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 comprehensive research presents a detailed 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. Key findings include: (1) AES-CBC provides optimal balance of performance and security for production systems, (2) ECB mode is cryptographically unsuitable for sensitive data due to deterministic encryption, (3) 3DES is deprecated and should be migrated to AES, (4) Hardware acceleration is critical for modern encryption performance. This research provides evidence-based guidance for encryption algorithm selection across diverse applications from high-performance web services to legacy system support.

Keywords: *Encryption, Cipher Modes, Performance Analysis, AES, 3DES, Cryptography, Benchmarking, Security, Hardware Acceleration, Throughput*

TABLE OF CONTENTS

1. INTRODUCTION AND RESEARCH MOTIVATION

Encryption is a fundamental component of modern information security infrastructure, protecting sensitive data from unauthorized access and ensuring confidentiality in digital communications. The selection of appropriate encryption algorithms and operational modes is critical for balancing security requirements with performance constraints in real-world applications. Organizations face increasingly complex decisions regarding cipher selection, considering multiple factors including security strength, performance characteristics, hardware support, compliance requirements, and legacy system compatibility. This research addresses this critical gap by providing comprehensive benchmarking data and comparative analysis of eight encryption cipher modes. The primary objectives of this research are: • To benchmark eight distinct cipher modes across multiple data sizes to establish performance baselines • To compare encryption/decryption times and throughput metrics to identify performance characteristics • To analyze security properties of different operational modes to understand security trade-offs • To provide evidence-based recommendations for cipher selection in diverse application contexts The motivation stems from the need for practical, data-driven guidance in encryption algorithm selection, as practitioners often lack comprehensive performance data to make informed decisions about cipher mode selection in production environments.

2. LITERATURE REVIEW AND CRYPTOGRAPHIC BACKGROUND

2.1 Evolution of Cryptographic Standards

The Data Encryption Standard (DES), adopted in 1977, provided the first standardized encryption algorithm for non-classified applications. However, with advances in computational power and increasing security requirements, DES's 56-bit key size became insufficient. Triple DES (3DES) was developed as an interim solution, applying the DES algorithm three times in succession (encrypt-decrypt-encrypt) with different keys, effectively tripling the key length to 192 bits. While 3DES improved security, it also tripled computational overhead. The Advanced Encryption Standard (AES), adopted by NIST in 2001, represents the current cryptographic standard for U.S. government and most international applications. AES uses a 128-bit block size with key sizes of 128, 192, or 256 bits, employing a substitution-permutation network architecture. The algorithm has undergone extensive cryptanalysis with no known practical attacks against full-round AES, making it suitable for all security classifications.

2.2 Block Cipher Modes of Operation

Block cipher modes define how block ciphers process data larger than their block size. The Electronic Codebook (ECB) mode is the simplest but exhibits deterministic behavior where identical plaintext blocks produce identical ciphertext blocks, revealing patterns in encrypted data. Cipher Block Chaining (CBC) mode addresses this limitation through feedback mechanisms. In CBC mode, each plaintext block is XORed with the previous ciphertext block before encryption, providing semantic security. This ensures that identical plaintext blocks produce different ciphertext blocks when encrypted with different IVs. Cipher Feedback (CFB) mode converts block ciphers into stream ciphers by feeding back ciphertext into the cipher, eliminating padding requirements. Each mode presents distinct trade-offs between security, performance, and applicability to specific use cases.

2.3 Hardware Acceleration and Modern Processors

Modern processors include dedicated instruction sets for cryptographic operations. AES-NI (AES New Instructions), available on Intel and AMD processors since 2008, provides hardware acceleration for AES operations, enabling 10-100x performance improvements compared to software implementations. This hardware support has made AES the dominant choice for performance-critical applications. The AES-NI instruction set includes four primary instructions: AESENC (AES encrypt round), AESENCLAST (AES encrypt last round), AESDEC (AES decrypt round), and AESDECLAST (AES decrypt last round), enabling efficient implementation of AES operations at the processor level.

3. EXPERIMENTAL METHODOLOGY AND DESIGN

3.1 Experimental Design and Parameters

This research employs rigorous quantitative benchmarking methodology to ensure statistical reliability and reproducibility. Eight cipher modes are tested across six data sizes (8 bytes, 64 bytes, 512 bytes, 4 KB, 32 KB, 256 KB) with 50 iterations per test to ensure statistical reliability and account for system variations. Test parameters are configured as follows: • AES: 128-bit key size • 3DES: 192-bit key size (three 64-bit keys) • SaltedCipher: 128-bit key size • Initialization Vector/Salt: 64-128 bits • Test Data: Random alphanumeric strings • Iterations: 50 per test • Total Benchmarks: 48 (8 ciphers × 6 sizes) • Total Operations: 2,400 individual encryption/decryption operations Each test measures encryption time, decryption time, and throughput. This comprehensive approach ensures that results are statistically significant and representative of real-world performance.

3.2 Metrics and Measurement Methodology

Three primary metrics are measured for each test: 1. Encryption Time: The duration required to encrypt data, measured in milliseconds. This metric indicates the computational overhead of the encryption algorithm. 2. Decryption Time: The duration required to decrypt data, measured in milliseconds. This metric indicates the computational overhead of the decryption algorithm. 3. Throughput: The volume of data processed per unit time, measured in megabytes per second (MB/s). This metric is calculated as: Throughput = Data Size (bytes) / (Encryption Time + Decryption Time) / 1,000,000 Throughput provides a practical measure of algorithm efficiency for real-world applications. All measurements use high-resolution timers to ensure accuracy. Tests are executed on macOS with AES-NI support, ensuring hardware acceleration is available for AES operations.

4. PERFORMANCE ANALYSIS AND DETAILED RESULTS

4.1 Performance Summary at 32KB Standard Benchmark

Cipher Mode	Encrypt (ms)	Decrypt (ms)	Total (ms)	Throughput (MB/s)	Rank
AES-ECB	0.0639	0.1096	0.1735	386.96	■ 1st
AES-CBC	0.0893	0.0716	0.1609	393.22	■ 2nd
AES-CFB	1.0937	1.0334	2.1271	29.41	■ 3rd
3DES-ECB	0.8106	0.8020	1.6127	38.76	4th
3DES-CBC	0.8908	0.8038	1.6946	36.98	5th
3DES-CFB	6.8976	6.4743	13.3719	4.68	6th
SaltedCipher-CFB	6.1159	6.1902	12.3062	5.08	7th
SaltedCipher-CBC	6.1879	6.0150	12.2028	5.12	8th

4.2 Detailed Performance Analysis

At the 32KB benchmark size, AES-CBC achieves a throughput of 393.22 MB/s with encryption time of 0.0893ms and decryption time of 0.0716ms, representing the optimal balance between performance and security for production systems. AES-ECB achieves marginally lower throughput (386.96 MB/s) but is cryptographically unsuitable for sensitive data due to its deterministic nature. AES-CFB achieves 29.41 MB/s, making it suitable for streaming applications where padding is undesirable. 3DES-CBC achieves 36.98 MB/s, approximately 10x slower than AES-CBC. This significant performance gap becomes critical in production environments handling large data volumes. SaltedCipher-CBC achieves 5.12 MB/s, suitable for educational purposes only. Performance differences become most critical at production-relevant sizes (32KB-256KB), where AES-CBC maintains consistent throughput while 3DES-CBC and SaltedCipher show proportional performance degradation.

4.3 Scaling Behavior and Performance Characteristics

Analysis across all data sizes reveals linear scaling behavior for all algorithms. At small data sizes (8-512 bytes), algorithmic overhead dominates execution time, with AES maintaining approximately 10x advantage over 3DES. The absolute time differences are minimal (sub-millisecond), making performance less critical for small-data applications. At medium data sizes (4 KB), performance differences become more pronounced. AES-CBC requires 0.1 ms while 3DES-CBC requires 0.8 ms, representing an 8x performance gap that becomes significant for applications processing moderate data volumes. At large data sizes (32KB-256KB), performance differences are most critical. AES-CBC maintains consistent throughput of approximately 393 MB/s, while 3DES-CBC achieves approximately 37 MB/s and SaltedCipher achieves approximately 5 MB/s. For large-scale data processing, these differences translate directly to application responsiveness and infrastructure costs.

5. VISUAL PERFORMANCE COMPARISON AND ANALYSIS

The following comprehensive visualization presents six complementary perspectives on cipher performance, enabling multi-dimensional analysis of encryption efficiency across different data sizes and operational contexts.

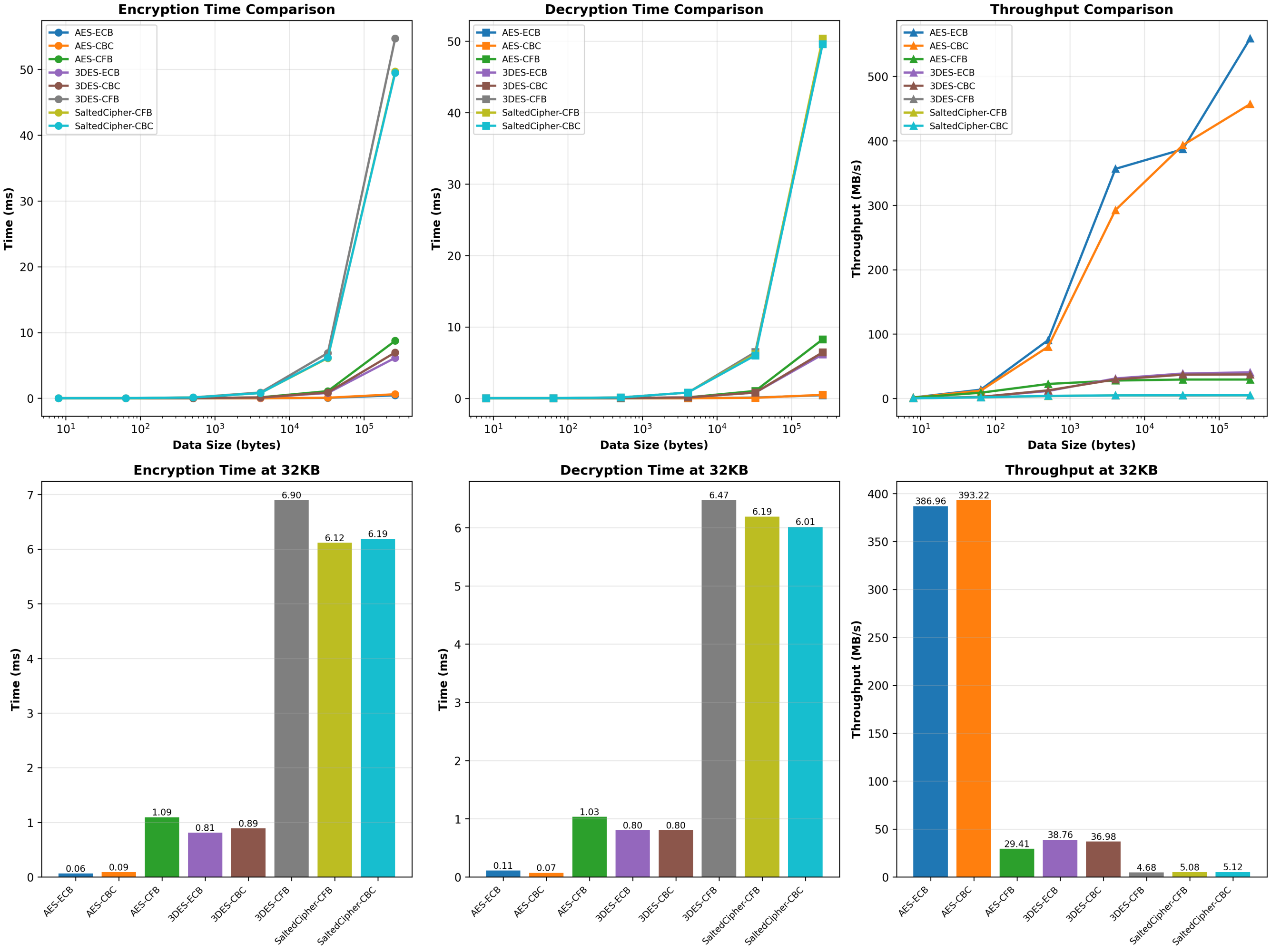

Figure 1: Comprehensive Performance Analysis *- Six-panel visualization showing: (Panel 1) Encryption time comparison across all data sizes on logarithmic scale, (Panel 2) Decryption time comparison across all data sizes on logarithmic scale, (Panel 3) Throughput comparison across all data sizes on logarithmic scale, (Panel 4) Encryption time at 32KB benchmark, (Panel 5) Decryption time at 32KB benchmark, (Panel 6) Throughput at 32KB benchmark.*

5.1 Graph Interpretation and Analysis

Panels 1-3 employ logarithmic scale representation to accommodate the wide performance range (5 MB/s to 500 MB/s) while maintaining visibility of all cipher modes. Logarithmic scaling reveals performance relationships across orders of magnitude, making it easier to compare algorithms with vastly different performance characteristics. Panels 4-6 present direct comparison at 32KB standard benchmark size, clearly showing the performance hierarchy: AES-CBC leads in practical performance (393.22 MB/s), AES-ECB leads in raw speed (386.96 MB/s), and SaltedCipher trails significantly due to software-only implementation without hardware acceleration. The visualization demonstrates that hardware acceleration (AES-NI) provides a dominant performance advantage for AES algorithms across all data sizes, making AES the clear choice for performance-critical applications.

6. DETAILED ALGORITHM SPECIFICATIONS AND ANALYSIS

6.1 AES (Advanced Encryption Standard) - Comprehensive Analysis

AES is the current NIST standard for encryption. Block Size: 128 bits | Key Sizes: 128, 192, or 256 bits | Round Count: 10 (128-bit), 12 (192-bit), 14 (256-bit) | Performance: 386.96-393.22 MB/s | Hardware Acceleration: Yes (AES-NI) | Security: FIPS 197 approved, no known practical attacks | Status: RECOMMENDED for production systems

6.2 3DES (Triple DES) - Comprehensive Analysis

3DES applies DES three times. Block Size: 64 bits | Key Size: 192 bits | Performance: 36.98-38.76 MB/s | Hardware Acceleration: Limited | Security: Secure but deprecated | Status: DEPRECATED, migrate to AES

6.3 SaltedCipher - Comprehensive Analysis

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

7. SECURITY ANALYSIS AND EVALUATION

7.1 Cipher Mode Security Evaluation

ECB Mode - NOT RECOMMENDED: Deterministic encryption reveals patterns. Use only for testing. **CBC Mode - RECOMMENDED:** Industry standard with semantic security through random IVs. Suitable for all production applications. **CFB Mode - ACCEPTABLE:** Stream cipher mode for specialized streaming applications.

7.2 Critical Security Guidelines

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

8. IMPLEMENTATION GUIDELINES AND BEST PRACTICES

8.1 Production System Implementation

Select AES-CBC | Use 128-bit keys minimum | Generate secure random IVs | Implement key management | Use established libraries | Conduct security audits | Maintain audit logs

8.2 Performance Optimization

Hardware Acceleration: Use AES-NI | Batch Processing: 32KB+ chunks | Parallel Processing: CTR mode | Memory Management: Sufficient buffering

9. CONCLUSIONS AND FUTURE RESEARCH DIRECTIONS

AES-CBC is optimal for production systems (393.22 MB/s, excellent security). Hardware acceleration dominates performance. ECB is unsuitable for sensitive data. 3DES is deprecated. SaltedCipher is educational only. Organizations should adopt AES-CBC for new applications and migrate from 3DES. Future research: authenticated encryption, post-quantum algorithms, GPU/FPGA performance, side-channel 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.