HISTORY OF CRYPTOGRAPHY

Chernyakova M., *student*

Cryptography (or cryptology; derived from Greek κρύπτω *kryptó* "hidden" and the verb γράφω *gráfo* "to write" or λέγειν *legein* "to speak") is the practice and study of hiding information. It's is one of the oldest fields of technical study we can find records of, going back at least 4 000 years. Ciphering has always been considered vital for diplomatic and military secrecy. Cryptography probably began in or around 2000 B.C. in **Egypt**, where hieroglyphics were used to decorate the tombs of deceased rulers and kings. These hieroglyphics told the story of the life of the king and proclaimed the great acts of his life.

The **ancient Chinese** used the ideographic nature of their language to hide the meaning of words. Messages were often transformed into ideographs for privacy, but no substantial use in early Chinese military conquests is apparent.

In **India**, secret writing was apparently more advanced, and the government used secret codes to communicate with a network of spies spread throughout the country.

The cryptographic history of **Mesopotamia** was similar to that of Egypt, in that *cuneiforms* were used to encipher text. This technique was also used in Babylon and Assyria. In the Bible, a Hebrew ciphering method is used.

The **Greek writer Polybius** invented the 5 x 5 Polybius Square, widely used in various cryptographic systems.

During the **Middle Ages**, cryptography started to progress.

By 1860 large codes were in common use for **diplomatic communications**, and cipher systems had become a rarity for this application. **The invention of telegraph and radio pushed forward the development of cryptographic protection of telecommunications**: the speed and the volumes of data traffic became considerable and more vulnerable to interception and decryption.

In the 20th century mathematical theory and computer science have both been applied to cryptanalysis. As the science of cryptology becomes increasingly sophisticated, most nations have found it necessary to develop special governmental bureaus to handle diplomatic and military security (the National Security Agency in theUnited States).

Great minds in Cryptography

Julius Caesar used his famous substitution cipher (the 'Caesar Cipher'), which shifted each letter four places further through the alphabet. **Sir**

Francis Bacon celebrated bilateral cipher. The 'wheel cipher' was invented by **Thomas Jefferson** around 1795, and although he never did very much with it, a very similar system was re-invented for use in World War II by the US Navy, which then called it the Strip Cipher. **Ronald L. Rivest, Adi Shamir** and **Leonard M. Adleman** invented the RSA computer-encryption algorithm. It was published in the September 1977 issue of Scientific American. Even today, it is used to keep text secret. Pretty Good Privacy (PGP) was released in 1991 by American **Phil Zimmerman**. To this day, it is considered a very secure way of communication across the Internet.

Did you know: CryptoBytes

In the period of **Renaissance** the creativity in many spheres also gave impulse to cryptography as a science and as an art of secret communications between the monarchs and emperors, like **Leonardo da Vinci, Cardinal Richelieu** and the **Kings of France Louis XII-XIV**. The «coding of messages», the substitution of words and figures by symbols and numerals of previously agreed character became wisely used in government correspondence. And the services of specialists in coding and decoding of secret letters became available as a result of this practice.

The writer **Edgar Allan Poe** had a great fascination with cryptography. Besides numerous references to it in his stories, he conducted his own cryptographic challenge in December 1839.

The workload of **(Russian)** code machine operators was enormous: between 1941 and 1945 they coded and decoded more than 1,6 million messages (or 1500 telegrams in cipher per day).

During WW2, **the neutral country Sweden** had one of the **most effective cryptanalysis departments** in the world. It was formed in 1936, and by the time the war started, employed 22 people. The department was divided into groups, each concerned with a specific language. The Swedes were very effective in interpreting the messages of all the warring nations. They were helped, however, by bungling cryptographers.

In a short story by Sir Arthur Conan Doyle, *The Adventure of the Dancing Men*, **Sherlock Holmes** is confronted by a simple substitution cipher. He solves the crime by deciphering a code in which the cipher text elements are hieroglyphics of little dancing men. Holmes figures these symbols are some kind of secret code.

Zolotova S.G., *EL adviser*