****

# Practices for Secure Software Report

Table of Contents

[Practices for Secure Software Report 1](#_Toc138006130)

[Document Revision History 3](#_Toc138006131)

[Client 3](#_Toc138006132)

[Developer 4](#_Toc138006133)

[1. Algorithm Cipher 4](#_Toc138006134)

[2. Certificate Generation 5](#_Toc138006135)

[3. Deploy Cipher 5](#_Toc138006136)

[4. Secure Communications 5](#_Toc138006137)

[5. Secondary Testing 6](#_Toc138006138)

[6. Functional Testing 8](#_Toc138006139)

[7. Summary 9](#_Toc138006140)

[8. Industry Standard Best Practices 9](#_Toc138006141)

[9. Citations 10](#_Toc138006142)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **June 18, 2023** | **Jonathan Miller** | **Initial Revision** |

## Client



## Developer

Jonathan Miller

## Algorithm Cipher

1. *Provide a brief, high-level overview of the encryption algorithm cipher.*

The cryptographic encryption algorithm that I decided to use is the SHA3 – 256 algorithm cipher. I decided to use this algorithm cipher because it is the latest standard for cryptographic encryption according to the Federal Information Processing Standards Publication 202. SHA3 is the latest technology used to ensure that the original message was not altered to a different message with the same hash value (collision resistance). (Pritzker & May, 2015) It is important to avoid collisions so that the original message does not get intercepted and replaced with a malicious message that has the same hash, or checksum, value.

I have decided to use the 256-bit version of SHA3 that will always output a 256-bit long string for the digest, or checksum, value. A 256-bit digest is sufficient for the message that was encrypted in this assignment.

1. *What is the purpose of the cipher's hash functions and bit levels?*

A cipher uses hash functions to turn plaintext into ciphertext. The cipher will translate the data into another set of data using a function to encrypt the data. For each data translation a key will be generated to decrypt the translated data.

This generated key will have a bit level to determine the length of the key. The higher the bit level, the more secure the algorithm will be due to the higher number of permutations that a key can take on.

1. *Explain the use of random numbers, symmetric versus non-symmetric keys, and so on.*

Encryption algorithms will use cryptographic pseudorandom number generators to create secure keys for decryption. This will prevent the unlikely event of predicting a key.

Algorithm ciphers can use either one or two encryption keys for encryption/decryption. Symmetric ciphers will create one key for both encryption and decryption, while asymmetric ciphers will utilize both a public and private key for encryption and decryption, respectively. (Manico et al., 2015)

1. *Describe the history and current state of encryption algorithms.*

Encryption algorithms in the past, such as DES (Data Encryption Standard) generated keys of only 56 bits in length. This allowed for brute force attacks for generating the correct key to decrypt data. Since there were only 2^56 different permutations of a DES key, computers were able guess the correct key by trying all possible permutations until the correct one was found.

To combat this, 3DES (Triple Data Encryption Standard) was formed. This basically performed DES three times on the data and led to key lengths of 168 bits. The block size of 3DES is only 64-bits and it led to block collision attacks if it was used to encrypt large amounts of data with the same key. (Triple des 2023)

Currently, as of FIPS 197, AES is the new encryption standard. This can produce key sizes of up to 256 bits in length, and it is currently impossible to brute force a key. However, with the emergence of AI technologies, AES keys may be brute forced in the near future.

## Certificate Generation

A computer screen with white text

Description automatically generated with low confidence

## Deploy Cipher

A screenshot of a computer

Description automatically generated with medium confidence

## Secure Communications

A screenshot of a computer

Description automatically generated

## Secondary Testing

A screenshot of a computer screen

Description automatically generated with medium confidence

A picture containing text, screenshot, font, document

Description automatically generated

## Functional Testing

A screenshot of a computer program

Description automatically generated with medium confidence

## Summary

1. *Refer to the Vulnerability Assessment Process Flow Diagram. Highlight the areas of security that you addressed by refactoring the code.*

The areas of security that apply to the Artemis Financial’s application include the following:

* APIs – This application uses the spring boot framework to utilize RESTful APIs.
* Cryptography – This application uses a cryptographic cipher to encrypt data.
* Client/Server – This application deploys a secure server that a client connects to.
* Code Quality – This application relies on secure coding practices and patterns to mitigate security vulnerabilities.

1. *Discuss your process for adding layers of security to the software application.*

Artemis Financial needs their application to be without security vulnerabilities. To accomplish this, the areas of security that were affected by this application were identified. Then, the code was reviewed for potential security vulnerabilities.

Artemis Financial stated that they needed data to be encrypted. This then led to the implementation of a hash function that utilized the latest standard for cryptographic algorithm ciphers, SHA-256. The data that was sent to the client was encrypted using the SHA-256 algorithm cipher to create a checksum for the data. They also needed their code to be secured with the HTTPS protocol, so a self-signed key was created and utilized in the spring boot application. Lastly, functional testing was performed to ensure that the code was secure and functioning as expected.

## Industry Standard Best Practices

1. *Explain how you used industry standard best practices to maintain the software application’s current security.*

This application utilizes industry standard best practices to defend against cross-site scripting, protect sensitive data, and prevent injection attacks. To do this, the Spring Boot framework was utilized to implement a secure server using HTTPS and a self-signed key. The application involved the implementation of a RESTful API with secure endpoints using industry standard coding best practices. Functions that were not needed by the end user were marked as private so they could only be accessed by the server controller class member function for hashing.

1. *Explain the value of applying industry standard best practices for secure coding to the company’s overall wellbeing.*

Applying industry standard best practices for secure coding is essential for a company’s overall wellbeing. Without secure coding best practices, company assets such as money, card numbers, trade secrets, personal information, and passwords could be accessed by attackers.

These attackers could use this obtained information to steal money from the company or its consumers. They could also use obtained trade secrets to gain an advantage in the market. Or they could DDOS attack your website and create downtime that results in major losses in revenue.

If any of these attacks successfully occur, there could be major regulatory fines and penalties that could cost your company great sums of money as well as consumer confidence that may not ever be re-obtained. Therefore, security vulnerabilities could ultimately lead to the collapse of the company, and secure coding practices should be taken into consideration throughout the entire SDLC.

## Citations

Information Technology Laboratory , Pritzker, P., & May, W., SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions 1–2 (2015). Gaithersburg, MD; National Institute of Standards and Technology.

Manico, J., & Detlefsen, A. (2015). Symmetric and Asymmetric Cryptography. In *Iron-clad java: Building secure web applications*. essay, McGraw-Hill Education.

Wikimedia Foundation. (2023, April 18). *Triple des*. Wikipedia. https://en.wikipedia.org/wiki/Triple\_DES