Malachi Okongwu

CS305 M4

May 27, 2025

**Recommendation Report for Artemis Financial**

**Encryption Algorithm Recommendation**

After a thorough evaluation of Artemis Financial’s need to encrypt long-term archive files securely, and in reference to the Java Security Standard Algorithm Names provided by Oracle (Oracle, n.d.), I recommend using the Advanced Encryption Standard (AES) with a 256-bit key length (AES-256). AES-256 is one of the most widely used and vetted symmetric encryption algorithms and is approved by the National Institute of Standards and Technology (NIST) for protecting sensitive data (NIST, 2001).

**Justification for the Recommendation**

1. **Security Protection Best Practices**

AES-256 provides robust defense against brute-force attacks due to its large key space (2^256 combinations), which makes unauthorized decryption computationally infeasible. When implemented with secure key management and side-channel countermeasures, it offers a high level of data confidentiality (Daemen & Rijmen, 2002).

2. **Risks and Considerations**

While AES-256 is highly secure, improper implementation (such as weak key storage or insecure modes of operation) can expose vulnerabilities. Additionally, AES-256 requires more computational resources compared to AES-128 or AES-192, which may impact performance on low-powered devices. However, for archive files—where data is accessed infrequently—this performance cost is minimal and justified.

3. **Regulatory Compliance**

AES is a globally accepted encryption standard and fully compliant with government regulations such as FIPS 140-2, HIPAA, GDPR, and GLBA. Using AES-256 ensures that Artemis Financial meets stringent legal requirements for data encryption and secure archiving (NIST, 2001).

4. **Practical Usage Considerations**

AES-256 is supported in virtually all modern cryptographic libraries and hardware security modules. It supports various cipher modes (such as CBC and GCM), allowing flexibility based on operational needs. It’s ideal for securing large volumes of archival data, and its wide adoption ensures long-term viability and interoperability.

**Further Considerations**

**Symmetric vs. Asymmetric Keys**

AES is a symmetric encryption algorithm, meaning the same key is used for both encryption and decryption. While symmetric encryption is faster and ideal for large data volumes, it requires secure key distribution. For archival use, where the data owner manages both encryption and decryption, symmetric encryption is appropriate.

**Bit Levels and Hash Functions**

AES-256 refers to a 256-bit key, offering the highest level of brute-force resistance in the AES family. A larger bit level translates to exponentially more combinations an attacker would need to guess, making it suitable for long-term security.

While AES itself is not a hash function, systems that use AES often pair it with cryptographic hash functions like SHA-256 to provide message integrity and authentication. For example, a hash may be used to create a Message Authentication Code (MAC), ensuring that archived files haven't been tampered with.

**History and Current State of Encryption Algorithms**

AES was developed by Vincent Rijmen and Joan Daemen and selected by NIST in 2001 to replace the aging Data Encryption Standard (DES). Unlike DES, which became vulnerable to brute-force attacks due to its small 56-bit key size, AES offers modern cryptographic strength and scalability. AES has become the de facto standard in commercial, government, and open-source encryption solutions and continues to stand up against cryptanalysis in real-world applications.

Conclusion

AES-256 is the most appropriate cipher for Artemis Financial’s encryption needs due to its high security, regulatory compliance, and practical applicability for archiving purposes. While more resource-intensive than some alternatives, its long-term security benefits far outweigh the costs, especially for data that must remain protected for many years.

References

Daemen, J., & Rijmen, V. (2002). The design of Rijndael: AES - The Advanced Encryption Standard. Springer.

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.

National Institute of Standards and Technology (NIST). (2001). Announcing the Advanced Encryption Standard (AES) (FIPS PUB 197). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

Oracle. (n.d.). Java Security Standard Algorithm Names. https://docs.oracle.com/javase/9/docs/specs/security/standard-names.html#cipher-algorithm-names