****

# 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** | **08/10/2023** | **Mitchel Harmon** |  |

## 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

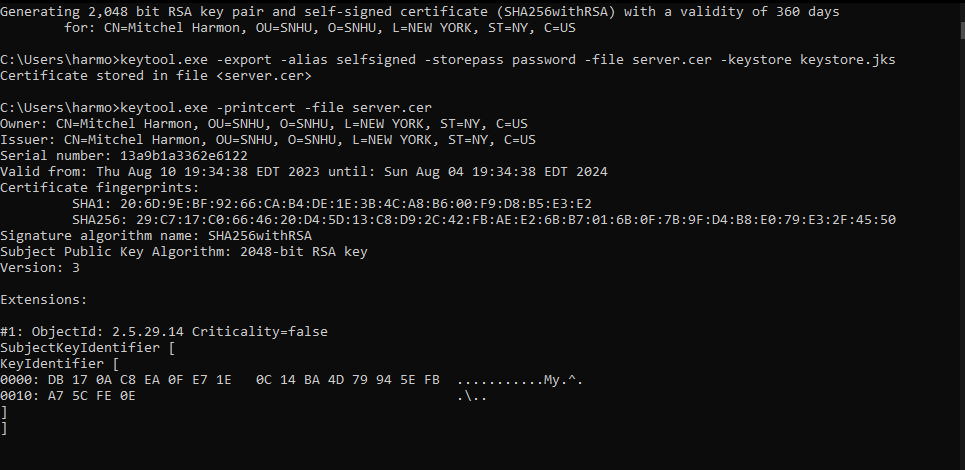
Mitchel Harmon

## Algorithm Cipher

Artemis Financial deals with important financial data so encrypting that data is a necessary precaution in avoiding the data being seen by anyone unauthorized. AES would be the best option when it comes to encrypting sensitive financial data and is used by the U.S government. AES uses three block ciphers which are AES-128, AES-192, and AES-256, while each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128,192 and 256 bits (Bernstein & Cobb,2021, para. 7). AES employs symmetric encryption which involves converting plaintext to ciphertext using the same key to encrypt and decrypt the data. Another encryption is RSA (Rivest-Shamir-Adleman) algorithm which is more commonly used in web browsers, VPN’s and various other applications. RSA uses asymmetric cryptography which has a public and private key that only allows decryption with the related key and is employed with two separate endpoints. RSA performance is poor due to its speed not being convenient for processing large amounts of data so while the security of RSA might be good the processing power of RSA doesn’t hold a candle to AES. RSA by itself would not be sufficient to safeguard the sensitive bank data but can be used in tandem with AES to provide the benefits of both. The earliest evidence of encryption can be traced back to ancient Egypt, the tomb of Khnumhotep II contained unusual hieroglyphs that were used to hide the meaning of the text. (Team T, 2022).

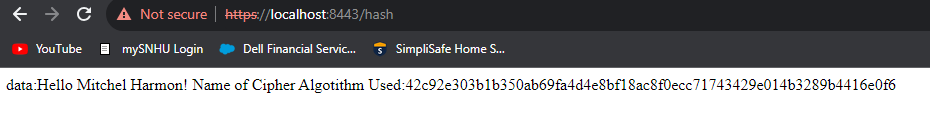
## Certificate Generation

Insert a screenshot below of the CER file.



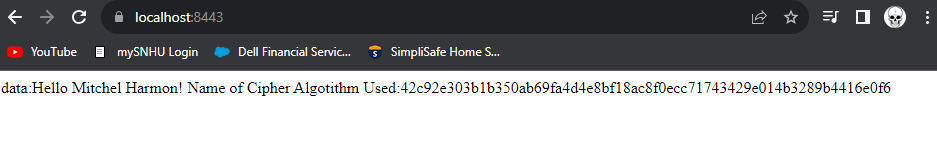
## Deploy Cipher

Insert a screenshot below of the checksum verification.



## Secure Communications

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



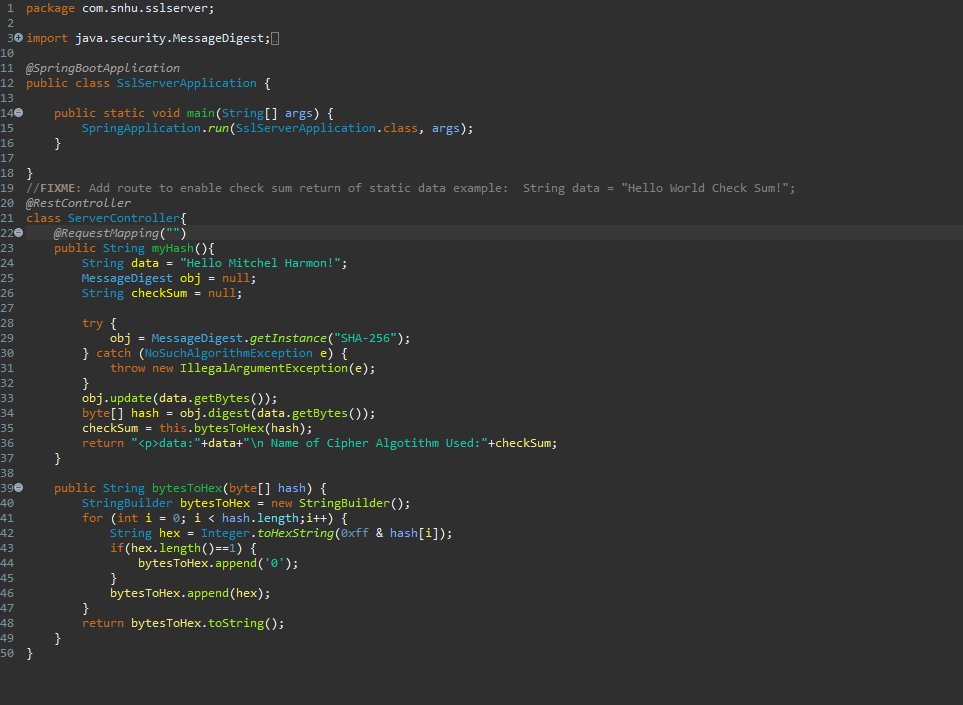
## Secondary Testing

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



## Functional Testing

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



## Summary

I refactored the code to address the cryptography vulnerability by using the hash function for checksum verification. Using the spring framework, I was able to use restful API. Lastly, using the certification and keystore I was able to address the server/client vulnerability.

## Industry Standard Best Practices

One use of industry standard best practices is the use of hash functions so the user can tell if the data they are receiving has been tampered with. Another use of industry standard best practices was the use of CA’s to secure the application by ensuring the trustworthiness and authenticity of it.

**Citations**

* Bernstein C., & Cobb M. (2021, September). Advanced Encryption Standard (AES). TechTarget. <https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard?Offer=abt_pubpro_AI-Insider>.
* Neha T. (2020, May 5th). Advanced Encryption Standard (AES). Binary Terms. https://binaryterms.com/advanced-encryption-standard-aes.html
* Team T. (2022, January 14). The history of encryption: the roots of modern-day cyber-security. Tresorit. https://tresorit.com/blog/the-history-of-encryption-the-roots-of-modern-day-cyber-security/