MATHEMATICIANS ON CRYPTOLOGY

Lada Stachovcová

> *All nature is merely a cipher and a secret writing. The great name and essence of God and his wonders, the very deeds, projects, words, actions, and demeanor of mankind – what are they for the most part but a cipher?*
>
> Blaise de Vigenère

Cryptology (i. e. the science concerned with message content encryption) is very old discipline and its history is closely associated with the history of communication. Author of this paper begs to dip into one of its stages, into Europe of the second half of the 16th century, with an effort to note encryption activies of men better known for their contributions to mathematics today.

Ancient times

The first known text containing intentional type transposition, one of the main characteristics of cryptology, is dated to ancient Egypt, 1900 BC. Its author, a scribe of nobleman Khnumhotep II, used uncustumary hieroglyphics without effort to hide content of the text, but to make it more serious and respectable. Later, epitaphs ciphered for the purpose of attracting passers and making them decipher the text content, were usual – Egyptians believed that the blessing contained in epitaph and read by another person was transfered to the deceased.

Situation in ancient India was rather different. Perhaps the most interesting mention about ciphers occured in well–known textbook of erotics, the *Kāma-sūtra*, where secret writing is one of the 64 arts that woman should know and practise.

But cryptology came into its own primarily in military and political diplomacy.

Ciphers on duties

In Europe, ciphers were ordinarily used in diplomatic services since the end of 15th century. Each country had its cipher ensemble, great cryptologists were also employed at the Pope's Court. These men were real crypto–professionals concentrated on practical problems of encoding and decoding. On the opposite side, there were amateurs concerned with ciphers as hobby. They worked out more theoretical methods, but their results affected cryptology much more later, at the end of 19th century.

A French lawyer **Françoise Viète** (1540–1603) belonged to the first group. Since August 1598 Viète worked as a royal private counsellor of French king Henry IV of Navarre. This was a period of French Wars of Religion. As a Protestant, Henry found himself in contest with Catholic Fraction – The Holy League, that refused the Protestant king and occupied Paris and other major cities of France. The League was supported by king Philip II of Spain, who wanted the throne of France for his daughter Isabela and, moreover, Philip was also of Catholic religion. And it just happened that an encoded letter, addressed to Philip and dated October 28, 1598, fell into Henry's hands.

Viète was certainly known for his mathematical abilities. As a Protestant, he was one of Henry's most loyal supporters and, moreover, it has been just one year since he had solved a Spanish message addressed to Spanish force headquarters of the Holy League, so Henry asked him to decode that letter.

The message was encoded using a method called *nomenclator*. It was the most used method in that time that consisted of monoalphabet substitution cipher and a list of codes. *Monoalphabet cipher* is a simple transformation of alphabet which the language uses to alphabet of cryptogram (ciphertext) – this alphabet could contain both letters or characters and digits. But this system causes that the letter frequency of language is transfered from message text (plaintext) to cryptogram and comparision of these frequencies makes the deciphering much more easier. Therefore letters with high frequency were substituted with more equivalents – this system is called *homophonic cipher*. Further nomenclator contained a code list of words, names or syllables that were also repeated in message more often.

Deciphering of nomenclator was laborious and lengthy. It required time, patience, and experience. Decipherer could follow up characteristic of the language and search for special pairs or trinities repeated in the cryptogram. It was also usual in that time that codelist had been made out in alphabetic order and so one could find some connections there.

Anyway, history shows that in many cases the nomenclator was cracked.

The message Viète had to decipher was encoded using a nomenclator that consisted of the usual alphabet with homophonic substitutions plus a code list of 413 terms (there were groups of letters: LO=*Spain*, groups of underline numbers: $\underline{64}$=*confederation* or dotted numbers: $\dot{9}\dot{4}$=*Your Majesty*). Moreover, the message contained so called *nulls* - null was a character which did not substitute any of characters of origin alphabets.

Despite Viète's experience and abilities it lasted more than four months to decipher the message. On March 15, 1598 Viète sent Henry the completely decoded letter (although he had previously submitted its pieces). However, though the letter contained intimate details of enemy's negotiations, Henry IV received its decoded version one day after the Battle of Ivry, where he had defeated enemy's superior forces.

Viète succesfully continued with letters decoding. (It is known Philip II was so exasperated by French awareness of his military plans that he complained to the Pope that black magic was being employed against his country. Though, Spanish ciphers were known to be obsolete so Philip's complaint yielded only derision to him.) But Viète's pride for his cryptoanalytic abilities caused he commited a diplomatic mistake. When he talked with Venetian Ambassador to France, he revealed so much about his knowledge of Venetian ciphers that the Ambassador reported it to the Venetian Council of Ten and The Council promptly changed their existing cipher.

Ciphers as amusement

Apart from men engaged in decoding of real messages there were learned persons concerned with ciphering from the theoretical point of view. They invented and developed another type of cipher to which most of today's systems of cryptography belong. This cipher is called *polyalphabet substitution* and as the name implies, it involves more cipher alphabets. In that time these alphabets were contained in so called *tabula recta* (see Table 1).

Each letter of message is ciphered using another row, i.e. alphabet. We could move row by row respectively – first letter cipher using first row, the second letter using the second row and so on and repeat this procedure over and over. Thus, for example, the sentence IN PRINCIPIO ERAT VERBUM is ciphered by this way:

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

Table 1: Tabula recta

plain	i	n		p	r	i	n	c	i	p	i	o		e	r	a	t		v	e	r	b	u	m
cipher	I	O		R	U	N	S	I	Q	Y	S	Z		Q	E	O	I		M	V	J	U	P	H

And because each letter of plaintext is ciphered with different alphabet, the frequency of characters in ciphertext is much more aligned. Better security of this system is guaranteed by the key word or sentences. The key is repeatedly written above the secret message and letters of the message are ciphered by rows starting with corresponding key letter. Chosen key word DOMINUS gives the folowing result:

key	D O	M I N U S D O M I	N U S D	O M I N U S
plain	i n	p r i n c i p i o	e r a t	v e r b u m
cipher	M B	B A V H U M D U X	R M S X	J Q A O P E

It is clear that a key that would change more often would provide more security than a key that is used over and over. The ultimate ideal, of course, is a key that changes with each message. One of the men who proposed to use the message itself as its own key was **Girolamo Cardano** (1501–1576).

Although among CARDANO's 131 publications none of them was explicitly devoted to cryptology, he provided some information and his own achievements on ciphering in two of these works – *De Subtilitate* (1550) and *De Rerum varietate* (1556). Both of these books were in fact popularization of science. Among others CARDANO described here the classic cipher methods of antiquity, gave some rules for solving messages and for developing secret link and also offered a few methods of his own.

One of these was his *autokey.* In polyalphabet cipher he employed the plaintext as a key to encipher itself, staring the key over from the begining with each new plaintext word.

key	S I C	S I C E	S I C E R G O E L
plain	s i c	e r g o	e l e m e n t i s
cipher	L R E	X A I S	X T G Q V T H N D

Although the autokey was a great idea, CARDANO formulated it defectively. First, the deciphering was not uniform. In alphabets contained in Table 1 cipher L could stand for a plaintext f keyed with an F as well as for plaintext s and key S. Second, and worse, the receiver was in the same position as cryptoanalyst because it is enough to decipher the first word of the plaintext and this will unlock the rest of the message. Therefore, CARDANO's system of autokey failed. (Later on, more effective autokey system turned up; reader is referred to name *Blaise de Vigenère* and any book about cryptology.)

Although CARDANO's autokey method did not function well and remained uninfluential, CARDANO made his contribution to cryptology with another system: a steganographic system which bears his name, so called *Cardano Grille.* Steganography is sometimes considered to be a part of cryptography. However, while cryptography aims to hide the content of the message, steganography targets message existence itself.

Cardano Grille is template of stiff material (for example cardboard or metal) with series of square or rectangular slots designed to fit over a standard sheet of paper. The sender writes his message in the slots, removes the grille and fills in the remaining spaces any innocuous–sounding cover message. The receiver simply places his grill on the message he has received and reads the text through the windows. The only problem with the grille is that sometimes the cover message would look strange and so betray the existence of a hidden message. This grille was very popular and number of countries used it in their diplomatic correspondence in the 1500's and 1600's.

Cardano's known interest in numbers and combinations was certainly the reason that encouraged him to attempt to evaluate all variations inherent in cryptographic system. He described a certain monoalphabetical substitution which could correspond to 27-letter alphabet and stated: *The number of possible arrangements of this alphabet will reguire 28 digits and such a number of arrangements could not be contained in many books.* It is not so important that he made a mistake (we have better tools for finding out that 27!, i.e. the number of permutation of 27-term set, require not 28 but 29 digits). But he considered this very large number of possibilities of realizing a cryptogram as *proof* of the impossibility that cryptoanalyst ever reaches a solution. This was rather misleading and, unfortunately, this faith in large numbers lasted for a very long time. Because as methods of cryptography develop, so the cryptoanalytic ones do, and resistence of cryptosystem against testing one key after another (*brute force attack*) is far to be guarantee of its safety.

References

[1] Kahn, D.: *The Code-Breakers.* Simon & Schuster Inc., New York 1996.

[2] Luger, J.: *Code Making And Code Breaking.* Loompanics Unlimited, Washington 1990.

Lada Stachovcová
Department of Mathematics
Masaryk University
Janáčkovo nám. 2a
662 95 BRNO
Czech Republic
e-mail: stlada@atlas.cz