Module Four Assignment:

Algorithm Ciphers

Elizabeth Marticello

Southern New Hampshire University

CS 305-11883-M01 Software Security 2025 C-4

Professor Albanie Bolton

Due Date: July 27th, 2025

Algorithm Cipher

Recommendation

Given Artemis Financial's security vulnerabilities and needs for the most secure cipher that offers encrypting long-term files I have utilized numerous resources to recommend Advanced Encryption Standard (AES) over everything else listed on Oracle's list of Cipher Algorithm Names (Oracle, n.d.), including Rivest-Shamir-Adleman (RSA). During my research, I limited Oracle's list down to two feasible options, one being symmetrical and the other asymmetrical: being AES and RSA respectfully.

One of the biggest reasons for making my decision was due to the varying use cases both AES and RSA offer. The former is optimized for file encryption and database protection, while the latter is used more for secure email, digitized signatures, and key exchange (Poggi, 2025). Another large deciding factor was the speed of each cipher. AES is proven to be faster for larger datasets when compared to RSA (Poggi, 2025).

Security Protection Best Practices

When using AES for Artemis Financial's file encryption, the best security practices focus on encrypting stored data securely and managing encryption keys carefully. Tools like Keyczar can simplify AES encryption and help ensure proper implementation. Since AES is symmetric, the same key is used for both encryption and decryption, making it critical to rotate keys regularly, store them securely, and keep them separate from the encrypted data to prevent unauthorized access (Manico & Detlefsen, 2014).

Risks of Recommendation

The primary risk of recommending AES is its susceptibility to brute-force attacks (GeeksForGeeks, 2025a). A brute-force attack occurs when an attacker repeatedly tries different keys or password to guess the correct one through trial and error. While this risk exists in principle, AES's strong design and large key size (128, 192, and 256 bits) make brute-force attacks unlikely (Manico & Detlefsen, 2014).

Government Regulations

With Artemis Financial being a financial company that saves personal information about client's banking accounts and cards, when Artemis functions within the United States they must abide by the Payment Card Industry Data Security Standard (PCI DSS). Compliance with this regulation with help Artemis Financial overcome vulnerabilities pertaining to transmission of cardholder data to service providers and protect client data (Security Standards Council, 2018).

Algorithm Cipher Implementation

The AES algorithm cipher will be used by Artemis Financial to encrypt and secure its long-term files, ensuring that sensitive financial and client data remains protected while stored. As a symmetric encryption method, AES uses the same secret key for both encryption and decryption, making it highly efficient for securing large amounts of static data. Once implemented, files will be encrypted before being archived and can only be accessed or decrypted by authorized personnel with the proper key (Poggi, 2025). This approach provides strong confidentiality, aligns with industry regulations such as PCI DSS, and helps safeguard Artemis Financial's data against unauthorized access or potential breaches.

Best Cipher

After much research into Oracle's standard list and other resources, AES stands out as the best choice for Artemis Financial's needs. AES offers a balanced combination of strong security and efficiency. Unlike asymmetric ciphers like RSA which are better suited for key exchange and digital signatures, AES is optimized for encrypting large volumes of data quickly, making it ideal for securing long-term files. Its support for 128, 192, and 256-bit key lengths offer flexible levels of protection (Oracle, n.d.).

Reasons Not to Choose Most Secure Cipher

Using the most secure cipher would require specific hardware requirements. If Artemis Financial was experiencing resource constraints I would have to take that into consideration for my recommendation. Another concern would be compatibility; some environments or legacy systems may not support the strongest ciphers. These restraints would force a trade-off between security and usability.

Justification

Hash Functions and Bit Levels

Hash functions are like digital fingerprints for inputting data. According to GeeksForGeeks (2025b), *"Cryptographic hash functions are mathematical algorithms that transport input data into a fixed-length sequence of characters, referred to as a hash value. Hash functions are essential to securing information digitally by allowing data verification and authentication"* (para.1).

In AES and similar ciphers, bit levels define both the operation and security of encryption. AES uses a fixed 128-bit block size, which processes data in uniform chunks to enhance efficiency and prevent attacks that exploit variable lengths. Additionally, larger key size increases the

number of possible key combinations and encryption rounds, making brute-force attacks much more difficult (GeeksForGeeks, 2025c).

Use of Random Numbers and Symmetric VS Non-Symmetric Keys

Random numbers play a critical role in AES encryption by ensuring the unpredictability and security of generated keys. Since AES is a symmetric cipher, the same key is used for both encryption and decryption. This differs from asymmetric encryption, such as RSA, which uses a public and private key pair. In symmetric encryption, maintaining strong randomness is crucial because if the single shared key is compromised, both encryption and decryption are exposed. Using cryptographically to secure random number generators guarantees that AES keys are unguessable and well-suited to protect Artemis Financial's sensitive client data (Manico & Detlefsen, 2014).

History and Current State of Encryption Algorithms

Some of the earliest encryption methods date back to ancient Sparta, where scrambled letter arrangements protected military communications. During World War I, similar techniques were used to hide military telegram codes. In the 1970s, the Data Encryption Standard (DES) became the first cryptosystem officially used by the U.S. government. However, DES was eventually replaced in 2001 by AES due to its much longer key lengths and stronger resistance to modern hardware attacks (Schneider, n.d.).

Given its proven history, robust key sizes, reliance on strong random numbers, and efficiency in symmetric encryption, AES is the most secure and appropriate cipher for Artemis Financial's long-term file encryption needs.

Resources

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

Poggi, N. (2025, June 2). *Symmetric and asymmetric encryption explained: RSA vs. AES*. PreyProject. https://preyproject.com/blog/types-of-encryption-symmetric-or-asymmetric-rsa-or-aes

(2025a, July 23). *Https://www.Geeksforgeeks.Org/computer-networks/difference-between-aes-and-rsa-encryption/*. GeeksForGeeks. https://www.geeksforgeeks.org/computer-networks/difference-between-aes-and-rsa-encryption/

Manico, J., & Detlefsen, A. (2014). *Iron-Clad Jaca: Building Secure Web Applications*. McGraw Hill Computing. https://learning.oreilly.com/library/view/iron-clad-java/9780071835886/?sso_link=yes&sso_link_from=SNHU

Security Standards Council (2018, July 2). *PCI DSS Quick Reference Guide*. PCI Security Standards. https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

(2025b, July 23). *Cryptography Hash Functions*. GeeksForGeeks. https://www.geeksforgeeks.org/competitive-programming/cryptography-hash-functions/

(2025c, July 23). *Advanced Encryption Standard (AES)*. GeeksForGeeks. https://www.geeksforgeeks.org/computer-networks/advanced-encryption-standard-aes/

Schneider, J. (n.d.). *A brief history of cryptography: Sending secret messages throughout time*. https://www.ibm.com/think/topics/cryptography-history