since the 1980s, and is dedicated to the development of equipment and cryptographic systems that now impact all civil society. Cryptology became really a discipline when it was definitively used to manage the running of computer networks.

THE TIME OF SECRET MESSAGES

Cryptology – from Greek *Kryptos*, to hide – combines two distinct topics: cryptography develops methods to hide the meaning of messages, whereas cryptanalysis tries to outsmart them. For a long time, cryptanalysis was based on a quantitative and qualitative analysis of written language, but gradually mathematics has pervaded it, changing its nature and practices, especially since mechanization has considerably increased the potential of cyphering procedures, and blocked at the same time the possibilities of breaking the code by hand. The history of this mutation, marked by secrecy, is neither linear nor uniform. Let's remind ourselves of some of the milestones.

1. Mono-alphabetic cypher

The first methods of secret transmission consisted in concealing the message itself. Aeneas Tacticus, the Greek military of the 4th century B.C. described many methods in the Chapter 31, "About Secret Messages", of his book *How to survive under Siege*. The message might be concealed either in the shoes of a soldier, or under his breastplate, or it could be tattooed on his head when cropped, or registered by points added to an ordinary letter. These methods are not part of cryptography, they are called today *Steganography*.

The idea of hiding the meaning of a written text, by operating a shift of letters of the alphabet by 3 places, is mentioned by Suetonius in *The Twelve Caesars* (*De vita Caesarum*) [SUE]. Its use was not a military, but a private one.

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

Fig. 1. The shift of letters corresponding to the "Caesar cipher", applied to modern Latin alphabet.

Despite our ignorance of the texts, this cypher was undoubtedly made more complex by extending to any shift in the number of letters. So extended, the "Caesar cypher" had a long posterity. It was used during the American Civil War by Confederate officers, as well as by the Russian army in 1915 [KAH, p. 216]. Nowadays, a 13 place shift is at the core of the so called ROT13 system used at the early time of Internet as a very basic way to hide the sense of electronic mails. The number 13 was chosen so that it is the same procedure that hides and

reveals the message. But unlike the presentation made in many histories of cryptology, at Caesar's time, this process was not perceived as a "modulo 26 addition"! It was just an elementary manipulation of the alphabet.

From the 8th century, Arab scholars initiated the opposite approach which consisted in searching for the hidden meaning of a cryptogram. The mathematician, astronomer and philosopher Al-Kindi (801-873) produced the first known table of occurrences of letters for a language alphabet and presented its basic method.

> "One of the tricks we use to remove the obscurity of a book, if the language is already known, is to find a text that contains as many [letters] as in a book, then we call "first" the most frequent letter, "second" the next in abundance, and "third" the one that follows in abundance, and so on until you have completed all of the letters. Then we look in the text from which we wish to remove the obscurity and we classify the letters, then we look at the most frequent. We call it "the first letter." And the one that follows in abundance, we call it "the second letter." And the one that follows them in abundance, we call it "the third letter", and so on until exhausting all the letters of the text from which we extract the obscurity" [MRA 2003, p. 125].

The birth of cryptanalysis in the Arab world – this "science to extract obscurity" – did not stop at comparing the number of occurrences of the letters, a method which would become the "frequency analysis". It inventoried the "tricks" that allow quantitative and qualitative analysis of cyphered messages more subtly by examining all cyphering options: frequent or impossible associations of letters, identification of probable words as honorary titles or agreed formulas. This systematic study of the peculiarities of language originated in a specific linguistic context; it was carried by the codification process of the Arabic language, which was a fundamental cultural and administrative unification factor of the conquered territories, from the Indus Valley to the Iberian Peninsula. The desire to assimilate all previous knowledge required an extensive work in translation – from Greek, Syriac, Persian and Sanskrit – and lead to the writing of numerous treatises of language analysis. This same linguistic context led to the birth of algebra by the very same scholars, conceived as a work of literary classification of problems in the natural Arabic language [RAS, pp. 1-29]. This constitutes one of the first relationships between cryptology and mathematics.

These political and cultural imperatives were the foundation to the development of a school of cryptology – cryptography and cryptanalysis – that flourished until the 14th century. It is in this context that Ibn Dunaynir (1187-1229) inaugurated a first numerical cyphering method:

> **Chapter 26 :**
> "For the transcription, in order to obscure [the text] from one of the combined methods, let us have recourse to the number corresponding to the letter and double it once, or twice or several times, and this will hide the meaning to those who will read. Here follows an example " **التوفيق ولي الله** " (The benevolent God) :
>
> **ر كـ ق س ي ب ض س ب كـ س ي ب ي س س ب**
>
> Here is *ba* (**ب**), which the numeral value is two, and which is the double of the numeral value of *ali* (**ا**), and *sin* (**س**) which the numeral value is sixty and which is the double of the numeral value of *lam* (**ل**). The same for the remainder. So admire this pretty method"[3]

[3] Trad. Abderrahman Daif in [DUR-GUI, ch. 2].

Remark : In Arabic language, the numeral value of a letter is a number which is attributed to it according to a pre-established code, and recognized by everybody. Here is the explanation of this example :

Lettre	ق	ي	ف	و	ت	ل	ا	ي	ل	و	ه	ل	ل	ا
valeur numérale	100	10	80	6	400	30	1	10	30	6	5	30	30	1
Double	200	20	160	12	800	60	2	20	60	12	10	60	60	2
Transcription	ر	كـ	قس	يب	ض	س	ب	كـ	س	يب	ي	س	س	ب

Fig. 2. Ibn Dunaynir, « Treasure to clarify ciphers », [MRA 2005, p. 127].

It is quite likely that these works were transmitted to Europe at the time of the Renaissance. For instance, an Arabic book on the alphabets was published in English by the orientalist John von Hammer in 1806, and studied by the specialist of the Arabic language Sylvestre de Sacy in 1810, before inspiring Champollion to break the hieroglyphics [MRA 2003, p. 45].

2. From codebooks to polyalphabetic cypher

At the same period, in terms of cryptology, Medieval Europe was less advanced than the Arab-Muslim civilization. The methods remained rudimentary.

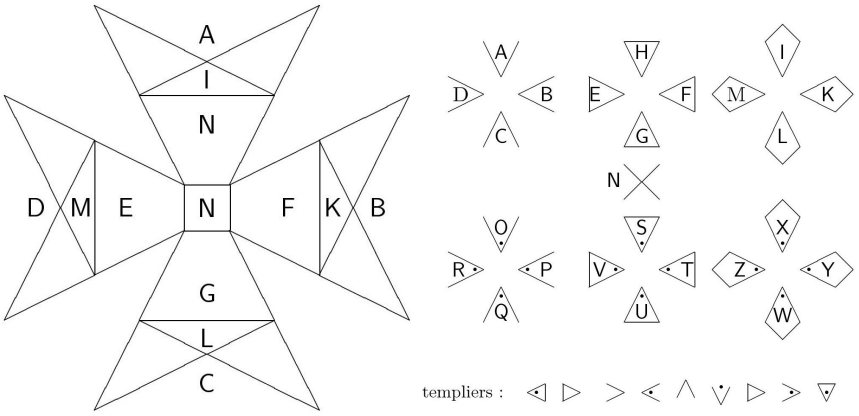

Fig. 3. The cyphering method founded of the Maltese cross

For example, the Templars replaced letters by the forms which enclosed them, inside the eight points of the Maltese cross, the emblem of their order [HEB, p. 41]. They were convinced that the mystery surrounding these obscure symbols was enough to ensure the confidentiality of their missives.

Protection of correspondences against espionage acquired paramount importance at the time of the emergence of new power centers in the major Italian cities and the Royal courts. The "black chambers", generally made up of a specialist assisted by numerous operators, played an important political role. It was by these means that Phelippes Thomas (1556-1625), the head of Elizabeth I's (1533-1603) service of cyphering, revealed the betrayal of Mary

Stuart (1542-1587). The specialist was sometimes a mathematician. Thus François Vieta (1540-1603), best known for his early works in symbolic algebra, helped King Henry IV (1553-1610) to break the secrecy of the correspondence between the Catholic League and the Spanish King Philip II (1527-1598). During the English Civil War, John Wallis (1616-1703), best known for his works on algebra and early integration, worked on behalf of the English Parliament breaking the code in messages between King Charles I (1600-1649) and his followers. He then entered the service of his son Charles II (1630-85) at the time of the Restoration (1660).

3. Towards the polyalphabetic cypher

Many practices tended to complicate the mono-alphabetic encryption to thwart the use of frequency analysis. The homophonic cypher (1401) of Simeone de Crema gave several possible signs for the most frequent letters, signs that the operator chose at random when cyphering. Research evolved in two directions: codebooks and polyalphabetic cypher.

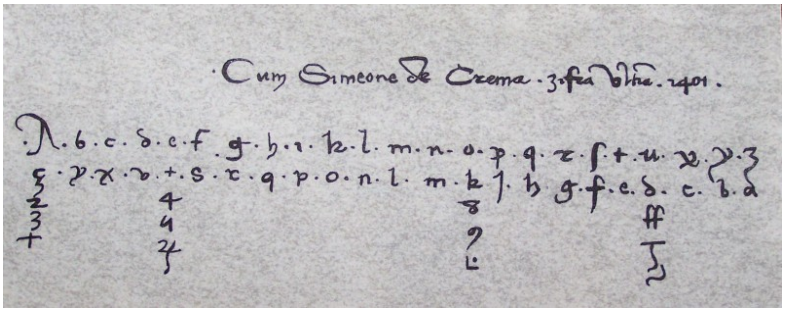

Fig. 3. Chiffrement homophone de Simeone de Crema. [KAH, p. 107].

On the one hand, codebooks were dictionaries associating common words with substitution letters or figures. Created by the cypher secretaries, they had the form of books such as the "Grand Chiffre du Roy" Louis XIV (1638-1715), prepared by Antoine Rossignol (1600-1682): it included 587 entries, many of which represent syllables. It was broken much more later, in 1893, by the French military Etienne Bazeries (1846-1931).

On the other hand, the treatise *Componendis Cyphris* (1466) of the Florentine architect Leon Battista Alberti (1404-1472), known for his treaties on perspective, introduced a new practice based on an encrypting dial [ALB]. The letters of the plain text are chosen on the outer fixed disk. It includes 20 capital letters (the letters *H*, *J*, *K*, *U*, *Y* and *W* are missing) and the numbers 1, 2, 3 and 4, that may be used to encode high frequency words. For instance, the sequence 1234 may signify "King Philip II". In the 24 sectors of the mobile disk, the letters that correspond to the cyphered message appear in lower cases and are in a random order. The sender and the receiver each have the same dial. They agree to an index indicated by a letter on the mobile disk, for example the letter *k*. In the cryptogram, the first of the letters written in capital letters, for example *B*, indicates that the letter *k* must be placed in front of the letter *B*. Any new position of the mobile disk leads to a new alphabet. So, there are as many cyphering alphabets as possible positions of the mobile disk. The same word can be cyphered in one way at one point in the message and by another way later in the same message. The first polyalphabetic encryption was thus invented. However, it remained locally mono-alphabetic and frequency analysis can still work on some portions of the cryptogram.

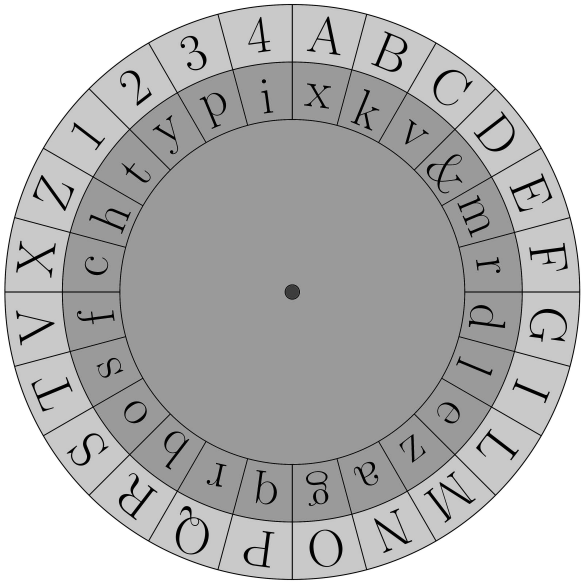

Fig. 4. Alberti disk. Illustration Ph. Guillot.
Example of cryptogram: BqxboGqvgiMteRkomcoyvXilya

> "From this starting point, each letter of the ciphertext represents the letter in the section immediately above it. After writing three or four letters, I can change the position of the index so that *k* is situated below the *D*. So in my message, I will write a capital *D*, and from this point, *k* will no more mean *B*, but the letter *D* and all the letters in the fixed disk will have new equivalents" [KAH, p. 128].

By passing from the disk to a table, the method progressed to cyphering alphabet that changed for each letter. The posthumous work of the German Benedictine abbot Johannes Heidenbert, known as John Trithemius (1462-1516), titled *Polygraphia Libri Sex* (1518) contains the so-called *Recta Transpositionis Tabula*, or *Tabula Recta,* which cyphers the first letter of the plaintext with the first alphabet, the second letter with the second, etc.

a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w
b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a
c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b
d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c
e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d
f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e
g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f
h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g
i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h
k	l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i
l	m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k
m	n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l
n	o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m
o	p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n
p	q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o
q	r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p
r	s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q
s	t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r
t	u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s
u	x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t
x	y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u
y	z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x
z	w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y
w	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z

Even if this cypher is polyalphabetic, it remains poor: in fact, as soon as the method is revealed, there is no more secret, and everything becomes clear [KAH, p. 136].

Giovan Battista Belaso (1505-1553), in *La cifra del Signor Belaso* (1551), added to the table the notion of "key," which enabled the cyphering of the clear message by choosing the alphabets in the order of letters of an easily remembered and modifiable word that he calls the "countersign" [KAH, p. 137].

> "For example, suppose our countersign is the little verse *Virtuti omnia parent* (to be through virtue). Suppose also that we want to write these words *Lamarta Turchesca partira a cinque di Luglio* (The Turkish army will leave on july fifth). We will place it on the paper as follows:
>
> ```
> Virtuti omniapare ntvirtu t pa iomnia rentvi
> lamarta turchesca partira a cinque di luglio.
> ```

Hence, using the above *Tabula recta,* the cryptogram is obtained:

```
FIDTMNI HGELHTCKA CTMCALU T LYWDDE SI CWTEDY.
```

Henceforth, the secret is reduced to the countersign. Knowledge of the process does not help anymore to break the code.

After an initial synthesis of Giambattista della Porta (1535-1615), in his *De furtivis literarum notis* (1563) [POR], the ultimate form of this polyalphabetic cyphering with key is presented in the *Traicté des chiffres* (1586) written by the French diplomat Blaise de Vigenère (1523-1596), which covered an impressive panorama on the history of languages and their secrets [VIG]. But the social secrecy surrounding these practices was such that the "Vigenère cypher" would be repeatedly reinvented: the Jesuit Gaspar Schott introduced the Gronsfeld cypher in 1734 with a numerical key; the English Admiral Charles Beaufort (1774-1857), best known for his nautical wind scale, gave a variant that exchanged the role of the key letter and of the message letter in the table of alphabets; and a dentist in Bristol, John HB Twaites, asked for expertise and patent in 1854 at the *Journal for the Society of Arts,* exposing himself in return to the sarcasms of the mathematician Charles Babbage (1791-1871) who had just precisely at that time broken the Vigenère cypher.

But, facing a concern to cypher a large amount of messages by unskilled operators, this major innovation had little impact, because it was too complex to implement and was susceptible to many transcription errors. The codebooks remained the major tool of cryptography until the mid-18th century. The last codebook established in France was designed in the 1970s by the French Colonel André Cattieuw, then in charge of the Central Cypher Services, [DUR-GUI, ch. 5]. It included more than fifty thousand entries. The mechanization of cyphering would definitely make these codebooks obsolete.

4. The opening of cryptanalysis to mathematics

Mathematics began to intervene in cryptanalysis while the symbolization of algebra was unified during the 17th century. Despite the frequency analysis and the use of probable words initiated by Arab scholars, deciphering without key remains a difficult and laborious work, which must also rely on hard work and a bit of good luck. Mathematics was introduced very slowly in cryptography, as the secret impeded the transmission of knowledge. François Vieta was the appointed code-breaker when Henri IV became King of Navarre in 1589. He was the

author of numerous code books. He was also the first author in France – before René Descartes (1596-1650) – to present a symbolization of algebra, the "*logistique spécieuse*", where he already studied the properties of algebraic equations, particularly the relationships between roots and coefficients. Shortly before his death, he left to the Prime Minister Sully a text on cryptology where he details his methods for recovering plaintexts from cryptograms sent between Spain and Italy during the European wars of Religion. His specific mathematical approach relied on his systematic way of dealing with the problem, more than by any use of equation resolution modes, that were yet themselves under development. He initiated a deductive approach, which he called the "infallible rule" [DEL].

> INFALLIBLE RULE: *Among three consecutive letters, there is always one or more of the five vowels A, E, I, O or U.*

This rule was especially infallible in Spanish language. Vieta explains how it works on a mono-alphabetic encryption. The first job was to find the vowels, and the historian of science Peter Pesic attributed to this specific search the choice of Vieta to represent the unknowns of algebraic equations by vowels, while the present use of *x*, *y*, *z* was initiated by Descartes few decades later [PES].

At this point, Viète could not entirely give up the use of significance. Once the vowels determined, common sense, intuition, speculation and hard brainwork had still to intervene, making use of the context and meaning of the messages.

Two and a half centuries later, the polyalphabetic cypher acquired an extended use while some mechanical refinements secured its execution and extended its diffusion. Thomas Jefferson (1743-1826), later President of the United States of America (1801-09), and co-author of the Declaration of Independence, in 1790, whilst secretary of state of George Washington, developed a cylinder made by 26 rotating disks on the edge of which was printed an alphabet in disorder. To cypher the message, the operator had just to align the letters of the message by rotating the disks. The transmitted cryptogram was the sequence of letters that lay on any other line. To decrypt the cryptogram, the receiver had the same cylinder. He had just to align the letters of the cryptogram and to read the only line which seemed to make sense among the other ones.

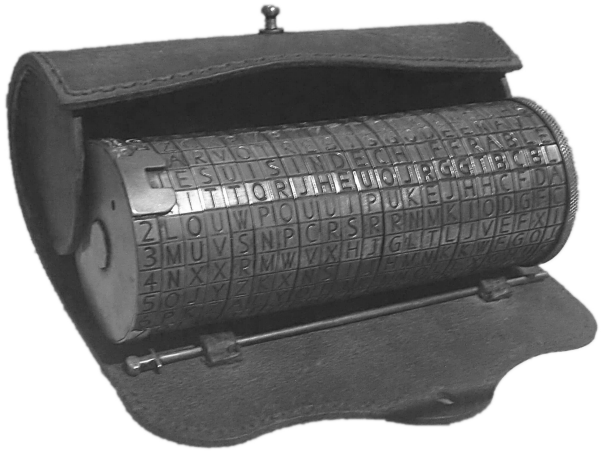

Fig. 5. The Bazeries cylinder.
Item exhibited at the Museum of Telecommunications de Rennes. Cliché Ph. Guillot.

Changing the key means changing the disk order. This device would be reinvented by Étienne Bazeries (1846-1931) in 1891 – the same who also broke the Vigenère cypher in 1893 –, and the Italian Colonel Darcos in 1900. In the United States, a variant of this cylinder, the cylinder M-94, improved by Colonel Joseph O. Mauborgne (1781 -1971), was used by the US military between 1922 and 1942.

5. Babbage's first attempt to break the Vigenère's cypher

Nowadays, Babbage is often referred to as a "pioneer of computers", but this is rather an anachronism. Actually, inside a group of Cambridge algebraists, he initiated a new approach to algebra, named "Symbolical Algebra", where symbols were completely disconnected from any meaning, and simply combined by laws of operation. From this idea, and from his own thinking on the Industrial Revolution, Babbage designed the plans of a complex machine, "the Analytical Engine", which could perform the whole operations of this Symbolical Algebra. It was in fact an automatic calculator with an external program [DUR].

In this context, from 1831 to 1870, he collected materials on cryptology, which he intended to publish as the "Philosophy of Decyphering". The manuscript testifies to a constant activity, recognized by his peers. This work was produced simultaneously with the birth of telegraph, and one of its inventors, Charles Wheatstone (1802-75), was a friend of Babbage. But Babbage's cryptographic activity did not take place within the framework of this invention. He regularly practiced cryptography with some of his learned friends, namely Davies Gilbert, the president of the *Royal Society,* and with the geologist William Fitton and his sister Mrs James [BAB, ff. 8-9].

The secret message Babbage broke in 1846 was written as a challenge by his nephew he had initiated in cryptology. It was composed with the Vigenère polyalphabetic cypher a few weeks before, but with three different keys : Murray, Cacoethes and Somerset. So, solving the puzzle was specially difficult. Numerous trials were needed. Babbage resorted to frequency analysis, but much more to probable words, specially for the usual header and conclusion of the message, *my dear uncle* and *your affectionate nephew* [BAB, f. 63].

```
PYRI  ULOFV
murr  aymur
dear  uncle

POVVMGN  MK  UO  GOWR  HW  LQ  PGFJHYQ
cacoeth  es  ca  coet  he  sc  acoethe
nothing  is  so  easy  as  to  perform

OJAV  MSN  WIJHEEHPR  BRVGRUHEGK, EFF WJSR  RVY
scac oet   hescacoet  hescacoeth, esc acoe  the
what  you  perfectly  understand, and when  you

CPOY  VSP,  PX  OKLN  PI  XXYSNLA  SELF  XG
scac  oet,  he  scac  oe  thescac  oeth  es
know  how,  it  will  be equally   easy  to

FEEWTALV  LJIU, WR  MOI EGAP  HMFL  ML  YINZ
cacoethe  scac  oe  the scac  oeth  es  caco
decipher  this  in  the mean  time  it  will

TNGDDG  YQIV  UYEAP-BQL
ethesc  acoe  thesc-aco
puzzle  your  brain-box
```

```
WJQV  PGYK  STRITLMHFOFI EWTAWK
some  rset  somersetsome rsetso
ever  your  affectionate nephew

        TIEJC
        merse
        henry
```

Several important new features should be noticed in this work.

• Babbage referred to letters by their numerical order in the alphabet, starting with 1 for A.

```
19  20  18   9  20  12  13   8   6  15   6   9
 S   T   R   I   T   L   M   H   G   O   F   I
18  14  12   4  17  18   4  19  18  14  12   4
 A   F   F   E   C   T   I   O   N   A   T   E
 1   6   6   5   3  20   9  15  14   1  20   5
 S   O   M   E   R   S   E   T   S   O   M   E
```

• From there, for each letter of the message, he immediately identified the relationship between the cypher, the key and "the translation", that is the initial message, which he wrote as a "cryptographic equation" [BAB, ff. 58-59]:

cipher = key+ translation – 1
translation = cipher – key + 1

• At the bottom of the very page where Babbage wrote the cyphered message and the plaintext together with the keys, three little tables, one for each key, indicated this relation in a new form. This time, the order number for the letters was no longer from 1 to 26, but from 0 to 25. So, we can argue that only after he recovered the plaintext, Babbage recognized the relationship between his work and the *Disquisitiones Arithmetica* (1801) where the mathematician C. F. Gauss (1777-1855) just presented his modular arithmetic.

Table 1

Substract	N°	Rem
6)	0	24
	1	12
	2	20
	3	17
	4	17
	5	0

Table 2

Substract	N°	Rem
9)	0	18
	1	2
	2	0
	3	2
	4	14
	5	4
	6	19
	7	7
	8	4

Table 3

Substract	N°	Rem
8)	0	19
	1	18
	2	14
	3	12
	4	4
	5	17
	6	18
	7	14

One of his subsequent public intervention on this subject would explicitly rely on modular arithmetic [BAB ff. 133-179]. In 1854, a dental surgeon from Bristol, Mr John Thwaites, wrote to *The Journal of the Society of Arts,* asking it to patent what he considered as a very new form of cyphering that he had just invented. He claimed it would be very useful for maintaining the privacy of exchanges transmitted by telegraph. In fact, his invention was just a new material form of the Vigenère's cypher, presented with adjacent sliding strips, each of them carrying an alphabet: in fact, a linear form of the Jefferson's cylinder [FRA].

When asked by the *Society of* Arts as an expert, Babbage answered ironically that Thwaites' invention could be broken very easily. Mr Thwaites sent a second letter with a

message cyphered two times, the first with a 3-letter key, the second with a 8-letter key. He considered it as particularly difficult to solve.

The plaintext:

Soft, sir, one word more,
They are both in either's powers : but this swift business
I must uneasy make, lest too light winning
Make the pne word more, I charge thee
That thou attend me, thou dost here usurp
Upon this island as a spy, to win it
From me, the lord on't.

The cryptogram:

UTMU[4], DQV, UKS, LKZT, LRWN, FLHL, HPG,
SVUS, QR, KFHWAZI, ORBNDW, EHA, RJZZ,
THQJZ, YHIEVURV, N, VGWW, HUCCJF,
NLSI, RBGI, PWE, KLLQF, ALAUGPX, TBVM,
XNB, DGEHU, KLLQF, SQR, DMTU, TPCM, M
IEOGCM, JGHJ, CTEW, GOMW, RAUPVH, SB,
HWKC, TNVY, QQVH, HZSTG, BQZV, XNFG
XOTQMG, FB, M, WSL, AM, YZU, JE, NVUJ,
AT, PPU, KRWM, AR'W.

Babbage immediately showed that the double cyphering was useless, as it worked as a single one, resulting from the composition of the two others, TWO and COMBINED. Moreover, he gave the plaintext, but he did not explain how he found it. He just gave the detailed computation for each letter of the message, from this key with 24 letters, using the Gaussian modular arithmetic. This is an abstract of his calculation :

Rest	Tabular Nb	Rest	Tabular Nb
0	24	12	22
1	2	13	8
2	17	14	16
3	7	15	25
4	1	16	3
5	11	17	5
6	8	18	9
7	4	19	12
8	6	20	4
9	23	21	3
10	14	22	13
11	15	13	7

For instance, as *w* is the 145th letter of the cyphered message,
and as 145 = 6 x 24 + 1
we have to choose, the number facing 1 in this table, which is 2.
As *w* is the 23th letter of the alphabet,
the difference 23 – 2 gives the place of the initial letter, which is *u*.

[4] Once he found the two keys, Babbage corrected the 2nd letter of the first word in the cryptogram, which should be *g* instead of *t*

When he broke the Vigenère's cypher, Babbage still worked in a private framework, inside a social group close to learned societies, dealing with isolated messages. In his view, cryptography matched a mind game, in accordance with his own view on symbolical algebra. Even if he used mathematics for breaking the Vigenère's cypher, he worked also by numerous trials and still on isolated encyphered messages. Anyway, he did not provide any systematic method to follow.

Such a method was published in 1863 by the German infantry officer Major Friedrich Wilhelm Kasiski (1805-81) in *Die Geheimschruften und die Dechiffrir-Kunst*, written after his retirement [KAS]. This method was a refinement of frequency analysis, still used nowadays. The cyphered message has to be long enough, and the length of the key is first determined by locating repetitions of groups of letters. These repetitions suggest that the same word might have been encyphered with the same letters of the key. So, the distance between these repetitions may be supposed to be a multiple of the length of the key. Once this length is known, the encyphered message can be divided into sub-messages, each of them being formed by letters cyphered with the same letter of the key. Then, the frequency analysis can be applied to each of these sub-messages.

Until the 19th century, even if opportunities for mathematics to occur in cryptology were not regular, this regularity came firstly from the introduction of material practices and technical devices, and secondly from an afterthought on their use. The extension of telegraph as a material network, and its adoption by military troops some decades later, was the first step of this process, leading to explicit new requirements for cyphering.

FROM SECRET MESSAGES TO CRYPTOGRAPHIC SYSTEMS

The nature of secret exchanges was radically new when Auguste Kerckhoffs (1835-1901) introduced the idea of a "cryptographic system" in 1883. He presented the conditions by which secret could be preserved when messages transmitted by telegraph had to pass through a host of hands. Nowadays, Kerckhoffs is often presented as a precursor of the concept of cryptographic system in mathematical terms. But his essential idea was to give up thinking cryptography for isolated messages between particular individuals, and to work on the whole system of secret telegraphic exchanges.

From the beginning of the 20th century, the implementation of widely available material networks played a key role to impose new requirements in secret messages transmission. Thanks to a randomly perforated tape, in 1919, Gilbert Vernam (1890-1960) integrated the cyphering method inside the teletype. And when Claude Shannon (1917-2001) defined mathematically how to measure the "amount of information", he characterized "secrecy systems" by working analogically both on telecommunication systems and cryptography. In 1973, Horst Feistel (1915-1990) was in charge of developing cryptographic algorithms when he produced the block cypher *DES* (*Data Encryption Standard*). A few years later, Whittfield Diffie (born in 1944) and Martin Hellmann (born in 1945) introduced the very new idea of public key cryptosystems, before it was later materialized through the RSA algorithm in 1978.

1. The principles of a secure transmission by telegraph

What was at stake in Kerckhoffs' text was to define how to organize the cyphering process in order to preserve the secret of messages while passing through all levels of military hierarchy during this transmission.

Jean Guillaume Hubert Victor François Alexandre Auguste Kerckhoffs von Nieuwenhof (1835-1901), son of a Belgian landlord, was graduated in Arts and Humanities, and travelled in Europe before settling in France, where he taught modern languages, essentially German in Paris. Together with Martin Schleyer (1831-1912), he firmly promoted a new universal artifical language, named *Volapuk,* which was very successful, butt had only a brief life during the 1880s. We know his interests for military affairs from the book *The Codebreakers by* David Kahn. He got "embroiled in some minor political difficulties after the defeat of 1870" [KAH, p. 231], and he failed to obtain the chair of German language at the *Ecole Militaire Supérieure* in 1878, because a clerk had failed to note that he was naturalized as a French citizen since 1873.

In his double paper "La cryptographie militaire", published in 1883 in the *Journal des Sciences Militaires,* and immediately edited as a book, Kerckhoffs carefully distinguished between a cypher designed for private correspondence and a military cyphered telegraph based transmission:

> "We have to distinguish between a cyphered writing system, designed for momentary exchange of letters between a few isolated individuals, and a method of cryptography adjusting for an unlimited time the correspondence between the various army chiefs. These ones, indeed, may not change their agreements at their discretion, and at any time; moreover, they should never keep with them any object or writing which is likely to help the enemy on the meaning of secret dispatches that might fall into his hands"[5] [KER, I p. 12].

From the first pages, Kerckhoffs named a cryptographic system, and went on directly with what he named *The Desiderata of military cryptography,* expressing the consequences of the transmission of messages by telegraph on the organization of cyphering, namely:

> "A system is needed, which has to carry out exceptional conditions, which I summarize under the following headers :
> 1. The system has to be physically, if not mathematically, indecupherable,
> 2. It must not require secrecy, and could fall into the hands of the enemy without disadvantage,
> 3. The key is to be communicated and memorized without the aid of written notes, and it is to be changed or modified at the discretion of the correspondents,
> 4. IT HAS TO BE APPLICABLE TO TELEGRAPHIC CORRESPONDENCE,
> 5. It has to be portable, and its usage or its operation must not require the assistance of several people,
> 6. Finally, it is necessary, given the circumstances in which the application is controlled, that the system has an easy use, asking neither mental strain nor the knowledge of a long series of rules to follow" [KER I, p. 12].

These laws were not purely theoretical. They were based on the existence of a material communication system: the telegraph. The fourth condition was of course central, because it determined the other ones. Before surveying the state-of-the-art in military cryptography, Kerckhoffs first concern was to examine what had to be changed in military secret practices because of this transmission by telegraph. Consequently, what was essential was to yield a cypher system which could resist long enough so that the military operations so concealed

---

[5] In this paper, the passages extracted from French texts are translated by the authors.

could be conducted. It is what Kerckhoffs meant in his first condition.

This new mode of transmission required simplicity, reliability and speed; and it provided cryptograms with five letters blocks, as it is still the case nowadays. Moreover, the secret feature of military correspondence had to be compatible with the collective use of telegraph, where numerous people were involved. Kerckhoffs drew two major consequences. First of all, an absolute secret was no more possible. Tables, dictionaries, mechanical designs, even messages, were likely to fall into the hands of the enemy, or readable by lower levels of military hierarchy. Kerckhoffs considered that this new state of affairs was not correctly understood by the French military officials during the Franco-Prussian war in 1870, and that the lack of direct communications between Paris and the war front partially explained the defeat. So, his laws drew the consequences of the resulting change in the nature of secret : only the keyword was now essential. Secondly, the cryptographic system had to be practiced in peace time as well as in war time, and to be taught in military schools:

> "The administration should absolutely abandon the secret methods, and establish in principle that it will only accept a process that can be taught openly in our military schools,……. it will be only when our officers would have studied the principles of cryptography and learned the art of decyphering, that they will be able to avoid many blunders […] to which are necessarily exposed all the profane" [KER I, p. 14-15].

Teaching was a new step in the transmission and diffusion of cryptography, producing textbooks in a more systematic way. In France, Kerckhoffs had effective consequences on cryptography, which was regularly cultivated at the *Ecole Polytechnique* at least until the World War I. Several authors of this school produced textbooks, new methods and even plans for mechanical designs. In 1888 for instance, Gaétan de Viaris (1847-1901), in four papers published in an engineer journal, *Le Génie Civil*, theorized the algebraic approach of Babbage, writing the four possible forms of cryptographic equations related to Vigenère's cypher. In June 1918, the French Captain Georges-Jean Painvin (1886-1980), from the same *Ecole Polytechnique*, broke the cypher of the famous "Victory Telegram", which resulted in the failure of the last German offensive. And even if cryptography was less cultivated in France after World War I, Colonel Marcel Givierge (1871-1931) – later to be General – produced an important *Cours de Cryptographie* in 1925, which would be part of Shannon's training manuals [GIV].

Nowadays, cryptological textbooks refer to the laws of Kerckhoffs in a mathematical form. For instance, a report intended for computer engineers asserts : "the laws of Kerckhoffs assert that the security of a system stemmed form the secrecy of the key, not from the secret of the algorithm". But this is an anachronistic interpretation of Kerckhoffs, as there was neither trace of mathematics nor of algorithm in Kerckhoffs' text.

2. The security of teletype transmission

The unbreakable system of Gilbert Vernam (1890-1960), known as the "one-time-pad system", came from trade affairs. Vernam was neither a linguist nor a mathematician, but an engineer. He was in charge of the security of teletypes for secrecy for sale at the *American Telephone & Telegraph Company* (AT&T) in Manhattan from 1915. Once more, il is impossible to find any trace of algorithm in his patent filed in 1919. This patent described rather the operations which occurred inside the teletype, as the process was entirely mechanized.

With a teletype, the transcription of telegraph operations becomes automatic. It uses the keyboard of a typewriter and a printing device. The text is stored on a perforated tape. Characters are encoded by the code of Émile Baudot (1845-1903), invented for teletypes, named telegraphic code, or "Alphabet International CCIT n° 2". These teletypes were widely used until 1980 by news agencies.

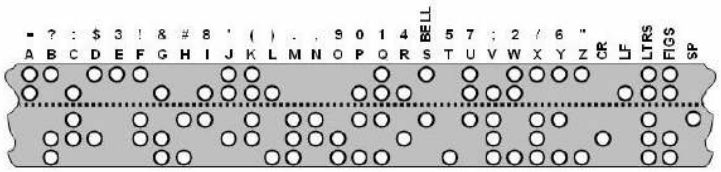

Fig. 7. Alphabet perforated on a tape according to the Baudot code.
http://luthorien.altervista.org/Tools/images/baudot.jpg

Each character of the alphabet is coded by five binary units. The electrical flow – or its lack – drilled – or not – a hole through the ribbon, what Vernam symbolized by a "+" or a "–". A special coding also symbolized the switching from figures to letters. So, the Baudot code could represent 60 characters.

A + + – – –	B + – – + +	C – + + + –	D + – – + –
E + – – – –	F + – + + –	G – + – + +	H – – + – +
I – + + – –	J + + – + –	K + + + + –	L – + – – +
M – – + + +	N – – + + –	O – – – + +	P – + + – +
Q + + + – +	R – + – + –	S + – + – –	T – – – – +
U + + + – –	V – + + + +	W + + – – +	X + – + + +
Y + – + – +	Z + – – – +	3 – – – + –	4 – + – – –
8 + + + + +	(+)+ + – + +	9 – – + – –	/ – – – – –

(3 = carriage return, 4 = line feed, 8 = letter shift, + = figure shift, 9 = space, / = null)

Fig. 8. How Vernam symbolized the alphabet perforated on a tape according to the Baudot code.

Therefore, coding remained linked to the existence of the perforated tape on which the marks of this coding were carried. Transmission of messages on such perforated tapes introduced new security problems.

> "This invention relates to signaling transmission and especially to telegraph systems. Its object is to insure the secrecy in the transmission of messages and further, to provide a system in which messages may be transmitted and received in plain characters or a well-known code but in which the signaling impulses are so altered before transmission over the line that they are unintelligible to anyone intercepting them" [VER, p. 1 lines 8-17].

The key is coded on a second perforated tape of the same length as the original message, and its marks are generated randomly. It is no longer a word of the language, but it is not yet a mathematical object. The machine combines each mark of the tape message with the corresponding mark of the key tape in an electro-mechanical way, without any human intervention. The combination rule is as follows :

hole	[after]	hole	[gives]	space
hole	[after]	space	[gives]	hole
space	[after]	hole	[gives]	hole
space	[after]	space	[gives]	space

Today, this can be translated by the operator XOR– exclusive or – or by the *modulo* 2 addition of figures 0 and 1. Here, Vernam wrote as an engineer speaking to other engineers facing a mechanical issue : the automation of cyphering. His patent described it in strictly technical terms, and only with an example :

> "Let us suppose that the first character of the message to be transmitted is « A ». The code signal of « A » is « ++---- », where « – » represents an « open » or « spacing » impulse and « + » represents a « closed » or « marking » impulse …. The code for the letter « B » is « +—++ ». The sending of « A »…..means that the contacts 25 and 26 will be closed, while the contacts 27, 28 and 29 are open. ….. The presence of the letter « B » in the code transmitter means that contacts 36, 39 and 40 ….. will be in contact with the bus-bar 32, which is connected to battery, and that contacts 37 and 38 …. will be in contact with the bus-bar 33 which is grounded" [VER, p. 8 lines 4-39].

The main interest of this invention was that the cyphering operation was the same as the decyphering one : for each mark, combining the key symbol with the cryptogram symbol gave back the plaintext symbol. As cyphering and decyphering were identical operations, only one type of mechanism was needed, and human intervention was eliminated from the communication circuit. So, the risk of all errors was reduced accordingly. But the key must be used only once, what Vernam still described with an example. In fact, if the same key was used twice, as the combination of a key symbol with itself was null, the combination of corresponding symbols from two cryptograms would give the same result as the combination of corresponding symbols from the plaintexts. And if one plaintext can be known by another way, the other one can easily be read by still adding the cryptographic equation.

This cryptographic system was adopted by AT&T as early as 1917, and also by the Navy whose equipment was built by the Western Electric Company, a manufacturing company of AT&T. In 1918, Major Joseph O. Mauborgne (1881-1971), from the Armed Signal Corp. established that the only safe key was "endless and senseless", that is a random key, equal in length to the message itself [KAH, p. 398], so that no regularity at all could be used to apply the frequency analysis on any sub-message. Shannon would establish the proof of this assertion in his theory of information [SHA2, p. 682].

But the enormous number of key tapes to be transmitted hindered a universal use of this very safe and very efficient system. It was reserved for communications with a high degree of confidentiality, for example between President Roosevelt and the British Prime Minister Churchill during the World War II, or for the "Red Phone" during the Cold War. Anyway, Vernam cypher signed the birth of automatic cryptography.

3. Some mathematical breakthroughs in Cryptology

From Kerckhoffs breakthrough, the notion of "cryptographic system" became central. In 1888, the naval officer Gaétan de Viaris (1847-1901), a marquis of Italian origin, graduated at the *Ecole Polytechnique,* published four papers on cryptography under the heading "Variétés" in the engineers' journal *Le Génie Civil*. Recalling Kerckhoffs' *desiderata*, he focused on the compatibility between cryptographic methods and the efficiency of their telegraphic transmission. Moreover, he wrote the four possible forms of cryptographic equations related to Vigenère type of cyphering. So, he generalized Babbage's algebraic approach:

> "Let c, χ, γ respectively denote the letters of the plaintext, of the cryptogram and of the key. They will also denote the numerical values of these letters.
> From the cryptographic equation - .... we can derive the 4 following equations:

(1) $c + \gamma = \chi$
(2) $26 + c - \gamma = \chi$
(3) $\gamma - c = \chi$
(4) $26 - (c + \gamma) = \chi$

... , It will be recognized that equation (1) $c + \gamma = \chi$ represents the Vigenère system, and that equation (3) $c + \chi = \gamma$ represents the Beaufort system. Equations (2) and (4) differ from (1) and (3) only by the substitution of the letters γ of the key by their complementary value $26 - \gamma$.

(...) The interest of these tables is purely theoretical, we have only wanted to show that the equation $c + \gamma + \chi = \lambda$ is, to some extent, the synthesis of the primitive equations, and of simple application; it is more general, more flexible. It introduces a new element λ into the relation between c, γ, χ, the element λ being in fact a new unknown. Two fixed elements being given: a telegraphic text […], and a key agreed in advance – and so not modifiable –, we can obtain as many encrypted texts as the different values λ can take. Moreover, if we consider the construction of a reversible cryptographic apparatus, cyphering and decyphering, we may choose this equation as the principle of the apparatus, because of its perfect symmetry [VIA, p. 38].

In spite of the plans he gave for such a cyphering machine, with a printing system on paper tape, De Viaris' attempt to present Vigenère cypher in a mathematical way did not lead to any new cryptographic system: it was just a new theoretical presentation of cryptography.

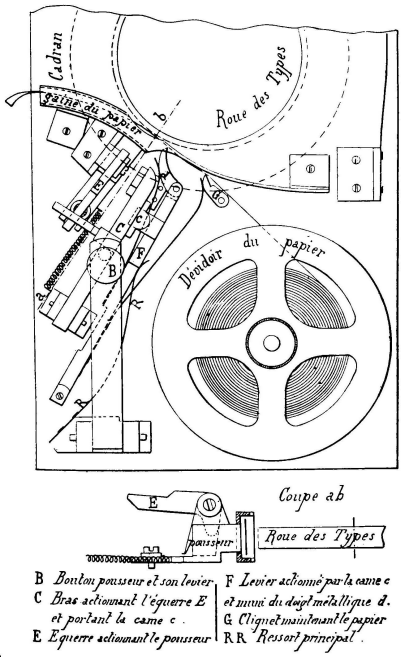

Fig. 6. Plate pf the cyphering machine by De Viaris.
Le Génie civil, 1rst of september 1888, Tome XIII, N° 18, p.279.

Anyway, these attempts for mathematically translating cryptographic processes did not occur continuously. Forty years later, in 1929, the mathematician Lester S. Hill (1890-1961), then assistant professor at Hunter College in New York, published in the *American Mathematical Monthly* a paper entitled "Cryptography in an Algebraical Alphabet". It was the first systematic use of cryptography in algebra in a mathematical journal. The article opens with an explicit reference to the congruence of Gauss, and translated cryptographic processes in mathematical operations in modular arithmetic:

"Let a_0, a_1, ..., a_{25} denote any permutation of the letters of the English alphabet; and let us associate the letter a_i with the integer i. We define operations of modular addition and multiplication (*modulo* 26) over

the alphabet as follows: $a_i + a_j = a_r$, $a_i * a_j = a_t$, where r is the remainder obtained upon dividing the integer $i + j$ by the integer 26 and t is the remainder obtained on dividing i * j by 26. The integers i and j may be the same or different" [HIL 1929, p. 306].

Hill used matrix with which several letters could be cyphered simultaneously. In his paper, he gave examples in dimension 3 and 4. But here is an example in dimension 2.With this cyphering of letters:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
17	9	22	6	7	18	15	24	21	5	4	16	2	3	10	8	19	20

s	t	u	v	w	x	y	z
25	13	12	23	1	14	11	0

numbers can be assembled by pairs which are considered as components of vectors. The cyphering matrix transforms these vectors into other vectors which are in turn transcribed in letters. The operations are performed *modulo* 26. Thus, for the plaintext message *Mississippi* and this cyphering matrix:

$$\begin{pmatrix} 2 & 3 \\ 23 & 17 \end{pmatrix}$$

the two first letters *M* and *I* are cyphered by the vector (2, 13) and the cyphering matrix changes it into (67, 40), that is (15, 13) *modulo* 26, which gives the letters *g* and *r*. The same method applied to successive bigrams of the plaintext leads to the cryptogram *gtiuthbcxpdq*.
To decipher this cryptogram, just apply the inverse matrix:

$$\begin{pmatrix} 1 & 9 \\ 17 & 20 \end{pmatrix}$$

Of course, it is necessary that the cyphering matrix be invertible, that is to say that its determinant is invertible in the ring of integers *modulo* 26. In other words, it has to be coprime with 2 and 13.

Setting the Hill system was very laborious for operators and the lack of mechanical means resulted in frequent errors. Hill patented a device that could cypher blocks of 6 letters. It had a series of gears connected by a chain, and was secretly used by the US government to cypher radio code trigrams [KAH, p. 408]. At the end of the World War II, Hill was involved in the teaching staff of the short-lived US Army University in Biarritz (France), which was part of a more general program of education for the GI soldiers staying in Europe. His major contributions to the US Navy and State Department systems of code were only revealed after his death.

Hill's work had a significant impact. Formulating previous cyphering systems in mathematical terms revealed their weaknesses and suggested new techniques for decyphering. Mathematicians were very interested by this work, particularly Adrian Albert (1905-1972), the director of communication division at the *Institute for Defense Analysis* (IDA). He highly appreciated the elegance and power of hill’s work, and gave the name « Hill cypher » to his polygraphic system. At the meeting of the *American Mathematical Society* in 1941, Albert claimed that he switched cryptology on the mathematical side:

"We shall see that cryptography is more than a subject permitting mathematical formulation, for indeed it would not be an exaggeration to state that abstract cryptography is identical with abstract mathematics" [KAH, p. 410]

4. Cryptology and theory of information

The lasting connection between mechanization and mathematization of cryptology took place during World War II, in several conflicting countries. In the USA, it was essentially led by Claude E. Shannon (1916-2001), both engineer and mathematician, best known for the enormous impact of his theory of information on digital technologies today. This double skill had obvious consequences on his works.

In 1936, Shannon joined the *Massachusetts Institute of Technology* (MIT) in Boston as an assistant in the research group of Vannevar Bush (1890-1974), where had been designed and built the first working differential analyzer in 1927. Shannon was in charge of the maintenance of this impressive machine designed to approximate graphically numerical solutions of differential equations. The circuits of this machine connected analog integrators to mechanisms for operations, with many feedback loops. Shannon worked to simplify its logical organization to avoid breakdowns and to optimize its running. In his master thesis, "A symbolic Analysis of Relay and Switching Circuits" (1937), he established a "perfect analogy" between these circuits and the propositional calculus of Boole's logic he had studied at the University of Michigan. This paper provided for the first time a common language for mathematicians and engineers working on mathematical machines: the language of binary operations on 0 and 1. It was immediately used at the *Bell Telephone Laboratories*, where Shannon worked from 1941 to 1956. He deepened his mathematical research, both in "A Mathematical Theory of the Differential Analyzer" (1941) – which plays an essential role in the control of large analog computers – and in his Ph. D. directed by Bush, "An algebra for theoretical genetics" (1942).

Analog Between the Calculus of Propositions
and the Symbolic Relay Analysis

Symbol	Interpretation in relay circuits	Interpretation in the Calculus of Propositions
X	The circuit X.	The proposition X
0	The circuit is closed	The proposition is false
1	The circuit is open	The proposition is true
X + Y	The series connection of circuits X and Y	The proposition which is true if either X or Y is true
XY	The parallel connection of circuits X and Y	The proposition which is true if both X and Y are true
X'	The circuit which is open when X is closed, and closed when X is open	The contradictory of proposition X.
=	The circuits open and close simultaneously	Each proposition implies the other

Fig. 7. Shannon, « A symbolic Analysis of Relay and Switching Circuits [SHA1, P. 475-76]

As of 1940, Shannon joined the *Office of Scientific Research and Development* (OSRD), which coordinate research between universities, industry and Defense, directed by Vannevar

Bush himself. He developed both an anti-aircraft machine gun[6], M-9, and a secret speech digital processing system, the X-Project. So, he had the opportunity to compare the analog signal and the digital cypher system. These parallel researches led him to identify the uncertainty coming from noise in the signal transmission, and the uncertainty coming from the ignorance of the key by the cryptanalyst. In his two crucial publications, "Communication Theory of Secrecy Systems" (1949), written in 1946, and "Mathematical Theory of Communication" (1948), Shannon treated an encrypted system and a noisy communication channel with the same mathematical framework. The diagrams exhibited in these two papers are significant of this similarity between the two systems.

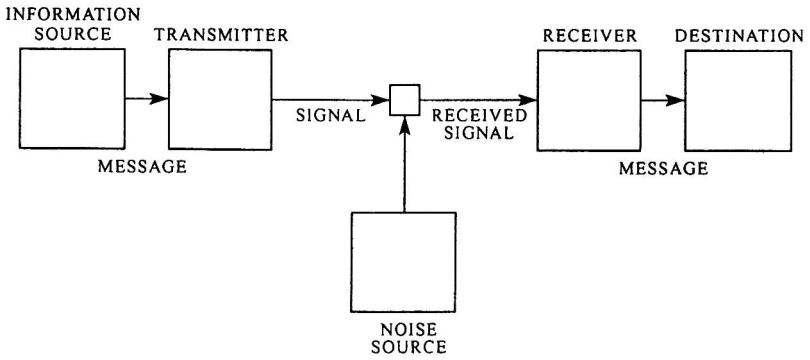

Fig. 1—Schematic diagram of a general communication system.

Fig. 8. C. E. Shannon, "A Mathematical Theory of Communication" [SHA3, p. 380]

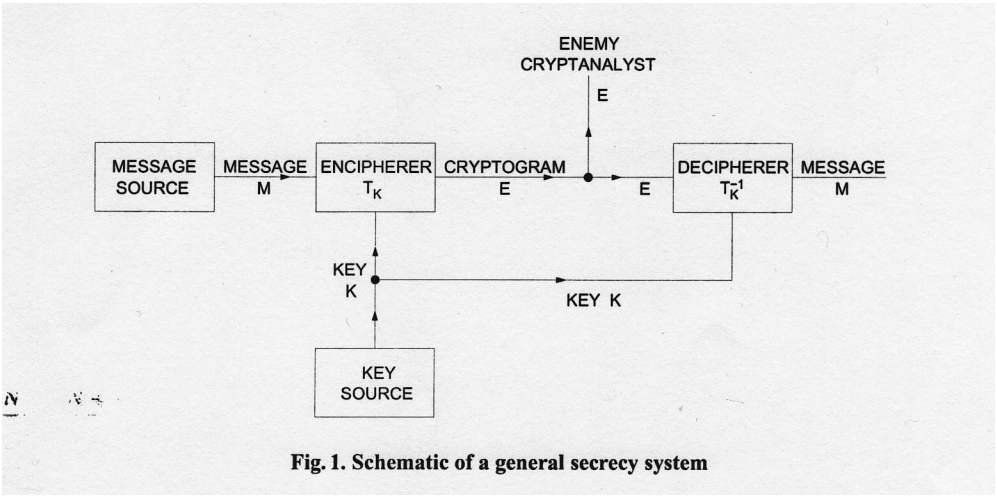

Fig. 1. Schematic of a general secrecy system

Fig. 9. C. E. Shannon, "Communication Theory of Secret Systems", [SHA2, p. 661]. .

Before Shannon's work, Ralph V.L. Hartley (1888-1970), Harry T. Nyquist (1889-1976) and Alan M. Turing (1912-1954), had already introduced logarithms to represent the additive character of information. But Shannon went further as he founded a probabilistic definition of the "amount of information", essentially relied on an experimental approach:

---

[6] Ninety units of this machine were sent to England, where they helped to destroy one quarter of German missiles V 1. Nine hundred units were at work during D-Day [SEG, pp. 93-95].

"Suppose we have a set of possible events whose probabilities of occurrence are p_1, p_2, ….., p_n. *These probabilities are known but that is all we know concerning which event will occur*. Can we find a measure of how much "choice" is involved in the selection of the event or of how uncertain we are of the outcome?
If there is such a measure, say $H(p_1, p_2, ..., p_n)$, it is reasonable to require of it the following properties:
1. H should be continuous in the p_i.
2. If all the p_i are equal, $p_i = 1/n$, then H should be a monotonic increasing function of n.
3. If a choice be broken down into two successive choices, the original H should be the weighted sum of the individual values of H ……
Theorem 2: The only H satisfying the three above assumptions is of the form:

$$H = -k\sum_{i=0}^{n} p_i \log_2 p_i$$

where K is a positive constant" [SHA3, p. 385].

Then, Shannon chose $k = 1$ in order to identify this formula to the definition of the entropy of a system, previously obtained in statistical mechanics. This mathematical definition measures the number of choices that a message represents among all possible messages, p_i being the probability of occurrences of each of them. It relates to the cryptanalyst seeking to recover the plaintext from the cryptogram, and to the engineer as well, facing to the noise which disturbs the quality of transmission. For the first time, Shannon considered noise as a random variable.

The level of abstraction of Shannon's two papers is quite remarkable. Shannon dealt with the latest developments of mathematical set theory, function theory, measure theory and probability theory. But this level of abstraction is also rooted in the injunction of the military authorities not to reveal anything that could indicate possible applications.

A secrecy system is defined as a set of operations or transformations T_i , from the set of all possible messages to the set of all possible cryptograms. The cryptogram E is the image of a message M by such a transformation T_i characterized by the key i – which is now clearly random – such that:

$$E = T_i (M)$$

Shannon made clear that these transformations must have a unique inverse, so that, while deciphering, a unique plaintext message can be recovered from the cryptogram by this reverse transformation:

$$M = T_i^{-1} (E)$$

Then, he defines two combining operations, which allow him to define the set of encryption systems as a linear associative algebra, and to analyze the composition of simple systems in complex systems. Various known cyphering modes, from Caesar to Vernam were then reinterpreted in this mathematical formulation. *A priori* probabilities were associated with each key and each message, which the cryptologist knows from the stochastic nature of natural language. If, for example, the possible messages are the sequences of letters of length N in a language, the *a priori* probabilities are nothing else but the frequencies of the letters of that language. Shannon also defined *a posteriori* probabilities:

"If the enemy intercepts the cryptogram, he can calculate from it the *a posteriori* probabilities of the various possible messages and keys which might have produced this cryptogram. This set of *a posteriori* probabilities constitutes his knowledge of the key and message after the interception. "Knowledge" is thus identified with a set of propositions having associated probabilities" [SHA2, p. 649].

Shannon's stochastic view of language supported new concepts, particularly "confusion" and "diffusion", which will help to secure the quality of the cyphering functions. In natural language, each of these probabilities depends on previous choices, allowing to characterize the entire sequences of letters as a discrete Markov process, which is assumed to be ergodic, that is to say statistically homogeneous. This leads also to the famous concept of redundancy, which allows both to theorize the work of a cryptanalyst and to tackle noise in communications systems:

> "Associated with a language there is a certain parameter *D* which we call the redundancy of the language. *D* measures, in a sense, how much a text in the language can be reduced in length without losing any information. As a simple example, since *u* always follows q in English words, the *u* may be omitted without loss. Considerable reductions are possible in English due to the statistical structure of the language ….. Redundancy is of central importance in the study of secrecy systems" [SHA2, 49 p. 656-57].

Redundancy measures the fact that the number of transmitted symbols is greater than what is strictly necessary to understand the message. So, it can be used to correct transmission errors, for instance to replace the word "endependance" by "independence" at the reception or decyphering a message. In natural language, the syntax is a source of redundancy. This redundancy can help the cryptanalyst to complete his work from sufficient information to guess the rest of the words. A text with little redundancy will require a longer cryptogram. Moreover, the error correcting codes add redundancy to the transmitted symbols in order to correct errors automatically. In most cases, it is only the redundancy that ensures the uniqueness of the solution. Shannon established the required amount of cryptogram to ensure this uniqueness; he called it the uniqueness distance. In parallel, for telecommunications, Shannon sought to reduce the frequency bandwidth by relying on the fact that the human voice is very redundant. Between cryptology and communications, redundancy plays an opposite role: the cryptanalyst seeks to obtain a null redundancy, while the communication engineer is looking for a high redundancy.

It is often said that the measure of the amount of information implies that Shannon gave up any reference to the meaning of messages. We would rather say that his view changed the way to consider meaning. He first considered meaning from the engineer's view:

> "[The] semantic aspects of communication are irrelevant to the engineering problem. The significant aspect is that the actual message is one selected from a set of possible messages. The system must be designed to operate for each possible selection, not just the one which will actually be chosen since this is unknown at the time of design" [SHA2, p. 379].

But in his two main papers, Shannon's writing style reflects the constant attention he paid to the meaning of probabilities he introduced. The mathematical statements of his theorems are systematically translated in the language of the engineer. And he doubts the relevance of the term "enemy", because of its military origin. Indeed, the question of meaning did not disappear at all from Shannon's work, but the formula defining the amount of information makes explicit the change which occurred on the notion of system by Shannon's mathematical conceptualization. It does not relate anymore to the content of individual messages within the system, but it concerns exclusively the set of all possible messages with all possible keys, and it intends to clarify the conditions that will allow to control the communication system as a whole, seen from outside. Shannon clearly raised the issue of the place of enunciation, but from a technical point of view. It is essential to understand what is at stake in a cryptographic system, and it is unfortunately overshadowed when cryptographic textbooks focused on the communications only between two persons, usually "Alice and Bob".

This issue would be raised again later, from a philosophical point of view, in the debates on the meaning of "autonomy" in cybernetics.

At the same time, in Poland in the 1930s and in Great-Britain during World War II, reading the Nazi messages encrypted on the Enigma machine and on the Lorentz machine also induced the junction of mathematics and mechanical devices for cryptanalysis. The history of this episode is important enough to be analyzed in a separate second paper.

5. Cryptosystems for computing in the binary language

After World War II, the notion of algorithm gradually became established in the practice of computers, first in wired form, then as an integrated program. This notion was not a new one: it had always been associated with numerical problems in mathematics, particularly since the use of series to approximate functions. What was new was its implementation in machines. The increasing use of computers in large networks needed cryptography to be developed on a new scale, and the nature of secrecy still changed in several ways.

In the United States, when Horst Feistel (1915-1990) wrote in 1973 that computers "now constitute, or will soon constitute, a dangerous threat to individual privacy", he was not anxious for "lovers and thieves", but for the security of international trade and free competition between companies. The issue was no longer solely a concern for “military men and diplomats", it became of "public concern" [FEI, p. 15]. Pressed by a growing civil demand for standardization, particularly from banks, the *National Bureau of Standards* (NBS) promoted the publication of cryptographic algorithms.

Feistel was one of the first non-government researchers to work on the theorization of encryption systems on computers. He studied physics at the MIT and worked successively in cryptology for the *Air Force Cambridge Research Center* (AFCRS) and for the Thomas Watson Research Center of the firm *International Business Machines* (IBM). Feistel developed new cyphering architectures in this context, particularly the algorithm *Data Encryption Standard* (DES), which was the first public encryption algorithm. The NBS launched a call for tenders in 1977 to produce a cryptographic system to be used by companies, and *IBM* won the competition.

In this algorithm, Feistel fully mobilized the binary encoding writing and the concept of algorithm. His block cypher was founded on the idea of splitting the message in two blocks, and performing on each on them a combination of successive encryptions by alternating substitutions and permutations. Substitutions ensured what Shannon defined as the "confusion" of probabilities associated with the initial letters of the message, by changing the number and the distribution of the symbols 0 and 1. Permutations generated the "diffusion" of probabilities by mixing symbols. These transformations were carried out electronically, and repeated on several layers through which the message was crossing. The LUCIFER system, one of the first Feistel algorithms, used blocks of 128 binary symbols, and a key of the same length. At the exit, the symbols resulted from very sophisticated functions, especially non-linear functions, of all input symbols [FEI, p. 21].

The transmitted message is supplemented by several other elements:
- a password to ensure its authenticity,

- a correcting code to curb possible garbles over transmission,
- and another password to restrict the exchange of messages to a predetermined group of recipients.

The block cipher judiciously mixed the figures of the original message with these additions, so that someone foreign to the system could not distinguish them. Thus, Feistel encryption combined the strength of the encryption system with a good resistance to the accidental or intentional corruption of messages.

The publication of the DES marked a turning point: it was the first public encryption algorithm. This was not without risk: it corresponded to a reasonable choice only if the algorithm on which the encryption mode is safe. But the intervention of the NSA (*National Security Agency*) in the ultimate design of the DES led its users to suspect the existence of « backdoors » or traps that would have allowed this institution to break the system. DES was, however, the most used encryption system with a secret key for twenty years. In 1997, the significant increase in the power of computers made possible to find the key by exhaustive computation. So the NSA standardized successively a triple DES and a AES system (*Advanced Encryption Standard*) in 2000, this time by an international call for tenders.

6. Public key cryptosystem

Even if the cryptographic algorithm was now public, all the problems arising from computer networking were not resolved. As communications became electronic, as increasing trade produced such a change of scale in exchanges, the transportation and distribution of keys between protagonists "from one end to the other of the planet" [DIF-HEL] became an enormous problem. To sign agreements and settle transactions required not only to ensure the confidentiality of messages, but also their authenticity. In 1976, Whitfield Diffie (born 1944), a graduate of the MIT, with Martin E. Hellman (born 1945), professor at Stanford University, inaugurated the public key cryptography and announced a "revolution in cryptography". They started from Shannon's and Feistel's view of a cryptographic system as a family of invertible transformations, and imagined new solutions involving two keys, one public and one secret:

> "In public key cryptosystem enciphering and deciphering are governed by distinct keys, E and D, such that computing D from E is computationally infeasible (e.g., requiring 10^{100} instructions). The enciphering key E can thus be publicly disclosed without compromising the deciphering key D.…. A third party eavesdropping on this exchange must find it computationally infeasible to compute the key from the information overheard" [DIF-HEL, p. 29].

"Computationally infeasible" means that the "cost measured by either the amount of memory used or the running time is finite but impossibly large". So, the mathematical expression of the security conditions of electronic exchanges for cryptosystems induced to distinguish the security level of cryptosystems according to the kinds of attack which it has to resist to. And new concepts can still be defined, founded on the theory of algorithms and of complexity, such as authentication of the user, digital signature, backdoors.

These concepts relied on encryption by a one-way function, for which it is computationally impossible to get the pre-image of an element. The inverse function is however accessible to the holder of an additional information, known only to him, called backdoor. In a public key cryptosystem, the secret key uses this backdoor, but a malicious designer could divert the method for producing a backdoor encryption, by which he could

"break the system after he has sold it to a client and yet, falsely to maintain his reputation as a builder of secure systems" [DIF-HEL, p. 37].

Nevertheless two more years with further research were needed to achieve Diffie and Hellman's ambitions, that is to say to find relevant one-way functions. The RSA system, named after its authors Ronald Rivest (born in 1947), Adi Shamir (born 1952) and Leonard Adleman (born 1945), is founded on the difficulty of factoring large integers. Cryptology now invests mathematical problems known to be difficult to solve, within algebra and number theory. Interactions between cryptology and mathematics actually go further with the use of algebraic geometry: elliptic curves and pairings of points enable to obtain new cryptographic functions.

7. Cryptographic theory and proofs of security

To appreciate the value of a new system has always been a central issue for cryptographers. Since Diffie and Hellman reformulated cryptography in mathematical terms, the security of cryptographic systems, named "proven security" – is supposed to be ascertained by mathematical theorems. The principle of such proofs is to reduce a successful cryptographic attack to a difficult mathematical problem. In fact, it is a conditional security, meaning that "this protocol is immune to an attack of type X only if the mathematical problem Y is computationally difficult". As long as the mathematical problem does not have a solution accessible in practice, the attack of the system is thus ascertained unsuccessful.

The major problem with this kind of evidence is that the existence of intrinsically difficult problems is not established. Of course, the multiplication of large prime numbers appears today as a one-way function, because multiplication has a polynomial complexity, whereas the best algorithms known to factorize the product have a strictly superior complexity. But no one knows if an effective algorithm could be found tomorrow. To date, neither the existence nor the non-existence of such an algorithm has been demonstrated.

Since public keys were designed, a community of cryptographic researchers relies on the mathematical analysis of algorithms to establish cryptography on a theoretical basis. They try to establish cryptographic activity as a science to ensure user confidence. But as the security proofs are conditional, the possibility of reducing cryptography to these theoretical foundations becomes problematic. For Neal Koblitz, for example [KOB], these proofs, which he prefers to describe as arguments, are used to impress those who are strangers to the field and who have little understanding of their true meaning, especially users. Between cryptologists and mathematicians, each group invests the status of the other to endorse its own development, both symbolically and financially.

Conclusion

This paper shows that the introduction of mathematics within cryptography and cryptanalysis needed a long process and specific reasoning of their manual and mechanical practices. Cryptology now invades a large scope of our daily practices, either in computing or in every day life. Yet, as it has been practiced in military circles during very long periods, it still functions in a way that maintains some features of war context, such as secret communications inside reserved groups, or the habit to consider those outside of the system as

enemies. It also stops us from thinking about the consequences of these secret practices, as the recent Snowden affair revealed. So perhaps everyone among us would gain to think more about the use of cryptology: it would be important for democracy.

References

[ALB] Alberti, L. B., 2000, « De cyphris », *Actes du Congrès International de Paris,* held in 1995,, edited by F. Furlan, P. Laurens, S. Matton, Paris, Vrin, et Turino, Nino Aragno editore, 2000, pp. 705-725, éd. F. Furlan & al.

[BAB] Babbage, Ch., n. d., « Philosophy on Deciphering », manuscript, London, British Library, Add. Mss. 37205.

[BEL] Belaso, G. B., 1553, *La cifra del sig. Giovan Battista Bellaso, gentil'huomo bresciano, nuovamente da lui medesimo ridotta à grandissima brevità et perfettione*, Venetia, 1553.

[DEL] Delahaye, J.-P., 2003, « Viète, inventeur de la cryptanalyse mathématique », *Pour la Science*, n° 313, novembre 2003, pp. 90-95.

[DUR-HEL] Diffie (W] et Helmann M., 1976, « New Directions in Cryptology », *IEEE Transactions on Information Theory*, 1976, vol. 22, n° 6, pp. 644-654.

[DUR-GUI] (eds) Durand-Richard, M.-J. et Guillot, Ph., 2014, *Cryptologie et mathématiques, une mutation des enjeux,* Paris, L'Harmattan, 2014.

[FEI] Feistel, H., 1973, « Cryptography and Computer Privacy », *Scientific American,* 1973, vol. 128, n° 5, pp. 15-23.

[FRA] Franksen, O. I., *Mr Babbage's Secret, the tale of a cypher and APL,* Vedbaek (Denmark), Strandberg Forlag, 1984.

[GIV] Givierge, M., 1925, *Cours de cryptographie,* Nancy-Paris-Strasbourg, éds Berger-Levrault, 1925.

[HEB] Hébrard, P., 2001, *La cryptologie dans l'Histoire,* volume 1, *Essai sur l'histoire secrète des chiffres de l'antiquité à la première guerre mondiale,* édition privée interne ARCSI.

[HIL] Hill, L., 1923, « Cryptography in an Algebraic Alphabet », The American Mathematical Monthly, Vol 36, n° 6, Juin-Juillet 1929, pp. 306-312

[KAH] KAHN, D., 1996, *The Codebreakers, the Story of Secret Writing*, New York, McMillan Publications, 1996.

[KAS] Kasiski, W., *Die Geheimschruftten und die Dechiffrir-Kunst,*

[KEL] Kelly, Th., 1998, « The Myth of the Scytale », *Cryptologia*, vol. 22, n° 3, july 1998, pp. 244-260.

[KER] Kerckhoffs, A., 1883, « La cryptographie militaire », *Journal des sciences militaires,* vol. IX, janv. 1883, pp. 5-38 ; vol. X, fév. 1883, pp. 161-191.

[KOB] Koblitz, N., 2007, « The Uneasy Relationship between Mathematics and Cryptography », *Notices of the AMS*, september 2007, vol. 54, n° 8, pp. 972-979.

[MRA] (eds.) Mrayati, M., Meer Alam, Y., & al-Tayyan, M.H., 2003, *Al-Kindi's Treatise on Cryptanalysis*, Riyadh, King Faisal Center for Research and Islamic Studies, 2003.

— id., 2005, *Ibn ad-Dunaynir's Book : Expositive Chapters on Cryptanalysis*, Riyadh, King Faisal Center for Research and Islamic Studies, 2005.

[PES] Pesic, P., 1997, « Secrets, Symbols and Systems : Parallels between Cryptanalysis and Algebra, 1580-1700 », *Isis*, vol. 88, n° 4, dec. 1997, pp. 674-692.

— id., 1997, « François Viète, father of Modern Cryptanalysis. The two Manuscripts », *Cryptologia*, vol. 21, n° 1, 1997, pp. 1-29.

[POR] Porta, G. Della, *De furtivis litteratum notis*, Naples, 1583.

[RAS] Rashed, R., *Entre arithmétique et algèbre : recherche sur l'histoire des mathématiques arabes*, Paris, Les Belles Lettres, 1984.

[SEG] Segal, Jérôme, Le zéro et le un, histoire de la notion scientifique d'information au 20e siècle, Paris, Syllepse, 2003.

[SHA1] Shannon, C. E., 1937, « A Symbolical Analysis of Relay and Switching Circuits », *Transactions of the American Institute of Electrical Engineers,* 1938, n° 57, pp. 713-723, *in Shannon's Collected Papers,* pp. 471-495.
http://paradise.caltech.edu/CNS188/shannon38.pdf

[SHA2] Shannon, C. E., 1946-49, « Communication Theory of Secrecy Systems », *The Bell System Technical Journal,* 1946-49, vol. 28, pp. 656-711.

[SHA3] Shannon, C. E., 1948, « A Mathematical Theory of Communication », *The Bell System Technical Journal*, july-october 1948, vol. 27, pp. 379-423 et 623-656.

[SUE] Suetoni, Tranquilii Vita Divi Iuli, http://bcs.fltr.ucl.ac.be/SUET/CAES/ texte.html.

[TRI] Trithème, J., 1518, *Polygraphiae libri sex, Ioannis Trithemii abbatis Peapolitani, quondam Spanheimensis, ad Maximilianum Ceasarem*, Oppenheim, J. Haselbergii de Aia, 1518.

[TUR] Turing, A. M., (ed.) Copeland, B. J., 20 04, *The Essential Turing, Smeinal Writings in Computing, Logic, Philosophy, Artifical Intelligence and Artifical Life, plus the Secrets of Enigma,* Oxford, the Oxford University Press.

[VER] Vernam, G., « Secret Signaling System », *United States Patent Office,* patented July 22, 1919.

[VIA] Viaris, G. de, « Cryptographie », *Le Génie Civil,*1888, tome XXIII, pp. 24-27, pp. 38-39, pp. 55-56, pp. 72-75, pp. 84-88, pp. 104-107.

[VIG] Vigenère, B. de, 1596, *Traicté des Chiffres, ou secrètes manières d'escrire*, Paris, Abel Langelier, 1596.