Victor Udeh  
CS305 M4  
Feb 4th, 2024 **Recommendation Report for Artemis Financial**

**Encryption Algorithm Recommendation**

After thorough consideration of Artemis Financial's needs for securing long-term archive files and in accordance with the Java Security Standard Algorithm Names provided by Oracle (Oracle, n.d.), we recommend the **Advanced Encryption Standard (AES) with a 256-bit key length (AES-256)** as the most appropriate encryption cipher. AES-256 is not only endorsed by security experts but also approved by the National Institute of Standards and Technology (NIST) for encrypting sensitive information (NIST, 2001).

**Justification for the Recommendation**

1. **Security Protection Best Practices**: AES-256 offers superior protection against brute force attacks due to its large key size and complexity. It has been proven secure against current attack vectors, including sophisticated attacks such as side-channel attacks when implemented with proper countermeasures (Daemen & Rijmen, 2002).
2. **Risks and Considerations**: The primary risk associated with AES-256 is the potential for improper implementation, which can lead to vulnerabilities. However, following best practices for cryptographic implementation minimizes this risk. While AES-256 does require more computational resources than AES-128 or AES-192, the added security justifies this cost for long-term archival purposes where access frequency is low (Menezes, van Oorschot, & Vanstone, 1996).
3. **Regulatory Compliance**: AES is globally recognized and compliant with current government regulations on data encryption, ensuring that Artemis Financial meets legal standards for data protection (NIST, 2001).
4. **Practical Usage Considerations**: AES-256 can be efficiently implemented in software and hardware, supports various modes of operation for different application needs, and is widely supported across platforms and technologies (Daemen & Rijmen, 2002).

**Further Considerations**

* **Symmetric vs. Non-Symmetric Keys**: AES-256 uses a symmetric key mechanism, which requires secure key management practices to ensure that the key remains confidential and is only accessible to authorized parties (Menezes et al., 1996).
* **History and Current State of Encryption**: AES was adopted as a standard by NIST in 2001 after a public competition to find a successor for the older DES (Data Encryption Standard). It has since become the most widely used encryption standard for secure data transmission and storage worldwide (Daemen & Rijmen, 2002).

**Conclusion**

AES-256 is recommended for Artemis Financial's archival encryption needs due to its balance of security, compliance, and practicality. Implementing AES-256 with proper cryptographic practices will ensure the long-term security of Artemis Financial's archived data against evolving threats.

**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*. Retrieved from <https://docs.oracle.com/javase/9/docs/specs/security/standard-names.html#cipher-algorithm-names>