Encryption Recommendations for Artemis Financial's Long-Term Archive Files

I am writing to provide recommendations for encrypting Artemis Financial's long-term archive files. As a developer and security expert, I understand the critical importance of securing sensitive data, and I believe that employing the Advanced Encryption Standard (AES) is a sound choice for this purpose.

Here are the key considerations and recommendations regarding AES encryption and the security protection best practices:

a. It is essential to consider all potential risks associated with encrypting long-term archive files. These risks may include data breaches, unauthorized access, loss of encryption keys, and the potential for vulnerabilities in the encryption software. Regularly assessing and updating security measures can mitigate these risks.

b. Ensure that the encryption method aligns with the most current government regulations and compliance standards applicable to financial institutions. Compliance with regulations such as GDPR, HIPAA, or industry-specific mandates is crucial.

c. The AES algorithm cipher should be employed for encrypting the archive files. AES is widely recognized for its security and efficiency, making it a suitable choice for protecting sensitive data. Ensure that the encryption process is well-documented and integrated into the company's data management policies(U.S).

d. AES is the recommended cipher due to its robust security features. It is a symmetric-key algorithm with key lengths of 128, 192, or 256 bits, making it highly resilient against brute force attacks. AES has undergone extensive scrutiny by security experts and is trusted worldwide for data encryption.

e. While AES is highly secure, there might be specific reasons why an alternative cipher may be chosen. For example, if legacy systems or software require a different encryption algorithm, it may be necessary to use a transitional solution. However, it is crucial to thoroughly assess the security implications and potential risks associated with such choices.

P.S. Overview of AES Encryption Algorithm Cipher

To provide a brief overview justifying our recommendation of the Advanced Encryption Standard (AES) for Artemis Financial, let's delve into the key aspects of this encryption algorithm:

1. Purpose of Hash Functions and Bit Levels

One of the primary purposes of hash functions is to ensure data integrity(December). When data is transmitted or stored, it can be susceptible to accidental or malicious alterations. Hash functions create a fixed-size, unique "digest" or "hash value" from the input data. Hash functions generate a fixed-size output (the hash value) regardless of the size of the input data. This means that even a tiny change in the input data will result in a significantly different hash value. As a result, hash values are unique representations of their input data. They are critical for data integrity verification but serve a different purpose from encryption. Bit Levels: AES operates at different key lengths - 128, 192, or 256 bits. These key lengths determine the strength of encryption. Longer keys offer greater security but may be computationally more intensive.

2. Use of Random Numbers

AES relies on key expansion, which uses pseudo-random numbers derived from the encryption key. These random numbers enhance the algorithm's security by introducing unpredictability into the encryption process. AES employs symmetric key encryption, meaning the same key is used for both encryption and decryption. This is in contrast to non-symmetric (asymmetric) encryption, which uses a pair of public and private keys.

3. History and Current State of Encryption Algorithms

AES was established in 2001 by the National Institute of Standards and Technology (NIST) as a replacement for the aging Data Encryption Standard (DES)(CSRC). DES had become vulnerable to modern computing power. AES was selected after a rigorous competition that involved various encryption algorithms. It has since become the de facto standard for symmetric-key encryption worldwide due to its security, efficiency, and widespread support in software and hardware. The AES algorithm's strength lies in its mathematical properties, such as the substitution-permutation network (SPN) structure, which provides strong resistance against cryptographic attacks.

December. (2023) Briefing\_Book\_to\_COV.pdf. Retrieved September 23, 2023, from https://csrc.nist.gov/CSRC/media/Projects/Crypto-Standards-Development-Process/documents/Briefing\_Book\_to\_COV.pdf

CSRC (2023) Development of the Advanced Encryption Standard | CSRC. Retrieved September 23, 2023, from <https://csrc.nist.gov/pubs/journal/2021/08/development-of-the-advanced-encryption-standard/final>

U.S. (2023) PDF.js viewer. Retrieved September 23, 2023, from <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf>