УДК 811.111+004.056.55

HISTORY OF CRYPTOGRAPHY AND ITS USAGE

© Беспалько Я. А., Пигарева М.Н.

e-mail: Yasha.9047@gmail.com

Самарский национальный исследовательский университет имени академика С. П. Королёва, г. Самара, Российская Федерация

Encryption – is a method of disguise of initial meaning of the text or another document, which provides the corruption of its original content. Transformation of a common, understandable content into a code is known as coding. Whereby it's implied to be a mutual synonymous matching between the text symbols and the code. Therein a basic difference between coding and encryption. Frequently people make a mistake thinking, of encryption and coding as two similar things, but in reality they are not. To recover encoded message, you simply need to know the method of coding, as distinguished from encryption where you should know the key besides the encryption method. In this context the key meant to be a certain condition of characteristics in ciphering. It is possible to encrypt not only a text, but a different types of data such as: images, data bases and processors.

Humanity had been using encryption from the appearance of the first secret information, which had no possibility to become public.

The main point of encryption is to prevent review of initial message from people who haven't got the key of encryption.

The goal of my report is to show the importance of cryptography in human history in different time periods. I want to tell about varieties of cyphers their difference and commons, to tell about their reliability and usage. I used the most well-known cyphers such as Ceasar's cipher, The Great French Cipher, I also want to tell about war time cryptography namely the Enigma machine code which was used by the German army during WWII and how it was decoded by the British scientists.

Encryption is used nowadays to help people secure their private info. Lots of bank accounts, messengers and e-mails are using different types of cyphering, my goal is to provide an example of most trustful encryption method. As an example I used modern messengers and their code bases.

To show the most reliable messenger to secure your info I made a list of characteristics for every one of those and compare them. Throughout research I found messenger that in my opinion is rational to use.

References

1. Rivest, Ronald L. (1990). "Cryptography". In J. Van Leeuwen. Handbook of Theoretical Computer Science.
2. "Cryptology (definition)". Merriam-Webster's Collegiate Dictionary (11th ed.).
3. Cryptography: Theory and Practice, Third Edition (Discrete Mathematics and Its Applications), 2005, by Douglas R. Stinson
4. https://core.telegram.org/mtproto -main page of "Telegram" website
5. Alexander, C. Hugh O'D. (c. 1945), Cryptographic History of Work on the German Naval Enigma
6. Agar, Jon (2001). Turing and the Universal Machine.
7. Kahn, David. "The Man in Iron Mask -- Encore et Efin, Cryptologically."
8. A Short History of Cryptography
9. Abbott, Frank Frost (1901). A History and Description of Roman Political Institutions.