UDC 004.7 **doi: 10.26906/SUNZ.2026.1.058**

Gennadii Golovko, Oleksandr Rudenko

National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine

COMPARATIVE ANALYSIS OF MODERN CRYPTOGRAPHIC CIPHERS AND THE AES ALGORITHM

Abstract. The growing intensity of cybersecurity threats has made information protection a critical issue in the modern digital landscape. Cryptographic algorithms serve as a fundamental mechanism for maintaining data confidentiality and integrity across information systems. The Advanced Encryption Standard (AES) continues to be one of the most trusted and extensively deployed encryption algorithms; however, a range of modern cryptographic alternatives has emerged, offering different performance and security characteristics. This paper presents a comparative analysis of both symmetric and asymmetric ciphers based on key criteria such as security level, computational efficiency, and resistance to cryptographic attacks. The strengths and weaknesses of each algorithm are examined, along with their suitability for various application environments. Particular emphasis is placed on the practical use of AES and competing ciphers in sectors including finance, telecommunications, and healthcare. The results of the comparison provide guidance for selecting appropriate cryptographic solutions for safeguarding sensitive data and contribute to a broader understanding of the effectiveness of contemporary cryptographic technologies.

Keywords: cryptography, functions, cypher, aes, operator, algorithm.

Introduction

In the modern digital world, the issue of information protection has become extremely relevant. Cryptographic algorithms are the basis for secure data transmission, protection of confidential information, and the functioning of most cybersecurity systems. Among the numerous encryption methods, AES (Advanced Encryption Standard) occupies a special place, which has become the international standard for block data encryption [1].

The growing dependence of society on digital technologies has significantly increased the volume of sensitive data processed and transmitted through open communication channels. Financial transactions, personal records, medical information, and government data are constantly exposed to potential cyber threats. In this context, cryptographic protection plays a crucial role, as it provides a mathematically grounded mechanism for preventing unauthorized access, data leakage, and information manipulation. Unlike organizational or software-based security measures, cryptographic methods ensure data protection even in untrusted environments, making them a fundamental component of modern information security systems. However, the development of information technology, the emergence of new types of threats, and the need for efficiency for devices with limited resources prompt us to compare AES with modern alternatives [2].

The purpose of this article is to review and compare several modern cryptographic ciphers with the AES algorithm according to the main criteria: security, speed, resource efficiency, and application prospects.

1. Overview of the AES algorithm

AES, also known as Rijndael, was officially adopted as the encryption standard by the National Institute of Standards and Technology (NIST) in 2001. It is a symmetric block cipher that encrypts data in 128-bit blocks and supports key sizes of 128, 192, and 256 bits. Its security is achieved through a multi-layered structure of substitutions, permutations, and linear transformations applied over multiple rounds, which provides strong resistance against cryptanalytic attacks [3]. One of the key strengths of AES is its combination of high security and efficiency. Unlike older algorithms such as DES, AES can withstand modern attack techniques, including differential and linear cryptanalysis. Its robustness has been thoroughly tested over decades of academic and practical scrutiny, making it one of the most trusted cryptographic algorithms for protecting sensitive information.

AES also benefits from widespread hardware support. Many modern processors include AES-NI instruction sets, which allow encryption and decryption operations to be executed directly by the CPU, significantly improving performance. This hardware acceleration makes AES suitable for both high-performance server environments and resource-constrained devices that require fast and reliable encryption.

The practical applications of AES are extensive. It is widely used in securing internet communications through protocols such as TLS and IPsec, in wireless networks including Wi-Fi, in cloud storage solutions, and in enterprise security systems. Its ability to protect data while maintaining high speed and low computational overhead has made it a default choice for both governmental and commercial applications.

In the current digital landscape, organizations face an increasing number of sophisticated cyber threats, including ransomware, data breaches, and targeted attacks on critical infrastructure. AES plays a pivotal role in mitigating these risks by ensuring that sensitive data remains encrypted and unreadable even if intercepted. Its proven resilience against cryptanalytic attacks and compatibility with modern cybersecurity frameworks make it a fundamental tool for defending against both external and internal threats, protecting personal, corporate, and governmental information.

Moreover, AES's flexible key sizes allow organizations to balance performance and security based

on specific needs. For example, AES-128 provides strong security with minimal computational cost, while AES-256 offers an even higher level of protection suitable for long-term data confidentiality in critical environments.

2. Modern Cryptographic Ciphers

2.1. ChaCha20-Poly1305. ChaCha20-Poly1305 is a stream cipher combined with an authentication mechanism that ensures both confidentiality and data integrity. It was designed to achieve high performance in software-based implementations, particularly on mobile and embedded platforms where hardware acceleration for AES is unavailable.

The ChaCha20 algorithm relies on simple arithmetic operations such as addition, rotation, and XOR, which contributes to its speed and resistance to cryptographic attacks. Today, ChaCha20-Poly1305 is widely deployed in modern communication protocols, including TLS 1.3 and QUIC, and is used by major platforms such as Google, Cloudflare, and OpenVPN [4].

2.2. Twofish and Blowfish. Twofish was one of the final candidates in the AES standardization process. It is a symmetric block cipher that operates on 128-bit blocks and supports key lengths of up to 256 bits. The algorithm is based on a Feistel network structure, which provides flexibility and strong cryptographic properties. Although Twofish performs well in software environments, its more complex design generally makes it slower than AES [5].

Blowfish, introduced in 1993, is the predecessor of Twofish. Despite being used in certain legacy systems, Blowfish is now considered outdated due to its fixed 64-bit block size, which does not meet the security requirements of modern cryptographic applications [6].

2.3. Serpent. Serpent is another algorithm that reached the final stage of the AES competition. It employs 32 rounds of encryption, resulting in a very high level of security. However, this design choice negatively affects performance, making Serpent slower compared to AES. As a result, Serpent is typically used in scenarios where security is prioritized over speed [7].

2.4. Lightweight Ciphers. The expansion of the Internet of Things (IoT) has increased demand for cryptographic algorithms that can function effectively on devices with limited processing power, memory, and energy resources. Lightweight ciphers such as PRESENT, Simon, and Speck are specifically designed for such environments. While they offer acceptable performance for sensor networks and embedded systems, these algorithms are generally less trusted than AES or ChaCha20 due to limited cryptanalysis and standardization [8].

3. Comparison criteria

Cryptographic algorithms are commonly evaluated using several fundamental parameters:

1. **Security.** AES remains a reference standard, as no practical attacks have been discovered that compromise its security. ChaCha20 is also considered robust against known cryptanalytic attacks, while Twofish and Serpent continue to provide sufficient security for real-world use. Blowfish, however, is regarded as obsolete because of its small block size [2].
2. **Performance.** In software-only implementations without hardware acceleration, ChaCha20-Poly1305 often outperforms AES by a factor of two to three. When AES-NI instructions are available, AES becomes the fastest option. Serpent is comparatively slow due to its high number of rounds, while Twofish offers moderate performance [2].
3. **Resource efficiency.** Lightweight ciphers require minimal memory and energy, making them suitable for constrained devices. AES demonstrates moderate resource usage, particularly when supported by hardware optimizations [2].
4. **Resistance to side-channel attacks.** Modern implementations of AES and ChaCha20 are designed to mitigate side-channel threats, including timing and power analysis attacks. Serpent is also noted for its resistance to such attacks because of its straightforward S-box structure [2].
5. **Areas of application.** AES is widely adopted in government, military, and enterprise systems. ChaCha20 is commonly used in mobile environments and modern network protocols. Twofish and Serpent are mainly applied in experimental or specialized security solutions [2].

4. Comparative analysis (Table 1)

Table 1 – **Comparative analysis**

Algo-rithm	Encryption type	Key length	Security level	Speed of operation	Main advantages	Main disadvantages
DES	Symmetric	56 bits	Low	High	Ease of implementation, historical significance	Low cryptographic strength, easily cracked by brute force
3DES	Symmetric	112/168 bits	Medium	Low	Higher level of security compared to DES	Slow operation, outdated approach
AES	Symmetric	128/192/256 bits	High	High	High speed, scalability, resistance to attacks, flexibility of application	Requires secure key exchange
RSA	Asymmetric	1024–4096 bits	High	Low	Secure key exchange, digital signatures	Slow encryption speed of large data, significant resources

4.1. Implementation Aspects and Practical Deployment Challenges. Beyond theoretical security and performance metrics, the real-world effectiveness of a cryptographic algorithm largely depends on implementation quality and deployment context. Even the strongest cipher may become vulnerable if

implemented incorrectly or integrated into insecure protocols. Therefore, practical considerations such as key management, operational modes, and resistance to implementation flaws are essential components of comparative evaluation [9]. One of the critical aspects of symmetric encryption is the selection of an appropriate mode of operation. AES, for example, can be deployed in various modes, including CBC (Cipher Block Chaining), CTR (Counter Mode), and GCM (Galois/Counter Mode). Among these, authenticated encryption modes such as AES-GCM have become the preferred standard because they provide both confidentiality and integrity protection. Improper configuration—such as reuse of initialization vectors or weak randomness—can significantly undermine security regardless of the algorithm's mathematical strength [6]. ChaCha20-Poly1305 addresses many of these concerns by integrating encryption and authentication into a unified construction. This design reduces the risk of configuration errors and simplifies secure implementation. As a result, it is often considered less error-prone in practice compared to block cipher constructions that require careful combination with separate authentication mechanisms. Another important implementation factor is protection against side-channel attacks. While theoretical cryptanalysis focuses on mathematical weaknesses, practical attacks often exploit timing differences, power consumption patterns, or electromagnetic emissions. Modern AES implementations frequently rely on constant-time execution and hardware instructions such as AES-NI to mitigate timing-based vulnerabilities. Similarly, ChaCha20 was intentionally designed to avoid data-dependent memory access patterns, thereby reducing exposure to timing attacks in software environments.

Resource constraints also influence deployment decisions. In embedded systems, memory footprint and energy consumption can be decisive factors. Lightweight ciphers are optimized for minimal hardware gates and reduced computational complexity, making them attractive for microcontrollers and sensor networks. However, in high-throughput server infrastructures, hardware-accelerated AES typically achieves superior performance and scalability [4].

Interoperability and ecosystem support further affect practical adoption. AES benefits from two decades of widespread integration into operating systems, network protocols, cryptographic libraries, and hardware modules. This maturity ensures compatibility, long-term support, and comprehensive security evaluation. By contrast, newer or more specialized algorithms may lack extensive tooling, certification frameworks, or regulatory recognition, which can limit their deployment in governmental or highly regulated sectors [8].

4.2. Risk Assessment and Algorithm Selection Strategy. When selecting a cryptographic algorithm, organizations must consider a comprehensive risk assessment framework. The decision should not rely solely on theoretical security strength but should also account for operational lifespan, threat models, infrastructure capabilities, and regulatory requirements.

For short-term data protection in controlled environments, AES-128 may provide sufficient security with optimal performance. For long-term confidentiality, especially in government or critical infrastructure systems, AES-256 is often recommended due to its higher resistance to potential future computational advancements. In mobile and cloud-based applications where hardware acceleration is unavailable, ChaCha20-Poly1305 may offer superior performance without compromising security [6].

In IoT ecosystems, the choice becomes more nuanced. While AES can be implemented efficiently in hardware, extremely constrained devices may benefit from lightweight algorithms. Nevertheless, such decisions must carefully balance efficiency gains against reduced cryptanalytic maturity and potential interoperability challenges.

Ultimately, no single algorithm can be considered universally optimal for all scenarios. Instead, cryptographic agility—the ability to transition between algorithms as threats evolve — has become an essential principle of modern cybersecurity architecture. Systems should be designed to support algorithm updates without requiring complete infrastructure replacement, thereby ensuring long-term adaptability [6].

5. Future Trends in Symmetric Cryptography and Post-Quantum Considerations

The continuous advancement of computing technologies has a direct impact on the development of cryptographic systems. One of the most significant emerging challenges is the potential rise of quantum computing, which threatens many classical encryption schemes. Although symmetric algorithms such as AES are more resistant to quantum attacks than asymmetric ones, long-term security considerations remain essential.

Quantum algorithms like Grover's algorithm could effectively reduce the security level of symmetric ciphers by half. Consequently, AES-256 is increasingly recommended for applications that require long-term data protection. This highlights the adaptability of AES, which can maintain its relevance by increasing key size without altering the underlying algorithm. [8]

At the same time, modern cryptographic research emphasizes the importance of simplicity and resistance to implementation-based attacks. Algorithms such as ChaCha20 demonstrate that efficient and transparent designs can enhance both security and performance.

In addition, the growing number of IoT and embedded systems continues to drive interest in lightweight cryptographic solutions. While these ciphers are not intended to replace AES in critical infrastructures, they serve as valuable alternatives for environments with strict resource limitations.

6. Standardization efforts by organizations such as NIST remain crucial in shaping the future of cryptography. The widespread adoption of AES and ChaCha20 illustrates the importance of extensive analysis, transparency, and long-term trust in cryptographic standards [9].

Conclusions

The conducted analysis confirms that AES continues to be the "gold standard" of symmetric

encryption, offering a balanced combination of strong security, high performance, and broad hardware support. Nevertheless, modern stream ciphers such as ChaCha20-Poly1305 provide notable advantages in software-based and mobile environments. Twofish and Serpent remain secure alternatives, although their performance is generally inferior to that of AES. Lightweight ciphers play an increasingly important role in IoT applications, where resource efficiency is critical.

Therefore, the selection of a cryptographic algorithm should be based on specific operational requirements, including available resources, performance constraints, and desired security level. AES remains a universal solution, while modern ciphers effectively complement it in specialized use cases.

Conflicts of interest

The authors declare that they have no conflicts of interest in relation to the current study, including financial, personal, authorship, or any other, that could affect the study, as well as the results reported in this paper.

Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technologies when creating the current work.

REFERENCES

1. Sovin Ya., Khoma V. Comparison of AEAD algorithms for embedded systems of the Internet of Things. Lviv Polytechnic, 2019. ena.lpnu.ua. DOI: https://doi.org/10.23939/csn2019.01.076
2. Comparative study of the implementation of block ciphers for devices with limited resources (review). News of Higher Education Institutions. Radioelectronics, 2023. radio.kpi.ua DOI: https://doi.org/10.20535/S0021347023050011
3. Comparative Analysis of AES, Blowfish, Twofish, Salsa20, and ChaCha20 for Image Encryption. arXiv, 2024. arxiv.org DOI: https://doi.org/10.48550/arXiv.2407.16274
4. Alanazi, H. et al. New Comparative Study Between DES, 3DES and AES Within Nine Factors. arXiv, 2010. DOI: https://doi.org/10.48550/arXiv.1003.4085
5. Shevchuk, Y. Analytical Approach to Evaluating the Effectiveness of Cryptographic Methods in Modern Information Security Systems. Futurity Proceedings, 2023. DOI: https://doi.org/10.5281/zenodo.15095109
6. Golovko G., Rudenko O., Batrachenko. A., Ryzymenko R, Organization of information protection at the "Drive Petrol" enterprise using a cryptographic algorithm AES. DOI: https://doi.org/10.26906/SUNZ.20 24.1.050
7. G. Golovko, D. Iievliev Enhanced authorization for secure management of sensitive data in hybrid applications Системи управління навігації та зв'язку 2 (72) 2023. – С .98-100. – Doi: https://doi.org/10.26906/SUNZ.2023.2.098
8. G. Golovko, M. Kalynovych Specifics of implementation of the on asymmetric encryption Algorithm elliptic curves Системи управління навігації та зв'язку 1 (71) 2023. – С .84-90. – Doi: https://doi.org/10.26906/SUNZ.2022.4.066
9. G. Golovko, M. Tolochyn Using the AES encryption method in practice Системи управління навігації та зв'язку 4 (70) 2022. – С. 71-74. – Doi: https://doi.org/10.26906/SUNZ.2022.4.071

Received (Надійшла) 23.10.2025
Accepted for publication (Прийнята до друку) 04.02.2026
Publication date (Дата публікації) 27.02.2026

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Головко Геннадій Вячеславович – кандидат технічних наук, доцент, доцент кафедри комп'ютерних та інформаційних технологій і систем, Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна;
Gennadii Golovko – Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Computer and Information Technologies and Systems, National University "Y. Kondratyuk Poltava Polytechnic", Poltava, Ukraine;
e-mail: GenVGolovko@ukr.net, ORCID Author ID: http://orcid.org/0000-0002-1745-1321.

Руденко Олександр Антонович – кандидат технічних наук, доцент кафедри комп'ютерних та інформаційних технологій і систем, Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна;
Oleksandr Rudenko – Candidate of Technical Sciences, Associate Professor of the Department of Computer and Information Technologies and Systems, National University "Y. Kondratyuk Poltava Polytechnic", Poltava, Ukraine;
e-mail: olexantr@gmail.com; ORCID Author ID: https://orcid.org/0000-0002-7110-0653;
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57203147373.

Порівняльний аналіз сучасних криптографічних шифрів та алгоритму AES

Г. В. Головко, О. А. Руденко

Анотація. Зростання інтенсивності кіберзагроз у сучасному цифровому середовищі робить захист інформації критично важливим завданням. Криптографічні алгоритми є фундаментальним механізмом забезпечення конфіденційності та цілісності даних в інформаційних системах. Стандарт розширеного шифрування AES (Advanced Encryption Standard) залишається одним із найбільш надійних і широко застосовуваних алгоритмів, проте з'являється дедалі більше сучасних криптографічних альтернатив із різними характеристиками безпеки та продуктивності. У роботі проведено порівняльний аналіз симетричних і асиметричних шифрів за ключовими критеріями, зокрема рівнем захищеності, обчислювальною ефективністю та стійкістю до криптографічних атак. Розглянуто переваги й обмеження кожного алгоритму, а також оцінено доцільність їх використання в різних прикладних середовищах. Особливу увагу приділено практичному застосуванню AES та конкуруючих алгоритмів у фінансовій сфері, телекомунікаціях і медицині. Отримані результати сприяють вибору оптимальних криптографічних рішень для захисту конфіденційної інформації та поглиблюють розуміння ефективності сучасних криптографічних технологій.

Ключові слова: криптографія, функції, шифр, AES, оператор, алгоритмю