DOI: https://doi.org/10.36910/6775-2524-0560-2024-57-02
UDC 004.056

Dymova Hanna, Candidate of Technical Sciences, Phd., Associate Professor
https://orcid.org/0000-0002-5294-1756
Kherson State Agrarian and Economic University, Kherson, Ukraine

STUDY OF CRYPTOGRAPHIC SECURITY OF COMPUTER NETWORKS

Dymova H. Study of Cryptographic Security of Computer Networks. The article examines modern aspects of cryptographic protection of computer networks, which are critically important in the context of growing information threats and cyberattacks, in particular in the context of military operations in Ukraine. The key tasks related to ensuring the confidentiality, integrity, and availability of information, as well as the challenges facing cryptographic systems in the context of the rapid development of computing power and attack methods, are considered. The article contains an analysis of the historical development of cryptography, starting from its fundamental principles laid down by Claude Shannon, to modern methods such as symmetric and asymmetric encryption, hash functions, digital signatures, and public key infrastructure (PKI). Classical algorithms, including DES, 3DES, AES, RSA, ECC, as well as standards that demonstrate high efficiency in ensuring information security, are considered. A comparative analysis of these algorithms is conducted, their strengths and weaknesses are identified, in particular, taking into account modern challenges such as attacks based on machine learning and the development of quantum computing. Particular attention is paid to the latest threats, including Side-channel and Fault injection attacks that exploit side information or errors in cryptographic systems. These threats are becoming especially relevant for resource-intensive and embedded systems, as well as Internet of Things (IoT) devices. The article emphasizes the importance of developing post-quantum cryptographic algorithms that can provide protection against attacks that exploit the capabilities of quantum computers. It also discusses the need to improve symmetric and asymmetric encryption mechanisms, hash functions, and security protocols to increase their resistance to modern attacks. Based on the analysis, recommendations are proposed for developers of information protection systems aimed at increasing the effectiveness of computer network protection. Particular attention is paid to the implementation of integrated solutions that combine symmetric and asymmetric encryption, digital signatures, and modern cryptographic protocols to ensure multi-level security.

Keywords: cryptography, computer networks, symmetric encryption, asymmetric encryption, quantum cryptography, hash functions.

Димова Г.О. Дослідження криптографічного захисту комп'ютерних мереж. У статті досліджено сучасні аспекти криптографічного захисту комп'ютерних мереж, що є критично важливими в умовах зростання інформаційних загроз та кібератак, зокрема в контексті військових дій в Україні. Розглянуто ключові завдання, пов'язані із забезпеченням конфіденційності, цілісності та доступності інформації, а також виклики, які постають перед криптографічними системами в умовах стрімкого розвитку обчислювальних потужностей та методів атак. Стаття містить аналіз історичного розвитку криптографії, починаючи з її фундаментальних засад, закладених Клодом Шенноном, до сучасних методів, таких як симетричне та асиметричне шифрування, хеш-функції, цифрові підписи та інфраструктура відкритих ключів (PKI). Розглянуто класичні алгоритми, зокрема DES, 3DES, AES, RSA, ECC, а також стандарти, які демонструють високу ефективність у забезпеченні безпеки інформації. Проведено порівняльний аналіз цих алгоритмів, визначено їхні сильні та слабкі сторони, зокрема з урахуванням сучасних викликів, таких як атаки на основі машинного навчання та розвиток квантових обчислень. Особливу увагу приділено новітнім загрозам, серед яких атаки типу Side-channel та Fault injection, що використовують побічну інформацію або помилки в роботі криптографічних систем. Ці загрози стають особливо актуальними для ресурсомістких та вбудованих систем, а також пристроїв Інтернету речей (IoT). У статті підкреслено важливість розробки постквантових криптографічних алгоритмів, здатних забезпечити захист від атак, які використовують можливості квантових комп'ютерів. Також обговорено необхідність удосконалення механізмів симетричного та асиметричного шифрування, хеш-функцій та протоколів безпеки з метою посилення їх стійкості до сучасних атак. На основі проведеного аналізу запропоновано рекомендації для розробників систем захисту інформації, що спрямовані на підвищення ефективності захисту комп'ютерних мереж. Особливу увагу приділено впровадженню інтегрованих рішень, які поєднують симетричне та асиметричне шифрування, цифрові підписи та сучасні криптографічні протоколи для забезпечення багаторівневої безпеки.

Ключові слова: криптографія, комп'ютерні мережі, симетричне шифрування, асиметричне шифрування, квантова криптографія, хеш-функції.

Formulation of the problem. The modern development of information technologies is accompanied by a rapid growth in the volume of data transmitted through computer networks. In the context of military operations in Ukraine, the issue of information security is becoming particularly relevant, as cyberattacks and information threats are becoming an important tool in hybrid warfare. This leads to increased requirements for the reliability of cryptographic protection, which must provide resistance to current and even potential attack methods [1]. Attackers, including state actors, are using increasingly sophisticated methods of hacking cryptographic systems, which creates new challenges for developers of encryption algorithms. In this regard, there is a growing need for a detailed analysis of existing cryptographic protection methods, an assessment of their stability, and the development of innovative approaches to guarantee the secure functioning of computer networks, especially in conditions of military aggression.

Research analysis. The history of modern cryptography began with one person – Claude Elwood Shannon (April 30, 1916 – February 24, 2001) – an American scientist, professor at the Massachusetts Institute of Technology. Shannon was fascinated by cryptography as it existed in the first quarter and up to the middle of the 20th century. Not a single major invention by a scientist in cryptography and information theory was possible without military intervention, since cryptography was a military technology. The most valuable result of C. Shannon's collaboration with the Office of Strategic Services was "A Mathematical Theory of Communication", published by "The Bell System Technical Journal" in 1948, and the mathematical theory of secret keys that followed [2]. These works became the basis for many inventions and discoveries.

Presentation of the main material and justification of the obtained results. Ensuring the confidentiality, integrity, and availability of information in computer networks is one of the key tasks of modern information security systems, especially in the context of military operations in Ukraine. Cryptography plays a central role in data protection, providing encryption and authentication mechanisms to prevent unauthorized access even in the face of increased cyberattacks. At the same time, the constant development of data processing technologies and the growth of computing power are contributing to the emergence of new types of attacks, including attacks using artificial intelligence or quantum computing. This threatens the reliability of traditional cryptographic algorithms, especially in the conditions of their operation in military or critical information systems. In this context, research into the stability of cryptographic systems and the development of innovative approaches to their improvement are urgent scientific and practical tasks. The article presents an analysis of existing cryptographic protection methods, identifies their strengths and weaknesses in light of modern threats, and offers recommendations for increasing the effectiveness of information protection in computer networks in conditions of increased cyber threats.

One of the oldest ciphers is the Caesar cipher. If we make a narrow classification, the Caesar cipher is comparable to the simple substitution cipher, since it uses the replacement (substitution) of a symbol with another, which is located in the alphabet at a fixed position from the one being replaced (Fig. 1).

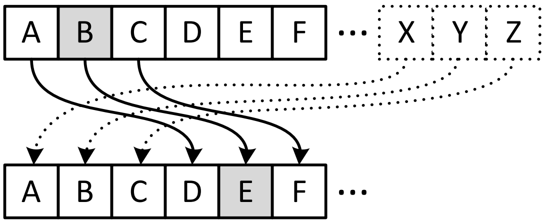

Fig. 1. Monoalphabetic substitution (Caesar cipher)

The cipher received its name in honor of the Roman Emperor Gaius Julius Caesar (Julius Caesar). He used a cipher for secret correspondence. However, modern cryptanalysis does not regard the Caesar cipher as a cipher of acceptable strength. The Vigenere cipher was a continuation of the development of the Caesar cipher [1]. These algorithms are symmetric.

Symmetric encryption is based on using the same key for both encryption and decryption of data. This approach provides high speed of information processing and is relatively simple to implement, but there is a problem with secure key exchange. Examples of such algorithms are DES (Data Encryption Standard), AES (Advanced Encryption Standard) and GOST 28147-89. Symmetric encryption is actively used to ensure data protection in disk systems and communication channels.

Asymmetric encryption uses two related keys: a public key for encryption and a private key for decryption. This approach simplifies key management and allows for digital signatures, but is slower than symmetric encryption. Examples of this type of algorithm include RSA (Rivest-Shamir-Adleman) and elliptic curve cryptography (ECC). Asymmetric encryption is primarily used to protect symmetric encryption keys, as well as to ensure authenticity and non-repudiation in electronic transactions [2, 3].

Hash functions convert an arbitrary-length input text into a fixed-length hash value (hash fingerprint). They are used to verify data integrity and create digital signatures. Examples of such functions include MD5 (Message Digest Algorithm 5), SHA-1 (Secure Hash Algorithm 1), and SHA-256. Hash functions play a key role in cryptographic algorithms and are widely used in security protocols such as SSL/TLS.

Digital signatures are used to verify the authenticity and integrity of messages or documents. They are created using a private key and verified using a public key. Examples include DSA (Digital Signature

Algorithm), RSA, and ECDSA (Elliptic Curve Digital Signature Algorithm). Digital signatures provide a reliable mechanism for identifying the signer and guaranteeing the integrity of the signed document.

A public key infrastructure (PKI) is a system responsible for managing digital certificates and public keys. PKI provides tools for creating, revoking, and verifying certificates that authenticate keys. Its structure includes certification authorities (CAs), registration authorities (RAs), and other components. PKI serves as the foundation for many security systems, such as SSL/TLS, electronic signatures, and electronic payments [2, 4].

Cryptographic protocols provide secure data transmission over insecure communication channels using a combination of symmetric and asymmetric encryption, hash functions, and digital signatures. Examples of such protocols include SSL/TLS (Secure Sockets Layer / Transport Layer Security), IPSec (Internet Protocol Security), and PGP (Pretty Good Privacy). They guarantee the confidentiality, integrity, and authenticity of transmitted data, which is a key aspect of information security on the Internet.

Let's take a look at existing cryptographic security standards [5, 6].

DES (Data Encryption Standard) is a symmetric block cipher algorithm created in the 1970s that uses a 56-bit key to encrypt 64-bit blocks of data. DES remained the primary encryption standard for several decades, but its key length eventually became insufficient to provide protection against brute force attacks. In the context of cryptographic security of computer networks, this algorithm is considered obsolete due to its poor resistance to modern attacks.

3DES (Triple DES) was created as an improvement over DES and uses three sequential stages of data encryption or decryption using three different keys. Due to the increased effective key length of up to 168 bits, 3DES is more resistant to cryptographic attacks. However, its high computational complexity and low data processing speed limit its use in modern computer networks where high performance is required.

AES (Advanced Encryption Standard) is a modern symmetric block cipher standard designed to replace DES. The algorithm supports 128-, 192-, and 256-bit key lengths and processes data in 128-bit blocks. Due to its high performance and resistance to a wide range of cryptographic attacks, AES has become the primary choice for protecting information in computer networks. It is used in military, government, and commercial systems, providing a high level of security.

GOST 28147-89 is a symmetric block cipher standard developed in 1989 in the Soviet Union and later used in post-Soviet countries. It uses a 256-bit key to encrypt 64-bit blocks of data. The algorithm is based on principles similar to DES, but has its own unique features that ensure its resistance to cryptographic attacks. In the context of computer network protection, GOST 28147-89 remains an interesting object for study, although its use is limited due to regional specifics.

RSA (Rivest-Shamir-Adleman) is one of the most famous asymmetric encryption algorithms, developed in 1977. It uses a pair of keys - a public key for encryption and a private key for decryption. The RSA mechanism is based on the complexity of factoring large numbers, which provides a high level of security. The algorithm is widely used to ensure the confidentiality and authenticity of data in computer networks, as well as to create digital signatures, which emphasizes its importance in modern information protection systems.

ECC (Elliptic Curve Cryptography) is a modern asymmetric encryption method that uses the mathematical properties of elliptic curves. Due to its high cryptographic strength with short key lengths, ECC provides efficiency and security, which is critically important in resource-constrained environments. This algorithm is widely used in modern cryptographic protocols such as SSL/TLS and PGP, providing reliable data protection in computer networks.

MD5 (Message Digest Algorithm 5) is a cryptographic hash function created in 1991 that generates a 128-bit hash of an arbitrary input message. It has long been used to verify data integrity, but due to vulnerabilities to collisions, its use in cryptography is no longer recommended. In the context of cryptographic security of computer networks, MD5 is considered obsolete.

SHA-1 (Secure Hash Algorithm 1) is a hash function developed in 1993 that produces a 160-bit hash. It has been widely used to ensure data integrity and authenticity, but collision vulnerabilities have reduced its reliability. Today, SHA-1 is not recommended for use in new cryptographic systems, particularly in computer network security.

SHA-256 (part of the SHA-2 family) is a member of the SHA-2 family of hash functions, designed as a more secure alternative to SHA-1. It generates a 256-bit hash, providing a high level of security and efficiency. SHA-256 is widely used in modern security protocols and cryptographic applications, such as blockchain, digital signatures, and information protection in computer networks.

Let us summarize all the described cryptographic standards in a comparative table (Table 1).

Table 1 – Comparison of cryptographic standards

Standard	Encryption/ hashing type	Key/hash length, in bits	Security	Speed	Algorithm type	Application	Use in networks
DES	symmetrical	56	low	high	block	general	outdated
3DES	symmetrical	112, 168	average	average	block	general	outdated
AES	symmetrical	128, 192, 256	high	high	block	general	+
ГОСТ 28147-89	symmetrical	256	high	high	block	general	–
RSA	asymmetrical	1024, 2048, 4096	high	average	block	digital signatures	+
ECC	asymmetrical	160, 224, 256	high	average	block	digital signatures	+
MD5	hash function	128	low	high	hashing	integrity control	outdated
SHA-1	hash function	160	average	high	hashing	integrity control	–
SHA-256	hash function	256	high	high	hashing	integrity control	+

Analysis of modern cryptographic protection methods shows that algorithms such as AES-256 and ECC with keys of sufficient length provide a high level of resistance to classical attacks. In particular, AES-256, due to its key length and block cipher structure, demonstrates high efficiency in protecting data confidentiality. ECC, based on the complexity of mathematical operations on elliptic curves, allows achieving a similar level of security using shorter keys, which is a significant advantage for resource-intensive systems. However, current trends in technology development create new challenges for cryptographic protection of computer networks, among which the following are particularly important:

- attacks based on machine learning;
- the development of quantum computing.

Modern machine learning technologies allow attackers to analyze cryptographic algorithms to uncover hidden vulnerabilities. Such techniques can be used to predict weaknesses in encryption keys or algorithms, which poses serious threats to traditional security systems.

The emergence of quantum computers poses a significant threat to existing asymmetric cryptosystems such as RSA and ECC. By using Shor algorithms, quantum computers will be able to efficiently factor large numbers or calculate discrete logarithms, which significantly undermines the security of classical cryptographic algorithms. This necessitates the development and implementation of post-quantum cryptographic methods that can withstand such threats.

Threat and vulnerability analysis in the field of cryptographic protection of computer networks reveals a wide range of modern challenges that go beyond traditional attacks such as DoS/DDoS, Man-in-the-Middle (MitM) and phishing. Today's threats are becoming increasingly sophisticated and include Side-channel attacks and Fault injection attacks.

Side-channel attacks are aimed at exploiting side information that occurs during the operation of cryptographic devices or algorithms. For example, analyzing the execution time of operations, energy consumption, or electromagnetic radiation can allow attackers to gain access to cryptographic keys or other confidential data. This type of attack is especially dangerous for embedded systems, IoT devices, and smart cards, where resources for protection are limited.

Fault injection attacks are based on the deliberate introduction of errors into the execution of cryptographic algorithms. Impacting the hardware or software environment, for example by changing voltage, radiation, or introducing defects into the program code, can cause the algorithm to malfunction. This allows attackers to obtain additional information about the internal structure of the system or cryptographic keys. Fault injection attacks are a serious threat to hardware devices such as processors and cryptographic modules.

Modern approaches to cryptographic protection reflect the need to adapt to new challenges associated with the evolution of technologies and attack methods. The main areas are:

– Post-quantum cryptography. With the development of quantum computers, there is a need to create cryptographic algorithms that are resistant to quantum attacks. Post-quantum cryptography is based on mathematical approaches such as lattices, codes, multidimensional polynomial equations, and other complex computational problems. Its development is aimed at ensuring long-term information security in the face of future quantum threats.

– Homomorphic encryption. This is an innovative approach that allows calculations to be performed on encrypted data without the need to decrypt it. Homomorphic encryption opens up new possibilities for secure data processing in cloud environments where privacy protection is critical. It finds applications in financial systems, medicine, and other areas where sensitive data is processed.

– Identity-based cryptography (IBC). This approach simplifies key management by using unique user identifiers, such as email or name, as public keys. IBC reduces the complexity of a public key infrastructure (PKI) and simplifies the authentication and encryption processes, making it attractive for large-scale systems with a large number of users.

– Using machine learning for protection. Machine learning methods are becoming a powerful tool in the fight against modern threats. The use of artificial intelligence algorithms allows you to detect anomalies, analyze network traffic, predict possible attacks and prevent intrusions in time. Machine learning is also used to optimize encryption processes and develop new protective mechanisms.

Conclusions and prospects for further research. Cryptographic protection remains a key element in ensuring the security of computer networks, especially in the context of modern challenges caused by military actions and increased cyberattacks. In the context of war in Ukraine, the need to protect critical infrastructure that ensures the functioning of government institutions, energy systems, the financial sector and military communications is growing. Cryptographic algorithms play a crucial role in ensuring the confidentiality, integrity and availability of data.

However, with the emergence of new threats, such as machine learning-based attacks and the development of quantum computers, traditional encryption methods may not be enough. Cybercriminals are using increasingly sophisticated techniques, which requires continuous improvement of protective technologies. In this context, the development of post-quantum cryptography is becoming a priority, as it is aimed at ensuring resistance to quantum attacks. New algorithms based on lattices, codes and other mathematical approaches promise to become reliable protection in the era of quantum computing.

At the same time, the use of machine learning opens up new opportunities for building security systems. Artificial intelligence algorithms allow you to detect anomalies, analyze cyberattacks in real time, and predict potential threats. Such solutions are especially relevant for protecting networks in conditions of constant cyber threats that arise during military conflicts.

Given today's challenges, it is important to continue research into improving cryptographic methods, adapting them to national security needs and global trends. Particular attention should be paid to integrating the latest technologies into security systems, which will allow for effective countermeasures against threats.

References

1.Stallings W. (2016) Cryptography and Network Security: Principles and Practice. Pearson; 7th edition.

2.Phillips D.T. & Garcia-Diaz A. (1981) Fundamentals of Network Analysis. Prentice-Hall, Inc., Englewood Cliffs, N.J.

3.Dymova, H. (2021). Analiz metodiv otsinky efektyvnosti system fizychnoho zakhystu [Analysis of methods for assessing the effectiveness of physical protection systems]. Computer-Integrated Technologies: Education, Science, Production, (45), 12-18. https://doi.org/10.36910/6775-2524-0560-2023-53-07

4.Dymova H. (2024) Development of a Software Application Algorithm for Solving Computer Network Optimization Problems. Débats scientifiques et orientations prospectives du développement scientifique: c avec des matériaux de la VI conférence scientifique et pratique internationale, Paris, 1er Mars 2024. Paris-Vinnytsia: La Fedeltà & UKRLOGOS Group LLC. DOI: https://doi.org/10.36074/logos-01.03.2024.051 .

5.Dymova, H. (2023). Application of Fast Fourier Transform to the Speech Signals Scrambling. Computer-Integrated Technologies: Education, Science, Production, (53), 44-49. https://doi.org/10.36910/6775-2524-0560-2023-53-07

6.Dymova H. (2023) Application of Characterization Analysis Methods to Investigation of Logical Networks Structures. Theoretical and Empirical Scientific Research: Concept and Trends with Proceedings of the V International Scientific and Practical Conference. Oxford, United Kingdom: European Scientific Platform. DOI: https://doi.org/10.36074/logos-23.06.2023.34.