****

# CS 305 Project Two

**Practices for Secure Software Report**

**Table of Contents**

[Document Revision History 3](#_heading=h.1fob9te)

[Client 3](#_heading=h.3znysh7)

[Instructions 3](#_heading=h.2et92p0)

[Developer 4](#_heading=h.tyjcwt)

[1. Algorithm Cipher 4](#_heading=h.3dy6vkm)

[2. Certificate Generation 4](#_heading=h.1t3h5sf)

[3. Deploy Cipher 4](#_heading=h.4d34og8)

[4. Secure Communications 4](#_heading=h.2s8eyo1)

[5. Secondary Testing 4](#_heading=h.17dp8vu)

[6. Functional Testing 5](#_heading=h.3rdcrjn)

[7. Summary 5](#_heading=h.26in1rg)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **07/16/2021** | **Tyler Owens** |  |
| **1.1** | **08/14/2021** | **Tyler Owens** |  |

## Client



## Developer

Tyler Owens

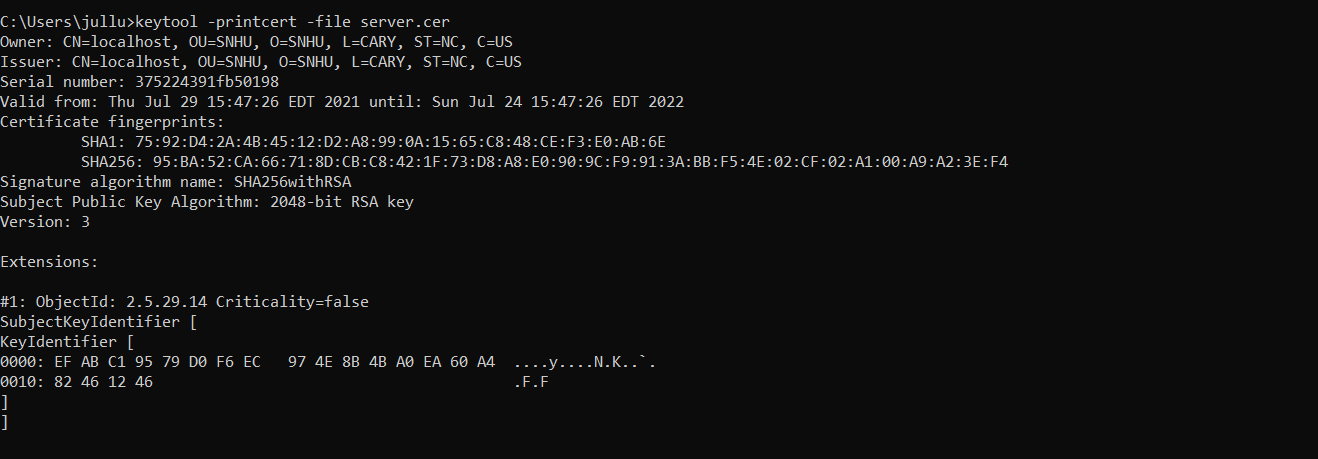
## 1. Algorithm Cipher

As a financial company, data security should be a top concern when creating a program. When creating any code, potential avenues of attack would need to be considered. Developers will need to follow security protocols and avoid anti-patterns. Since the company deals in financial information, all of the data it handles will need to be considered potentially harmful if compromised, along with the normal intellectual property of the company. Currently the USA has standards for encryption for financial data so we will have to follow their protocols when encrypting data. To comply we will need a certified cypher to encrypt all customer and internal data. The best cypher to use is AES which has as high of an encryption bit as possible (at least 128). We might not choose to go with the highest encryption bit because it will come at a cost of size which could lead to expensive memory constraints or speed issues.

The Cypher (AES 128) will be used to encrypt and decrypt the data, helping prevent it from being read even if it is intercepted or stolen. Hash functions are sure to encrypt (scramble) the data into a form that is unreadable without decrypting it, so even if data is stolen or intercepted it is useless. The bit level or a cipher will determine how “scrambled” the encrypted data is, the larger the bit level, the harder the encryption is to break but the data will consume more storage space. AES 128 is on the lower end of very good encryption but would be safer if the bit levels were raised at the cost of space. Random numbers are used to make sure the cyphers are unpredictable and basically impossible to reverse engineer without the key. AES is a symmetric algorithm, meaning that the encrypted data can be decrypted which will be necessary for stored data, non-symmetric algorithms are used to generate keys that can show if data have been compromised or tampered. Encryption Algorithms have had to constantly evolve because as computers have become exponentially more powerful, they are also able to easily crack old algorithms. Algorithms have evolved to a level in which the more secure ones are virtually unbreakable without the key and will not be breakable until major leaps in computing power have been made.

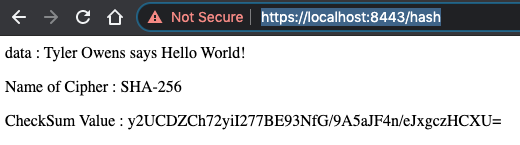
## 2. Certificate Generation

Self Generated certificate

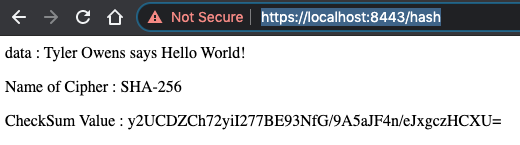


## 3. Deploy Cipher

Verification of checksum value using a short string and displayed through use of RESTful API.

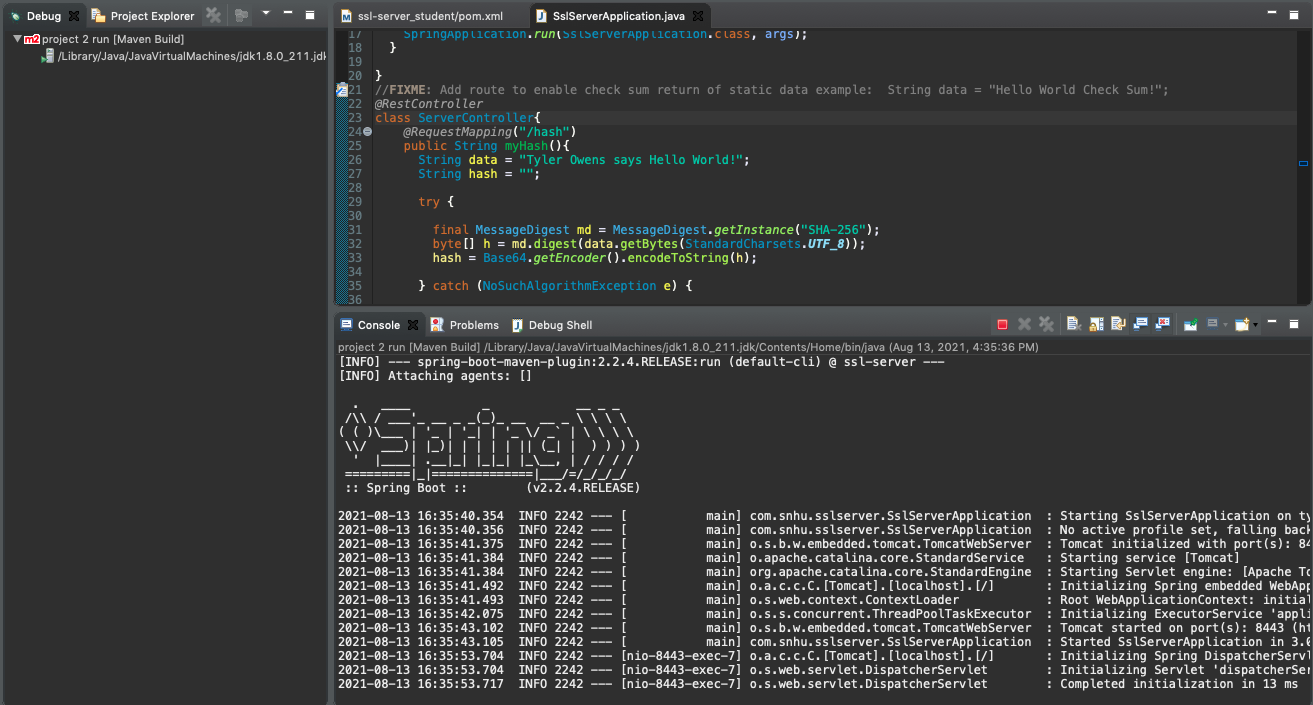


## 4. Secure Communications



## 5. Secondary Testing

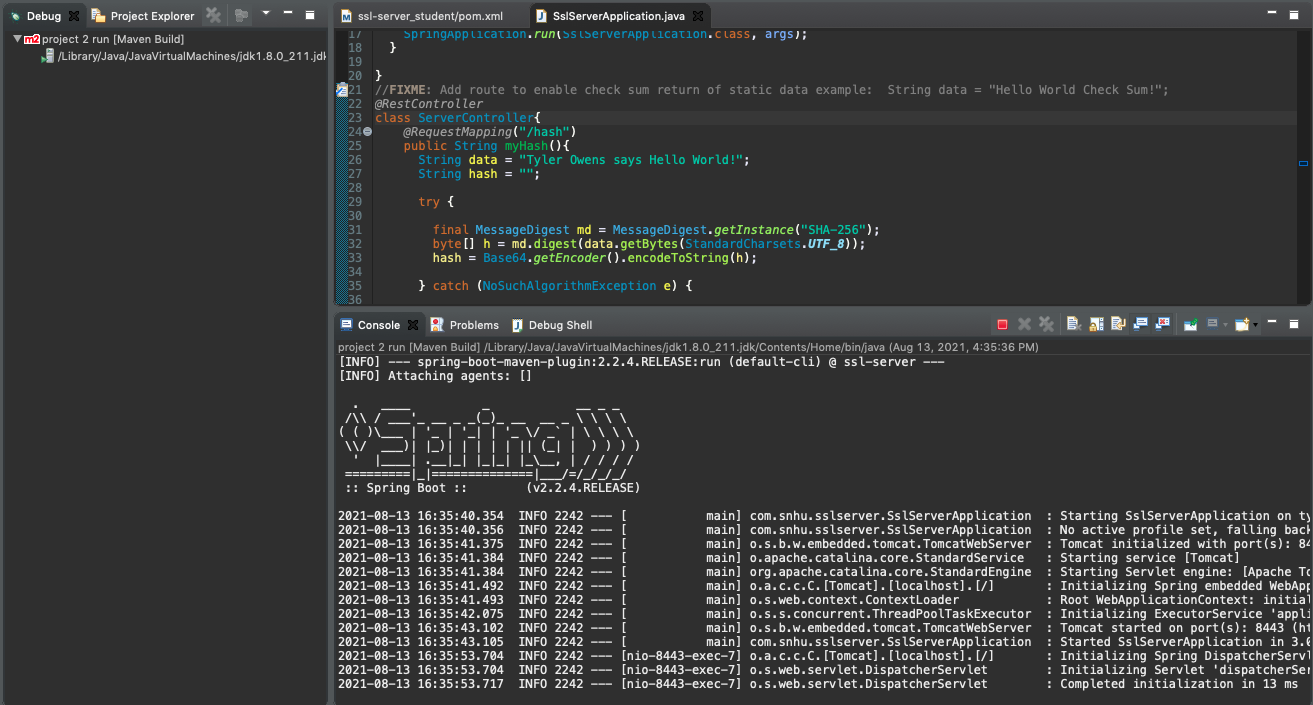
Refactored code executing without errors



**The dependency check report**



## 6. Functional Testing



## 7. Summary

The code has been refactored to start the process of increasing the security of the application. Cryptography from the Vulnerability Assessment Process Flow Diagram has been added to the project for a large security layer. An AES-128 SHA algorithm will be used to create checksums that will verify that data has been transferred securely without manipulation. I have also reviewed the code and ran it through tests to ensure quality and that there are no additional errors to cover.

More layers of security will need to be added to help ensure the safety of the software. Data validation will need to be added when client data is taken by the program so that any malicious data is not processed. Encryption will also need to be added to any stored data so that even if it is stolen or accessed, it can not be used.

Security is not just something to be thought about when making a program but just as importantly when maintaining it. Any newly discovered vulnerabilities will need to be patched in old code or old security protocols may need to be rethought about for new functionality. Code will need to be regression tested regularly and as any new features or fixes are deployed.