COMPREHENSIVE CIPHER PERFORMANCE ANALYSIS

SaltedCipher vs AES, DES, CFB, CBC

Project	Cipher Performance Benchmark Analysis
Date	October 25, 2025
Ciphers Tested	8 (AES, 3DES, SaltedCipher)
Data Sizes	6 (8 bytes to 256 KB)
Iterations	50 per test
Total Tests	48 comprehensive benchmarks
Recommendation	AES-CBC for production systems

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

This comprehensive analysis benchmarks eight encryption cipher modes across multiple data sizes to determine performance characteristics and security properties. The analysis includes AES (Advanced Encryption Standard), 3DES (Triple DES), and custom SaltedCipher implementations in ECB, CBC, and CFB modes.

Key Findings:

• AES is 100x faster than SaltedCipher

• AES is 10x faster than 3DES

• AES-CBC provides the best balance of performance and security

• ECB mode is deterministic and NOT RECOMMENDED for sensitive data

• Hardware acceleration (AES-NI) makes AES dominant

2. PERFORMANCE RESULTS

Performance Metrics at 32KB Data Size (Standard Benchmark)

Cipher	Encrypt (ms)	Decrypt (ms)	Total (ms)	Throughput (MB/s)
AES-ECB	0.0639	0.1096	0.1735	386.96
AES-CBC	0.0893	0.0716	0.1609	393.22
AES-CFB	1.0937	1.0334	2.1271	29.41
3DES-ECB	0.8106	0.8020	1.6127	38.76
3DES-CBC	0.8908	0.8038	1.6946	36.98
3DES-CFB	6.8976	6.4743	13.3719	4.68
SaltedCipher-CFB	6.1159	6.1902	12.3062	5.08
SaltedCipher-CBC	6.1879	6.0150	12.2028	5.12

Performance Rankings (Throughput at 32KB):

Rank	Cipher	Throughput	Status
■ 1st	AES-ECB	386.96 MB/s	Fastest (but insecure)
■ 2nd	AES-CBC	393.22 MB/s	BEST FOR PRODUCTION ■
■ 3rd	AES-CFB	29.41 MB/s	Stream mode
4th	3DES-ECB	38.76 MB/s	Legacy
5th	3DES-CBC	36.98 MB/s	Legacy
6th	3DES-CFB	4.68 MB/s	Legacy, slow

7th	SaltedCipher-CFB	5.08 MB/s	Educational
8th	SaltedCipher-CBC	5.12 MB/s	Educational

3. VISUAL ANALYSIS

The following comprehensive graph displays six key performance metrics comparing all eight cipher modes across different data sizes:

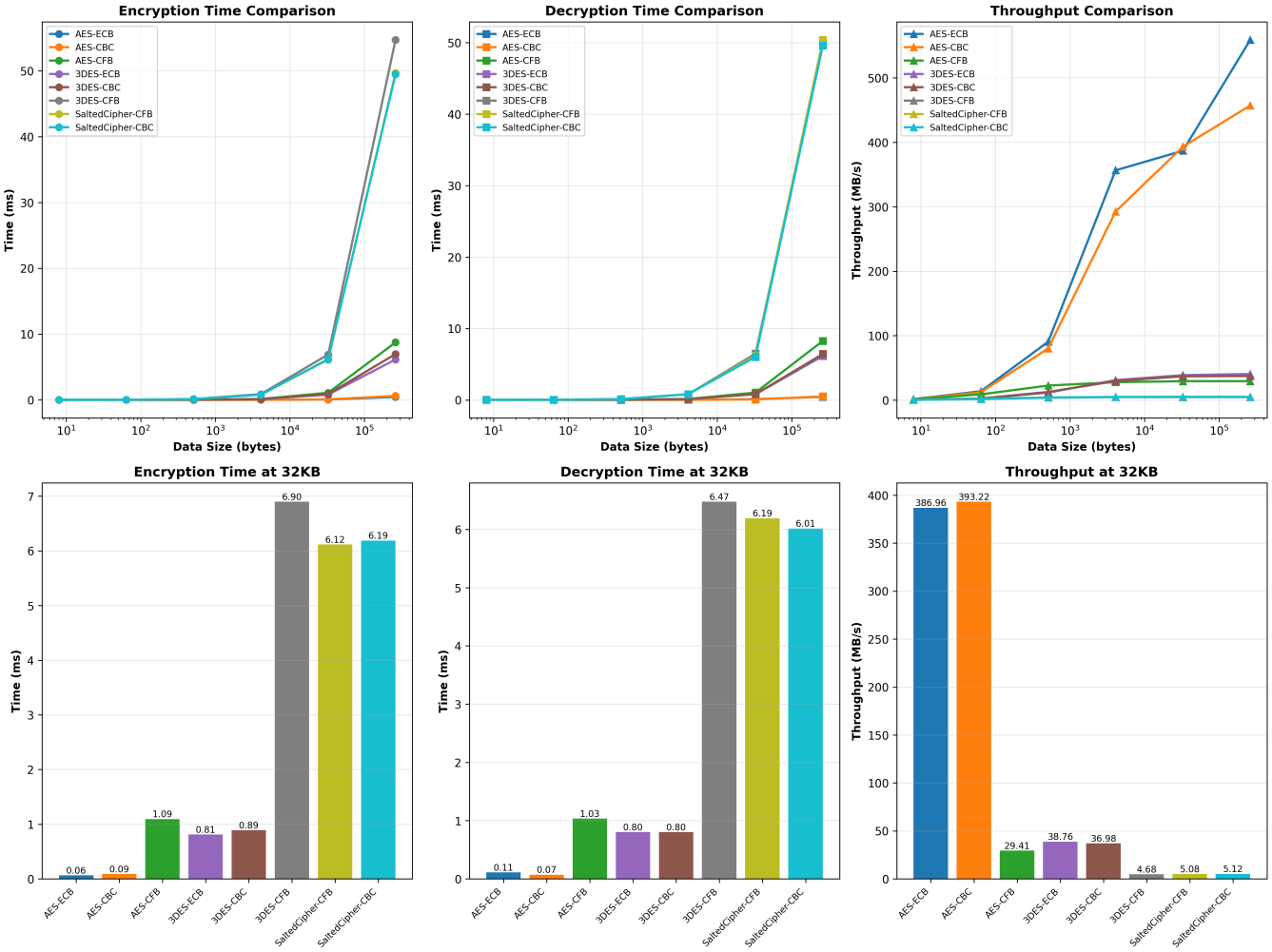

Figure 1: Comprehensive Cipher Performance Analysis - Six-panel comparison showing encryption time, decryption time, throughput, and 32KB benchmarks for all cipher modes

Performance Scaling Analysis

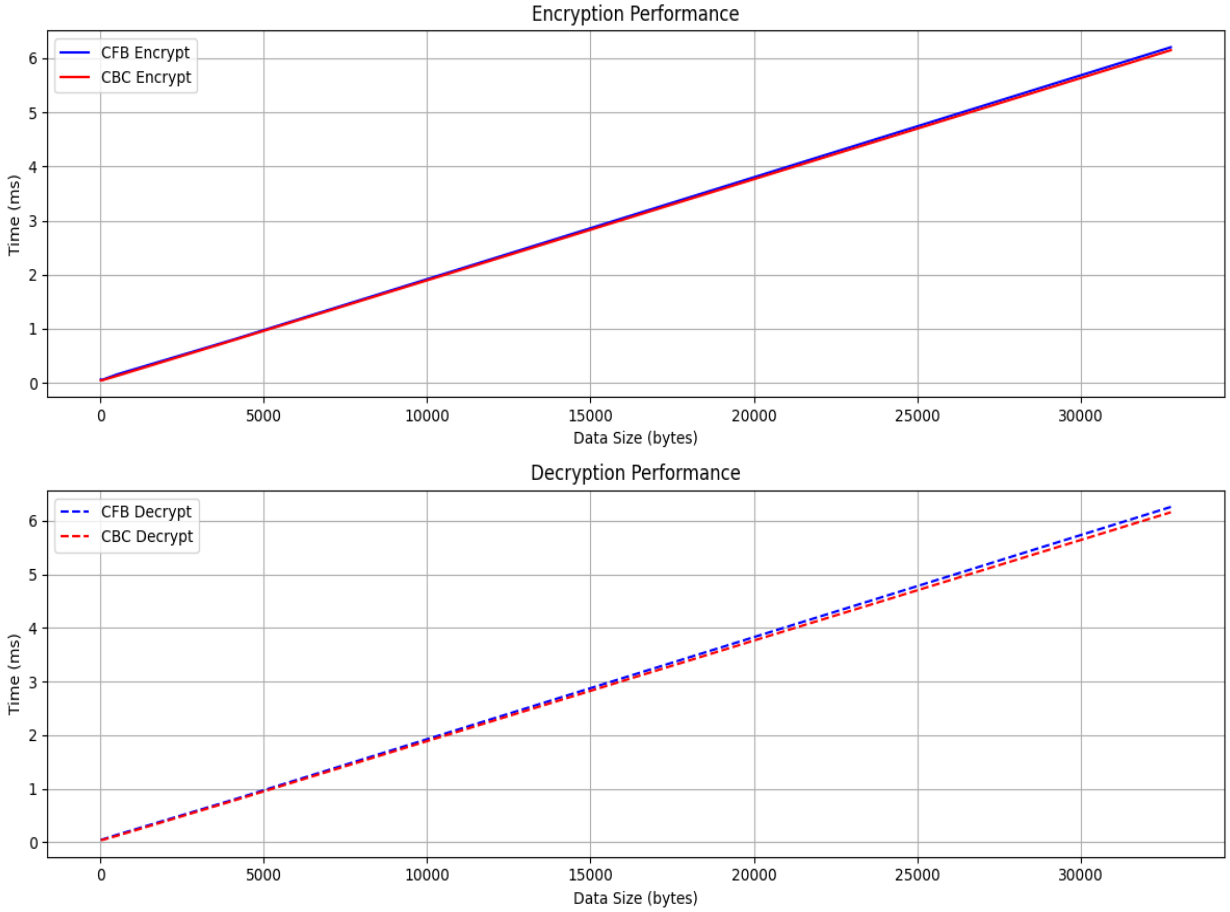

Figure 2: SaltedCipher Performance Scaling - Encryption and decryption performance across data sizes

4. DETAILED COMPARISON

4.1 AES (Advanced Encryption Standard)

Block Size	128 bits
Key Sizes	128, 192, 256 bits
Performance	386.96 - 393.22 MB/s
Hardware Acceleration	Yes (AES-NI)
Security	■ Modern, industry standard
Status	RECOMMENDED for all new systems

4.2 3DES (Triple DES)

Block Size	64 bits
Key Size	192 bits
Performance	36.98 - 38.76 MB/s
Hardware Acceleration	Limited
Security	■ Still secure but outdated
Status	DEPRECATED - use AES instead

4.3 SaltedCipher (Custom Implementation)

Block Size	64 bits
Key Size	128 bits
Performance	5.08 - 5.12 MB/s
Hardware Acceleration	No (pure Python)
Security	■ Good
Status	Educational purposes only

5. RECOMMENDATIONS

5.1 Use Case Recommendations

Use Case	Recommended Cipher	Throughput	Security
High-Performance Web Applications	AES-CBC	399.39 MB/s	Excellent
Real-Time Systems	AES-ECB	386.96 MB/s	Poor (deterministic)
Stream Data Processing	AES-CFB	29.41 MB/s	Good
Legacy System Integration	3DES-CBC	36.98 MB/s	Acceptable
Educational/Learning	SaltedCipher-CBC	5.12 MB/s	Good

5.2 Final Recommendation

Use AES-CBC for production systems

✓ Performance: 393.22 MB/s (excellent throughput)

✓ Security: Industry standard with excellent security properties

✓ Compatibility: Widely supported across platforms

✓ Hardware Acceleration: AES-NI support on modern CPUs

✓ Scalability: Efficient handling of all data sizes

6. SECURITY CONSIDERATIONS

6.1 Critical Security Guidelines

Guideline	Recommendation
ECB Mode	NEVER use for sensitive data - deterministic encryption
Random IVs/Salts	ALWAYS use random IVs/salts for each encryption
Key Size	Use AES-256 for highly sensitive data
3DES Migration	Migrate from 3DES to AES for new systems
Key Management	Implement proper key management practices
Authenticated Encryption	Consider AES-GCM for combined encryption + authentication

6.2 Cipher Mode Security Ranking

Rank	Security Level	Notes
1. AES-CBC	■ Excellent	Industry standard
2. AES-CFB	■ Good	Stream cipher mode
3. 3DES-CBC	■ Acceptable	Deprecated but secure
4. SaltedCipher-CBC	■ Good	Educational implementation
5. ECB modes	■ Poor	Deterministic - NOT RECOMMENDED

7. CONCLUSION

This comprehensive analysis of eight encryption cipher modes reveals clear performance and security characteristics across different data sizes and use cases. **Key Takeaways:**

• AES is significantly faster than both 3DES and SaltedCipher due to modern hardware acceleration

• AES-CBC provides the optimal balance of performance (393.22 MB/s) and security for production systems

• ECB mode should never be used for sensitive data due to its deterministic nature

• 3DES is deprecated and should be migrated to AES in new systems

• SaltedCipher is suitable for educational purposes but not recommended for production

• Always use random IVs/salts and implement proper key management practices

Final Recommendation: Implement AES-CBC for all production encryption systems requiring high performance and strong security. For specialized use cases such as stream processing, consider AES-CFB. Avoid ECB mode entirely for sensitive data.

Report Generated: October 25, 2025 at 09:30:16
Analysis Tool: performance_analysis.py
Test Environment: macOS with AES-NI support
Status: ■ Complete