****

# Practices for Secure Software Report

Table of Contents

[Document Revision History 3](#_Toc102040754)

[Client 3](#_Toc102040755)

[Instructions 3](#_Toc102040756)

[Developer 4](#_Toc102040757)

[1. Algorithm Cipher 4](#_Toc102040758)

[2. Certificate Generation 4](#_Toc102040759)

[3. Deploy Cipher 4](#_Toc102040760)

[4. Secure Communications 4](#_Toc102040761)

[5. Secondary Testing 4](#_Toc102040762)

[6. Functional Testing 4](#_Toc102040763)

[7. Summary 4](#_Toc102040764)

[8. Industry Standard Best Practices 4](#_Toc102040765)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **2.25.2024** | **Moe Gutierrez** |  |

## Client



## Instructions

Submit this completed practices for secure software report. Replace the bracketed text with the relevant information. You must document your process for writing secure communications and refactoring code that complies with software security testing protocols.

* Respond to the steps outlined below and include your findings.
* Respond using your own words. You may also choose to include images or supporting materials. If you include them, make certain to insert them in all the relevant locations in the document.
* Refer to the Project Two Guidelines and Rubric for more detailed instructions about each section of the template.

## Developer

Moe Gutierrez

## Algorithm Cipher

In the realm of cybersecurity, choosing the right encryption algorithm is paramount to safeguarding sensitive data. In this essay, we will delve into the intricacies of selecting an appropriate cipher for our client, **Artemis Financial**, and provide constructive recommendations based on security vulnerabilities.

**1. Brief Overview of the Encryption Algorithm Cipher**

Our recommended choice for Artemis Financial is the **Advanced Encryption Standard (AES)**. AES is a symmetric-key block cipher that has gained widespread adoption due to its robustness and efficiency. It operates on fixed-size blocks of data and employs a secret key for both encryption and decryption. The three key lengths available for AES are 128, 192, and 256 bits.

**2. Hash Functions and Bit Levels**

To enhance security, we propose using **SHA-256** (Secure Hash Algorithm 256-bit) as the hash function within the AES framework. Here’s why:

* **SHA-256**: This cryptographic hash function produces a fixed-length 256-bit digest for any input data. With an astronomical number of possible hash combinations (approximately 1.1579209e+77), it remains virtually impervious to brute force attacks and collision vulnerabilities. Notably, SHA-256 is endorsed by the **National Institute of Standards and Technology (NIST)** as a standard encryption cipher.

**3. Symmetric vs. Non-Symmetric Keys**

**Symmetric Keys**

* **AES Symmetric Keys**: In AES, the same secret key is used for both encryption and decryption. This simplicity ensures efficient processing and is suitable for scenarios where secure communication channels exist between parties. Symmetric keys are well-suited for Artemis Financial's needs, as they provide fast data transformation without the overhead of managing multiple keys.

**Non-Symmetric Keys**

* **Asymmetric (Non-Symmetric) Keys**: In contrast, asymmetric keys involve a pair of distinct keys: a public key for encryption and a private key for decryption. While non-symmetric keys offer enhanced security (especially for key exchange), they introduce computational overhead. Typically, the public key is openly shared, allowing anyone to send encrypted messages, while the private key remains confidential.

**4. Historical Context and Current State of Encryption Algorithms**

**Historical Perspective**

* **Data Encryption Standard (DES)**: In the past, DES was the de facto encryption standard in the United States. However, DES faced vulnerabilities due to its small key size (56 bits) and susceptibility to brute force attacks. Over time, DES was superseded by more robust algorithms.

**Current Landscape**

* **AES**: The adoption of AES as the US federal standard in 2002 marked a significant shift. AES has withstood rigorous cryptanalysis and remains secure. Its widespread use in secure messaging applications, financial institutions, and government agencies attests to its reliability.
* **Post-Quantum Cryptography**: As quantum computing advances, the need for post-quantum encryption algorithms becomes critical. Researchers are exploring lattice-based, code-based, and multivariate polynomial-based schemes to withstand quantum attacks.

**5. Recommendations and Future Considerations**

To fortify Artemis financials security posture:

1. **Implement AES with SHA-256**: Deploy AES with a 256-bit key length and SHA-256 for hashing. Regularly update keys to mitigate risks.
2. **Monitor Quantum-Safe Algorithms**: Stay informed about post-quantum cryptography developments. As quantum computers evolve, transition to quantum-safe algorithms when necessary.
3. **Thorough Testing**: Rigorously test the encryption implementation, including key management and data integrity checks.
4. **Education and Awareness**: Educate employees about encryption best practices and the importance of secure coding.

In conclusion, my recommendation aligns with industry standards, balancing security, and efficiency. By adopting AES with SHA-256, Artemis Financial can safeguard client data while maintaining operational agility.

## Certificate Generation

Insert a screenshot below of the CER file.

[Insert screenshots here.]

## Deploy Cipher

Insert a screenshot below of the checksum verification.

[Insert screenshots here.]

## Secure Communications

Insert a screenshot below of the web browser that shows a secure webpage.

[Insert screenshots here.]

## Secondary Testing

Insert screenshots below of the refactored code executed without errors and the dependency-check report.

[Insert screenshots here.]

## Functional Testing

Insert a screenshot below of the refactored code executed without errors.

[Insert screenshots here.]

## Summary

[Insert text.]

## Industry Standard Best Practices

[Insert text.]