Joshua Williamson  
Module Four Algorithm Ciphers Assignment

Artemis Financial must adopt a robust encryption solution to protect its long-term archive files. Given the highly sensitive nature of financial data, selecting a cipher that balances maximum security with considerations such as performance, regulatory compliance, and effective key management is essential. Recent reports can highlight how outages severely disrupt operations and how financial institutions are frequent targets of cyberattacks. After a careful review, the Advanced Encryption Standard (AES) with a 256-bit key length shows as the most appropriate choice.

AES is a symmetric block cipher recognized for its speed, efficiency, and proven resilience against attacks. A 256-bit key length provides extremely strong protection against brute-force attempts, making decryption by unauthorized parties impossible. This level of security is vital for protecting financial records, which often include sensitive personal data such as Social Security numbers and addresses. Given the high stakes, the highest degree of protection is warranted.

Implementing AES does present challenges with key management. Since symmetric encryption uses a single key for both encryption and decryption, organizations must prioritize secure key storage and distribution. Strong key management practices such as hardware security modules (HSMs) and routine key rotation add complexity but significantly strengthen overall security.

Compliance is another important factor. Artemis Financial must meet the requirements of financial regulatory authorities, which typically mandate strict encryption standards and key management protocols. By aligning with these guidelines and adopting best practices, the company can achieve compliance while ensuring robust protection of its archives.

In addition to key length, AES works best when combined with strong hash functions such as SHA-256 or SHA-3. These functions provide integrity verification, ensuring that encrypted data has not been tampered with. AES also relies on random numbers, to guarantee that even identical pieces of plaintext produce different ciphertext outputs. This randomness prevents attackers from detecting patterns in encrypted data.

It is also important to recognize the tradeoffs between symmetric and asymmetric encryption. While asymmetric methods such as RSA or elliptic curve cryptography (ECC) are great for secure key exchange, they can be slower and less efficient for encrypting large amounts of data. AES, as a symmetric cipher, is far better suited for high-volume file and archive encryption because of its speed and efficiency.

AES was introduced in 2001 after the National Institute of Standards and Technology (NIST) conducted a global competition to replace the aging DES (Data Encryption Standard), which had become vulnerable to brute-force attacks. AES has since become the worldwide standard, approved by governments, financial institutions, and security professionals for safeguarding sensitive information. Its continued adoption underscores both its resilience against attacks and its long-term viability.

AES’s blend of speed, reliability, and advanced security makes it well-suited for file encryption. Its block cipher structure processes fixed-size data blocks using layers of substitution, permutation, and key mixing to produce highly complex ciphertext. When paired with a 256-bit key, AES offers superior resistance to modern attack methods. Based on these factors, adopting AES-256 is the most effective and secure path forward for Artemis Financial.

## References

Bernstein, C., & Cobb, M. (2021, September 24). Advanced Encryption Standard (AES). TechTarget. Retrieved September 18, 2025, from https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard

Cohen, B. (n.d.). AES-hash - csrc.nist.rip. Retrieved September 18, 2025, from https://csrc.nist.rip/groups/ST/toolkit/BCM/documents/proposedmodes/aes-hash/aeshash.pdf