****

# CS 305 Project Two

**Practices for Secure Software Report**

Table of Contents

[Document Revision History 3](#_Toc33111302)

[Client 3](#_Toc33111303)

[Instructions 3](#_Toc33111304)

[Developer 4](#_Toc33111305)

[1. Algorithm Cipher 4](#_Toc33111306)

[2. Certificate Generation 4](#_Toc33111307)

[3. Deploy Cipher 4](#_Toc33111308)

[4. Secure Communications 4](#_Toc33111309)

[5. Secondary Testing 4](#_Toc33111310)

[6. Functional Testing 5](#_Toc33111311)

[7. Summary 5](#_Toc33111312)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **12/11/20** | **Arooj Saeed** | **Describing cipher** |

## 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

Arooj Saeed

## 1. Algorithm Cipher

According to my point of view, the best encryption algorithm cipher is AES also known as “Advanced Encryption Standard”. As stated in the guide of AES “The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.”

As the Artemis financial has to keep their user information secure, this cipher will help them to keep the data safe from all the security attacks. After reviewing the code manually, we need to focus more on securing user input as it is the basic and far most important thing. We also need to have secure client and server relationship in order to protect our companies policies. This cipher is used in the form of ciphertext and decode the data back to its original shape. The ciphertext secure the information of our clients from getting leaked or stolen.

I found out that “A cryptographic hash function is a mathematical function used in cryptography. Typical hash functions take inputs of variable lengths to return outputs of a fixed length. A cryptographic hash function combines the message-passing capabilities of hash functions with security properties”(Frankenfield, 2020). There are few differences between symmetric and non-symmetric keys. The Symmetric-key algorithms use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. Whereas the non-symmetric keys encrypts and decrypts the data using two separate yet mathematically connected cryptographic keys. These keys are known as a 'Public Key' and a 'Private Key. Now the non-symmetric or asymmetric is used and is considered more secure.

## 2. Certificate Generation

CA is used for security as it creates the website trusted. According to digicert.com, “Partnering with a Certificate Authority (CA) allows system integrators, managed service providers, IT consultants, hosting providers, and others to expand their business by offering data security in addition to their products and services”. It has  Same or higher level of security compared to public-key authentication.

This is what I am getting

Text

Description automatically generated

## 3. Deploy Cipher

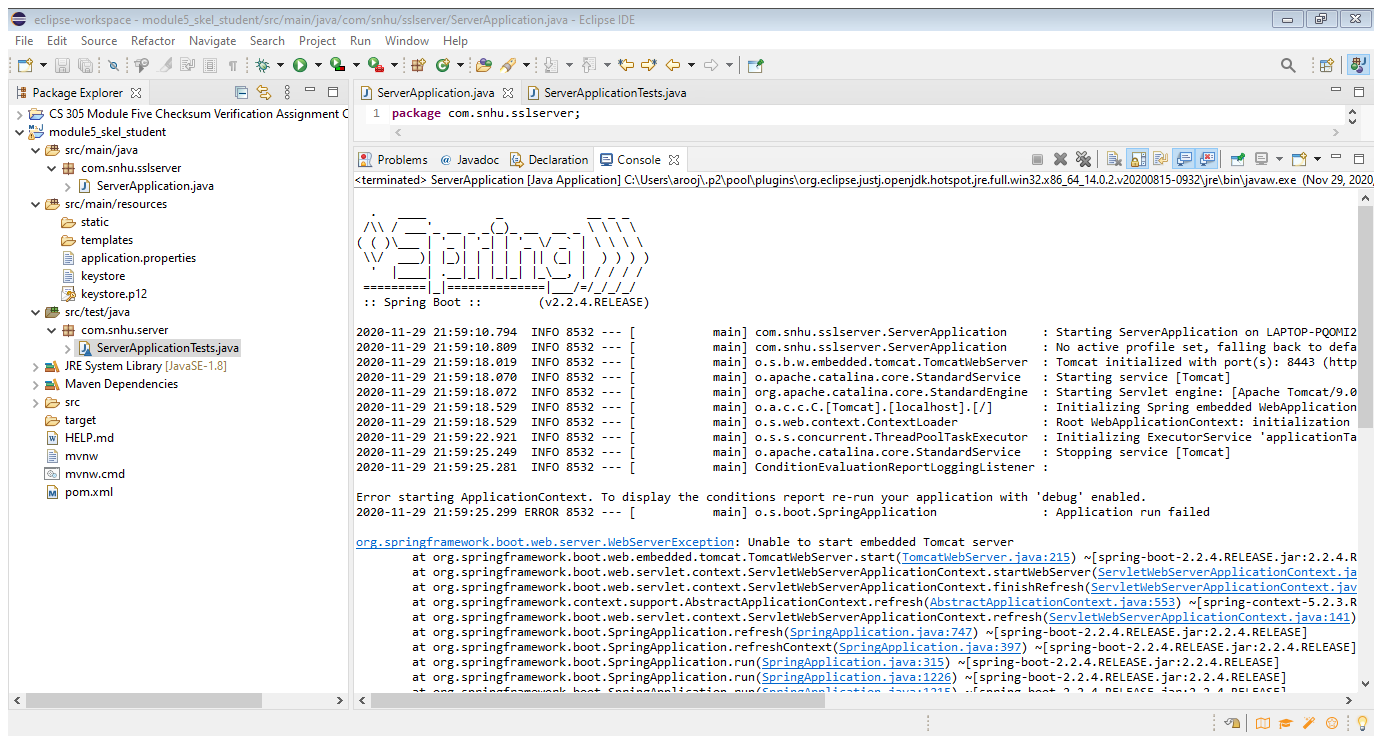
## Text Description automatically generated

## 4. Secure Communications

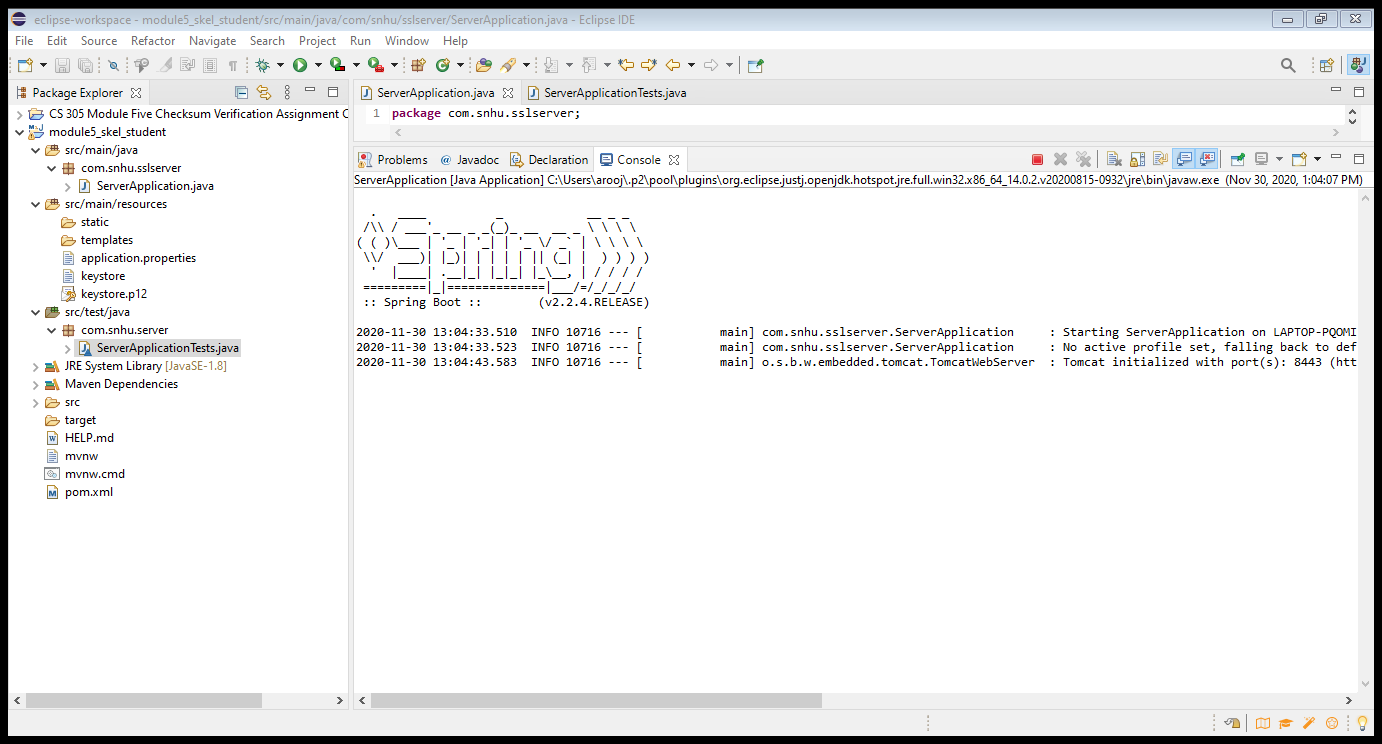
Graphical user interface, application, Word

Description automatically generated

## 5. Secondary Testing



## 6. Functional Testing



## eclipse-workspace - rest-service/pom.xml - Eclipse IDE

## 7. Summary

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext.

Citation:

Frankenfield, Jake. “Cryptographic Hash Functions Definition.” *Investopedia*, Investopedia, 28 Aug. 2020, www.investopedia.com/news/cryptographic-hash-functions/.