****

# 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** | **12/8/2022** | **Glenn Lehman** |  |

## 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

Glenn Lehman

## Algorithm Cipher

At the highest level an algorithm cipher is applied to a single value or the content of a file to proctect the information from unintended disclosure. Thes aglorithm are designed based on mathematatical calculation derived from the study of complexity theory. In the US the National Institute of Standards and Technology (NIST) is the offical source for AES (Advanced Encryption Standards) and SHA (Secure Hash Algorithm) (Dworkin, 2022). These ciphers are frequently denoted by short code like AES-256, SHA-1, or SHA-256 to name a few. SHA-256 is recommended as a sufficent standard fro this project and will adequatly balance security and performance.

A cipher algorythim a hash function internally. This function is responsible for converting the input into a cipher string of a specific length. Each hash function has a bit level, for example SHA-256 has a bit level of 256. This number reduces the likelyhood of a collision between two different data elements being hashed to . Todate no colloission has been found when using SHA-256.

Another factor in ciphers are random numbers. There happen to be two types of random number gernerators: Pseudo-random number generators (PRNGs) and true random number generators (TRNGs). A PRNG produces a number by using a seed value the same seed number will always produce the same seed. These random nubers are used inside of hash function to prevent the reverse engineering of a hashed vlue.

Encryption algorthims hace improved over time. With the advent of computers it became easier to attack an algorthim with brute force. This would allow codes to be broken. Many standards from the late 20th century can be broken by a standard laptop computer today. As such ciphers are increasing in complexity. It is expected that once we enter the age of quantium computing the SHA-256 standrd will be quickly broken.

## Certificate Generation

Insert a screenshot below of the CER file.

[Insert screenshots here.]

## Deploy Cipher

Insert a screenshot below of the checksum verification.

[Insert screenshots here.]

## Secure Communications

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

[Insert screenshots here.]

## Secondary Testing

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

[Insert screenshots here.]

## Functional Testing

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

[Insert screenshots here.]

## Summary

[Insert text.]

## Industry Standard Best Practices

[Insert text.]

Reference

Dworkin, M. , Barker, E. , Nechvatal, J. , Foti, J. , Bassham, L. , Roback, E. and Dray, J. (2001), Advanced Encryption Standard (AES), Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.FIPS.197 (Accessed December 8, 2022)