Module Four: Assignment

Joshua Wozny

CS-305,

Southern New Hampshire University



Artemis Financial desires to secure its systems by using encryption and other security best practices. Encryption has a rich history that traces back to ancient times with the Caesar a and the Vigenere ciphers. (Tutorial: Caesar and Vigenere Ciphers | CodeHS, 2023) Modern encryption was developed in the 20th century starting after World War I, and continues to this day using machines and later computers to perform the complex calculations needed to provide secure communication. Cryptography has become even more important in the Digital age, requiring the development of secured authentication for use in a distributed system like the internet, and more recently the Cloud. (“Cryptology - Manual, Mechanized, and Information Age | Britannica,” 2023).

One area that Artemis has identified for immediate attention is archived files. To ensure secure file storage of archived files, I would recommend using the Advanced Encryption Standard Algorithm (AES). AES is a widely used symmetric encryption algorithm that provides a high level of security and has been adopted as standard encryption by the US government. It supports key sizes of 128, 192, and 256 bits and is considered secure for most applications. Depending on the sensitivity of the archived files any of the available key sizes are appropriate, but I recommend the 256-bit size to err on the side of caution. (Java Security Standard Algorithm Names, 2017).

Random numbers are crucial in cryptography to add an element of uncertainty to generate secure keys, seeds, and other cipher elements to make it harder for bad actors to deduce the key needed to decode an encrypted data source. Keys are used to encrypt and decrypt data at rest and in transit. AES uses a symmetric key in which the same key is used to encrypt and decrypt data. To ensure communication using a symmetric key, the key must be only shared with trusted clients securely. Asymmetric key algorithms, also known as public-key algorithms, use a pair of mathematically related keys: a public key and a private key. The public key is freely distributed, while the private key is kept secret. Asymmetric key algorithms like RSA are not typically used for encrypting large amounts of data due to their computational overhead. However, they are crucial in key exchange protocols and certificate-based authentication (Java Security Standard Algorithm Names, 2017).

If additional security is needed for specific files, password-based encryption such as BBKDF2 can be used. This Algorithm should be paired with the AES encryption algorithm for the reasons set forth above. Under all circumstances, key generation should employ a random key generation process using a cryptographically secure random number generator. It is also important that a secure AES mode of operation, like GCM, is used to protect against eavesdropping and tampering. It is also vital that vulnerabilities are assessed regularly, with keys updated based on these assessments – while considering risks associated with key management and storage (Java Security Standard Algorithm Names, 2017).

If the archived files need to be accessed from older systems that do not support AES-256, choose the strongest cipher available for that system or seriously consider upgrading these systems to minimize risk. Although costly, upgrading is the most secure solution, but if it is not feasible, utmost care must be taken to ensure all other best practices are being used to secure these files (What Are the Best Practices for Encrypting Data at Rest and in Transit?, 2023).

Consider the following best practices:

* Stay informed about the most current government regulations and requirements regarding encryption algorithms, key lengths, and compliance standards. Be aware of regulations in any country where Artemis Financial does business. Failure to comply will result in costly fines.
* Consider employing additional security measures, such as access controls, network security, and monitoring mechanisms, to defend against various types of security attacks.
* Implement secure transmission protocols, such as HTTPS or SFTP, to protect encrypted files during transit.

**References**

Cryptology - Manual, Mechanized, and Information Age | Britannica. (2023). In Encyclopædia Britannica. <https://www.britannica.com/topic/cryptology/History-of-cryptology>

Java Security Standard Algorithm Names. (2017). Oracle.com.

<https://docs.oracle.com/javase/9/docs/specs/security/standard-names.html#cipher-algorithm-names>

Tutorial: Caesar and Vigenere Ciphers | CodeHS. (2023). Codehs.com. <https://codehs.com/tutorial/jennifer/caesar-and-vigenere-ciphers>

What are the best practices for encrypting data at rest and in transit? (2023). Linkedin.com. <https://www.linkedin.com/advice/0/what-best-practices-encrypting-data-rest>

‌