posterus
Portál pre odborné publikovanie ISSN 1338-0087

History of cryptology – part 2.

Kolek Jan · Informačné technológie

14.11.2012

This article seeks to familiarize the reader with the history of cryptology from the first efforts of secret messages to the current use of ciphers to communicate in the world of information technology. The article provides a brief summary of the history of cryptology from the simplest methods of hiding codes and relevant message, in ancient times, when people began their correspondence secret, to some modern encryption algorithms currently used in the field of information technology, but also in other areas of human knowledge.

The work is divided chronologically by time of occurrence or discovery of the cipher (with a few exceptions due to consistency origin ciphers), but also depending on which part of the world appeared cipher, or where the code was extended and used. The text explains the basic principles of using simple ciphers to encrypt a short demonstration of text or an image for a better understanding of how the code worked. Also listed are enunciated and most important events and data related to cryptography and cryptanalysis.

2. Middle ages

In the middle ages there is a decline in the development of encryption. Exceptions are mainly Arab mathematicians.

2.1 The Byzantine Empire

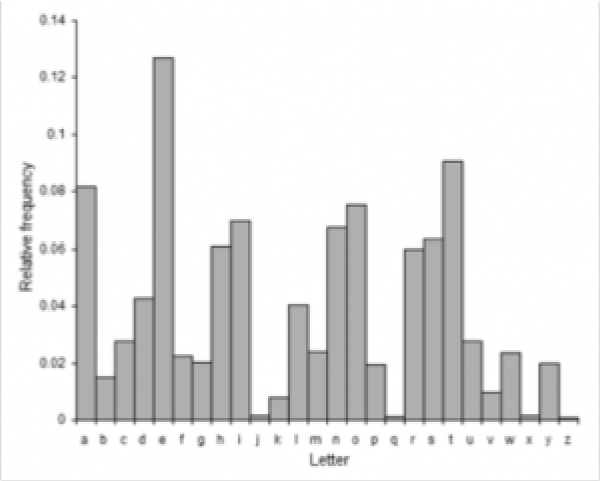
Around 750 AD, book was written for the Byzantine emperor dealing with the methods and procedures for encryption and decryption.

2.2 Arabian Peninsula

In 855 AD, Abu Bakr Ahmad wrote a summary of the known methods for encryption based on monoalphabetic substitution (substitution of one letter for another using only one alphabet). [2]

2.2.1 Frequency Analysis

The greatest discovery falling within the 9th cryptology century AD was the discovery of frequency analysis. Its discoverer was an Arab philosopher Abu al Josúf al Kindí. Frequency analysis is used to decipher monoalphabetic cipher using frequency sounds in words.



Picture 1.: Frequency Analysis

Every language has a certain frequency of occurrence of each alphabet character if you know the language in which the encrypted message is written, we can use frequency analysis to determine what the substitution was used. Frequency analysis is able to shorten the time solving monoalphabetic substitution of many years to a few tens of minutes. [4]

2.3 Europe

In Europe cryptology stagnated. Simple cipher, as substitution, replacing vowels different number of dots, and the like, are used only. Change came in the second half of the 14th century BCE.

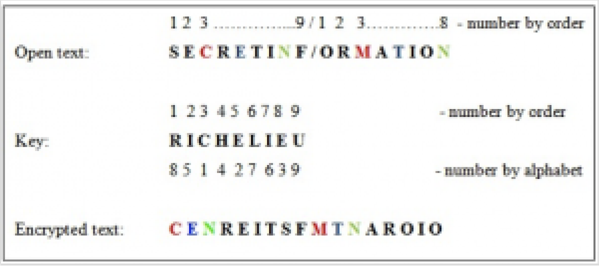
2.3.1 France

A) Gabrieli di Lavinde

Gabrieli di Lavinde created in 1379 for Pope set of 24 individual keys for communicating with different people. Set of keys in each merged the principles of homophonic substitution and file names and their code equivalents. This principle for encryption was after another 450 years of using in Europe. [1]

B) Cardinal Richelieu

Cardinal Richelieu used a simple transposition cipher using key words. Encrypted text number the first order. Number the key also in turn, but in addition it also according to number the order of the letters in the alphabet, as shown. We go by numbering the keys alphabetically from 1, 2, and 3 to end. Taking the third character from the encrypted text and give it to the first position. Furthermore, we take the fifth character and give it to the second position, and continue until the key length. If the encrypted text is longer than the key so it split into blocks of the same length as the key.



12 3 ....9 / 1 2 3.............8 - number by order

Open text: SECRETINF/ORMATION

1 23 45 678 9 - number by order

Key: RICHELIEU

85 1 4 27 639 - number by alphabet

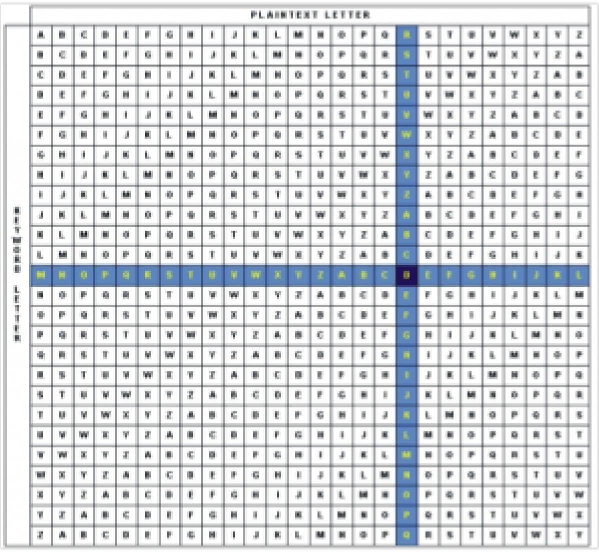
Encrypted text: CENREITSFMTNAROIO

Picture 2.: Cardinal Richelieu cipher

2.3.2 Germany

A) Johannes Trittheim

The founder of modern cryptography is considered a Benedictine abbot Johannes Trittheim of Spanheim. In 1518 he wrote the book “Steganography”. Principles of steganography encryption were described in his book. In these principles of steganography each letter is replaced with the letter in the table prepared in advance. In the same year he published the first printed book describes some of the known encryption systems called “Polygraphiae libri sex”. He described the table of alphabets and called it “Tabula recta.”



PLAINTEXT LETTER

KEYWORD LETTER

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

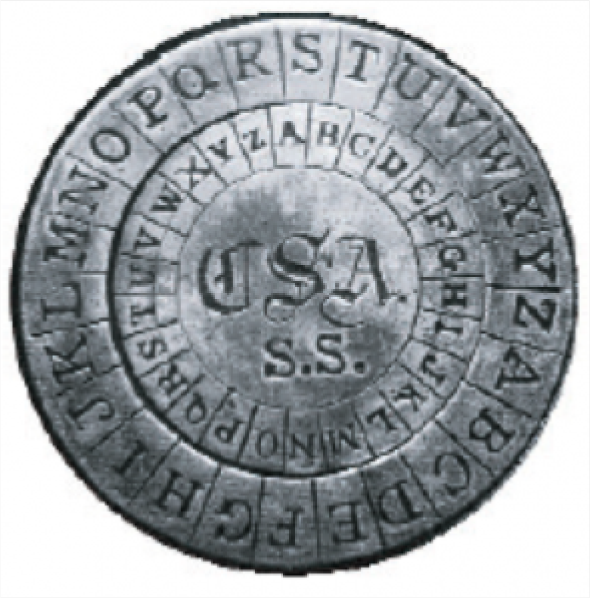
Picture 3.: Tabula recta

He used it to explain polyalphabetic encryption (use of multiple alphabets), but due to the greater effort encryption method has not reached practical use. Royal families, however, feared that revealed many secrets, he was declared a sorcerer in league with the devil. [1]

2.3.3 Italy

A) Leon Battista Alberti

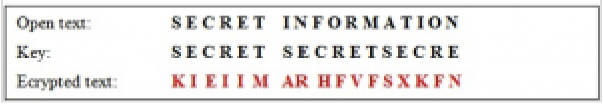
The most famous of his works is an essay written in 1467, where he introduced the basic principles of cryptanalysis, for example frequency of occurrence of various characters, using invisible ink, and so on. He was also prevents the possibility of deciphering codes. He proposed a method using multiple alphabets harder for breaking ciphers. This method is used for its disk encryption, which had two alphabets. The disc was made of copper and both alphabets could turn against each other, which increased the number of possible encryption of the text. For his great contribution to cryptography is called the father of cryptography. [1]



Picture 4.: Disk encryption

B) Geronimo Cardano

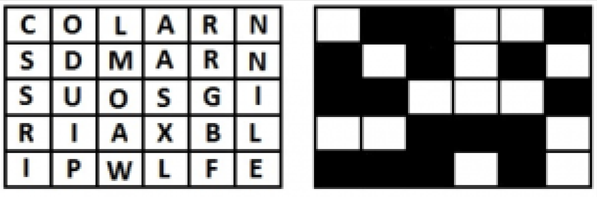
Milan physicist and mathematician Geronimo Cardano paid directly cryptology, but in two parts his works “De Subtiliate” and “De Rerum Varietate” he incorporate knowledge of cryptology. He described the ancient encryption methods, published instructions on how to secretly open foreign letters. Also created rules for solving ciphers, instructions for making invisible ink and also he added his own cipher. The first type of cipher was using the auto-key, when the key is taken as the actual beginning of cipher text for each separate word. For encryption used Tritteheim’s “Tabula recta”. [2]



Open text:	SECRET INFORMATION
Key:	SECRET SECRETSECRE
Ecrypted text:	KIEIIM AR HFVFSXKFN

Picture 5.: Auto-key cipher

The second type of cipher was the “Cardano’s grille”. In fact, it was the stenographic method, where the message was hidden in a number of other letters. When using the grid on the left text in right text is “Cardano’s grille”:



C	O	L	A	R	N
S	D	M	A	R	N
S	U	O	S	G	I
R	I	A	X	B	L
I	P	W	L	F	E

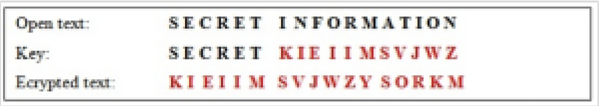
□	■	■	□	□	■
■	□	■	□	■	□
■	■	□	□	□	■
□	□	■	■	■	□
■	■	■	□	■	□

Picture 6.: Cardano’s grille

2.3.3 France

A) Blaise de Vigenére

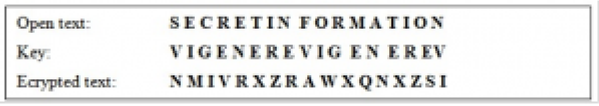
He was French diplomat who came from the work from Trittheim, Cardano and others. He published in 1586 work “Traicté des Schiffers”. The content of the book, although primarily focused on the occult sciences, but provided valuable information by quoting other authors. He mainly pursue to polyalphabetic ciphers. Among other things, improved Cardano’s car-key so he used only one word and another for encrypting already encrypted text used as the key, so as not to repeat the password.



Open text:	SECRET INFORMATION
Key:	SECRET KIEIIMSVJWZ
Ecrypted text:	KIEIIM SVJWZY SORKM

Picture 7.: Improved auto-key cipher

His own cipher, using repetitive slogans and “Tabula recta”, was more famous, even if repetitive password reduces the quality of ciphers. The polyalphabetic cipher became famous because they resist breaking almost 300 years. Still bears the name “Vigenére’s cipher” and is to some extent result of the historical development of ciphers. [5]



Open text:	SECRETIN FORMATION
Key:	VIGENEREVIG EN EREV
Ecrypted text:	NMIVRXZRAWXQNXZSI

Picture 8.: Vigenére’s cipher

To be continued…

Literature:

1. http://kryptologie.uhk.cz/historie.htm
2. http://www.fi.muni.cz/usr/jkucera/pv109/2003/xbitto.htm
3. http://dakota.skautkostelec.cz/skautska_stezka/praxe/historie_sifrovani.htm
4. http://hisorie-sifrovani.wz.cz/
5. http://en.wikipedia.org/wiki/Blaise_de_Vigen%C3%A8re
6. http://en.wikipedia.org/wiki/Johannes_Trithemius
7. http://en.wikipedia.org/wiki/Enigma