****

# 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** | **2/18/2023** | **Tristin Watson** | **Project Two** |

## Client



## Developer

Tristin Watson

## Algorithm Cipher

The algorithm that I chose is the MD2 Message-Digest algorithm. The MD2 Message-Digest algorithm is a padding algorithm which adds a 16-byte checksum at the end of a message. This checksum can avoid collisions. Without the 16-byte checksum, a collision can occur from the same hash generating the same text. The basic steps go append bytes, append checksum, initialize message, process message in 16-byte blocks, output. The code creates an instance of the MD2 algorithm by referencing the algorithm in an instance. Next, a byte array is created using the specified algorithm instance and the data’s bytes. The bytes array is then converted into a signum representation and creates a string hashText referenced from that signum. Lastly, the hashText is made into 32 bit by adding enough “0” strings to make 32.

## Certificate Generation

Certificate Form:

Text

Description automatically generated

I made a new certificate called sslserver.jks with an alias of sslserver but I forgot to take a screenshot of it after I made it. This is the screenshot of the previous certificate I made in week 5, but it shows the process to get a certificate.

Server.cer File:

Text

Description automatically generated

This is the updated server.cer file that I made on the 19th in week 7.

## Deploy Cipher



## Secure Communications



Says not secure but it is opened on an https with localhost:8443. I am not quite sure how to fix this issue.

## Secondary Testing

Text

Description automatically generated

Graphical user interface, text

Description automatically generated with medium confidence

## Functional Testing

Graphical user interface, text, website

Description automatically generated

## Summary

## The areas of security addressed in the refactored code are cryptography, client/server, code errors.

## Cryptography was addressed in the form of a cipher algorithm called MD2 Message Digest. Client/server security was addressed by creating a secure keystore certificate. The certificate allows for the use of https secure browsers. Lastly, code errors were handled when checking whether the specified cryptographic algorithm existed during the generation of it. Layers of security are a must have for a secure server. There are seven main layers of security and only three were covered to a decent degree, which leaves plenty of room for improvement. The layers of security covered already help secure the webpage well and help keep those with malicious intentions at bay.

## Industry Standard Best Practices

To ensure the security of the application, industry standard best practices are a must. An example of best practices used in the refactored code is a try/catch statement to help catch errors but still properly run the code. Try/catch statements help notice errors is a timely manner and keep programs from crashing. Secure coding goes hand in hand with industry best practices. Ensuring that a company has functioning and readable code for their engineers to work with is a must. The easiest way to perform this action is by following standard practices to a T, while also following secure coding practices. This means making sure all inputs a validated, all errors are handled properly, and code quality is at its peak.

Server Details:

Text

Description automatically generated

Code Editions:

Text

Description automatically generated

**Resources**

Kaliski, B. (1992, April 1). *The MD2 message-digest algorithm*. RFC Editor. Retrieved February 5, 2023, from <https://www.rfc-editor.org/rfc/rfc1319>

technopedia. (n.d.). *What is message digest 2 (MD2)? - definition from Techopedia*. Techopedia.com. Retrieved February 5, 2023, from <https://www.techopedia.com/definition/31699/message-digest-2-md2#:~:text=The%20process%20of%20the%20Message,and%20finally%20producing%20the%20output>.