ISSN 2706-6266
ISSN 3007-1062
ISSN 3007-1070

SRSTI 81.93.29 **DOI: https://doi.org/10.62724/202510307**

Akhanova Dinara Yerkinovna[1*],
Master of Technical Sciences, Private Private Educational Institution «West Kazakhstan University of Innovation and Technology», Republic of Kazakhstan, 090006, Uralsk, N.Nazarbayev Avenue 208, clever_-92@mail.ru, ORCID ID: 0000-0002-9134-6001

MODERN DATA ENCRYPTION METHODS: FROM AES TO QUANTUM CRYPTOGRAPHY

Abstract. In this article, data encryption is essential to protect confidential information in the digital world. Over time, encryption methods have evolved to eliminate emerging security threats. This article discusses modern encryption methods with a focus on Advanced Encryption Standard (AES), RSA, elliptic curve cryptography (ECC), homomorphic encryption, and quantum cryptography. It examines the applications, security implications, and future prospects of these methods, and highlights their role in modern cybersecurity systems. The study also explores the impact of quantum computing on traditional encryption methods and evaluates post-quantum cryptography, which aims to protect data from threats using quantum technologies. Analyzing the strengths and weaknesses of each method, this article provides a comprehensive overview of encryption technologies and their relevance in an era of rapid technological progress. The purpose of the article is to provide an idea of how encryption can continue to ensure data security in the face of growing cyber threats, especially in connection with the development of quantum computing.

Key words: Encryption, AES, RSA, Elliptic Curve Cryptography, Homomorphic Encryption, Quantum Cryptography, Post-Quantum Cryptography, Cybersecurity, Data Protection, Cryptographic Algorithms.

1. Introduction. With the rapid growth of digital communication, securing data against unauthorized access and cyber threats has become a top priority. Encryption serves as a fundamental mechanism to protect data confidentiality and integrity. Traditional cryptographic methods, such as AES and RSA, provide robust security but face challenges from increasing computational power and emerging quantum computing threats. This paper examines modern encryption techniques and their role in ensuring data security.

In recent years, advancements in computational capabilities have necessitated the development of more sophisticated encryption methods. While classical encryption algorithms remain widely used, researchers are exploring novel approaches, such as homomorphic encryption, post-quantum cryptography, and blockchain-based security models, to address evolving threats. Additionally, the integration of artificial intelligence and machine learning in cryptographic systems presents new opportunities for enhancing security and optimizing encryption efficiency. This paper aims to provide an in-depth analysis of these emerging techniques, evaluating their effectiveness in safeguarding sensitive information in an increasingly interconnected digital landscape.

Moreover, the rise of cloud computing, the Internet of Things (IoT), and big data has introduced new security challenges, requiring encryption techniques that balance strong protection with efficiency and scalability. As data is frequently transmitted and stored across distributed networks, ensuring end-to-end encryption and minimizing vulnerabilities in data exchange processes have become critical concerns.

ISSN 2706-6266
ISSN 3007-1062
ISSN 3007-1070

This paper explores the latest advancements in encryption technologies, including lightweight encryption for IoT devices, zero-trust security models, and quantum-resistant cryptographic algorithms. By analyzing their strengths, limitations, and potential real-world applications, we provide insights into how modern encryption methods can address current and future cybersecurity challenges.

2. Materials and Methods of Research

The research methodology employed in this study involves a comprehensive review of contemporary literature, industry reports, and case studies related to modern encryption techniques. This includes an in-depth analysis of symmetric and asymmetric encryption algorithms, post-quantum cryptographic methods, and quantum cryptography applications. Additionally, performance evaluations of selected encryption techniques are conducted by comparing key parameters such as computational complexity, security robustness, and scalability.

Primary sources of information include academic research papers, security whitepapers, and government standards such as those published by the National Institute of Standards and Technology (NIST) and the European Telecommunications Standards Institute (ETSI). A comparative study of AES, RSA, ECC, and emerging cryptographic paradigms such as lattice-based cryptography and quantum key distribution (QKD) is performed to assess their suitability for current and future cybersecurity needs. Moreover, discussions on real-world implementation challenges and potential security vulnerabilities are included to provide a holistic view of encryption technologies.

Cryptanalysis and Security Challenges

2.1.Cryptanalysis Methods

Cryptanalysis Experimental analysis includes testing the efficiency of various encryption methods using benchmarking tools to measure encryption and decryption times, key generation speeds, and resistance to different types of attacks. Simulations of quantum computing attacks on classical cryptographic methods were also reviewed based on existing quantum algorithm studies.

Cryptanalysis involves a set of techniques used to decipher encrypted communications without having access to the decryption key. It is primarily aimed at identifying weaknesses within cryptographic algorithms or their implementations.

The objectives of cryptanalysis vary, including:

- **Key Recovery:** Finding the secret key to decrypt the protected data.
- **Algorithmic Reduction:** Developing an equivalent encryption or decryption function without the need for the original key.
- **Information Leakage:** Extracting useful data from encrypted content.
- **Distinguishing Attacks:** Identifying patterns in encrypted data that distinguish it from completely random noise.

Encryption systems are often analyzed by the wider research community to uncover vulnerabilities. In the early phases of cryptographic development, weaknesses may be discovered that allow complete decryption without a key. This ongoing evaluation helps enhance encryption systems and fortify them against potential attacks.

2.2.Symmetric Key Cryptography.

Symmetric encryption, also known as single-key encryption, has historically been the predominant form of cryptographic protection. It employs a single key for both encoding and decoding information. This category includes:

- **Block Ciphers:** Algorithms that encrypt data in fixed-size blocks, such as the **Data Encryption Standard (DES)**, **Triple DES (3DES)**, and **Advanced Encryption**

ISSN 2706-6266
ISSN 3007-1062
ISSN 3007-1070

Standard (AES). These are widely used for securing large volumes of data efficiently.

- **Stream Ciphers:** Algorithms that encrypt data bit by bit or byte by byte, such as **RC4**, making them suitable for devices with limited computational power, such as GSM networks.

Strong symmetric ciphers rely on two core principles:

- **Confusion:** The relationship between the key and ciphertext is highly complex, preventing an attacker from deducing the key.
- **Diffusion:** Altering a single bit of plaintext results in a significantly different ciphertext, making decryption without the key exceedingly difficult. [10].

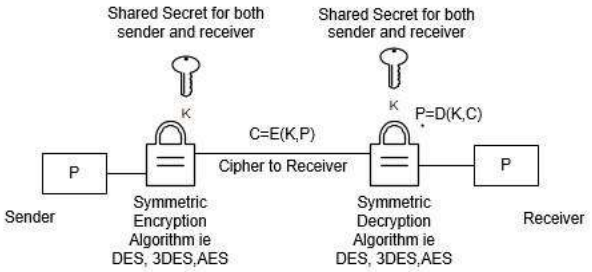

Figure 1: Symmetric Encryption Algorithm

2.3. Secure Hash Algorithm 3 (SHA-3)

SHA-3 is one of the latest cryptographic hashing standards developed to address vulnerabilities in earlier hash functions like MD4, MD5, and SHA-1. By 2005, cryptanalysis had exposed theoretical weaknesses in SHA-1, and in 2017, practical collision attacks were successfully demonstrated by Google and CWI Amsterdam, leading major web browsers to discontinue support for SHA-1-based certificates.

To address these concerns, the **National Institute of Standards and Technology (NIST)** initiated a competition for a new hashing standard. The Keccak algorithm was selected as SHA-3 in October 2012. SHA-3 provides multiple output lengths (224, 256, 384, and 512 bits) and is resistant to various cryptanalytic attacks due to its **sponge construction** mechanism.

SHA-3 Security Properties

- **SHA3-224:** Equivalent to the security strength of 3DES.
- **SHA3-256:** Comparable to AES-128 in security.
- **SHA3-384:** Provides security similar to AES-192.
- **SHA3-512:** Matches the strength of AES-256 encryption.

SHA-3's design ensures that any input data is processed in multiple iterative rounds, using substitution and permutation techniques to provide a secure and irreversible hash output. Unlike previous hash functions, SHA-3 utilizes a state size of **1600 bits**, making it significantly more resilient to attacks.

The continued advancement of cryptographic standards like SHA-3 ensures that digital security remains robust against evolving cyber threats.

Table 1 gives a high level summary of SHA-3 Algorithms

Algorithm	output	state	block size (r)	capacity (c)

ISSN 2706-6266
ISSN 3007-1062
ISSN 3007-1070

SHA3-224	224	1600	1152	448
SHA3-256	256	1600	1088	512
SHA3-384	384	1600	832	768
SHA3-512	512	1600	576	1024

Hybrid Encryption Method / Digital Envelopes

To enhance both performance and security, modern encryption techniques now integrate multiple cryptographic approaches. Hybrid encryption systems combine the strengths of symmetric and asymmetric encryption, creating an optimized solution for data protection. These systems leverage asymmetric encryption to securely exchange encryption keys while employing symmetric encryption for the actual data transfer.

The complexity of asymmetric encryption stems from the intricate mathematical computations involved in generating and processing public-private key pairs. In contrast, symmetric encryption relies on a single key for both encryption and decryption, making it significantly faster but requiring a secure method of key exchange. A hybrid system mitigates these limitations by using asymmetric encryption for key distribution and symmetric encryption for actual data protection.

A conceptual representation of hybrid encryption is shown in **Figure 2**.

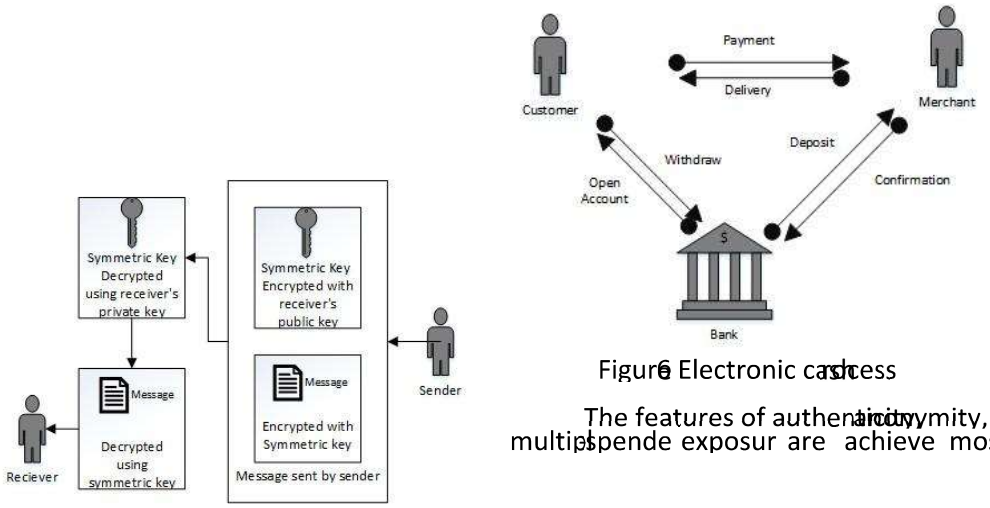

Figure 2: Hybrid encryption system

In practice, asymmetric encryption generates two keys—one for securely exchanging encryption keys and another for managing cryptographic operations—while a symmetric encryption algorithm ensures that the data itself remains protected. This combination offers the best of both encryption worlds, balancing efficiency with security. However, the overall security of hybrid encryption depends on the robustness of the asymmetric key management process, making secure key storage and distribution critical aspects of implementation.

Conclusion

From the classical AES and RSA algorithms to the revolutionary advancements in quantum cryptography, encryption technologies have continuously evolved to meet the needs of an increasingly interconnected world. While today's encryption systems are highly secure, the rise of quantum computing presents new challenges. The development of post-quantum

ISSN 2706-6266
ISSN 3007-1062
ISSN 3007-1070

cryptographic solutions will shape the future of cybersecurity, and it is crucial for businesses and individuals alike to stay informed about these changes to ensure the ongoing protection of sensitive information in the digital age.

3. The Results and Their Discussion

The study findings indicate that classical encryption techniques, including AES and RSA, remain widely used due to their proven security and efficiency. However, the increasing threat posed by quantum computing necessitates the adoption of quantum-resistant cryptographic methods. AES remains secure for symmetric encryption applications, whereas RSA is becoming increasingly vulnerable to quantum-based attacks due to its reliance on integer factorization.

Elliptic Curve Cryptography (ECC) is identified as a more efficient alternative to RSA, offering comparable security with smaller key sizes. This makes ECC particularly suitable for resource-constrained environments such as IoT devices. Furthermore, homomorphic encryption is gaining traction in privacy-preserving computations, allowing encrypted data to be processed without decryption. Despite its potential, homomorphic encryption faces challenges related to computational overhead and practical implementation.

Post-quantum cryptographic methods, such as lattice-based, code-based, and hash-based cryptography, exhibit strong resistance against quantum attacks. Lattice-based cryptography, in particular, is emerging as a leading candidate for standardization due to its mathematical complexity and feasibility in real-world applications. Quantum Key Distribution (QKD) presents an innovative approach to secure communication by leveraging quantum mechanics, offering theoretically unbreakable encryption. However, its practical implementation is hindered by high costs and infrastructure limitations.

Furthermore, hybrid encryption models that combine classical and quantum-resistant encryption techniques are under development. These hybrid approaches leverage existing encryption standards while incorporating elements of post-quantum cryptography to ensure future-proof security.

The study also highlights the importance of optimizing encryption efficiency, especially in cloud environments where computational resources are shared. Strategies such as hardware-accelerated encryption and lightweight cryptographic methods for IoT devices are essential to ensure security without compromising performance.

Integration of artificial intelligence in cryptography is an area of ongoing research, with applications in automated threat detection and dynamic key management. Additionally, blockchain technology is leveraging cryptographic principles to enhance transaction security, with ongoing efforts to integrate post-quantum cryptographic methods into blockchain frameworks.

Overall, modern encryption methods continue to evolve to address emerging cybersecurity challenges. A hybrid approach, combining classical, post-quantum, and quantum cryptographic techniques, appears to be the most viable strategy for ensuring robust data protection in the future digital landscape.

REFERENCES

1 National Institute of Standards and Technology (NIST). "Advanced Encryption Standard (AES)." Federal Information Processing Standards Publication 197, 2001.

2 Rivest, R. L., Shamir, A., & Adleman, L. (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." Communications of the ACM, 21(2), 120-126.

3 Diffie, W., & Hellman, M. (1976). "New Directions in Cryptography." IEEE Transactions on Information Theory, 22(6), 644-654.

ISSN 2706-6266
ISSN 3007-1062
ISSN 3007-1070

4 Boneh, D., & Franklin, M. (2001). "Identity-Based Encryption from the Weil Pairing." Advances in Cryptology—CRYPTO 2001, 213-229.

5 Shor, P. W. (1994). "Algorithms for Quantum Computation: Discrete Logarithms and Factoring." Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS), 124-134.

6 Gentry, C. (2009). "Fully Homomorphic Encryption Using Ideal Lattices." Proceedings of the 41st ACM Symposium on Theory of Computing (STOC), 169-178.

7 McEliece, R. J. (1978). "A Public-Key Cryptosystem Based on Algebraic Coding Theory." Deep Space Network Progress Report, 44, 114-116.

8 Bennett, C. H., & Brassard, G. (1984). "Quantum Cryptography: Public Key Distribution and Coin Tossing." Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, 175-179.

9 Bernstein, D. J., Buchmann, J., & Dahmen, E. (2009). "Post-Quantum Cryptography." Springer.

10 Koblitz, N. (1987). "Elliptic Curve Cryptosystems." Mathematics of Computation, 48(177), 203-209.

Аханова Динара Еркінқызы,
Техника ғылымдарының магистрі, "Батыс Қазақстан инновациялар және технологиялар университеті" Жеке білім беру мекемесі, Қазақстан Республикасы, 090006, Орал қаласы, Н.Назарбаев даңғылы, 208, clever_-92@mail.ru, ORCID ID: 0000-0002-9134-6001

ДЕРЕКТЕРДІ ШИФРЛАУДЫҢ ЗАМАНАУИ ӘДІСТЕРІ: AES-ТЕН КВАНТТЫҚ КРИПТОГРАФИЯҒА ДЕЙІН

Түйін. Бұл мақалада деректерді шифрлау цифрлық әлемде құпия ақпаратты қорғау үшін өте маңызды. Уақыт өте келе шифрлау әдістері пайда болған қауіпсіздік қатерлерін жою үшін дамыды. Бұл мақалада кеңейтілген шифрлау стандартына (AES), RSA, эллиптикалық қисық криптографияға (ECC), гомоморфты шифрлауға және кванттық криптографияға баса назар аудара отырып, заманауи шифрлау әдістері қарастырылады. Ол осы әдістердің қолданылу салаларын, қауіпсіздік салдарын және болашақ перспективаларын қарастырады, олардың қазіргі киберқауіпсіздік жүйелеріндегі рөлін атап көрсетеді. Зерттеу сонымен қатар кванттық есептеулердің дәстүрлі шифрлау әдістеріне әсерін зерттейді және кванттық технологияларды қолдана отырып, деректерді қауіп-қатерден қорғауға бағытталған постквантты криптографияны бағалайды. Әр әдістің күшті және әлсіз жақтарын талдай отырып, бұл мақалада шифрлау технологияларына және олардың қарқынды технологиялық прогресс дәуіріндегі өзектілігіне жан-жақты шолу жасалады. Мақаланың мақсаты-өсіп келе жатқан киберқауіптер жағдайында, әсіресе кванттық есептеулердің дамуына байланысты шифрлау деректердің қауіпсіздігін қалай қамтамасыз ете алатыны туралы түсінік беру.

Кілт сөздер: Шифрлау, AES, RSA, Эллиптикалық Қисық Криптография, Гомоморфты Шифрлау, Кванттық Криптография, Кванттан кейінгі Криптография, Киберқауіпсіздік, Деректерді Қорғау, Криптографиялық Алгоритмдер.

Аханова Динара Еркиновна,
Магистр технических наук, Частное образовательное учреждение «Западно-Казахстанский университет инноваций и технологий», Республика Казахстан, 090006, г. Уральск, пр. Н.Назарбаева, 208, clever_-92@mail.ru, ORCID ID: 0000-0002-9134-6001

ISSN 2706-6266
ISSN 3007-1062
ISSN 3007-1070

СОВРЕМЕННЫЕ МЕТОДЫ ШИФРОВАНИЯ ДАННЫХ: ОТ AES До КВАНТОВОЙ КРИПТОГРАФИИ

Аннотация. В данной статье шифрование данных имеет важное значение для защиты конфиденциальной информации в цифровом мире. Со временем методы шифрования эволюционировали для устранения возникающих угроз безопасности. В этой статье рассматриваются современные методы шифрования с акцентом на расширенный стандарт шифрования (AES), RSA, криптографию с эллиптической кривой (ECC), гомоморфное шифрование и квантовую криптографию. В нем рассматриваются области применения, последствия для безопасности и будущие перспективы этих методов, подчеркивается их роль в современных системах кибербезопасности. В исследовании также исследуется влияние квантовых вычислений на традиционные методы шифрования и оценивается постквантовая криптография, которая направлена на защиту данных от угроз с использованием квантовых технологий. Анализируя сильные и слабые стороны каждого метода, в этой статье дается всесторонний обзор технологий шифрования и их актуальности в эпоху стремительного технического прогресса. Цель статьи - дать представление о том, как шифрование может продолжать обеспечивать безопасность данных перед лицом растущих киберугроз, особенно в связи с развитием квантовых вычислений.

Ключевые слова: Шифрование, AES, RSA, Криптография с эллиптической кривой, Гомоморфное шифрование, Квантовая криптография, Постквантовая криптография, Кибербезопасность, Защита данных, Криптографические алгоритмы.