4-2 Written Assignment: Algorithm Cipher Recommendation

Armon Wilson

SNHU CS305

**Algorithm Cipher Recommendation**

For Artemis Financial, my recommended encryption algorithm is the Advanced Encryption Standard (AES), specifically AES-256. This recommendation is based on AES's strong security features, efficiency, and widespread acceptance within the industry. AES, a symmetric key algorithm, encrypts data in 128-bit blocks and supports key sizes of 128, 192, or 256 bits, with AES-256 providing the highest level of security (Java SE Security API, 2017). This makes it especially suitable for protecting long-term archival files by ensuring robust encryption that withstands various types of cryptographic attacks.

**Security Protection Best Practices**

To protect against various security threats, it is essential to follow the best practices such as employing strong encryption algorithms such as AES-256 and implementing robust key management protocols. Ensuring encryption keys are protected with hardware security modules (HSMs) or other secure key management systems is necessary. Regular updates to cryptographic protocols and the use of multi-factor authentication (MFA) contribute significantly to overall system security (Manico & Detlefsen, 2014). Regular security audits further support maintaining a secure environment for data protection.

**Risks of the Recommendation**

The main risk associated with AES-256 is its computational overhead compared to less secure encryption methods. AES-256 is well-optimized and supported by modern hardware, minimizing performance concerns. Another risk is the potential compromise of encryption keys, which could undermine the security of encrypted data. Therefore, strong key management strategies are essential to mitigate this risk and maintain data security (Manico & Detlefsen, 2014).

**Government Regulations**

Compliance with regulations such as GDPR and CCPA is crucial for protecting sensitive data. AES-256 is compliant with these regulations, as it is endorsed by NIST and included in FIPS 197, making it a suitable choice for regulatory compliance. Utilizing AES-256 helps Artemis Financial meet these requirements by providing high-level data security for archived files. Regular compliance audits and security checks are necessary to ensure adherence to these regulations (Java SE Security API, 2017).

**Usage of the Algorithm Cipher**

AES-256 will be used to encrypt Artemis Financial’s long-term archive files, ensuring that sensitive financial data remains secure over time. The same AES-256 algorithm and key must be used for both encryption and decryption processes to maintain data integrity and accessibility. This practice makes certain that only authorized users with the correct decryption key can access the data, providing strong protection against unauthorized access (Manico & Detlefsen, 2014).

**The Best Cipher and Its Advantages**

AES-256 is preferred due to its balance of security, performance, and industry acceptance. It offers strong encryption that resists known practical attacks, making it highly effective for protecting sensitive data. AES-256's efficiency in both hardware and software implementations also allows for handling large datasets with minimal performance impact (Manico & Detlefsen, 2014).

**Reasons to Avoid the Most Secure Cipher**

In certain cases, the most secure cipher might be avoided due to its complexity or performance overhead. AES-256's efficiency and support in contemporary hardware mitigate these concerns. While AES-256 requires careful key management, its security advantages and broad acceptance make it a top choice. The comprehensive features of AES-256 ensure it remains suitable for both current and future security needs (Manico & Detlefsen, 2014).

**Justification**

**Purpose of Hash Functions and Bit Levels**

Hash functions generate a fixed-size hash value from variable-size data, ensuring data integrity and authenticity. Bit levels refer to the size of the encryption key; higher bit levels, such as 256 bits in AES-256, offer stronger security by making brute-force attacks impractical. Although higher bit levels may require more processing power, they significantly enhance encryption security (Manico & Detlefsen, 2014).

**Use of Random Numbers and Key Types**

Random numbers are vital in cryptographic processes for generating secure keys and initialization vectors (IVs), ensuring unique and unpredictable encryption results. Symmetric keys, which use the same key for both encryption and decryption, are efficient and suitable for large datasets. In contrast, asymmetric keys use a pair of keys (public and private) and are typically used for secure key exchange. While asymmetric encryption is more suitable for key exchange, symmetric encryption like AES is preferred for encrypting data due to its speed and efficiency (National Institute of Standards and Technology [NIST], 2001).

**History and Current State of Encryption Algorithms**

Encryption algorithms have evolved considerably over time. Early algorithms like DES (Data Encryption Standard) became vulnerable due to advancements in computational power and cryptanalysis. AES, introduced as a successor to DES, offers enhanced security and efficiency. The current focus in encryption includes improving existing algorithms and developing quantum-resistant algorithms to address future threats posed by quantum computing. AES remains a critical component of modern encryption practices due to its balanced approach to security and performance (Manico & Detlefsen, 2014).

**Conclusion**

AES-256 is the most appropriate encryption algorithm for Artemis Financial’s long-term archive files. Its robust security features, regulatory compliance, and efficient performance make it an ideal choice for protecting sensitive financial data. Proper implementation and key management practices will ensure optimal data security, addressing both current and future needs.

**References**

Java SE Security API. (2017). *Cipher algorithm names*. Oracle. <https://docs.oracle.com/javase/9/docs/specs/security/standard-names.html#cipher-algorithm-names>

Manico, J., & Detlefsen, A. (2014). *Iron-Clad Java* (Chapters 6 & 8). McGraw Hill Computing.

National Institute of Standards and Technology (NIST). (2001, November 26). *Advanced encryption standard (AES)* (FIPS PUB 197). National Institute of Standards and Technology. <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf>