Southern New Hampshire University

CS-305-R1861

Bradly VanHoorebeke

4-2 Written Assignment: Algorithm Ciphers

9/24/2023

**Recommendation:**

For securing Artemis Financial's long-term archive files, the Advanced Encryption Standard (AES) algorithm cipher is the recommended choice. Here's a detailed justification that meets all the specified requirements:

**Algorithm Cipher Selection Justification:**

1. **Security Protection Best Practices:**
   * AES is selected based on established security best practices. It employs symmetric-key encryption, simplifying key management, which reduces the risk associated with key distribution. This aligns with best practices for minimizing attack vectors.
   * AES offers a range of key sizes (128, 192, and 256 bits) to enable Artemis Financial to select an appropriate balance between security and performance, following best practices for data protection.
2. **Identification of Risks:**
   * AES, while highly secure, may be vulnerable to advanced attacks in the future if computational power increases significantly or new attack methods are discovered. However, the risk of such breakthroughs is currently low, and AES is considered robust against known cryptographic attacks.
3. **Compliance with Current Government Regulations:**
   * AES is compliant with current government regulations, including those set by the National Institute of Standards and Technology (NIST) and Federal Information Processing Standards (FIPS). Using AES ensures that Artemis Financial meets current regulatory requirements.
4. **Usage of the Algorithm Cipher:**
   * AES will be used to encrypt long-term archive files. It provides confidentiality, ensuring that unauthorized parties cannot access the encrypted data. This aligns with best practices for data security, especially for sensitive financial information.
5. **Choice of the Best Cipher:**
   * AES is considered one of the best ciphers due to its security, efficiency, and versatility. Its symmetric-key nature simplifies key management, and it has withstood extensive cryptographic analysis and real-world testing.
6. **Reasons for Not Choosing the Most Secure Cipher:**
   * While AES is highly secure, no cipher can provide an absolute guarantee of security, as security risks continually evolve. Choosing a more secure cipher might introduce complexity and performance overheads that are unnecessary for the current threat landscape.

**Algorithm Cipher Purpose and Key Aspects:**

* **Hash Functions and Bit Levels**: AES employs secure hash functions and multiple rounds of substitution, permutation, and mixing operations to ensure data confidentiality and integrity. The number of rounds varies based on the key size (10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys).
* **Use of Random Numbers**: AES relies on a random initial key (symmetric key) for encryption and decryption. Secure random number generation is essential to its operation, preventing predictability.
* **Symmetric vs. Non-symmetric Keys**: AES is a symmetric-key algorithm, meaning the same key is used for both encryption and decryption. This simplicity simplifies long-term data encryption and aligns with best practices for efficient key management.
* **History and Current State of Encryption Algorithms**: AES was established as the encryption standard in 2001, replacing less secure algorithms like DES. Its current state is robust, and it remains a reliable choice for securing data.

By selecting AES as the encryption algorithm cipher for Artemis Financial's long-term archive files, we ensure adherence to security best practices, compliance with government regulations, efficient data protection, and alignment with current threat landscapes. This recommendation aims to safeguard sensitive financial data effectively.