SECTION 6. INFORMATICS AND CYBERNETICS

DOI: 10.46299/ISG.2024.MONO.TECH.2.6.1

6.1 Development of modern cryptographic information protection methods and techniques

The problem of information security in computer networks is relevant today. As practice shows, the larger and larger the network and the more valuable information is entrusted to the computers connected to it, the more people are willing to disrupt its normal functioning for the sake of material gain, simply out of ignorance or out of curiosity. These attacks know no national borders.

In the Internet - the largest computer network in the world, however, like any other, there is a constant virtual war, during which the organization of system administrators opposes the ingenuity of computer hackers, with the aim of ensuring information security. Cryptographic protection methods are based on the possibility of carrying out a certain information transformation operation, which can be performed by one (or more) IS user who has some secret part of additional information.

In classical cryptography, only one unit of confidential and necessarily secret information is used - a key, the knowledge of which allows the sender to encrypt the information, and the recipient to decrypt it. This encryption/decryption operation is most likely impossible without knowledge of the secret key [159].

In public-key cryptography, there are two keys, at least one of which cannot be deduced from the other. One key is used by the sender to encrypt information, the preservation of which must be ensured. The other is a receiver for processing the received information. There are applications in which one key must be non-secret and the other secret.

The main advantage of cryptographic methods of information protection is their provision of guaranteed stability of protection, which can be calculated and expressed in numerical form (the average number of operations or the amount of time required to open encrypted information or calculate keys).

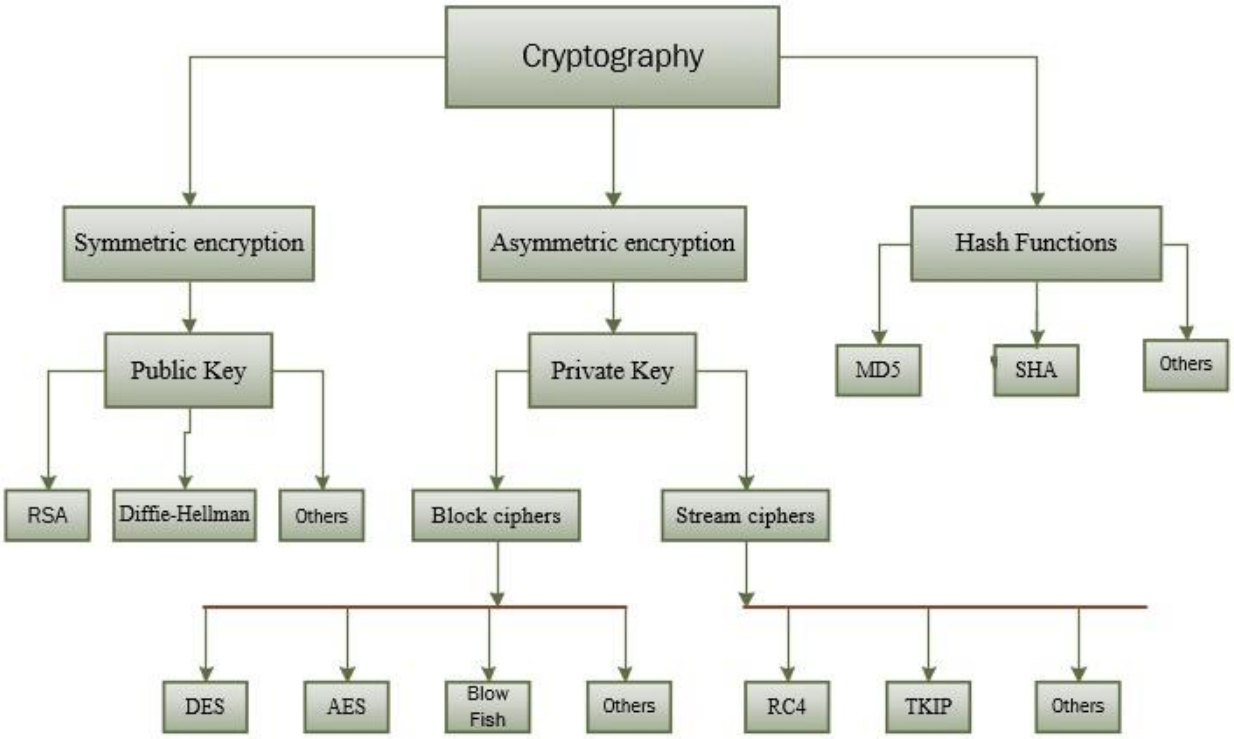
Encryption tools can be implemented both hardware and purely software. In any case, they must be certified, i.e. must meet certain requirements (standards). Otherwise, they cannot guarantee users the necessary encryption strength.

The use of several encryption algorithms of the same type for different purposes in the protection system is irrational. The best option is to create a system in which the means of crypto-protection are system-wide, act as an extension of the functions of the operating system and include certified encryption algorithms of all types (block and stream, with private and public keys).

Transparent encryption of all information on disks, which is widely recommended alongside developer protections, is justified only when the computer is used by only one user and the disk volumes are small. But in practice, even personal computers are used by groups of few users. And not only because there are not enough PCs for everyone, but also due to the specifics of the work of protected systems. Thus, the automated workplaces of control system operators are used by two to four operators who work ridiculously, and they cannot be considered as one due to the requirement of division of responsibility. That in an obvious situation it comes either to abandon the separation or to close the correspondence and allow the use of the cipher key by several operators, or to create closed separate disks for any of them and to close that very exchange of information, to store and transmit part of the information in the open, it is clear that in essence equilibrium rejection of the concept of transparent encryption of all information on disks [160].

Additionally, transparent disk encryption requires significant system overhead (time and performance). And not only directly in the process of reading and writing data. The fact is that reliable cryptographic closure of information presupposes a periodic change of encryption keys, and this leads to the need to re-encrypt all information on the disk using a new key (it is necessary to decrypt all information using the old one and encrypt it with using a new key). This requires considerable time. In addition, when working on a system with encrypted disks, delays occur not only when accessing data, but also when launching programs, which significantly slows down the computer. Therefore, cryptographic protection should be used limitedly, protecting

only that information that really needs to be protected from unauthorized access (Pic. 1).



Picture 1 – Types of Cryptography

Cryptology is divided into two parts: cryptography (encryption) and cryptanalysis. A cryptographer tries to find methods to ensure the secrecy or authenticity (authenticity) of messages. A cryptanalyst tries to perform the reverse task: to crack the ciphertext or to forge it so that it is accepted as genuine.

One of the basic assumptions of cryptography is that the enemy's cryptanalyst has the complete ciphertext and a known encryption algorithm, in addition to the secret key. Under these assumptions, the cryptographer develops a system that is robust to analysis based only on the ciphertext. In fact, some complication of the cryptographer’s task is allowed. An adversary’s cryptanalyst may have fragments of the plaintext and the corresponding ciphertext. In this case, the cryptographer develops a robust system when analyzing the plaintext. A cryptographer can even assume that an adversary's cryptanalyst is able to enter his plaintext and obtain the correct ciphertext using the secret key (chosentext-based analysis), and finally combine the last two possibilities (chosentext-based analysis).

Many of the attacker’s strategies can be blocked by cryptographic security measures, but it should be noted that most of the attacker's strategies are related to user and message authenticity issues [161].

Cryptographic protection subsystem. The subsystem combines the means of cryptographic protection of information and is designed to ensure the integrity, confidentiality, authenticity of critical information, as well as to ensure the legal significance of electronic documents in IS. In a number of functions, the subsystem cooperates with the NSD protection subsystem. Support of the cryptographic protection subsystem of the key management subsystem is provided by the SZY management subsystem.

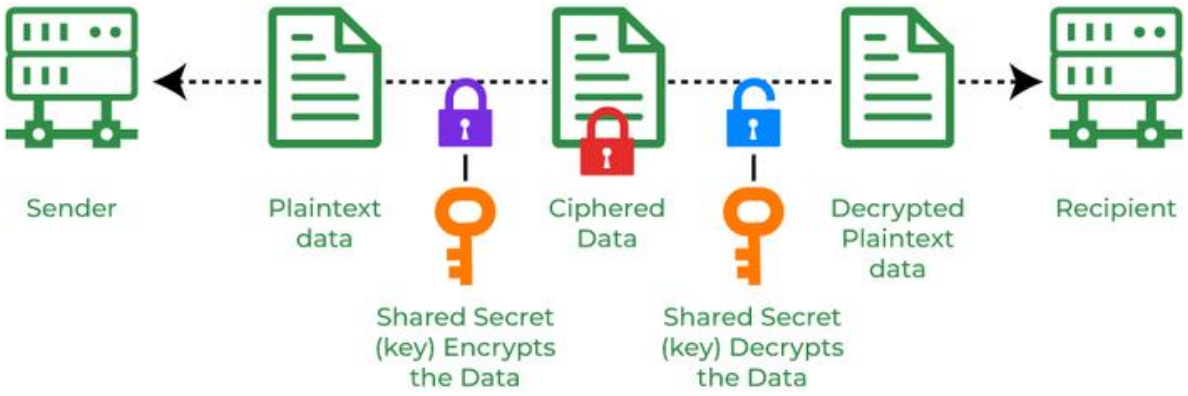
Structurally, the subsystem consists of:

- software tools for symmetric data encryption;
- hardware and software for digital signature of electronic documents (PAS CP). Functions of the subsystem include;
- ensuring the integrity of information transmitted through communication channels and information stored;
- impersonation protection of messages transmitted by communication channels;
- hiding the content of confidential messages transmitted by communication channels and stored on media;
- ensuring the legal significance of electronic documents;
- provision of data source authentication.

The functions of the subsystem are aimed at eliminating the most common message threats in automated systems:

- threats aimed at unauthorized access to information;
- unauthorized reading of information on machine media and in computer memory;
- illegal connection to equipment and communication lines;
- removal of information on power buses;
- interception of EMI from communication lines;

- threats aimed at unauthorized modification (integrity violation) of information:
- changing the service or content part of the message;
- message replacement;
- removal (destruction) of the message (Pic. 2).



Picture 2 – Symmetric Key Cryptography

Threats aimed at distorting the authenticity of the message sender:

- illegally assigning another user's identifiers, creating and sending an electronic document on his behalf (masquerade) or claiming that the information was received from some user, although it was created by the violator himself;
- retransmission of a document created by another user;
- distortion of critical fields of the document (formation date, serial number, address data, identifiers of the sender and recipient) [162].

Threats related to non-recognition of participation:

- refusal to create an electronic document;
- denial of receipt of an electronic document or false information about the time of its receipt;
- a claim that a recipient was sent information at a certain time that was not actually sent (Pic. 3).

Picture 3 – Asymmetric Key Cryptography

Authenticity of messages. The ultimate goal of encryption is to ensure the protection of information from unauthorized access, authentication, to ensure the protection of participants in information exchange from deception based on imitation, for example, forging ciphertext before the arrival of the real ciphertext, replacing (imposing) false information after the arrival of real encryption.

Information authentication means establishing the authenticity of information solely on the basis of the internal structure of the information itself, regardless of the source of this information, establishing by the legal recipient (perhaps an arbitrator) the fact that the received information was most likely transmitted by the legal sender (source) and that it was not replaced or distorted [163].

Any deliberate and accidental attempts to distort information are detected with a certain probability. The problem of authenticity manifests itself most fully in computer networks, where the following types can be distinguished:

- network user authentication – authentication of a network user who needs access to protected information or needs to connect to the network;
- network authentication – establishing the authenticity of the network accessed;
- authentication of arrays of programs and stored data – establishing the fact that this array has not been changed during the time when it was out of direct control, as well as solving questions about the authorship of this array of data;

- authentication of messages – establishing the authenticity of the content of a message received through communication channels and solving questions about the authorship of a message [164].

Solving the specified tasks is possible both with the use of classic encryption systems and public key systems. Cryptographic methods of information protection are based on the use of cryptographic systems, or ciphers. Cryptosystems make it possible to protect information with a high degree of reliability by means of its special transformation. One or more secret parameters unknown to the attacker are used in the crypto-transformation, which is the basis of the stability of cryptosystems.

Cryptosystems are divided into symmetric and asymmetric. In symmetric systems, message conversion (encryption) and reverse conversion (decryption) are performed using the same secret key shared by the sender and receiver of the message. In asymmetric or public-key systems, each user has his own key pair consisting of an encryption key and a decryption key (public key and secret key), while the public key is known to other users. The main methods are encryption, digital signature and impersonation of messages. Encrypting messages allows you to transform the original message (plain text) into an unreadable form. The result of the conversion is called a ciphertext. An attacker without knowledge of the secret encryption key cannot decrypt the ciphertext. Symmetric cryptosystems are usually used to encrypt messages [165].

Encryption provides:

- hiding the content of the message;
- authentication of the data source, only the owner of the secret key could generate and send the ciphertext; however, the electronic document has no legal significance, since falsification is possible on the part of the recipient, who also possesses the secret key.

Digital signature provides:

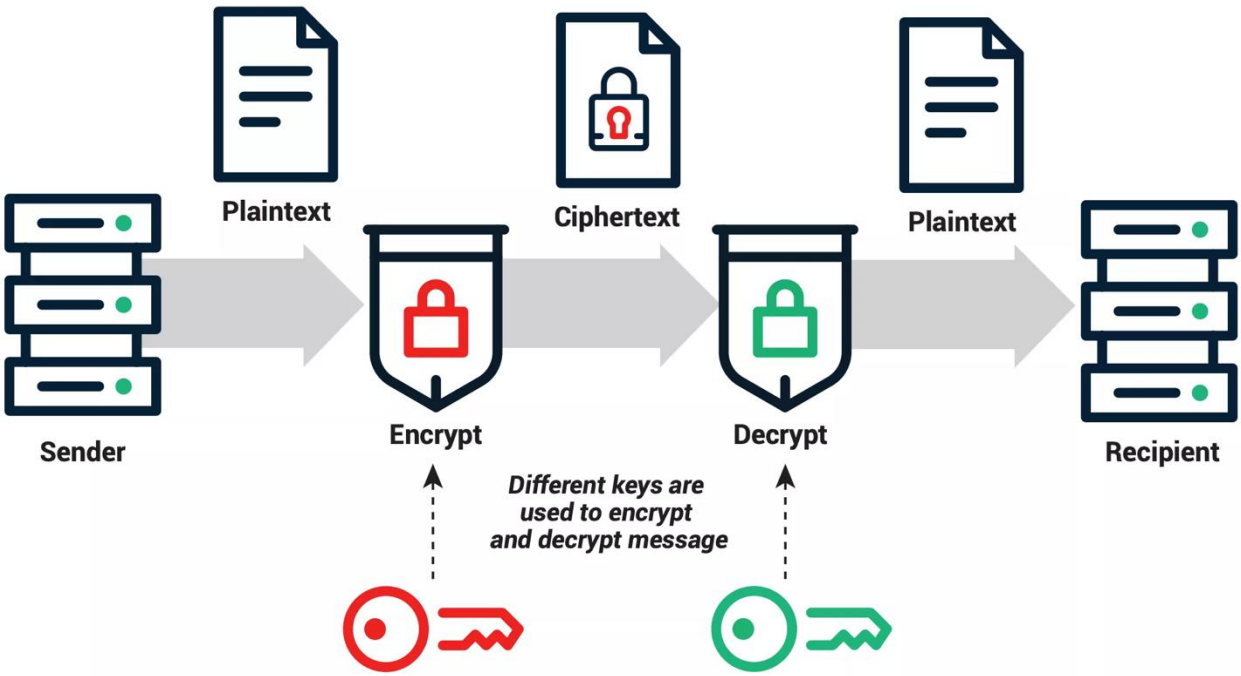
- authentication of the data source, only the owner of the secret asymmetric key could form a digital signature; the recipient has only a public key on which the signature can be verified, including by an independent third party;

- integrity of the message: an attacker cannot purposefully change the text of the message, as this will be revealed during the verification of the digital signature, which includes the encrypted checksum of the message; however, it may accidentally modify the ciphertext or impose a previously transmitted ciphertext;
- the legal significance of the message: a digital signature is equivalent in properties to a handwritten signature due to the impossibility of its forgery, the possibility of verification by the recipient of the document and an independent third party (arbitrator) and ensuring the authentication of the creator of the signature [166].

Imitation protection of messages consists in the formation of a checksum (imitation rate, message authentication code) based on the crypto algorithm attached to the message. After that, the message with the dummy insert is usually encrypted using a symmetric cryptographic algorithm. The principles of generating imitation rates (message authentication codes) are discussed in detail in the preliminary project «Development of a package of software tools for ensuring the legal validity of licenses through a digital signature»[167].

Imitation protection ensures – the integrity of the message in accordance with the properties of the checksum. Analysis of available methods of cryptographic transformations. Currently, both symmetric and asymmetric cryptosystems are widely used. Symmetric systems are used mainly for encryption, as well as for generating cryptographic checksums (imitation rates, hash functions). According to the method of using information encryption tools, stream and block symmetric encryption are usually distinguished. With stream encryption, each symbol of the source text is converted independently of the others, which allows encryption to be carried out simultaneously from data transmission over the communication channel. In block encryption, the source text is transformed indirectly, and the transformation of symbols within the block is interdependent. A large number of block encryption algorithms are known, including those adopted as national standards. The most famous American algorithm

is DES. Encryption of messages is carried out at the subscriber or channel level. Encryption tools are implemented software, hardware-software or hardware (Pic. 4).



Picture 4 – Model Encrypt

In addition, transparent disk encryption requires a significant overhead of system resources (time and performance). And not only directly in the process of reading and writing data. The fact is that reliable cryptographic closure of information involves the periodic change of encryption keys, and this leads to the need to re-encrypt all information on the disk using a new key (it is necessary to decrypt all information using the old and encrypt using the new key). It takes much time. In addition, when working in a system with encrypted disks, delays occur not only when accessing data, but also when starting programs, which greatly slows down the computer [168].

Therefore, it is necessary to use cryptographic protection in a limited way, protecting only that information that really needs to be closed from unauthorized access.