****

# 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** | **12/10/2022** | **Joan Estepan** |  |

## Client



## 

## Developer

Joan Estepan

## Algorithm Cipher

My client, Financial Artemis, needs to encrypt its archive files to ensure that its data is safe and secure by avoiding interceptions and eavesdropping. The algorithm cipher I recommend for this task is the algorithm AES or Advanced Encryption Standard. This algorithm is a 128- bit block cipher and it supports keys of 128, 192, and 256 bits. This type of encryption is used by the United States as the standard encryption algorithm, it is very efficient in all its forms, and it is known to be invulnerable to every type of attack except for brute force attacks. Brute force attacks are an exhaustive process and not very efficient at all, even though the encryption might be vulnerable to this type of attack the chance of success in the attack are extremely low and its efficiency at preventing every other type of attack make it the best option. There are also no regulations in the USA preventing the use of the AES algorithm.

Even though AES is widely considered the best cipher algorithm by many people, and it is the standard in most places, there are some instances where it might not be the best choice. AES is perfect for securing data at rest, such as databases, hard drives, etc. However, if we would like to send some data directly across the world to another country and have it encrypted end-to-end, we would use another encryption algorithm such as RSA which is way more effective at protecting data across geographical borders than AES. However, even though it is more effective for the job at hand, it does come with the downside that it is not as effective as AES when it comes to preventing attacks. The cipher functions used by AES are SHA-256 and SHA-384 and it supports keys of 128, 192, and 256 bits.

In the early 1970s the company IBM and their “crypto group”, created the first block cipher to protect the data of their customers known as DES, later on, the United States adopted this as the national standard to encrypt data until 1997. However, technology was not as big as it currently is and encryption was not as widespread. In the early 2000’s AES was created later on replacing the DES as the national standard and later on the Elliptic-curve cryptography was created as well. Fast-forward to the present, in this era of big data, encryption has become crucial to protect sensitive data from malicious hands.

## Certificate Generation

Insert a screenshot below of the CER file.

![Text

Description automatically generated]()![Text

Description automatically generated]()

## Deploy Cipher

![Graphical user interface, text, application

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

**![Text

Description automatically generated]()**

## Summary

The code for our client, Financial Artemis, complies with industry security testing protocols. The areas of security addressed from the Vulnerability Assessment Process Flow Diagram were, cryptography, client/server, code error and code quality. These assessments ensure that the code is safe and secure.

## Industry Standard Best Practices

In order to add layers of security to the code, we added a hash algorithm to encrypt the information in the code, the hashing algorithm used was SHA-256 which is the industry safest hashing algorithm to date, and it is used by the big companies and organizations all over the world. We also generated a certificate to stablish a secure connection between the browser and the server. It is extremely important to keep the company’s security up to industry’s standards to ensure that the company will be safe from any malicious attacks.