5 В Санкт-Петербурге арестовали подозреваемого в теракте на железной дороге [Электронный ресурс]. – Режим доступа : https://govoritmoskva.ru/news/364153/. – Дата доступа : 08.03.2023.

6 Bahn: саботаж на железной дороге на севере Германии [Электронный ресурс]. – Режим доступа : https://aussiedlerbote.de/2022/10/sabotazh-na-zheleznoj-doroge/. – Дата доступа : 08.03.2023.

7 Актуальные киберугрозы: I квартал 2022 года [Электронный ресурс]. – Режим доступа : https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/. – Дата доступа : 08.03.2023.

Получено 20.05.2023

ISSN 2227-1155. Сборник студенческих научных работ.
Вып. 28. Гомель, 2023

УДК 003.26:004.056

O. Y. ARSOBA (ET-11)
Research Supervisor – Master of Philology *E. L. BATURINA*

CRYPTOGRAPHY AS A TOOL FOR ENSURING INFORMATION SECURITY = КРИПТОГРАФИЯ КАК ИНСТРУМЕНТ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Cryptography protects information by encrypting it and is used in various fields. It includes symmetric and asymmetric encryption methods. Cryptography ensures data security in areas like personal data protection, financial transactions, and defense. However, it is not completely secure, and there is a risk of misuse. Despite this, cryptography remains crucial for data protection and plays a vital role in modern information technology.

Cryptography is a science that deals with protecting information from unauthorized access. It provides different ways to encrypt data so that only those who have the right to access it can read it. People have been using cryptography for thousands of years. The oldest cryptography techniques were transposition and substitution. In transposition, the letters in the enciphered word are re-arranged following some system or even randomly. For example, the word *code* can turn into *edoc*, *ecdo* or *dcoe*. Substitution is an alternative method that involves replacement of letters by other letters. To apply this technique, the sender and the receiver should agree in advance how the letters will be paired. If the pairs are c-m, o-p, d-l, e-a, the word *code* turns into the meaningless combination *mpla.* In the book «Gaelic Wars» written by Julius Caesar it is mentioned that the Romans used substitution to encipher their military messages. They simply replaced Latin letters by the Greek ones [1, p. 24].

The science of breaking ciphers appeared in the ninth century. It was an anonymous Arab scientist who came to the idea to check the frequency of letters in the Arab language. We don't know exactly who made the discovery that specific letters appear in texts with constant frequency, but it was crucial for cipher breaking.

The level of code security could sometimes change the course of history. In the 16th century, Mary Queen of Scots was executed by order of her cousin, Queen Elizabeth, for plotting against her. The main evidence against the Scottish queen were her letters. Mary's correspondence with catholic conspirators who wanted to dethrone the protestant queen Elizabeth was safely enciphered, and Mary believed that no one was able to break the code. But the English mathematician Thomas Phelippes deciphered the letters, Mary was found guilty and beheaded.

During the World War II, breaking the German Enigma code that was considered to be unbreakable saved thousands of lives of British, American and Soviet soldiers.

Today we regularly deal with cryptography. It is used in http protocols which are the basic part of the World Wide Web, in smartphones, in Internet banking. Modern online services would not exist without cryptography. Cryptography is used in many areas, including the protection of personal data, financial transactions, as well as in defense and intelligence activities. Modern cryptography methods protect data in various fields, including banking, government agencies, medicine, and technology companies. Secret codes ensure secure transfer of information using open communication channels, processing and storage of user passwords, secure storage of information on your personal computer as well as bank cards services.

Now there are a lot of different cryptography methods, but one of the most widely used ones is symmetric encryption. According to this method, users apply the same key to encrypt and decrypt the data which should be protected. Today, the Advanced Encryption System (AES) is considered to be one of the most popular symmetric encryption techniques. AES offers 128, 192, and 256-bit keys. It is a much more advanced technique than the 56-bit Data Encryption Standard (DES) that used to be popular in the recent past, because a 56-bit code has only 72 quadrillion possible keys and can be cracked in less than 24 hours. On the other hand, existing calculation capacities are not enough to decipher even a 128-bit code [2]. Symmetric encryption is fast and efficient, but if two parties exchange the secret key via the Internet, it can be stolen. The only way to provide security is to exchange secret codes personally, which is often impossible. Secondly, if the third party has got assess to the secret code, all messages, both preceding and future, can be deciphered.

The solution can be found with the help of asymmetric encryption, which uses a pair of keys: one to encrypt data and another one to decrypt it. Asymmetric encryption gives each user a pair of keys known as public and private. The public key is visible to everyone, while the private key is known only to its owner. Users can encrypt messages with their private key. These messages are decrypted by those who possess the public key.

One of the latest successful applications of cryptography is blockchain technology, which is used in cryptocurrencies such as bitcoin. Blockchain uses two main forms of cryptography: public key cryptography and hash functions. A hash function can be defined as «a function projects a value from a set with many (or even an infinite number of) members to a value from a set with a fixed number of (fewer) members» [3]. Thanks to cryptography, transactions in the blockchain are protected from fraud and manipulation.

However, like any technology, cryptography is not completely secure. It is dangerous to rely on cryptography because you don't get a response when something goes wrong. There are different methods for cracking ciphers. One of them is the key selection method, in which the attacker tries to use all possible combinations of codes one by one unless the right combination is found. There is a risk that cryptography could be used for malicious purposes, such as encrypting data to extort a ransom. In such cases, cryptography can become a tool for committing crimes, so it is necessary to balance between protecting data and ensuring the safety of society.

Nowadays cryptography continues to evolve, and modern encryption methods are becoming more complex and secure. Cryptography is an important information security tool and will only grow in importance in the future.

Cryptography has become an important and integral part of modern information technology. It helps ensure the confidentiality, integrity, and availability of data and enables protecting private data from unauthorized access. That is why cryptography is often considered to be the foundation of information systems security. Cryptography is a necessary tool for protecting information in the modern world. However, every user should bear in mind the fact that cryptography is not completely secure. Every cipher can potentially be broken. Therefore, the evolution of cryptography must continue to guarantee data security in an ever-changing threat environment.

LIST OF REFERENCES

1 **Singh, S.** The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography / S. Singh. – New York : Anchor Books, 2000. – 425 p.

2 Криптография и будущее децентрализованных вычислений [Электронный ресурс] // Oracle Labs. – Режим доступа : https://habr.com/ru/amp/publications/680650/. – Дата доступа : 20.05.2023.

3 HashFunction [Electronic resource] // Mathworld Wolfram. – Mode of assess : https://mathworld.wolfram.com/HashFunction.html. – Date of assess : 20.05.2023.

Получено 05.06.2023