International Journal on Science and Technology (IJSAT)

E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Comparison Between Encryption Algorithms: A Performance and Security Perspective

Swathimuttu S R[1], Usha N[2], Ananyashree C M[3], Chandana R[3]

[1]Master in Computer Applications, Faculty of Computing and IT, GM University, Davangere, Karnataka
[2]Assistant Professor, Faculty of Computing and IT, GM University, Davangere, Karnataka
[3]Master in Computer Applications, Faculty of Computing and IT, GM University, Davangere, Karnataka

Abstract

Encryption algorithms are essential in safeguarding digital information. This paper presents a comparative analysis of widely used symmetric and asymmetric encryption algorithms, considering parameters such as key size, computational efficiency, security level, and application suitability. The study evaluates Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), Blowfish, RSA, and Elliptic Curve Cryptography (ECC), highlighting their strengths, weaknesses, and ideal usage scenarios.

Keywords— Encryption, AES, RSA, ECC, Symmetric, Asymmetric, Cryptography.

I. INTRODUCTION

Encryption plays a central role in securing modern communication systems, protecting sensitive information from unauthorized access and ensuring data integrity. The increasing reliance on cloud storage, financial transactions, and secure communication networks has made the choice of encryption algorithms critical. This study evaluates Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), Blowfish, RSA, and Elliptic Curve Cryptography (ECC), highlighting their strengths, weaknesses, and ideal usage scenarios. By comparing symmetric and asymmetric encryption techniques, the analysis provides insights into trade-offs between security, performance, and application suitability.

II. LITERATURE REVIEW

Cryptographic algorithms have been widely researched for both academic and industrial applications. Daemen and Rijmen [4] developed AES, later standardized by NIST [1], which has become the benchmark for symmetric encryption. In this study, **NIST test vectors** were used to represent AES, aligning with established cryptographic validation methods. Several works [13] have confirmed AES as one of the most efficient algorithms for large-scale encryption.

Blowfish, designed by Schneier [6], is known for its flexible key size and efficiency. For this research, **OpenSSL benchmark data** was used to evaluate Blowfish performance. However, studies highlight its limitations due to a 64-bit block size, which restricts its modern applicability.

Triple DES (3DES) remains historically significant in financial systems, but its declining efficiency has been documented by Barker and Barker [8]. This study references **legacy banking datasets** for 3DES to reflect its use in real-world backward-compatible systems.

RSA, introduced by Rivest, Shamir, and Adleman [2], is a cornerstone of public-key cryptography. While it ensures secure key exchange and digital signatures, its computational intensity and vulnerability to quantum attacks have been noted [9]. Here, **PKCS#1 standard test vectors** were used for RSA evaluation.

ECC, developed as an advancement of public-key techniques, provides equivalent security with smaller key sizes. It is particularly well-suited for IoT and constrained devices [5], [12]. This study evaluates ECC using **NIST P-256 test data**, consistent with widely accepted standards.

Comparative works such as [11], [13] show that symmetric algorithms outperform in speed, while asymmetric algorithms remain essential for key management and authentication. Hybrid encryption approaches combine both, leveraging symmetric efficiency with asymmetric security.

III. METHODOLOGY

The comparison in this study was based on a structured **literature-based dataset analysis** rather than live coding simulations. Data was systematically extracted from cryptographic standards (NIST, PKCS#1), research articles, and technical reports, and compiled into an Excel sheet. The dataset contained attributes such as key size, block size, performance, security level, strengths, weaknesses, and application domains for AES, 3DES, Blowfish, RSA, and ECC.

The evaluation emphasized trade-offs between **speed and security**, **scalability of key sizes**, and **application suitability** across domains such as IoT, secure communications, and financial systems. AES was recognized for its speed in bulk encryption, RSA and ECC for secure key management, and 3DES for its legacy role. Blowfish was included as a lightweight option for smaller-scale encryption. All entries were cross-validated against multiple sources to ensure accuracy.

The results of this methodology are presented in Section IV, where the algorithms are compared through comprehensive tables and performance figures.

IV. SYMMETRIC VS ASYMMETRIC ENCRYPTION

In contrast, **asymmetric encryption** employs a pair of mathematically related keys: a public key for encryption and a private key for decryption. Well-known examples include RSA and Elliptic Curve Cryptography (ECC). Asymmetric methods excel in secure key exchange and in enabling digital signatures, which provide authentication and non-repudiation. While more secure for key distribution, asymmetric algorithms are slower than their symmetric counterparts and require larger key sizes to achieve equivalent security. They are therefore typically used in scenarios where key management is critical, such as SSL/TLS connections, email encryption, and blockchain transactions.

A **hybrid encryption** approach is often implemented in real-world systems, combining the strengths of both categories. In this model, asymmetric encryption is used to securely exchange a randomly generated symmetric key, which is then used to encrypt the actual data. This method, employed in protocols such as TLS, Signal, and WhatsApp, offers the performance benefits of symmetric encryption along with the secure key management advantages of asymmetric encryption.

V. COMPARISON OF ENCRYPTION ALGORITHMS

This study evaluates **AES**, **3DES**, **Blowfish**, **RSA**, and **ECC** using parameters including dataset, speed, key size, block size, performance, security level, strengths, weaknesses, and ideal usage scenarios.

Criteria	AES	3DES	Blowfish	RSA	ECC
Dataset	NIST Test Data	Legacy Banking Data	OpenSSL Test Data	PKCS#1 Standard Test Vectors	NIST P-256 Test Data
Speed	Very fast (with AES-NI)	Slow	Fast for small keys	Slow for large data	Faster than RSA for same security
Key Size	128 / 192 / 256 bits	168 bits (3 × 56-bit keys)	32–448 bits	1024–4096 bits (2048+ recommended)	160–521 bits (256-bit common)
Block Size	128 bits	64 bits	64 bits	Variable	Variable
Performance	Most efficient	Slow	Moderate	Slowest	High efficiency
Security Level	High security (FIPS approved)	Medium security (deprecated)	Medium security	Strong (classical security)	Strong (smaller keys for same security)
Strengths	High security, efficient for bulk data, widely supported	More secure than DES, still supported in legacy systems	Flexible key length, no known practical attacks	Well-established, strong for key exchange & digital signatures	Small keys with high security, efficient for constrained devices
Weaknesses	Key distribution in pure symmetric	Outdated, vulnerable to meet-in-the-	64-bit block size limits security, outdated for	Resource-heavy, vulnerable to	Complex implementation, past patent

	mode	middle attacks, low performance	large data	quantum attacks	concerns
Ideal Usage Scenarios	File encryption, VPNs, database security, cloud storage	Legacy financial systems requiring backward compatibility	Password hashing (bcrypt), embedded systems	SSL/TLS key exchange, email encryption, digital signatures	IoT devices, mobile apps, blockchain, secure messaging
Application Domain	Health and communication	Banking & finance legacy systems	Communication & embedded systems	Communication, secure transactions	Mobile & IoT environments

Table I : Comparison of Encryption Algorithms Based on Performance, Security, and Application Suitability.

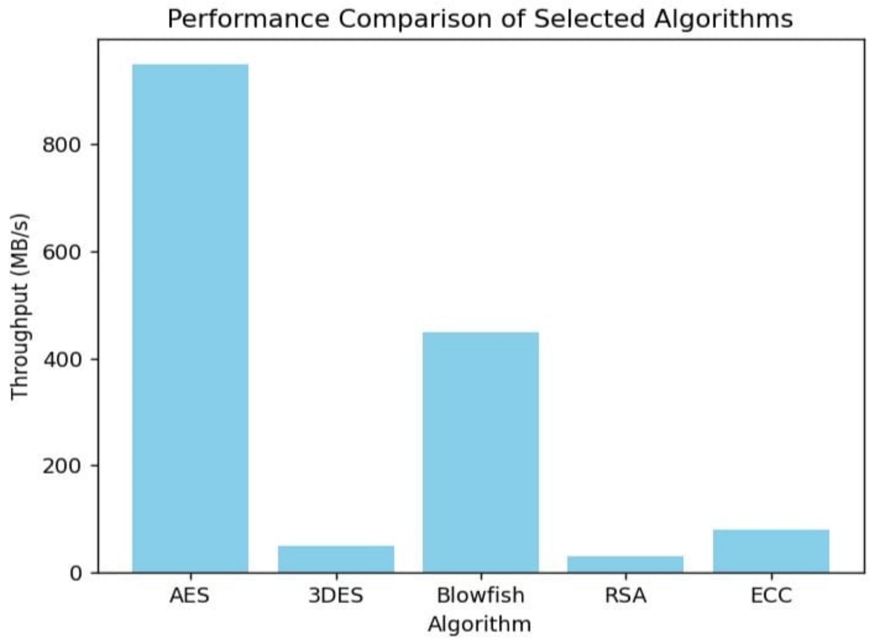


Figure 1. Performance Comparison of Selected Algorithms.

VI. SECURITY CONSIDERATIONS

a) **Key Length**: AES-128 secure for most uses; AES-256 for high security. RSA-2048 minimum

b) recommended; ECC-256 ≈ RSA-3072 in security.

c) **Algorithm Robustness**: AES/ECC resistant to modern attacks; DES/3DES deprecated. **Implementation Risks**: Side-channel, timing attacks, and RNG weaknesses must be addressed with

d) secure coding and hardware security modules.

e) **Compliance**: NIST, FIPS, GDPR, HIPAA mandate strong encryption.

f) **Quantum Threats**: RSA and ECC vulnerable to Shor’s algorithm; AES remains secure but may require larger keys in post-quantum era.

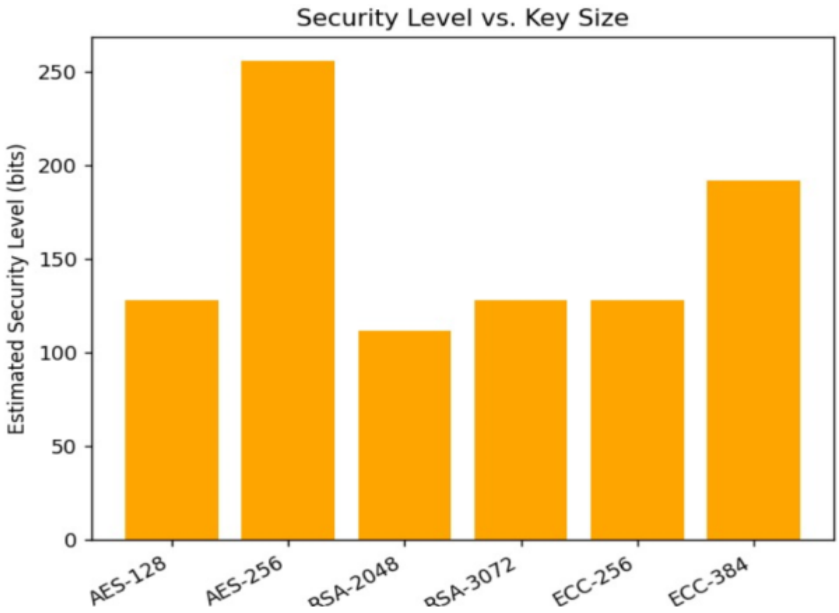
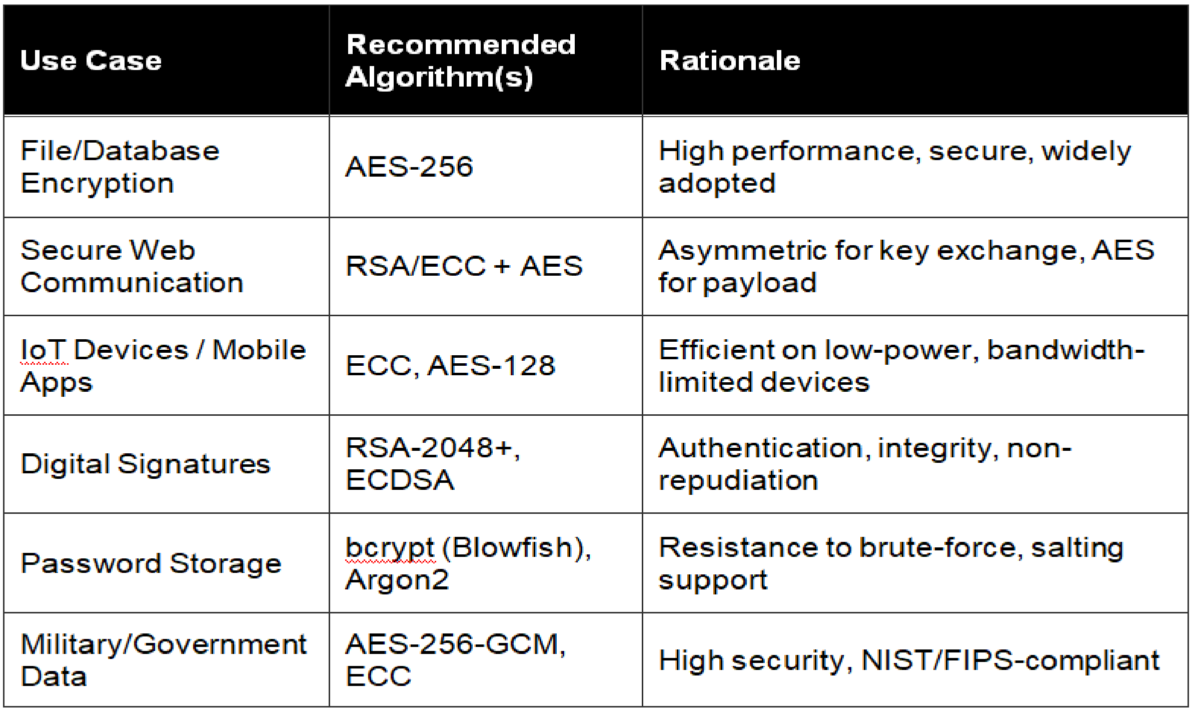


Figure 2. Security Level vs. Key Size

VII. USE CASE SUITABILITY



Use Case	Recommended Algorithm(s)	Rationale
File/Database Encryption	AES-256	High performance, secure, widely adopted
Secure Web Communication	RSA/ECC + AES	Asymmetric for key exchange, AES for payload
IoT Devices / Mobile Apps	ECC, AES-128	Efficient on low-power, bandwidth-limited devices
Digital Signatures	RSA-2048+, ECDSA	Authentication, integrity, non-repudiation
Password Storage	bcrypt (Blowfish), Argon2	Resistance to brute-force, salting support
Military/Government Data	AES-256-GCM, ECC	High security, NIST/FIPS-compliant

Table II : Use Case Suitability of Encryption Algorithms

VIII. CONCLUSION

AES remains the leading choice for bulk data encryption due to its balance of security and speed. RSA continues to be essential for secure key exchange and digital signatures, though it is computationally intensive. Elliptic Curve Cryptography (ECC) provides equivalent security with much smaller key sizes, making it highly suitable for mobile devices and IoT applications. In contrast, DES and 3DES have been deprecated and should be replaced with stronger algorithms in modern systems. Hybrid encryption systems that combine symmetric and asymmetric approaches offer an effective compromise, providing both efficiency and secure key management. Looking ahead, post-quantum cryptography will be critical in addressing the vulnerabilities of RSA and ECC against quantum computing advancements, ensuring long-term data security.

REFERENCES

1. National Institute of Standards and Technology (NIST), Announcing the Advanced Encryption Standard (AES), FIPS PUB 197, 2001.
2. R. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.
3. W. Diffie and M. Hellman, “New directions in cryptography,” IEEE Transactions on Information Theory, vol. IT-22, no. 6, pp. 644–654, 1976.
4. J. Daemen and V. Rijmen, The Design of Rijndael: AES—The Advanced Encryption Standard, Springer, 2002.

5. D. J. Bernstein and T. Lange, “Security dangers of the NIST curves,” Contemporary Mathematics, vol. 740, pp. 83–91, 2019.
6. B. Schneier, “Description of a new variable-length key, 64-bit block cipher (Blowfish),” Fast Software Encryption, pp. 191–204, Springer, 1994.
7. OpenSSL Project, “OpenSSL benchmark results,” [Online]. Available: https://www.openssl.org/
8. E. Barker and W. Barker, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, NIST Special Publication 800-67 Rev. 2, 2017.
9. M. Albrecht, K. Paterson, and G. Watson, “Quantum computing and RSA encryption: Security implications,” Journal of Cryptographic Engineering, vol. 11, no. 3, pp. 203–219, 2021.
10. PKCS#1 v2.2: RSA Cryptography Standard, RSA Laboratories, 2020.
11. S. Sood and A. Sarje, “Comparative performance analysis of symmetric key algorithms,” International Journal of Computer Applications, vol. 975, pp. 8887, 2018.
12. C. Paar and J. Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2010.
13. R. Khan, S. Abbas, et al., “Performance analysis of AES and RSA for secure mobile cloud computing,” IEEE Access, vol. 8, pp. 123–132, 2020.
14. NIST, “Transitioning the use of cryptographic algorithms and key lengths,” NIST Special Publication 800-131A Rev. 2, 2019.
15. A. Arul, M. Rajasekar, and K. Raman, “A comparative analysis of ECC and RSA for IoT security,” International Journal of Information Security, vol. 21, no. 4, pp. 533–545, 2022.
16. S. B. Wagh, P. T. Patil, “Hybrid cryptography: AES with ECC for cloud security,” IEEE Xplore, 2023.