****

# CS 305 Project Two

**Practices for Secure Software Report**

**Table of Contents**

CS 305 Project Two 1

Document Revision History 3

Client 3

Instructions 3

Developer 4

1. Algorithm Cipher 4

2. Certificate Generation 4

3. Deploy Cipher 4

4. Secure Communications 5

5. Secondary Testing 5

Summary 7

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **6 17 22** | **Branden Mccusker** |  |

## Client



## Instructions

Deliver this completed Practices for Secure Software Report documenting your process for writing secure communications and refactoring code that complies with software security testing protocols.

Respond to the steps outlined below and replace the bracketed text with your findings in your own words. If you choose to include images or supporting materials, be sure to insert them throughout.

## Developer

Branden Mccusker

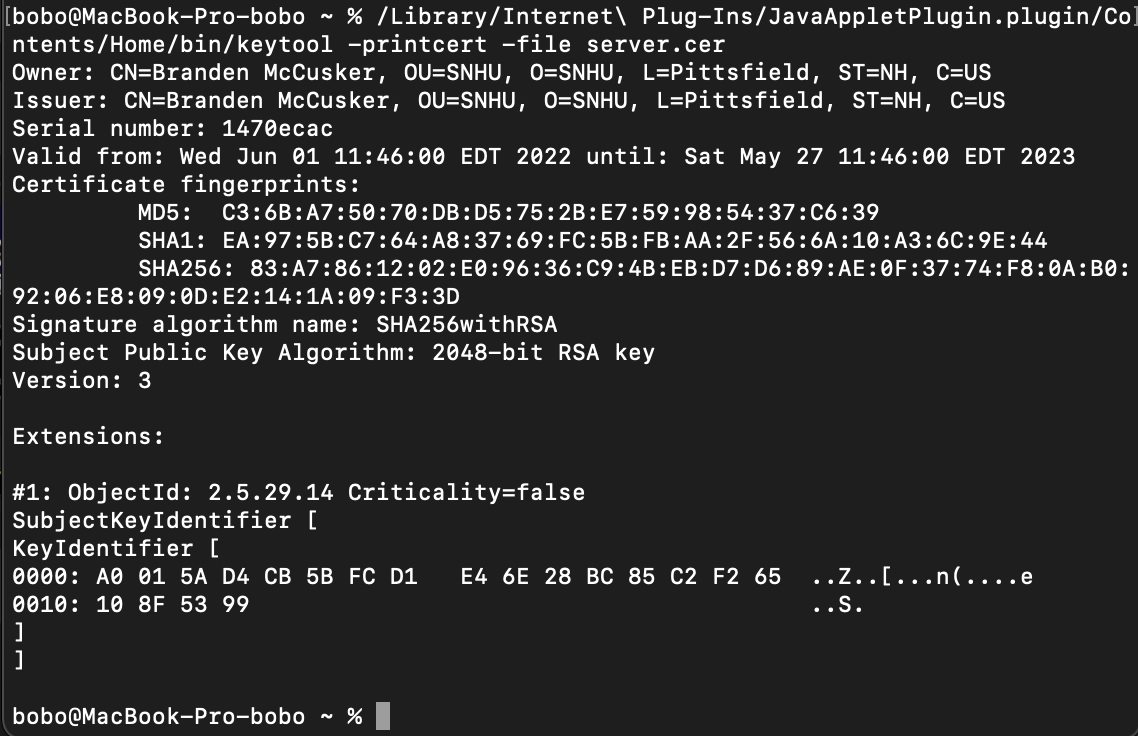
## 1. Algorithm Cipher

Determine an appropriate encryption algorithm cipher to deploy given the security vulnerabilities, justifying your reasoning. Be sure to address the following:

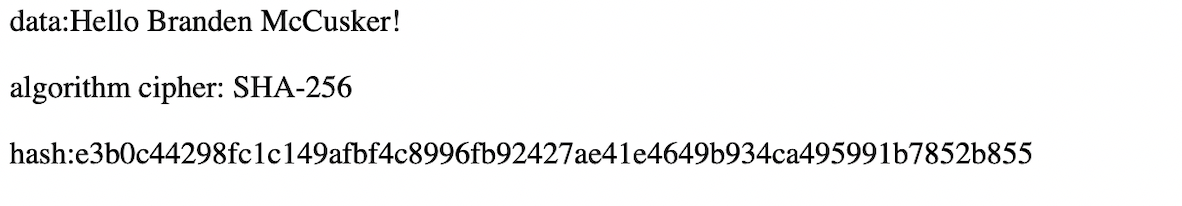
SHA-256 is an appropriate encryption algorithm cipher.

SHA ranges from 1 to 512 bit versions.

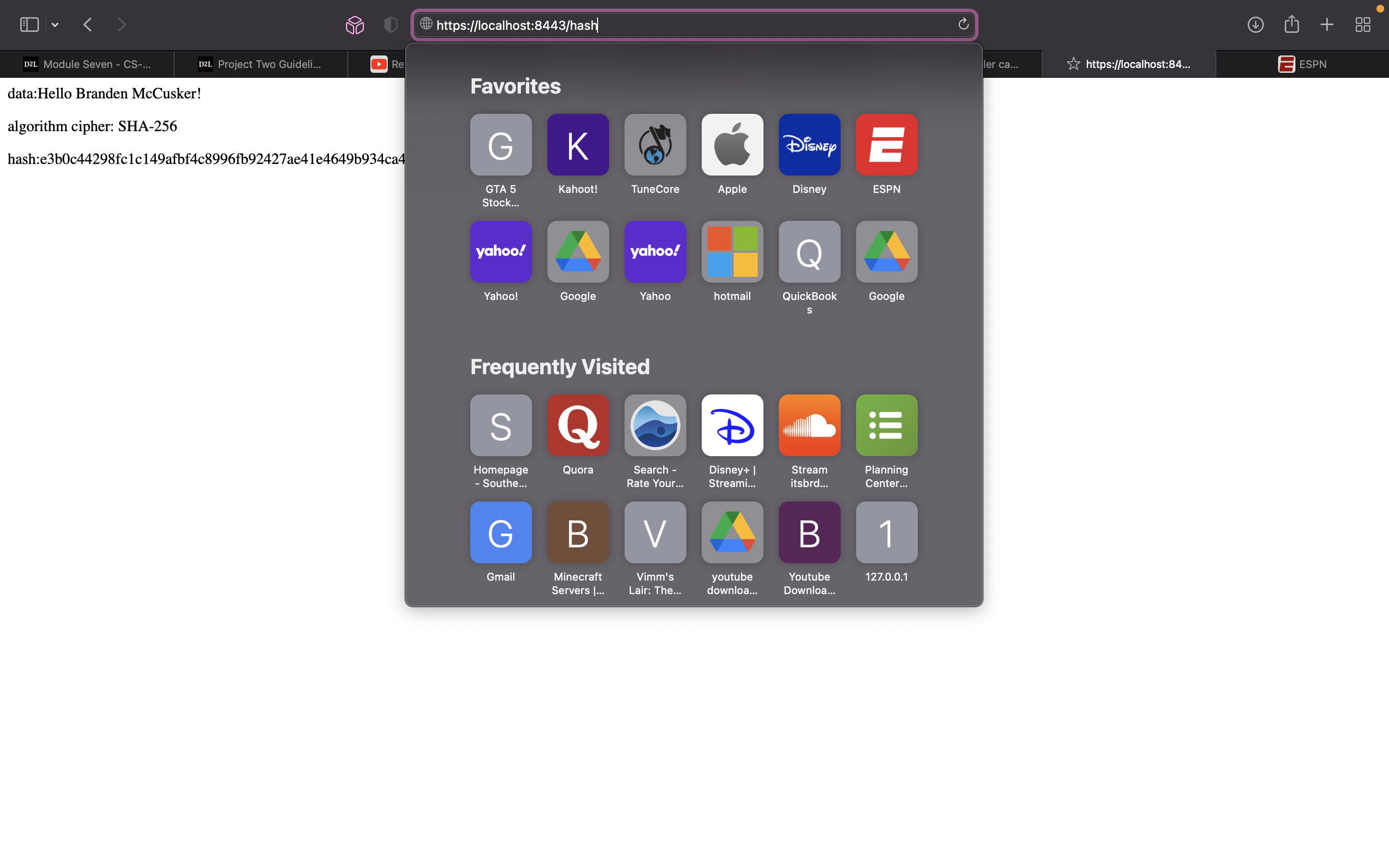
## 2. Certificate Generation

Generate appropriate self-signed certificates using the Java Keytool, which is used through the command line.

## 3. Deploy Cipher



## 4. Secure Communications



(Its fairly difficult to get a decent screenshot with the current version of Safari)

## 5. Secondary TestingImage

## Image

## Summary

By refactoring the code, I am now able to encrypt and secure data within the program through the implementation of SHA-256. Adding layers of security is vital for upkeeping its effectiveness, as any encryption method can be cracked over time. Our users can trust us with keeping their private information safe and secure, which will improve our company’s wellbeing. Maintaining current security means keeping your system up to date, as well as following safe information transfer practices.