UDC 316.774 74:004.056 DOI 10.36910/775.24153966.2022.73.7

T. Katkova

Doctor of Technical Sciences, Associate Professor Professor Department of Cybersecurity and Information Technology, University of Customs and Finance, Dnipro, Ukraine, V.Vernadsky street 2/4, Dnipro, Ukraine, 49000, takit777@gmail.com, http://orcid.org/0000-0002-1051-4262, 0562 471 882

SECURITY CRYPTOGRAPHIC PROTECTION OF SOVEREIGN INFORMATION RESOURCES

The development of new information technologies and the introduction of computer systems in all spheres of human activity have led to a sharp increase in the interest of a wide range of users in the problem of information security. Information protection is a set of methods and tools that ensure the integrity, confidentiality and accessibility of information when it is affected by threats of a natural or artificial nature, the implementation of which may harm the owners and users of information. Cryptography plays a leading role in ensuring information security in information and telecommunication systems, one of the main tasks is: ensuring the confidentiality, integrity and authenticity of transmitted data. Cryptography - the science of mathematical methods to ensure the confidentiality (inability to read information by others) and authenticity (integrity and authenticity of the author) of information. Today, cryptography, as a field of knowledge, and cryptographic protection of information, as a separate field of activity, concerns: issues of encryption, the latest e-commerce technologies, automated management systems, reporting and control, and so on. The formation of high-performance encryption methods (decryption) with high cryptographic stability is an important component in addressing information security. Methods of cryptographic protection of information are information encryption systems, algorithms for protection against imposition of false information (MAC codes and electronic digital signature algorithms) and cryptographic protocols for key distribution, authentication and confirmation of receipt (transmission) of information. Cryptographic stability of cryptographic information protection methods is a property of cryptographic algorithms and cryptographic protocols, which characterizes their ability to resist decryption methods (the process of unauthorized restoration of the original message text). Modern cryptography is characterized by the use of open encryption algorithms that involve the use of computing tools. To date, there are more than a dozen proven encryption methods that, when using a key of sufficient length and the correct implementation of the algorithm, make encrypted text inaccessible to cryptanalysis (the science of "breaking" cryptographic transformations).

In the process of work we have considered cryptographic methods and means of information protection, which are one of the elements of a comprehensive information security system. The types of encryption, as well as the essence of electronic signatures are highlighted. The legal bases of application of cryptographic methods of information protection are given.

Keywords: *complex information protection, cryptographic methods of information protection, legal basis for cryptographic information security, cryptographic information security software.*

Т.І. Каткова

ЗАБЕЗПЕЧЕННЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Розвиток нових інформаційних технологій і впровадження комп'ютерних систем в усі сфери людської діяльності стали причиною різкого зростання інтересу широкого кола користувачів до проблеми інформаційного захисту. Захист інформації – це сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умови впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди власникам і користувачам інформації. Провідна роль у забезпеченні інформаційної безпеки в інформаційно-телекомунікаційних системах відводиться криптографії, одними із головних задач є: забезпечення конфіденційності, цілісність та автентичність даних, що передаються. Криптографія – наука про математичні методи забезпечення конфіденційності (неможливості прочитання інформації сторонніми) і автентичності (цілісності і справжності автора) інформації. На сьогодні криптографія, як галузь знань, та криптографічний захист інформації, як окрема галузь діяльності, стосується: питань шифрувальної справи, новітніх технологій електронної торгівлі, систем автоматизованого управління, звітування та контролю тощо. Формування високопродуктивних методів шифрування(розшифрування) з високою криптографічною стійкістю є важливою складовою у вирішенні питання інформаційної безпеки. Методи криптографічного захисту інформації – це системи шифрування інформації, алгоритми захисту від нав'язування фальшивої інформації (MAC-коди та алгоритми електронного цифрового підпису) та криптографічні протоколи розподілу ключів, автентифікації та підтвердження факту прийому (передачі) інформації. Криптографічна стійкість методів криптографічного захисту інформації – це властивість криптографічних алгоритмів і криптографічних протоколів, що характеризує їх здатність протистояти методам дешифрування (процес несанкціонованого відновлення оригіналу тексту повідомлення). Для сучасної криптографії характерне використання відкритих алгоритмів шифрування, що припускають використання обчислювальних засобів. На сьогодні відомо більше десятка перевірених методів

шифрування, які при використанні ключа достатньої довжини і коректної реалізації алгоритму, роблять шифрований текст недоступним для криптоаналізу (наука "зламування" криптографічних перетворень).

В процесі роботи нами розглянуто криптографічні методи та засоби захисту інформації, які є одним з елементів комплексної системи захисту інформації. Висвітлено види шифрування, а також сутність електронних підписів. Наведено правові підстави застосування криптографічних методів захисту інформації.

Ключові слова: *комплексний захист інформації, криптографічні методи захисту інформації, правова основа криптографічного захисту інформації, програмні засоби криптографічного захисту інформації.*

Problem statement. In order to fully meet the needs of modern society, there is a need for information support in all spheres of human activity and, in particular, the reliable protection of information. This problem is particularly acute in connection with mass computerization, the association of computers in computer networks, and the use of the Internet.

The theory of information protection proves that if a protection system is built with consideration of all modern methods and means of protection, and if an enterprise has carefully selected and trained personnel who do not make mistakes, then deliberate actions of intruders in such a system are impossible. However, this is not entirely true. Over time, the protection system becomes obsolete, personnel change and lose vigilance, attackers find new ways of attacking and methods of overcoming protection that were unknown when the protection system was designed.

So, if you have reasonable expectations of the robustness of your information security system, you should still remember the basic rule of information security: no protection system can withstand the purposeful actions of a skilled intruder armed with modern technology for a long time. This rule has been developed by years of experience of information security specialists and is universal. It does not depend on the level of protection, the integrity of users and administrators, hardware, and software. The rule states that the problem is not whether intruders will break the protection system, but when they will do so. And the goal of information protection is to make sure that the system breakdown happens as late as possible.

Analysis of recent research and publications. The problems of creation and functioning of means of cryptographic protection of information have devoted enough publications in open sources, including such scientists as Ponomarenko V.S. [1], Verbitskyi O.V. [2], Khoroshko V. A. [3], Fal O.M. [4].

Ponomarenko V.S. in his works in systematic way deals with the creation of symmetric and asymmetric cryptographic systems for the protection of information.

Scientist Verbitskyi O.V. studies the problems of counteraction and investigation of crimes committed in the use of electronic computers, systems, and computer networks.

Scientists Khoroshko V. A. and Fal O. M. describe tools of the theory of disk encryption, key management procedures, the basics of development and implementation of cryptographic protocols, and the electronic digital signature mechanism.

Article purpose. Identify and process the main cryptographic methods and means of protection, and types of encryption. Analyze the software of foreign and Ukrainian developers, designed for the cryptographic protection of information.

Presentation of the basic material. One of the elements of a comprehensive information protection system is the cryptographic protection of information. This type of information protection is implemented by transforming information using keys based on mathematical methods. There are two purposes of using cryptographic methods - to conceal information by encrypting it and to confirm the significance of documents using an electronic digital signature. In other words, according to V. V. Popovskyi, cryptographic methods solve two problems - ensuring the confidentiality of information by preventing an attacker from extracting information from the communication channel and ensuring the integrity of information by preventing changes in information and entering false content in it [1]. There are two sections of science related to cryptographic methods: cryptography and cryptanalysis, which together form cryptology.

Cryptography studies mathematical transformations that allow information to be encrypted.

Cryptanalysis studies methods of decryption without knowing the secret key [1].

Means of cryptographic protection of information are divided into:

- means implementing cryptographic algorithms of information conversion;
- means, systems, and complexes of protection against imposition of false information using cryptographic algorithms of transformation of information;
- means, systems, and complexes designed for production and distribution of keys of

cryptographic protection of information;

- systems and complexes included in the information protection complexes against unauthorized access and using cryptographic algorithms of information conversion [2].

Means of cryptographic protection together with the key and other types of documentation, which provide the necessary level of protection, form a cryptographic system [2]. Encryption allows protecting information by turning it into incomprehensible text (ciphertext) with the possibility of further decryption (decryption). Both simple texts and computer files can be encrypted.

Encryption is divided into symmetric and asymmetric.

Symmetric encryption uses one secret key for both encryption and decryption. Asymmetric encryption uses a public key, and another secret key for decryption, generated using pseudorandom number generators.

Asymmetric encryption is also called public key encryption. The disadvantage of symmetric encryption is the need to pass the key to the person to the text is addressed, which entails its disclosure and decryption of information by attackers. The advantage of symmetric encryption is its higher speed than asymmetric encryption since asymmetric encryption uses longer keys, which increases the encryption time.

The way the text is encrypted is based on an algorithm and the encrypted text can only be decrypted using the key. One algorithm with different keys can be used to send messages to different recipients. Secrecy is determined by the key, not the algorithm since most algorithms are known to the general public. Due to the increase in computer performance, the probability of finding keys by trying combinations increases, so we have to use longer and longer keys, which increases the time for encryption [3]. An important characteristic of encryption methods is their cryptographic stability, i.e., for cryptographic protection of information in a computer network, it is necessary to create a special service, which generates keys and distributes them among the network users.

To create an electronic signature, the checksum and additional information is encrypted using the sender's private key. To avoid interception and reuse, a sequence number is included in the signature. An electronic signature allows to confirm the authorship of the document and guarantees the information integrity and absence of attempts to distort it. The document consists of the text, an electronic signature, and a user certificate, containing the user data, his identification name, and a decryption public key for the addressee's signature verification of the document [3].

E-signature allows to protect information from such criminal actions:

– “disclaimer of authorship,” when the author of a document disclaims authorship;

- “falsification” when the recipient of the document forges it;

- “alteration” when the recipient of the document makes changes to it;

- “masking” when a user masquerades as another user.

To confirm the message, the following conditions must be met:

– the sender must put a signature into the message that contains additional information that depends on the message and the recipient of the message, but is known only to the sender;

- a correct signature cannot be made without additional information;

- the signature must be time-dependent so that old messages cannot be used; this distinguishes an electronic signature from a handwritten one;

- the recipient must be able to verify that the signature belongs to the sender and is correct as far as the message is concerned.

Thus, an electronic signature is a type of password that depends on the sender, recipient, and content of the message [4].

According to the Law of Ukraine “On electronic documents and electronic document flow" an electronic signature is a mandatory requisite of an electronic document, which is used to identify the author and/or signer of an electronic document by other subjects of electronic document flow and imposition of an electronic signature completes the creation of an electronic document. The Law of Ukraine "On Electronic Digital Signature” determines the legal status of an electronic digital signature, according to which an electronic digital signature is a type of electronic signature obtained as a result of the cryptographic transformation of a set of electronic data attached to this set or logically combined with it and allowing to confirm its integrity and identify the signer.

The electronic digital signature is imposed using the private key and is verified using the public key. The procedure for cryptographic protection of restricted information, the disclosure of which causes

(may cause) damage to the state, society, or a person in Ukraine is determined by the Regulations on the Procedure for Cryptographic Protection of Information in Ukraine. According to this Regulation, for cryptographic protection of information constituting state secrets and official information created by order of state bodies or owned by the state, cryptosystems and cryptographic protection means approved for operation are used [6].

For cryptographic protection of confidential information cryptosystems and means of cryptographic protection are used that have a certificate of compliance [7].

There are a large number of software products designed for cryptographic protection of information, and foreign developers and Ukrainian.

One of the best programs for encrypting information is BestCrypt from the Finnish company Jetico. It allows you to create an encrypted container to store information on any type of media and is designed to work under both Windows and Linux. The program can optionally use one of the strongest algorithms implemented with a 256-bit key: Rijndael (AES), Blowfish, and Twofish. Newer versions of the Blowfish algorithm can use a 448-bit key [8].

The "Private Disk" program from the Moldovan company "Dekart" is also known. It allows you to create an encrypted virtual disk to store information. Encryption is performed using AES 256 algorithm. While working with information, files on virtual disk have the same properties as unencrypted ones, until the user does not lock the access. The virtual disk is protected from viruses, Trojans, and spyware using the built-in Disk Firewall [9].

There is a system of cryptographic protection of information "Karma" from the Ukrainian company "NetCom Technology". It is designed to ensure the use of electronic digital signature and encryption, in particular, in the legally significant electronic document flow. The peculiarity of this system is the possibility to add an image of a handwritten signature to the electronic digital signature. As a result, an electronic document will look like a paper one [10].

LLC "SKZ "CryptoSoft" offers a program complex of cryptographic protection of information "Cryptoserver" for work under MS Windows 8, MS Windows 10. This complex ensures the protection of data transmitted via unprotected public (Internet) or open (e.g., leased lines, MPLS) channels. Data is protected by encryption based on domestic encryption algorithms. The maximum level of access restriction for information protected by this suite is "confidential" [11].

Conclusions. Cryptography is a set of methods of data transformation, aimed at hiding their information content. A cryptographic information protection system is a set of cryptographic algorithms, protocols, and procedures for the formation, distribution, transmission, and use of cryptographic keys. The message itself is called plaintext. Changing the appearance of a message to hide its essence is called encryption.

Cryptographic protection can provide the conditions of confidentiality and integrity of transmitted data in open networks, as well as the anonymity of the object and the conditions of its involvement in the DIR.

References:

1. Ponomarenko, V. S., Zhuravlova, I. V., & Tumanov, V. V. (2003). *Osnovy zakhystu informatsii: navchalnyi posibnyk* [Fundamentals of information protection: a textbook]. Kharkiv: Vyd. KhDEU. [in Ukrainian].

2. Verbitskyi, O.V. (2018). *Vstup do kryptolohii* **[**Introduction to cryptology**]**. Lviv: Vyd-vo NTL **[**in Ukrainian].

3. Khoroshko, V. A., & Chekatkov A. A. (2017). Metody i zasoby zakhystu informatsiyi [Methods and means of information protection].Kyiv: Yunior [in Ukrainian].

4. Fal, O. M. (2003). Kryptohrafiya: osnovni ideyi ta zastosuvannya [Cryptography: basic ideas and applications]. Kyiv : IVTs Vydavnytstvo «Politekhnika» [in Ukrainian].

5. *Pro elektronni dokumenty ta elektronnyy dokumentoobih: Zakon Ukrayiny vid 22.05.2003 № 851-IV.* [On electronic documents and electronic document management: Law of Ukraine of 22.05.2003 № 851-IV]. URL: http://zakon4.rada.gov.ua/laws/show/851-15 (application date: 26.01.2022). [in Ukrainian].

6. *Pro elektronnyy tsyfrovyy pidpys: Zakon Ukrayiny vid 22.05.2003 № 852-IV*. [On electronic digital signature: Law of Ukraine of 22.05.2003 № 852-IV.]. URL: http://zakon4.rada.gov.ua/laws/852-15 (application date: 26.01.2022). [in Ukrainian].

7. *Pro Polozhennya pro poryadok zdiysnennya kryptohrafichnoyi zakhystu informatsiyi v Ukrayini: Ukaz Prezydenta Ukrayiny vid 22.05.1998 № 505/98.* [On the Regulations on the procedure for cryptographic protection of information in Ukraine: Decree of the President of Ukraine of 22.05.1998 № 505/98]. URL: http://zakon4.rada.gov.ua/laws/show/505/98 (application date: 26.01.2022). [in Ukrainian].

8. Private Disk naykrashcha prohrama dlya shyfruvannya fayliv [Private Disk is the best program for encrypting files]. URL: http://www.private-disk.net/ru (application date: 26.01.2022). [in Ukrainian].

9. *Systema «KARMA». Universalna systema kryptohrafichnoho zakhystu informatsii* (n.d.) [KARMA system. Universal system of cryptographic protection of information]. URL: http://www.eos.com.ua/eos/ua/products/carma (data zvernennia: 26.01.2022). [in Ukrainian].

10. Sira, O., & Katkova, T. (2017). Formation of securities portfolio under conditions of uncertainty. *Eastern-European Journal of Enterprise Technologies*, *1*(4 (85)), 49–55. https://doi.org/10.15587/1729-4061.2017.92283

11. Raskin, L., Sira, O., & Katkova, T. (2019). Dynamic problem of formation of securities portfolio under uncertainty conditions. *EUREKA Physics and Engineering*, *6*, 73–82. https://doi.org/10.21303/2461-4262.2019.00985