eISSN: 2229-3213 pISSN: 2229-3205
The Journal of Applied Science and Social Science
Volume 16,Issue 01 January , 2026

OPTIMIZATION AND TESTING OF DATA ENCRYPTION ALGORITHMS

Kokand University, Andijan Branch
Computer Engineering, Group 24_05
Student: ***Sobirova Muslimaxon Farhodbek kizi***
Email: muslimasobirova96@gmail.com
Phone: +998 94 782 13 18

Annotation

This study focuses on the optimization and testing of data encryption algorithms, which are critical for ensuring information security in computer systems and digital communications [1, 2, 10]. The research analyzes symmetric and asymmetric encryption methods, evaluates their performance, and proposes strategies for improving computational efficiency and robustness [3, 5, 6]. The results highlight the importance of selecting appropriate algorithms based on security requirements, processing speed, and resource consumption [4, 7, 8]. This work provides practical recommendations for software developers and cybersecurity specialists to enhance data protection and minimize vulnerabilities [2, 9, 10].

Keywords

data encryption, encryption algorithms, optimization, testing, cybersecurity, symmetric encryption, asymmetric encryption, performance evaluation.

Annotatsiya

Ushbu tadqiqot ma’lumotlarni shifrlash algoritmlarini optimallashtirish va sinovdan o‘tkazishga qaratilgan bo‘lib, ular kompyuter tizimlari va raqamli kommunikatsiyalarda axborot xavfsizligini ta’minlashda muhim ahamiyatga ega [1, 2, 10]. Tadqiqot simmetrik va assimetrik shifrlash usullarini tahlil qiladi, ularning samaradorligini baholaydi va hisoblash resurslarini tejash hamda xavfsizlikni oshirish bo‘yicha strategiyalarni taklif qiladi [3, 5, 6]. Natijalar shuni ko‘rsatadiki, algoritmlarni tanlashda xavfsizlik darajasi, ishlash tezligi va resurs iste’moli hisobga olinishi zarur [4, 7, 8]. Ushbu ish dasturchilar va kiberxavfsizlik mutaxassislariga ma’lumotlarni himoya qilish va zaifliklarni kamaytirishga amaliy tavsiyalar beradi [2, 9, 10].

Kalit so‘zlar

ma’lumotlarni shifrlash, shifrlash algoritmlari, optimallashtirish, sinov, kiberxavfsizlik, simmetrik shifrlash, assimetrik shifrlash, samaradorlikni baholash.

Аннотация

Данное исследование посвящено оптимизации и тестированию алгоритмов шифрования данных, которые имеют критическое значение для обеспечения информационной безопасности в компьютерных системах и цифровых коммуникациях [1, 2, 10]. Исследование анализирует симметричные и асимметричные методы шифрования, оценивает их производительность и предлагает стратегии повышения вычислительной эффективности и надежности [3, 5, 6]. Результаты подчеркивают важность выбора подходящих алгоритмов с учетом требований безопасности, скорости обработки и потребления ресурсов [4, 7, 8]. Работа предоставляет практические рекомендации разработчикам программного обеспечения и специалистам по кибербезопасности для усиления защиты данных и минимизации уязвимостей [2, 9, 10].

Ключевые слова

шифрование данных, алгоритмы шифрования, оптимизация, тестирование, кибербезопасность, симметричное шифрование, асимметричное шифрование, оценка производительности.

Introduction

In the modern digital era, the security of information has become one of the most critical concerns for individuals, organizations, and governments [1, 2]. With the rapid growth of

computer networks, cloud computing, mobile applications, and online services, sensitive data such as personal information, financial records, and confidential communications are constantly transmitted and stored in digital formats [3, 4]. This widespread exchange of information makes data highly vulnerable to unauthorized access, interception, and cyberattacks [5, 6]. Consequently, data encryption has emerged as a fundamental tool for ensuring confidentiality, integrity, and security in digital systems [2, 7].

Data encryption transforms readable information into a coded format that can only be accessed or decrypted by authorized parties. There are two main types of encryption: symmetric encryption, which uses the same key for both encryption and decryption, and asymmetric encryption, which uses a pair of public and private keys [3, 5]. Each approach has its own advantages and limitations in terms of processing speed, computational resources, and security strength [6, 7]. Therefore, optimizing encryption algorithms and thoroughly testing their performance is essential to achieve a balance between security and efficiency [8, 9].

The primary aim of this research is to study the methods for optimizing data encryption algorithms, evaluate their computational performance, and provide strategies for enhancing security without compromising processing speed [1, 2]. The study focuses on assessing both symmetric and asymmetric encryption algorithms, analyzing their strengths and weaknesses, and conducting practical tests to determine their suitability for various applications [3, 5]. By addressing these objectives, this research contributes to the development of more secure, efficient, and reliable data protection mechanisms for modern digital systems [4, 7].

Moreover, the study highlights the importance of algorithm selection based on specific requirements, such as the level of security needed, the type of data being protected, and the available computational resources [6, 8]. The results of this research can provide practical guidance for software developers, cybersecurity specialists, and IT professionals to implement effective encryption strategies and minimize vulnerabilities in digital systems [2, 9].

Research Methodology

This study employs a comprehensive research methodology to investigate the optimization and testing of data encryption algorithms [1, 3]. The methodology combines theoretical analysis, empirical evaluation, and computational experiments to provide a detailed understanding of encryption algorithm performance, efficiency, and security [4, 5]. A multi-step approach is adopted to ensure that all aspects of encryption optimization are systematically addressed [6, 7].

The first stage of the research is theoretical analysis, which involves a thorough review of existing literature, scientific articles, textbooks, and international standards related to data encryption [1, 2, 10]. During this phase, symmetric and asymmetric encryption algorithms, such as AES, DES, RSA, and ECC, are studied in detail [3, 5]. The principles, advantages, and limitations of each algorithm are analyzed, with particular attention to computational requirements, processing speed, and security strength [6, 7]. The theoretical analysis also considers international guidelines and best practices for encryption implementation, including recommendations from organizations such as OWASP and ISO/IEC [1, 10].

The second stage is empirical evaluation. This stage involves practical testing of selected encryption algorithms using real-world datasets and computational simulations [4, 5]. Metrics such as encryption and decryption speed, CPU and memory usage, and resistance to common attacks are measured [6, 8]. The evaluation focuses on determining which algorithms provide optimal performance without compromising security [7, 9]. Additionally, various parameter settings, key lengths, and algorithmic optimizations are tested to assess their effect on efficiency and robustness [3, 6].

The third stage involves comparative analysis and optimization techniques. The results obtained from empirical testing are compared to identify the most efficient and secure algorithms for different types of applications [4, 5, 7]. Optimization methods, including algorithmic enhancements, parallel processing, and hardware acceleration, are applied and analyzed [6, 8].

The study also evaluates trade-offs between performance and security, providing a framework for selecting algorithms based on specific requirements, such as low-latency environments or resource-constrained devices [2, 9].

Throughout the research, analytical and statistical methods are used to interpret data, quantify performance improvements, and validate experimental results [3, 7]. Visualization techniques, charts, and performance metrics are employed to clearly present findings [5, 6]. This systematic methodology ensures that conclusions drawn from the study are reliable, reproducible, and applicable in practical scenarios [1, 2].

Research Results

The research conducted on data encryption algorithms produced several significant findings regarding their optimization, performance, and security [3, 5]. The empirical tests and computational evaluations allowed for a systematic comparison of symmetric and asymmetric encryption algorithms, highlighting their strengths, limitations, and areas for improvement [4, 6].

The first key result concerns symmetric encryption algorithms, such as AES (Advanced Encryption Standard) and DES (Data Encryption Standard) [1, 3]. AES demonstrated high computational efficiency, faster encryption and decryption times, and strong resistance to known attacks, making it suitable for high-volume data processing [5, 6]. DES, while historically important, showed lower security strength and slower performance, indicating its limited applicability in modern systems [7, 8]. Optimization techniques, such as parallel processing and block size adjustments, were observed to enhance AES performance further, reducing computational overhead without compromising security [3, 5].

Regarding asymmetric encryption algorithms, such as RSA and ECC (Elliptic Curve Cryptography), the study revealed that these algorithms provide higher security for key exchange and authentication but are generally slower in processing large volumes of data compared to symmetric algorithms [4, 6]. The performance tests indicated that ECC offers equivalent security to RSA with shorter key lengths, resulting in faster computations and reduced memory consumption, making ECC particularly advantageous for resource-constrained devices and mobile applications [7, 9].

The research also analyzed the impact of key length and parameter selection on algorithm performance [3, 5]. Increasing the key length generally improved security but slightly decreased processing speed. Conversely, optimized parameter choices, such as using efficient key generation methods and precomputed tables, improved performance while maintaining adequate security levels [4, 6].

Another important result involved comparative analysis across different computing environments [2, 7]. Symmetric algorithms such as AES performed exceptionally well in high-performance computing environments, while ECC provided the best balance of security and efficiency in mobile and low-power systems [5, 8].

Finally, the study provided practical recommendations for software developers and cybersecurity specialists [2, 9]. Implementing AES for bulk data encryption, using ECC for secure key exchange, applying algorithmic optimizations, and balancing key length with processing efficiency are all essential steps for achieving robust and efficient encryption [3, 6].

Literature Review

Data encryption has long been recognized as a fundamental component of information security in digital systems [1, 2]. Numerous studies have examined encryption algorithms, their efficiency, and their applicability across different computational environments [3, 4]. Symmetric encryption methods, such as AES and DES, have been extensively studied for their fast processing speeds and suitability for bulk data encryption [5, 6].

Asymmetric encryption algorithms, including RSA and ECC, have also received considerable attention in the literature [3, 7]. Comparative studies emphasized that ECC provides

equivalent security to RSA but with shorter key lengths, resulting in higher efficiency in mobile and resource-constrained environments [4, 8].

Optimization techniques, including parallel processing, hardware acceleration, and efficient key generation, have been identified as essential for improving algorithm performance [5, 6]. Benchmarking and performance testing are critical steps in algorithm selection and implementation [7, 9].

International standards and guidelines, including OWASP and ISO/IEC, provide frameworks for secure implementation of encryption methods [1, 10].

Conclusion and Recommendations

This study focused on the optimization and testing of data encryption algorithms, emphasizing their critical role in ensuring information security in modern digital systems [1, 2].

The results indicate that symmetric algorithms, particularly AES, offer high computational efficiency and robust security for large volumes of data, while DES is less suitable for modern applications [3, 5]. Asymmetric algorithms such as RSA provide strong security for key exchange but require more computational resources, whereas ECC delivers equivalent security with shorter key lengths, making it optimal for resource-constrained devices [4, 6].

Based on the findings, recommendations include: implement AES for bulk data encryption, use ECC for secure key exchange and mobile applications, apply algorithmic optimization techniques, and select key lengths that balance security with computational efficiency [3, 7, 9].

Optimizing and testing encryption algorithms is essential for achieving secure and efficient data protection. This research provides actionable insights for deploying effective encryption strategies in diverse applications [2, 10].

References

1. OWASP Foundation. OWASP Mobile Top 10 Risks. OWASP, 2022. https://owasp.org
2. Smith, J. Data Encryption Techniques and Applications. New York: TechPress, 2018.
3. Kumar, R., Sharma, P. Performance Analysis of Symmetric and Asymmetric Encryption Algorithms. International Journal of Information Security, 2020, Vol. 15, Issue 2, pp. 45-58.
4. Lee, H. Optimization of Data Encryption Algorithms for High-Performance Systems. Journal of Cybersecurity, 2019, Vol. 7, Issue 3, pp. 112-125.
5. Chen, Y., Wang, L. Comparative Study of RSA and ECC in Mobile Applications. Cybersecurity Review, 2021, Vol. 9, Issue 1, pp. 34-50.
6. Patel, S. Techniques for Improving Encryption Algorithm Efficiency. Mobile Computing and Applications, 2020, Vol. 12, Issue 4, pp. 65-78.
7. Miller, D. Practical Implementation of Encryption Algorithms in Different Operating Systems. Journal of Information Technology, 2021, Vol. 18, Issue 2, pp. 89-102.
8. Alasmary, W., Alhaidari, F. Benchmarking and Testing of Encryption Algorithms. International Journal of Mobile Computing, 2020, Vol. 6, Issue 2, pp. 23-38.
9. Gupta, A., Singh, R. Security and Performance Trade-offs in Data Encryption. Information Security Journal, 2019, Vol. 28, Issue 1, pp. 55-67.
10. OWASP Foundation. Mobile Application Security Verification Standard (MASVS). OWASP, 2021. https://owasp.org