

УДК 004.4

Stanislav Omelchenko¹, Valentina Kuzmenko²

¹student of group CST-128 ZNTU

²senior teacher ZNTU

DEVELOPMENT OF CRYPTOGRAPHY

Cryptography is a science of mathematical methods for securing the confidentiality, integrity and authenticity of information. It was developed because of the practical need to transfer important information in the most reliable way. For mathematical analysis, cryptography uses an abstract algebra and probability theory toolkit.

For a long time cryptography implied only encryption - the process of converting ordinary information into obscure "rubbish". Decryption is the reverse process of reproducing information from ciphertext. A cipher is a pair of algorithms of encryption / decryption. The action of the cipher is guided by algorithms, and, in each case, by the key. The key is a secret parameter for a particular context when sending a message. The keys are of great importance, since without key variables, encryption algorithms are easily broken and unsuitable for use in most cases. Historically, ciphers are often used to encrypt and decrypt, without performing additional procedures such as authentication or integrity checking.

Until now, cryptography has been engaged exclusively in ensuring the confidentiality of messages - the conversion of messages from an understandable form into an obscure and inverse recovery on the recipient's side, making it impossible for readers to intercept or overheard without secret knowledge. In recent decades, the scope of cryptography has expanded to include not only the secret transmission of messages, but also methods for checking message integrity, sender / recipient identification, digital signatures, interactive verification, and secure communication technology.

A cryptographic algorithm, or a cipher, is a mathematical formula that describes the processes of encryption and decryption. To encrypt the open text, the crypto algorithm works in conjunction with the key - word, number or phrase. The same message is one algorithm, but different keys will be converted to different ciphertext. The security of ciphertext depends entirely on two things: the stability of the cryptographic algorithm and the secrecy of the key. The cryptographic algorithm, plus all the keys and protocols that lead them into action, form a cryptosystem. PGP is a cryptosystem.

For today's cryptography, open encryption algorithms are used which involve the use of computing means. It is known more than a dozen proven encryption algorithms, which using a key of sufficient length and correct implementation of the algorithm, make the encrypted text inaccessible for practical cryptanalysis. The most commonly used encryption algorithms are such as Twofish, IDEA, RC4 and others.

To conclude, a cryptography plays a crucial role in protection of personal data as well as in protection against illegal access and it needs to be increasingly improved.