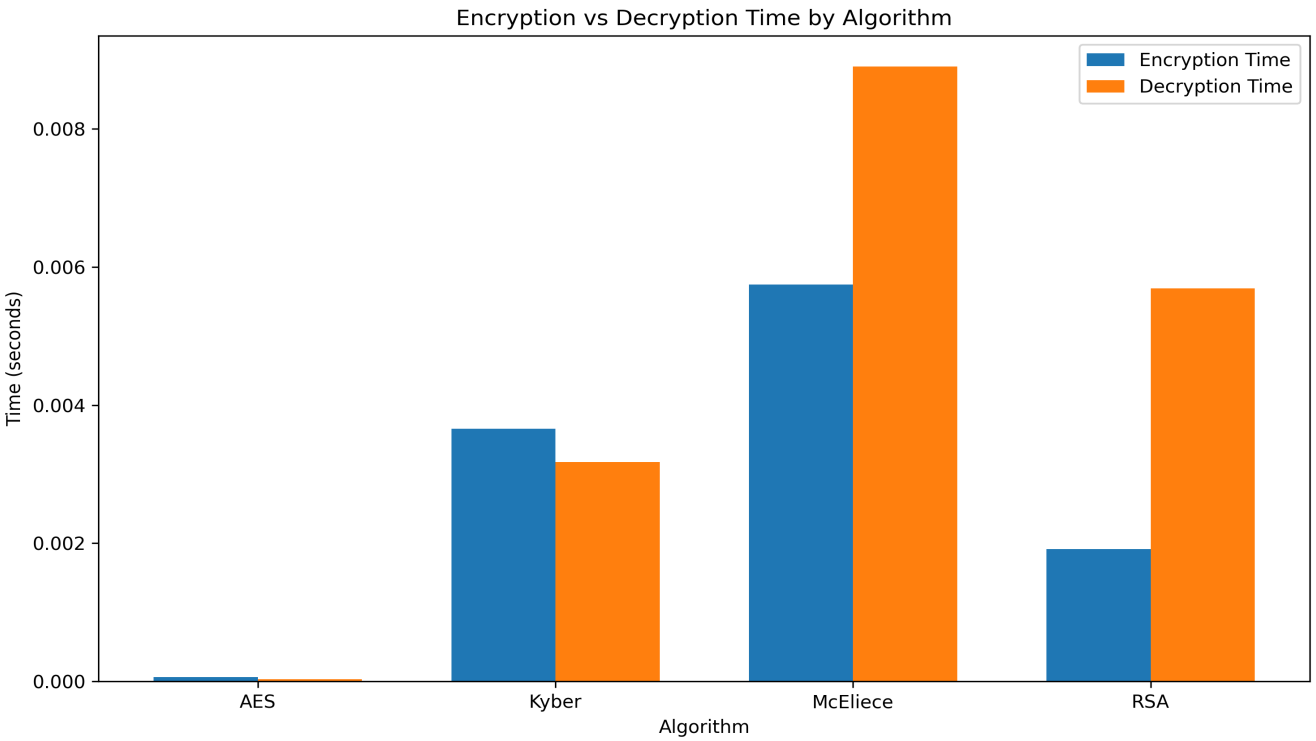
Encryption Algorithms Benchmark

This dashboard presents a comparative analysis of encryption algorithms, including traditional (AES, RSA) and post-quantum (Kyber, McEliece) approaches. The benchmark tests were performed on email data to measure performance and security characteristics.

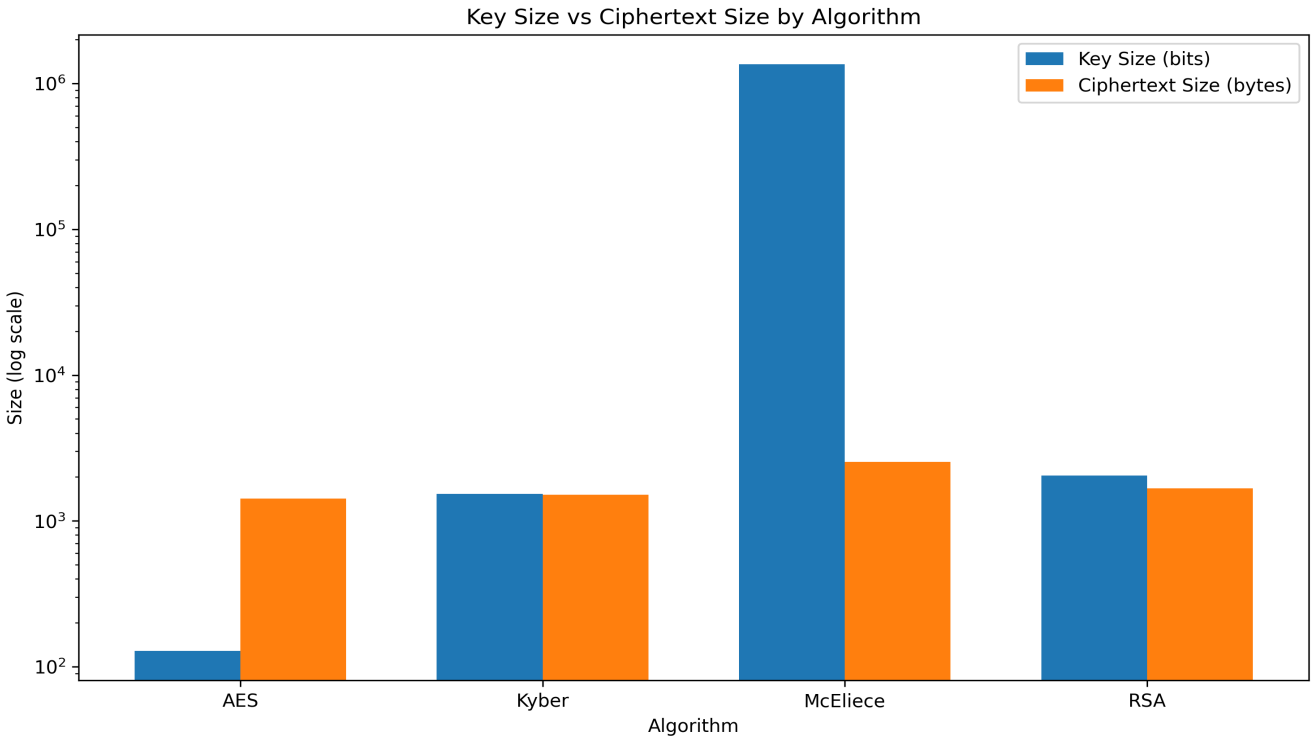
Algorithm Comparison Summary

Algorithm	Enc Time (s)	Dec Time (s)	Quantum-Resistant	Best Use Case	Cipher Size	Key Size (bits)
AES	0.000060	0.000029	No	Bulk Data Encryption	1423	128
Kyber	0.003660	0.003177	Yes	Post-Quantum TLS	1515	1536
McEliece	0.005744	0.008902	Yes	Post-Quantum Secure Messaging	2548	1357824
RSA	0.001914	0.005690	No	Secure Key Exchange	1671	2048

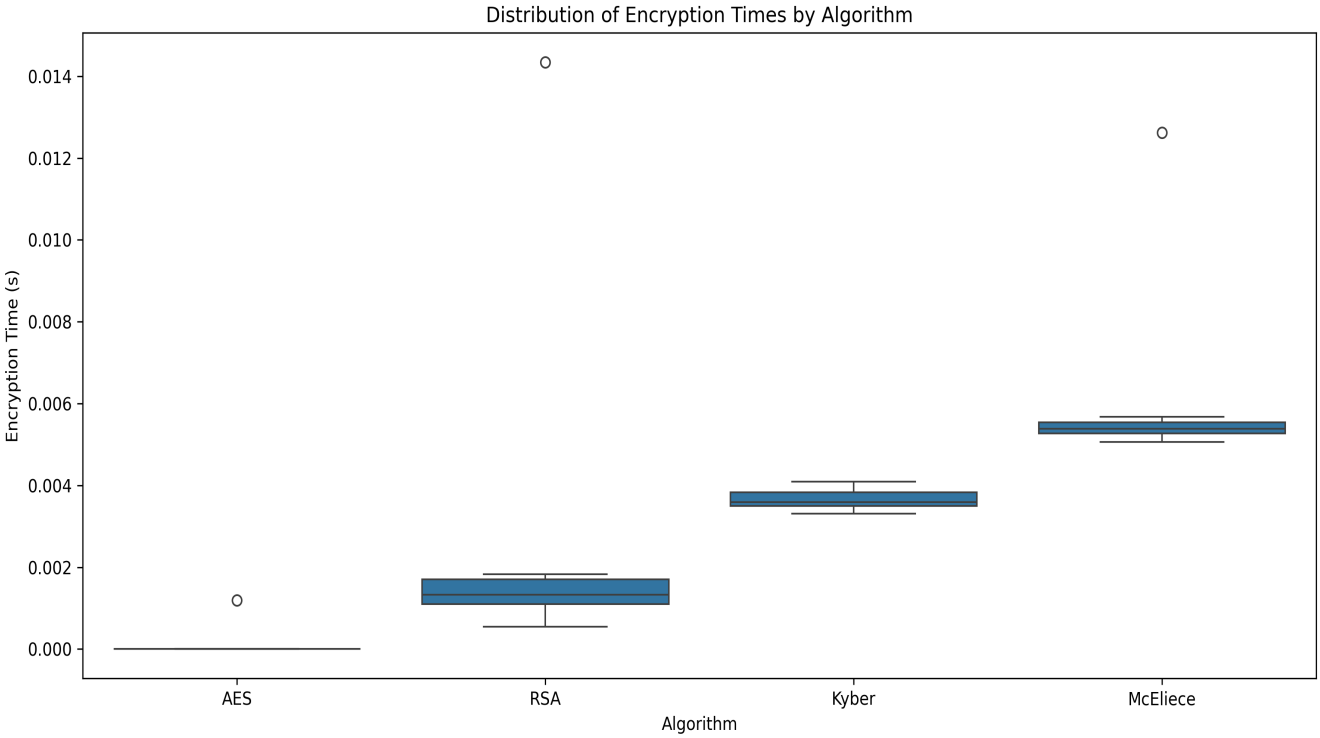
Encryption vs Decryption Time



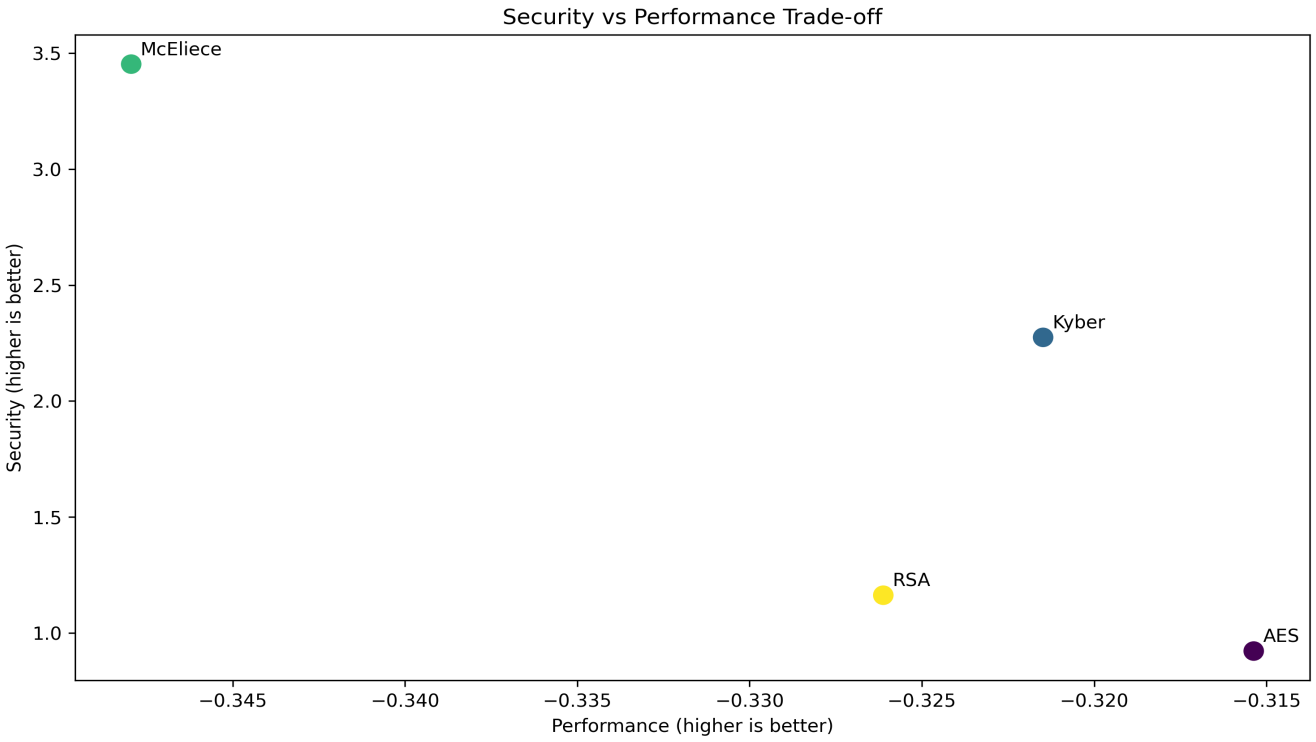
Key Size vs Ciphertext Size (Log Scale)



Distribution of Encryption Times



Security vs Performance Trade-off



Key Findings and Recommendations

• AES provides the fastest encryption times, making it ideal for performance-critical applications.

• AES offers the quickest decryption, which is important for real-time data access.

• AES uses the smallest key size, requiring less storage for key management.

• AES produces the smallest ciphertext, minimizing bandwidth and storage requirements.

• Kyber, McEliece are quantum-resistant, providing future-proofing against quantum computing threats.

• For sensitive data requiring long-term security, quantum-resistant algorithms are recommended despite the performance trade-offs.

• AES remains the most efficient choice for bulk data encryption where quantum resistance is not a concern.

• A hybrid approach combining classical and post-quantum algorithms may provide the best balance of security and performance.

Conclusion

This benchmark demonstrates the trade-offs between classical and post-quantum encryption algorithms. While classical algorithms like AES and RSA offer excellent performance, they are vulnerable to quantum computing attacks. Post-quantum algorithms provide future-proof security but at the cost of larger key sizes and ciphertexts. Organizations should consider their specific security

requirements, data sensitivity, and performance needs when selecting encryption algorithms. A strategic approach might involve using classical algorithms for everyday operations while beginning the transition to quantum-resistant algorithms for sensitive and long-lived data.