# SECURITY OF INFORMATION DATA

Ivanko A.F., Ivanko M.A., Kulikova E.V.
*Moscow Polytechnic University, Moscow, e-mail: alekfed@mail.ru, mihaleks@mail.ru, elena@kulikova.pp.ru*

The development of information technology makes it possible to use new opportunities in various spheres of life for a wide range of users. Often, personal problems are required to solve urgent problems, this is necessary to perform financial calculations, transfer funds from one card to another, to make utility payments and pay for goods in foreign online stores, etc. Unfortunately, on the Internet spaces and in the WEB-space there are scoundrels and dexterous swindlers who use various methods of deception to achieve their criminal goals. Our article is devoted to the study of systems used to protect personal data on modern information spaces. In the work, the most common methods of attacking encrypted data are studied in detail and presented. In addition, the problem of ensuring a high level of security of cryptosystems was considered, and some recommendations for its improvement were formulated. Our work can be useful for a wide range of users using information technology in everyday life.

**Keywords: information security, cryptosystems, cryptographic algorithm, key, data protection**

First of all, a few general considerations about the safety of Internet browsing. Try never to go to various other familiar sites where you are offered "free cheese". Remember, this is a trap. On such sites you can easily pick up computer viruses or become a bait for scammers. It can be a message that you have become the heir of a rich relative in a distant country, it may be a message that you need to take away the winnings. There may be reports of a desire to meet you, etc. Remember: all this entails negative consequences and can lead to the loss of your data, which later can be used by scammers. Today, various methods are used to protect information and our personal data, including cryptography methods.

The art of cryptography has been of interest to mankind since ancient times. Attempts to create unique cipher combinations were made at different times by the "great minds" of society. To date, cryptographic knowledge is used universally in virtually all spheres of human life, especially in the virtual world. And in its development, cryptography has reached its apogee today. In whatever time interval we have not considered this phenomenon, its main goal remains to this day unchanged – to protect information from unauthorized access. Is it possible to consider the developed cryptosystems reliable? How in the current conditions of the rapid development of information technology can secure personal data? We will try to answer the above questions in this work.

So, first of all, let us turn to the definition of the basic concepts. Cryptography, as a rule, is understood as the "science of data security, which searches for solutions to four important security issues – confidentiality, authentication, integrity and control of participants in the interaction" [7, p. 56]. In this case, security is achieved by converting existing information of one type into another, more unique and "closed", access to which is either impossible or impossible, or very difficult. This is due primarily to the fact that data protection is based on the creation of a so-called "key" – "the specific secret value of a set of cryptographic algorithm parameters that ensures the selection of one transformation from the set of transformations possible for this algorithm" [9, p. 72]. In turn, a cryptographic algorithm is called "a set of rules that is used to encrypt information, allowing to generate encrypted text that can not be read without decryption" [10]. Thus, a cryptosystem is, in fact, "a family of reversible transforms that can be selected with the help of a key, which transforms the protected information block into a ciphertext and vice versa" [7, p. 67].

There are many different types of cryptosystems, based on the division of which are the functions performed and the tasks assigned. Today, cryptosystems are used to ensure the secrecy of data, to authenticate their authenticity, as well as to prevent unauthorized access to a certain set of information [8]. In accordance with this, three types of cryptosystems are distinguished.

In turn, cryptosystems designed to "hide" information can be divided into encryption systems and cryptographic coding systems [8]. As you know, encryption consists in "converting data into an unreadable form using encryption-decryption keys". It is worth noting that encryption is the oldest method of cryptography. Recollections of this system were found by researchers in the works of Aeneas Tacticus, dating from the IV century BC [1]. Cryptographic coding has a slightly different character. It is caused by the transformation of messages into

message-dependent codes, depending on the messages themselves, in order to hide their content.

Cryptosystems of information authentication are divided into systems that help in establishing the authenticity of messages and systems, focused on establishing the reliability of the information sources used (users, networks, etc.) [8]. Here it is important to understand that the methods of authentication of information will be used different, depending on the conditions that ensure the authenticity of the data.

The last kind – cryptosystems, which are responsible for accessibility to a set of information – today is not independent, but consists of two of the above types.

Thus, many tasks put forward today in the information world can be solved by using cryptographic algorithms. As you can see, there is a multitude of ways to protect sensitive data from unauthorized treatment. But to what extent do the above systems meet the current realities that prevail in the vastness of the infomir? Is it possible today to get by with existing knowledge about data coding? Are these cryptosystems reliable in the 21st century?

So, it is already proved that by applying a sufficient amount of effort, it is possible to crack any cryptosystem. The amount of time is fully determined by the complexity of the planned work. Along with the development of cryptography as applied science, there is a continuous process of inventing more and more new ways of hacking cryptosystems, which it is not possible to list. But the most common ones are listed below.

*1. Attack aimed at encrypted text.* This method of "hacking" is one of the most difficult, because in this case the attacker operates with a minimum amount of information. He tries to "unravel" the cipher by all possible methods. The most banal in this case is the selection method, which, by the way, today can be implemented not by a person, but directly by a "machine", which uses certain programs in its work.

a) Attack on "block" ciphers.

This method of obtaining the necessary data is one of the simplest. It is known that "block" ciphers are applied to certain fragments (blocks) of the text. In modern conditions, block fonts are used for blocks of text, the length of which is 128 bits. Encryption of information occurs on the basis of the implementation of 32-bit operations, which is a significant drawback. After all, according to a number of scientists, the use of such operations makes it almost impossible to obtain an odd key. Thus, all "block" fonts generate even combinations. Consequently, this makes it easier for attackers: to build a simple discriminator based on the generation of possible even combinations is not difficult. With regard to the "breaking" of "block" fonts, the so-called "attack with the solution of equations" is singled out, the essence of which lies in the construction of linear and quadratic equations based on the received fonts and their further solution.

*2. Attack with known "open" text.* This method is relatively easy, because the attacker already has not only encrypted, but also "open" or original data. That is, the main goal here is to find the necessary key. Based on the operations performed, such attacks can be, firstly, autonomous. In other words, one in which a previously prepared "open" text or a fragment of it is processed by a cryptanalyst before obtaining the necessary ciphers. Secondly, the described attack can be autonomous. In this case, the "open" text is selected taking into account the font received by the attacker. Autonomous attack is more effective, efficient and efficient.

*3. Attack on asymmetric cryptosystems.* In 1975, an idea was put forward, based on the mathematical knowledge of a one-way function, on the development of cryptosystems with an "open" key, which provide a public encryption algorithm, and therefore have several keys: unclassified (encryption) and secret (decryption). Hence the name of the systems described is asymmetric [2]. To obtain the data of these systems, it is most expedient to apply the RSA algorithm (an abbreviation from the names of the creators Rivest, Shamir and Adleman). Scientists drew attention to the fact that the keys (open, closed), in fact, are functions of two large primes. It was concluded that the receipt of plain text on the available code and the "open" key is identical to the process of decomposition of a number into two factors. Thus, the protection of RSA is due to the difficult operations of factoring specific numbers.

Thus, today it is very difficult to give an example of a cryptosystem that would not have been hacked. How can I improve the level of protection of personal information?

Traditionally, information security is commonly understood as "the protection of information and supporting infrastructure against accidental or deliberate natural or artificial impacts, fraught with inflicting damage to owners or users of information and supporting infrastructure" [9, p. 85]. While the protection of information is called "a set of activities aimed at ensuring the confidentiality and integrity of

information processed, as well as the availability of information for users" [6, p. 45].

Very often security of cryptosystems is compared to a strong chain, the reliability of which directly depends on the quality of each link. Drawing an analogy, you can see that every element – key, protocol, etc. – must be thoroughly thought out in the protected cryptosystem. It has been scientifically proven that cryptosystems in which the ciphertext does not provide information about the "open" text are the most secure. You can only send information about the length of the latter. In this case, the key should not be shorter than the main message. As a rule, such a key does not provide for reuse.

Speaking about the security of cryptosystems, special attention should be given to choosing a reliable cryptographic algorithm, because, first of all, the level of protection of information depends on this. So, you can refer to already known algorithms that are published in specialized publications, you can use the services of professionals, profiled organizations, in rare cases, you can try to create your own algorithm. In other words, when deciding on the choice of an algorithm, it is necessary to concentrate as much as possible, to approach this issue in detail.

In order to increase the level of protection of cryptosystems based on encryption, one should perform block decoding, since in this case the code used will not be displayed in computer memory in an open form. It is also effective to carry out encryption with feedback, in which the key for decoding data depends on the information previously transmitted by the user. Today, researchers talk about the high effectiveness of using the "code in code" method. When implementing this scheme, "part of the protection mechanism is designed in the form of a resident module, whose task includes, for example, prohibiting writing to disk for some time or monitoring segment registers for changes" [5, p. 102]. To improve the level of data security is positively affected by combining cryptographic methods with compression. Separately, it is worth highlighting weak keys, the use of which reduces the level of cryptographic stability. To date, the problem of lack of verification of keys by the above parameter is quite common. Secure information can be provided when storing the key separately from the original data. Otherwise, even encryption, carried out with the help of a crypto-stable algorithm, is easily decrypted by intruders. Finally, the human factor plays an important role in the protection of information. After all, only the proper handling of the security system can cope with the task. Errors here are highly undesirable.

## Conclusions

I would like to note that although cryptosystems today are important elements in the protection of personal data, all methods of possible attacks have not been properly studied. It's hard to say what will happen over time, after all, we should not forget that simultaneously with the development of cryptosystems there is an improvement in the ways of "hacking", "interception" of ciphers, mortgages. Thus, in the current conditions of information gluten, the study of ways to ensure the reliability of cryptosystems, the derivation on their basis of new options for preventing unauthorized access to private data is of fundamental importance, since it is already clear that existing methods, which are being used everywhere, quickly become obsolete, scammers continue to search for new ones methods to deceive honest Internet users.

## References

1. Gardner M. A New Kind of Cipher That Will Take Millions of Years to Break. – Scientific American, 1977. – 124 p.

2. Wiener M.J. Cryptoanalysis of Short RSA Secret Exponents. – IEEE Transactions on Information Theory, 1990. – 558 p.

3. Belov E.B., Los V.P., Meshcheryakov R.V., Shelupanov A.A. Fundamentals of Information Security. – Moscow: Hot line – Telecom, 2006. – 544 p.

4. Introduction to the protection of information in automated systems: A manual for universities. – 2nd edition. – Moscow: Hot line – Telecom, 2004. – 147 p.

5. Devitin P.N., Mikhalsky O.O., Pravikov D.I., Shcherbatov A.Yu. Theoretical Foundations of Computer Security. – M.: Radio and Communication. 2000. – 190 p.

6. Protection of information in personal computers / A.V. Spesivtsev, V.A. Werner, A.Yu. Krutyakov et al. – M.: Radio and Communication, 1993. – 192 p.

7. ZEGZHDA PD Theory and practice of ensuring information security. – M.: Yachtsmen, 1996. – 302 p.

8. Classification of cryptoalgorithms [Electronic resource] Access mode: URL: lomasko.com/_ld/0/12_LV_.doc. (circulation date 11.12.2017).

9. Neil Koblitz, Course in Number Theory and Cryptography. – M., Scientific Publishing House: "TVP", 2001. – 254 p.

10. Basic information about the protection of software products. Cryptographic methods of information protection. Software systems for protection against unauthorized copying // Lectures on TRPP, SPP, Information Security, Standardization, Metrology and Certification [Electronic resource] Access mode: URL: http: //starik2222.narod.ru/trpp/lec2/34.htm (date 11.12.2017).

11. Ivanko A.F., Ivanko M.A. Information technologies in publishing. Tutorial. Moscow-MGUP them. Ivan Fedorov, 2013. – 136 p.

12. Vinokur A.I., Ivanko A.F., Ivanko M.A. Information systems in publishing: Textbook. allowance / A.И. Vinokur, A.F. Ivanko, M.A. Ivanko; Moscow. state. University of Ivan Fedorov. – Moscow: MGUE named after Ivan Fedorov, 2015. – 196 p.