Portál pre odborné publikovanie ISSN 1338-0087

History of cryptology – part 1.

Kolek Jan · Informačné technológie

03.10.2012

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.

1. Antiquity

The need for people to interact with each other is as old as humanity itself. But sometimes we cannot allow our communication being watched. This has led some four thousand years ago that people started their reports differently camouflage and concealment – was secret communication and the first crude ciphers. Cryptology initially developed very unevenly. Cipher formed in isolation in different parts of the world, some lasted a long time, and others survived extinction civilization that created them.

1.1 Ancient Egypt

In about 1900 BC in Egypt in Menet Khufu unknown master carved into the stone plates hieroglyphics depicting the life of his master. This act began the history of cryptology. A special feature of this method is that commonly used hieroglyphics were replaced with new ones that should exaggerate the importance of the acts of the master. It is therefore not directly cipher that would hinder reading of the text, but the florid decoration written (in this case, engraved) text. For example, instead of writing AD 2010 was used text “year of our Lord two thousand and tenth.” In a way, the encryption and the use of common hieroglyphs, because most of the population

could neither read nor write. [1] These hieroglyphs are the oldest surviving example of the use of the transformation of the text.

Picture 1.: Stone plate

1.2 Ancient India

In ancient India, indirectly origin and the word cipher. Originally it was the Arabic word sifr as indicating numeral zero. When translated into Latin, it was translated as zephirium, figure or also figure nihil. From Latin to French, the word translated as chiffre figure. In the 15th and 16 century, the role of the mysterious numbers zero at entry led to the fact that the code word was used to describe the mysterious and unknown things. Later the word was used to refer to figure all used numbers as we know it today. [3]

In famous book – Kamasutra from the author is described Vatsyanova Art "Making sense of the scriptures secret and secret characters" at the 43rd place between 64 arts (ie yoga), which every woman should learn in order to protect confidential and sensitive information from unauthorized disclosure person. [4] This yoga is called "mlecchita-vikalpa" and is divided into two ways. The first is "kauţiliyam" and the second "m-ladejiya". In India were also created basics of sign language, which is still used by deaf people and traders. [1]

1.3 Ancient China

In ancient China was not enhanced encryption. This was due to a very low level of education of the population. Among the captains and higher-ranking people were more preferred oral communication, when the messenger had to learn the text by heart and repeated communication to the addressee in person. Written messages are not encrypted, but packed into a ball, covered in wax and then hidden in the body of the messenger. [1]

1.4 Ancient Mesopotamia

In ancient Mesopotamia, instead of encryption used simple methods rather

reminiscent of confidentiality Steganography. [4] The oldest surviving work from about 1500 BC is a small clay tablet on which the hidden secrets of the glaze on ceramic vessels.

1.5 Hebrew ciphers

Hebrew masters and scholars were the first to use simple cipher based on substitution. It concerns three types of ciphers known as “Atbash”, “Albums” and “atbah”. The Cipher “Atbash” was the first letter of the alphabet replaced the last, second-last, etc. Nowadays, this corresponds to the substitution A = Z, B = Y, C = X, etc.. Cipher “Albam” alphabet divided into two halves and the first character of the first half of the match the first character of the second half. Nowadays, this corresponds to the substitution A = N, B = O, C = P, etc.

Most interesting was the cipher “atbah”, where the first 9 letters marked with numbers from one to nine and replaced with that matched the numbers add to 10 Another 9 letters were similarly encrypted, but was determined to supplement the Hebrew number 100 (in decimal system 28). What happened to the characters corresponding numeral 19 and above is not clear. Nowadays, this corresponds to substitution of A = I, B = H, C = G, D = F, ..., H = B, A = I, J = R, K = Q, ..., Q = K, R = J. [1]

Picture 2.: Table of Atbash cipher

1.6 Ancient Greece

Perhaps the most ciphers come from ancient Greece. But in addition to classical encryption have been widely used and steganography methods.

1.6.1 Herodotus

The work of Herodotus’ History “in some stories describe methods of steganography. Herodotus writes about how the Greek ambassador in Persia wanted to send a message to Asian cities to rise up against the Persian king scoundrel. But he knew that his messenger and the message was captured divulged, so let his slave head shave, wrote in her message, wait until your hair grows back again, and then he sent a slave with a message. The slave went through without difficulty and the rebellion was underway. [4]

Another method described in this work that the messenger with the message he was disguised as a hunter and the message was hidden in the abdomen don't skinned hare. The Messenger easily passed around the guards and the message was safely delivered. According to Herodotus, was the most important news story of Western civilization Report of the intentions of the Persians to conquer to Greece. This message was delivered to the waxed plates. Plates were first cleaned from wax, then report was written, and then were again coated with wax. These plates without alerting the guards and the message went through. [1]

1.6.2 Scytale

According to the story by Plutarch in the 5th century BC Spartan introduced the first military strategist's cryptology. They began to use the first mechanical device for encryption, "rendered" – a wooden sticks exactly the average. The rod was tightly wound strip of leather, parchment or canvas and this strip lengthwise hole was written message. After unwinding the strip on it leaving a mixture of meaningless characters. After re-wound on a rod of the same diameter was again hidden message can be read. [2]

Picture. 3.: Scytale

1.6.3 Polybius square

The Greek historian Polybius policies in the 2nd century BC, invented a code for the transmission of signaling messages over long distances. The basis of the code table, where the characters were arranged in a square:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Picture 4.: Polybius square

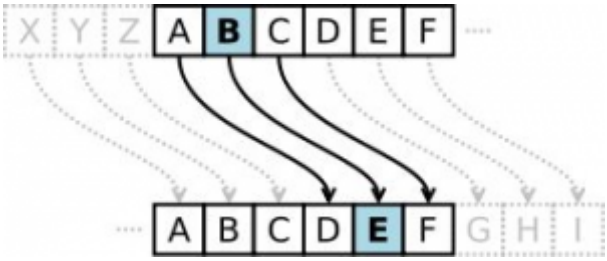
Each letter is represented by a pair of numbers. E.g. "P" is represented by 3 and 5 Polybius intended to represent the number of torches in both hands. So "P" represented 3 torches in his left hand and 5 torches in right hand. [1]

1.7 Ancient Rome

In ancient Rome did not use encryption too. Was a preferred sealing document with wax, which is still used occasionally.

1.7.1 Caesar cipher

One of history's most famous ciphers called Ceasar cipher. Ceasar for his correspondence with Cicero and other friends enjoyed a simple cipher, where each letter is replaced with the letter lying on three positions in the alphabet below. At present, this corresponds to substitution alphabet A = D, B = E, C = F, ..., X = A, Y = B, Z = C [3]



Picture 5.: Caesar 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