4-2 Written Assignment: Algorithm Ciphers

Joel De Alba

Southern New Hampshire University

Professor Aaron Demory

04/05/24

Given the sensitive nature of financial data and the potential consequences of unauthorized access or data breaches, Artemis Financial recognizes the imperative to implement robust security measures. This awareness stems from a commitment to safeguarding confidential information, ensuring compliance with industry regulations, and maintaining trust with clients and stakeholders. As a developer and security specialist, I conducted a thorough investigation to determine the best encryption algorithm cipher for Artemis Financial's specific requirements.

After careful consideration of various factors including security protection best practices, potential risks, compliance with government regulations, and usability, I recommend the implementation of the Advanced Encryption Standard (AES) algorithm cipher for encrypting Artemis Financial's archive files. Firstly, AES emerges as a compelling choice due to its well-established reputation as one of the most secure encryption methods available. Offering robust protection against a spectrum of security threats, including brute-force attacks and cryptanalysis techniques like differential and linear cryptanalysis, AES provides a formidable defense for sensitive data.

AES stands out as an optimal choice for Artemis Financial, aligning seamlessly with their security objectives and regulatory obligations. Its widespread global adoption and endorsement by the U.S. National Institute of Standards and Technology (NIST) underscore its reliability. AES's resilience against scrutiny further enhances its suitability. While acknowledging that no encryption algorithm is impervious to attacks, AES has withstood significant cryptanalysis, maintaining its status as a robust cipher. Its adaptable key length options (128, 192, or 256 bits) offer Artemis Financial the flexibility needed to address their specific security needs. Moreover, AES's adherence to stringent government regulations such as FIPS and GDPR ensures compliance with legal requirements. Lastly, AES's broad support across various software platforms facilitates seamless integration into Artemis Financial's existing infrastructure, minimizing operational disruptions and overhead costs.

The selection of the Advanced Encryption Standard (AES) algorithm cipher is substantiated by its utilization of secure hash functions, variable key lengths, and symmetric key encryption mechanisms, all of which contribute to robust data security. By employing AES, Artemis Financial benefits from the enhanced protection afforded by strong hash functions and variable key lengths, mitigating risks associated with brute-force attacks and unauthorized access. Moreover, AES's reliance on random number generation and symmetric key encryption guarantees enhanced encryption key strength and operational efficiency, supporting the protection of confidential data.

Although there are other encryption techniques outside AES, some of their disadvantages may limit their applicability to Artemis Financial's requirements. For example, because to their relatively small key lengths and vulnerability to brute-force attacks, older encryption algorithms like DES (Data Encryption Standard) and Triple DES, though formerly widely employed, are now regarded as antiquated and susceptible to modern cryptographic assaults. Like this, due to their somewhat slower processing speeds and higher computational cost, RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography) encryption, which rely on asymmetric key pairs, might not be the best choice for encrypting big archive files.

While some algorithms may provide unique benefits in certain cases, they may lack the general backing and standardization provided by AES, making them less interoperable and perhaps more difficult to apply across Artemis Financial's systems. Given the necessity for strong security, efficiency, regulatory compliance, and ease of integration, AES appears as the best option for ensuring the long-term protection of Artemis Financial's archive files.

Sources

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

Manico, J., & Detlefsen, A. (n.d.-b). Iron-Clad java. O’Reilly Online Learning. https://learning.oreilly.com/library/view/iron-clad-java/9780071835886/ch06.html

Sachin, M., & Kumar, D. (2010). Implementation and Analysis of AES, DES and Triple DES on GSM Network. IJCSNS International Journal of Computer Science and Network Security, 10, 298-303.

Aleisa, N. (2015). A Comparison of the 3DES and AES Encryption Standards. International Journal of Security and Its Applications, 9(7), 241-246.

Singh, P., & Kumar, S. (2017). Study & analysis of cryptography algorithms: RSA, AES, DES, T-DES, blowfish. Int. J. Eng. Technol, 7(1.5), 221.