****

# 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 5](#_Toc102040759)

[3. Deploy Cipher 6](#_Toc102040760)

[4. Secure Communications 6](#_Toc102040761)

[5. Secondary Testing 7](#_Toc102040762)

[6. Functional Testing 7](#_Toc102040763)

[7. Summary 8](#_Toc102040764)

[8. Industry Standard Best Practices 8](#_Toc102040765)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **12/06/2022** | **Jad Alrehaoui** | **Project 2 submission** |

## 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

Jad Alrehaoui

## Algorithm Cipher

As per IBM, a cipher algorithm is a mathematical formula designed specifically to obscure the value and content of data. Most of these cipher algorithms use a key to encrypt the data and either the same key or another complementary key is needed to decrypt the data back to the original form.

Hash functions are functions used to map the data according to the hash values which are used to index a fixed size table called hash table. Those tables are arbitrary sized to fixed sized values and also help to categories the data into the fixed size index in the table.

Bit level of the cipher refers to the cipher technique to be used according to the needs and requirement such as 128 bit encryption/cipher or 256. The higher the bit level, the higher the security level and the higher the processing power needed.

The basic difference between symmetric and asymmetric encryption is that symmetric encryption uses one key for encrypting and decrypting the data. Asymmetric encryption on the other hand uses a public key for encryption and a private key for decryption.

The use of random number in cryptography is needed in the key generation process to create a random yet strong key as well as for other cryptographic purposes such as initialization vectors and nonces.

Cryptography was used by ancient Spartans who used a leather strap wrapped around a wooden rod. The letters on the leather are meaningless when unwrapped, and the message makes sense only if the recipient has the correctly sized rod.

The Romans, invented a substitution cypher that shifts characters by three places, meaning A becomes D, B becomes E etc. A simple and effective encoding method at that time.

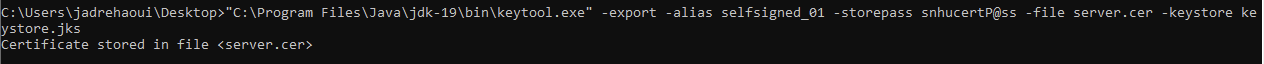
In the World War 2, a machine called enigma was invented which uses a key on a daily basis to encrypt the communication between intelligence services.

In the modern day, our lives rely on encryption as we rely on online services a lot. Now we use cryptocurrencies, governments uses cryptocurrencies to protect internal communications.

As more and more services move to the cloud and even objects (Internet of Things) communicate, encrypting data in transit and at rest is crucial. Cryptographers are continually developing and refining solutions to this challenge.

## Certificate Generation

## Text Description automatically generated



## Deploy Cipher

Text

Description automatically generated

## Secure Communications

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

Graphical user interface, text, application

Description automatically generatedGraphical user interface, text, application, email

Description automatically generated

Text, letter

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

## Secondary Testing

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

Graphical user interface, text, application, email

Description automatically generated

## Functional Testing

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

Text

Description automatically generated

## Summary

Following the Vulnerability Assessment Process Flow, I downloaded the sslServerApplication project, and added a controller to handle a Rest API to GET from /hash route. I implemented the SHA-512/224 as it is one of the most secure algorithms with the least number of collisions. It is highly recommended that this cipher be used.

## Industry Standard Best Practices

We would recommend daily check-ups which include a mixture of server updates, bug fixes and dependency checks. If we are to make any changes we need to run the dependency check and mitigate the contingencies before deploying to production.

This will reduce the risk of cyber attacks and protect the data held in the system and being communicated through the web server we are building. We always need to refer to the Vulnerability Assessment Process flow while adding features and fixing bugs so that we do not oversee any vulnerability and keep the system safe.

Thank you for reading !

**References:**

IBM (2021, March 08). Cipher algorithms and keys. IBM <https://www.ibm.com/docs/en/ztpf/1.1.0.15?topic=concepts-cipher-algorithms-keys>

Cyware Social (2019, November 30), Exploring the Differences Between Symmetric and Asymmetric Encryption, Cyware Hacker News

<https://cyware.com/news/exploring-the-differences-between-symmetric-and-asymmetric-encryption-8de86e8a>

Peter Smirnoff & Ulrich Scholten (2019, April 23) The Role of Random Number Generators in Relation to HSMs & Key Management. Cryptomathic.

<https://www.cryptomathic.com/news-events/blog/the-role-of-random-number-generators-in-relation-to-hsms-key-management#:~:text=The%20role%20of%20RNGs%20in,as%20initialization%20vectors%20and%20nonces>.

Thales Group(2022, November 21) A brief history of encryption. Thalesgroup

<https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption>