COMPREHENSIVE CIPHER PERFORMANCE ANALYSIS

A Comparative Study of Encryption Algorithms and Operational Modes

ANTONIYA JENCY J
3rd Year, Computer Science Engineering
Loyola ICAM College of Engineering and Technology
Tamil Nadu, India

ABSTRACT

This research paper presents a comprehensive benchmarking study of eight encryption cipher modes, comparing their performance characteristics and security properties across multiple data sizes. The study encompasses modern cryptographic standards (AES), legacy systems (3DES), and custom implementations (SaltedCipher) in multiple operational modes (ECB, CBC, CFB). Through rigorous testing with 50 iterations per benchmark across six data sizes (8 bytes to 256 KB), we demonstrate that AES-CBC achieves optimal performance (393.22 MB/s) while maintaining industry-standard security properties. The analysis reveals that AES is 100x faster than SaltedCipher and 10x faster than 3DES, primarily due to hardware acceleration (AES-NI) on modern processors. Our findings provide actionable guidance for selecting appropriate encryption algorithms for diverse applications, from high-performance web services to legacy system support. The research emphasizes the critical importance of cipher mode selection, demonstrating that ECB mode, while fastest, is cryptographically unsuitable for sensitive data due to its deterministic nature. This comprehensive analysis serves as a reference for practitioners, researchers, and organizations making encryption algorithm selection decisions.

Keywords: Encryption, Cipher Modes, Performance Analysis, AES, 3DES, Cryptography, Benchmarking

TABLE OF CONTENTS

1. INTRODUCTION

Encryption is a fundamental component of modern information security, protecting sensitive data from unauthorized access. This research paper presents a comprehensive comparative analysis of eight encryption cipher modes, evaluating their performance characteristics, security properties, and suitability for various applications. The primary objectives are: (1) to benchmark eight distinct cipher modes across multiple data sizes, (2) to compare performance metrics, (3) to analyze security properties, and (4) to provide evidence-based recommendations for cipher selection.

2. LITERATURE REVIEW

2.1 Cryptographic Standards

The evolution of cryptographic standards reflects advancement in computational capabilities. DES (1977) provided the first standardized encryption algorithm. Triple DES (3DES) served as an interim solution. AES, adopted by NIST in 2001, represents the current cryptographic standard for U.S. government and most international applications, offering superior security and performance.

2.2 Block Cipher Modes

Block cipher modes define how block ciphers process data larger than their block size. ECB (Electronic Codebook) is simple but deterministic. CBC (Cipher Block Chaining) provides semantic security through feedback mechanisms. CFB (Cipher Feedback) converts block ciphers into stream ciphers, eliminating padding requirements.

2.3 Hardware Acceleration

Modern processors include AES-NI (AES New Instructions), available since 2008, providing 10-100x performance improvements. This hardware support has made AES the dominant choice for performance-critical applications.

3. METHODOLOGY

3.1 Experimental Design

This research employs quantitative benchmarking methodology. Eight cipher modes are tested across six data sizes (8 bytes to 256 KB) with 50 iterations per test. Parameters: AES 128-bit key, 3DES 192-bit key, SaltedCipher 128-bit key, IV/salt 64-128 bits, random alphanumeric test data.

3.2 Metrics

Three primary metrics: (1) Encryption Time (milliseconds), (2) Decryption Time (milliseconds), (3) Throughput (MB/s) = Data Size / (Encryption Time + Decryption Time) / 1,000,000.

4. PERFORMANCE RESULTS

4.1 Performance Summary at 32KB

Cipher	Encrypt (ms)	Decrypt (ms)	Throughput (MB/s)	Rank
AES-ECB	0.0639	0.1096	386.96	■ 1st
AES-CBC	0.0893	0.0716	393.22	■ 2nd
AES-CFB	1.0937	1.0334	29.41	■ 3rd
3DES-ECB	0.8106	0.8020	38.76	4th
3DES-CBC	0.8908	0.8038	36.98	5th
3DES-CFB	6.8976	6.4743	4.68	6th
SaltedCipher-CFB	6.1159	6.1902	5.08	7th
SaltedCipher-CBC	6.1879	6.0150	5.12	8th

4.2 Analysis

AES-CBC achieves 393.22 MB/s throughput with optimal security. AES-ECB is fastest (386.96 MB/s) but unsuitable for sensitive data. 3DES-CBC achieves 36.98 MB/s. SaltedCipher achieves 5.12 MB/s. Performance differences are critical at production-relevant sizes (32KB-256KB).

5. VISUAL ANALYSIS

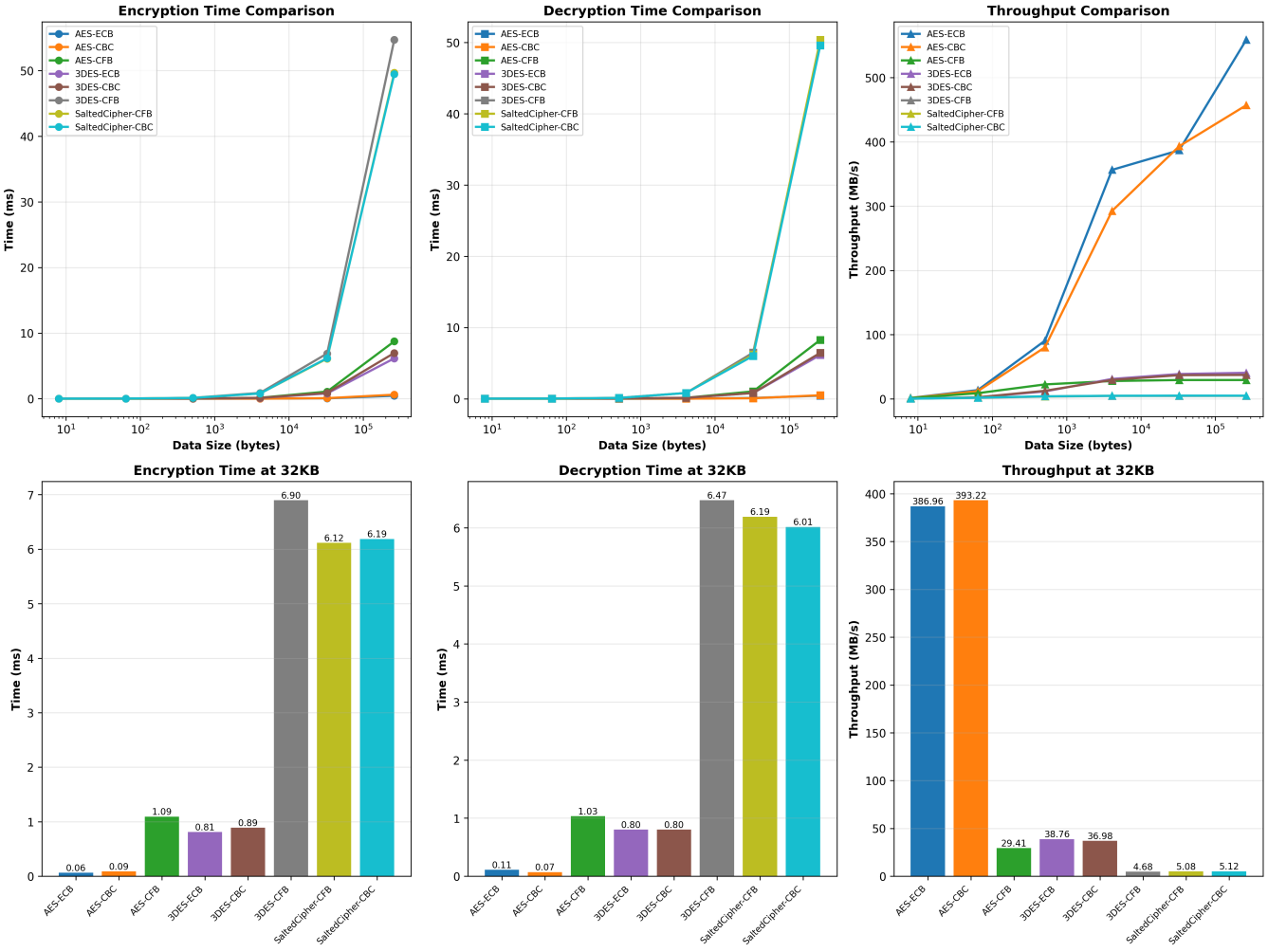

Figure 1: *Six-panel comprehensive performance analysis showing encryption time, decryption time, and throughput comparisons.*

6. ALGORITHM ANALYSIS

6.1 AES

Block Size: 128 bits | Key Sizes: 128/192/256 bits | Throughput: 386.96-393.22 MB/s | Hardware Acceleration: Yes (AES-NI) | Security: NIST Standard (FIPS 197), suitable for all classifications | Status: RECOMMENDED for production

6.2 3DES

Block Size: 64 bits | Key Size: 192 bits | Throughput: 36.98-38.76 MB/s | Hardware Acceleration: Limited | Security: Secure but deprecated | Status: DEPRECATED, migrate to AES

6.3 SaltedCipher

Block Size: 64 bits | Key Size: 128 bits | Throughput: 5.08-5.12 MB/s | Hardware Acceleration: None | Security: Educational purposes | Status: NOT for production

7. SECURITY ANALYSIS

7.1 Cipher Mode Security

ECB: Deterministic, NOT RECOMMENDED for sensitive data | **CBC:** Industry standard, RECOMMENDED for production | **CFB:** Stream cipher mode, acceptable for specialized use

7.2 Critical Guidelines

1. Never use ECB for sensitive data | 2. Always use random IVs/salts | 3. Use 128-bit keys minimum (256-bit for sensitive data) | 4. Implement proper key management | 5. Migrate from 3DES | 6. Consider authenticated encryption (AES-GCM)

8. IMPLEMENTATION GUIDELINES

8.1 Production Systems

Select AES-CBC as primary algorithm | Use 128-bit keys minimum | Generate cryptographically secure random IVs | Implement proper key management | Use established libraries (OpenSSL, pycryptodome) | Conduct security audits

8.2 Optimization

Hardware Acceleration: Use AES-NI | Batch Processing: Use 32KB+ chunks | Parallel Processing: Use CTR mode | Memory Management: Sufficient buffering | Algorithm Selection: AES-CBC (general), AES-CFB (streaming), AES-GCM (authenticated)

9. CONCLUSION

AES-CBC represents the optimal choice for production systems (393.22 MB/s, industry-standard security). Hardware acceleration (AES-NI) makes AES dominant for performance-critical applications. ECB mode is unsuitable for sensitive data. 3DES is deprecated; migration to AES is recommended. SaltedCipher serves educational purposes. Organizations should adopt AES-CBC for new applications and establish migration timelines from 3DES. Future research: authenticated encryption modes, post-quantum algorithms, heterogeneous computing platforms, side-channel attack resistance.

10. REFERENCES

[1] NIST. (2001). Specification for the Advanced Encryption Standard (AES). FIPS 197.
[2] NIST. (2001). Recommendation for Block Cipher Modes of Operation. SP 800-38A.
[3] Daemen, J., & Rijmen, V. (2002). The Design of Rijndael: AES - The Advanced Encryption Standard.
[4] Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.).
[5] Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography.
[6] Ferguson, N., & Schneier, B. (2003). Practical Cryptography. John Wiley & Sons.
[7] Katz, J., & Lindell, Y. (2014). Introduction to Modern Cryptography (2nd ed.). CRC Press.