Christian J. Busca

CS 305: Software Security

Artemis Financial: Encryption Algorithm Cipher

Southern New Hampshire University

Introduction

Artemis Financial is committed to securing its long-term archive files against unauthorized access and potential cyber threats. Choosing a strong encryption algorithm is essential for ensuring data integrity, confidentiality, and compliance with industry security standards. After careful evaluation, the Advanced Encryption Standard (AES-256) emerges as the optimal choice due to its proven security, efficiency, and widespread adoption in financial and governmental sectors.

Algorithm Cipher Recommendation

AES-256 is a symmetric block cipher, meaning it uses the same key for both encryption and decryption. It is widely regarded as the gold standard in encryption and is used by financial institutions, government agencies, and organizations handling sensitive data. AES-256 encrypts data in 128-bit blocks using a 256-bit key, providing strong protection against brute-force attacks. Even with the most advanced computing power, it would take billions of years to crack a 256-bit AES key using brute-force methods (Arora, 2012).

To maximize the security of AES-256 encryption, Artemis Financial must implement several key security measures, including secure storage and periodic rotation of encryption keys to prevent key exposure. The use of Hardware Security Modules (HSMs) is recommended for secure key storage (Swenson, 2018). Implementing multi-factor authentication (MFA) and enforcing role-based access control (RBAC) will further limit access to decryption keys. Additionally, Transport Layer Security (TLS) should be employed for encrypted data transmission, ensuring end-to-end protection (Bernstein & Cobb, 2021). Regular security audits

and compliance with FIPS 197 and NIST cryptographic standards will maintain robust encryption practices (NIST, 2023).

While AES-256 provides strong encryption, its security depends on proper implementation. The biggest risk is key exposure—if an encryption key is compromised, attackers can decrypt the data. To mitigate this risk, Artemis Financial should use key encryption keys (KEK) to encrypt and protect primary encryption keys, restrict key access to authorized personnel, and implement air-gapped or offline storage for highly sensitive keys (Swenson, 2018).

AES-256 is superior to older encryption methods like Data Encryption Standard (DES), which was deprecated due to its short 56-bit key length. Unlike asymmetric encryption (e.g., RSA), which uses separate keys for encryption and decryption, symmetric encryption like AES-256 is more efficient for large-scale data storage because it avoids the complexities of key exchange (Bernstein & Cobb, 2021).

By implementing AES-256 encryption, Artemis Financial will fortify its security framework, ensuring long-term data protection, regulatory compliance, and client trust. The robustness of AES-256, combined with proper key management and security best practices, will safeguard confidential financial records from unauthorized access and cyber threats.

References

Bernstein, C., & Cobb, M. (2021, September 24). What is the Advanced Encryption Standard (AES)? SearchSecurity. Retrieved Jan 30, 2025, from https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard

EETimes, M. A. (2012, May 7). How secure is AES against brute force attacks? EETimes. Retrieved Jan 30, 2025, from https://www.eetimes.com/how-secure-is-aes-against-brute-force-attacks/#:~:text=As%20shown%20above%2C%20even%20with,universe%20(13.75%20billion%20years).

Swenson, C. (2018, December 11). NIST's encryption standard has minimum $250 billion economic benefit, according to new study. NIST. Retrieved Jan 30, 2025, from https://www.nist.gov/news-events/news/2018/09/nists-encryption-standard-has-minimum-250-billion-economic-benefit

National Institute of Standards and Technology (NIST). (2001). "Advanced Encryption Standard (AES)." Federal Information Processing Standards Publication 197. Retrieved Feb 1, 2025, from https://doi.org/10.6028/NIST.FIPS.197

TechTarget. (2024). "Understanding AES-256 Encryption and Its Security Risks." Retrieved Jan 30, 2025, from https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard