****

# 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** | **12/17/2023** | **Michael Berry** |  |

## 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

[Insert your name here.]

## Algorithm Cipher

The Advanced Encryption Standard (AES) is the most suitable encryption algorithm considering Artemis Financial's imperative to secure their long-term archive files. Recognized for its robust security features, AES offers key sizes of 128, 192, or 256 bits, allowing for flexibility in tailoring security levels (Oracle, 2017). Its resilience has been confirmed by in-depth cryptanalysis. AES, being a block cipher, does not directly employ hash functions. Instead, it focuses on key expansion and bit manipulation for encryption strength. The AES algorithm's key sizes are determined by the selection of bit levels, which span from 128 to 256 bits. This allows for different security levels to be achieved.

Using random numbers is integral to AES, contributing to generating strong encryption keys. Being a symmetric key algorithm, AES employs the same key for encryption and decryption, emphasizing efficiency over the complexity inherent in non-symmetric (asymmetric) algorithms.

In tracing the history of encryption algorithms, AES was established by NIST in 2001 as a successor to the Data Encryption Standard (DES). AES is the global standard, widely acknowledged for its security, and adopted as a fundamental component of secure data transmission and storage.

## Certificate Generation

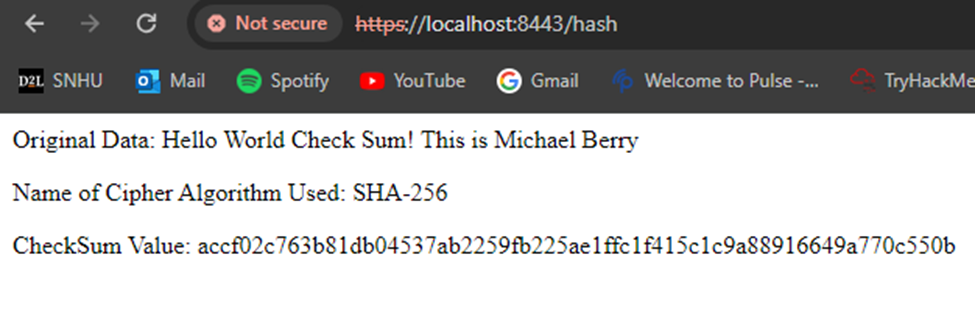
A screenshot of a computer

Description automatically generated

## Deploy CipherA screenshot of a computer Description automatically generated

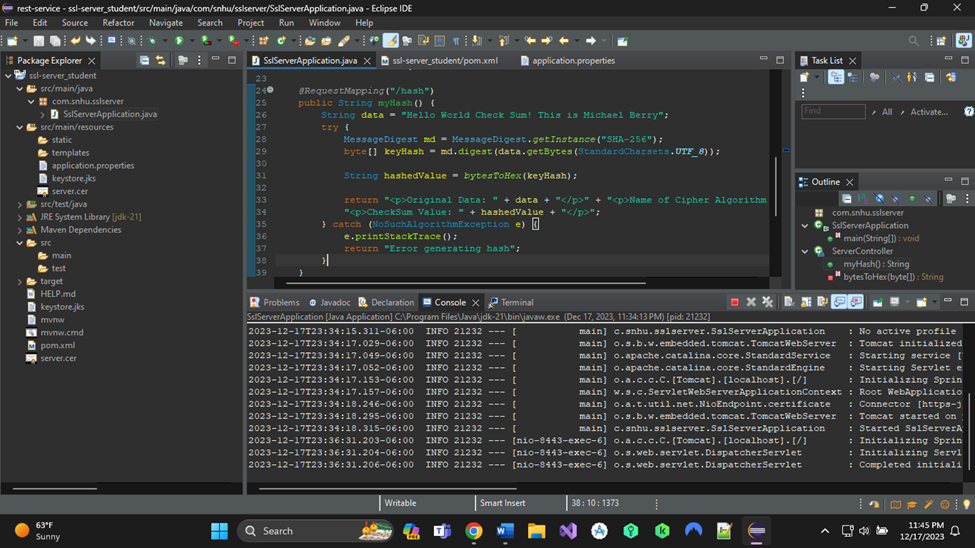
## A screenshot of a computer Description automatically generated

## Secure Communications



## Secondary Testing

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



A computer screen with many text boxes

Description automatically generated

A screenshot of a check

Description automatically generated

## Functional Testing

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

A screenshot of a computer

Description automatically generated

## Summary

## Industry Standard Best Practices

[Insert text.]