TO THE QUESTION OF CRYPTOGRAPHY

Boyko A.K., Maslyanitsa A. D.

Don State Technical University

The problem of the secret message transfer exists as long as the writing exists. Moreover, a long time ago the writing itself was the method of a secret transmission of information, as it was available only for reach and educated people. For the implementation of the secret transmission of messages from one addressee to another, there are two directions: first, you can try to hide the fact of the transmission of messages, secondly, it is possible to convert the message that the information contained in it wouldn't be available to a third person. Steganography deals with the first direction, with the second — cryptography.

Information technology is extensive and deeper into the everyday life of mankind. There are new ways of connecting people to change the way of information exchange. Come to their electronic counterparts replaced paper documents, and e-mail is now used more often than usual.

This deep integration of the electronic data exchange makes the development of information transfer technology to put information security issues in the first place.

Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries.

Probably not many people think about it, but cryptography is now found in almost every human being. Cryptography we use in everyday life, as well as during the working process: it is the system "Client - Bank", and the system of various statements through the Internet, and SUFD (Remote financial document management system), and so forth.

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it.

When using the means of cryptographic protection of information all information exchanged over a secure channel (encrypted to outsiders), which helps

protect data from intentional distortion or interception during communication between transmission points .

Also, the use of cryptographic information protection, encryption of data on storage devices, it will help protect your data in case of loss or theft of both the storage devices (flash drives , CD-drives) and the computer entirely.

Cryptooperation is a process of replacement and/or rearrangement of some or other symbols (bytes, bits) of an initial message using a special algorithm in accordance with the given key (a kind of a password).

There are two types of cryptooperation in cryptology: symmetrical and asymmetrical.

The first is sometimes called “a one-key cipher” or a cipher with a secret key. Symmetry lies in one secret key used for encryption and deciphering of one message. Symmetrical ciphers are best suited for cases when computer information is just stored on the hard disk, floppies or other mediums.

Therefore, another kind of cryptooperation is of special interest. Otherwise, it can be named a two-key cipher or a public-key cipher. The key for deciphering differs from the key used at encryption. These ciphers use one key to encipher the message and a different key to decipher the message.

Among the various methods of encryption are the following basic methods:

Algorithms of replacement or substitution - the characters of the original text are replaced by the symbols of another (or the same) alphabet, in accordance with a predetermined pattern, which is the key of this cipher. Separately, the method in modern cryptosystems is not used because - for very low cryptographic strength.

Algorithms reshuffle - the characters of the original text are interchanged on a certain principle, which is the secret key. Permutation algorithm itself has a low cryptographic strength, but is included as an element in many modern cryptosystems.

Algorithms XOR - source code symbols are formed with random characters. The most common example of encryption is considered files "username.rwl" in which Microsoft Windows operating system stores the passwords to the user's

network resources (entering a password for NT- servers, passwords DialUr wireless Internet access, etc.). When a user enters their password to log on to Windows, from his RC4 encryption algorithm is generated gamma (always the same), used to encrypt network passwords. Easy selection of the password is determined in this case by the fact that for Windows always prefer the same band.

Algorithms based on complex mathematical transformations using an expression of the original text. Many of them use the unsolved mathematical problems. For example, the Internet is widely used RSA encryption algorithm based on the properties of primes.

Combined methods. Consistent encryption source code with the help of two or more methods.

References:

1. Biggs, Norman (2008). Codes: An introduction to Information Communication and Cryptography. Springer. p. 171.
2. Gannon, James (2001). Stealing Secrets, Telling Lies: How Spies and Codebreakers Helped Shape the Twentieth Century. Washington, D.C.: Brassey's. ISBN 1-57488-367-4.
3. Shamir, A. (1979). "How to share a secret". Communications of the ACM (Association for Computing Machinery) 22: 612–613.
4. Williams, Christopher (11 August 2009). "Two convicted for refusal to decrypt data". The Register. Retrieved 26 March 2015.