****

# Practices for Secure Software Report

**Table of Contents**

[**Document Revision History 3**](#_heading=h.30j0zll)

[**Client 3**](#_heading=h.1fob9te)

[**Instructions 3**](#_heading=h.3znysh7)

[**Developer 4**](#_heading=h.2et92p0)

[**1. Algorithm Cipher 4**](#_heading=h.tyjcwt)

[**2. Certificate Generation 4**](#_heading=h.3dy6vkm)

[**3. Deploy Cipher 4**](#_heading=h.1t3h5sf)

[**4. Secure Communications 4**](#_heading=h.4d34og8)

[**5. Secondary Testing 4**](#_heading=h.2s8eyo1)

[**6. Functional Testing 4**](#_heading=h.17dp8vu)

[**7. Summary 4**](#_heading=h.3rdcrjn)

[**8. Industry Standard Best Practices 4**](#_heading=h.26in1rg)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **2/25/2024** | **Jesenia Roberts** | **Project Two Reflection** |

## 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

Jesenia Roberts

## Algorithm Cipher

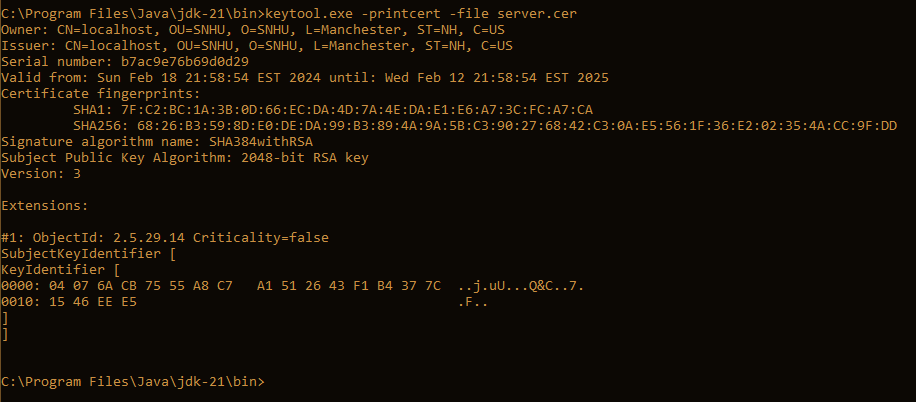
The algorithm cipher that would be best suited for Artemis Financial’s security is the Advanced Encryption Standard (AES). AES is verified in its security as the United States government uses AES to protect classified information due to its secure nature and fast performance. It uses a 128-bit block cipher which encrypts data into blocks of 128 bits each (Geeksforgeeks, 2021). The key length can range from 128 to 256-bit keys whereas DES only had a 56-bit key. The higher the bit key level, the more possible combinations there are, thereby the more secure the data (Bernstein & Cobb, 2021).

The National Institute of Standards and Technology (NIST) developed AES when it was announced to the public that DES had become vulnerable to attacks as a result of technological advancements (Bernstein & Cobb). AES was published on November 26, 2001, and has been a reliable source of encryption since (Computer Security Division, 2016).

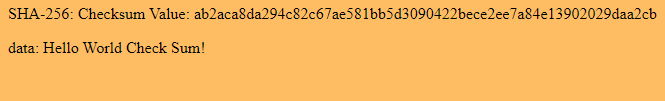
AES uses symmetric encryption, meaning that the same key uses the same secret key for both the encryption and decryption process (Das, 2023), whereas the opposite is true about asymmetric encryption. Asymmetric algorithms such as the Rivest–Shamir–Adleman algorithm (RSA) have a greater level of security than symmetric encryption like AES, but performance suffers as a result. Depending on the size of the archive files, this could mean that the archiving process could take a significant amount of resources when utilizing a method like RSA. Additionally, symmetric encryption is better suited for internal transfer whereas asymmetric encryption is more valuable for external transfers (Everything You Need to Know about AES-256 Encryption, n.d.).

The Gramm-Leach-Bliley Act (GLBA) requires that financial services ensure confidentiality, protect against unauthorized access, and protect against threats (Probasco, 2017). When used correctly and with a variety of other security measures in place as well, AES can contribute to meeting these federal standards. The “best” cipher is subjective depending on the security needs and resource tools, however, AES is a globally used encryption method that, while not the most secure method available, is overall the best fit for Artemis Financials.

## Certificate Generation



## Deploy Cipher



## Secure Communications



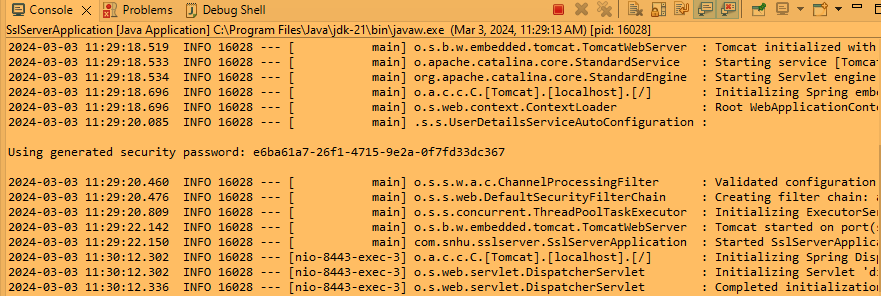
## Secondary Testing

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.



## Summary

The main areas of security that I have affected by refactoring the code were cryptography and client/server. The use of the cipher offers secure cryptography and the various generated certificates and secure protocols allow for more secure communication between client and server.

## Industry Standard Best Practices

## 

## The industry standard for cipher was used with SHA-256 as ciphers that use less than 256 bits are not recommended for use. The use of HTTPS for secure interactions is another example of best industry practices, as well as the generation of checksum certificates. By following these practices, it assures that there are multiple verified forms of security offered to the user when they are using the software.

## Resources

Bernstein, C., & Cobb, M. (2021, September). What is the Advanced Encryption Standard (AES)? Definition from SearchSecurity. SearchSecurity. <https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard>

Computer Security Division, I. T. L. (2016, December 29). AES Development - Cryptographic Standards and Guidelines | CSRC | CSRC. CSRC | NIST. https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-deve

lopment#:~:text=The%20Advanced%20Encryption%20Standard%20(AES

Das, D. (2023, October 10). Difference Between AES and SHA256. Medium. https://diptendud.medium.com/difference-between-aes-and-sha256-706d6b2eb2ef

Everything You Need to Know About AES-256 Encryption. (n.d.). Kiteworks | Your Private Content Network. https://www.kiteworks.com/risk-compliance-glossary/aes-256-encryption/#:~:text=Since%20AES%20is%20a%20symmetric

Geeksforgeeks. (2021, October 15). Advanced Encryption Standard (AES). GeeksforGeeks. https://www.geeksforgeeks.org/advanced-encryption-standard-aes/

Outlaw, M. (2021). How AES Encryption Works. In YouTube. https://www.youtube.com/watch?v=A8poO23ujxA

Probasco, L. (2017, April 25). Encryption Requirements for Banks & Financial Services. Townsendsecurity.com. https://info.townsendsecurity.com/encryption-requirements-for-banks-financial-services