Elliot Huh

CS-305

Project 2

Secure Software Report

**Algorithm Cipher**

Encryption algorithm ciphers are systems that convert regular text known as plain text into a different text known as cipher text. This process is known as encrypting. Also, the system can do the reverse, which is a process known as decrypting. This is down to increase security, It can help block out unauthorized access and help prevent interceptions and data leaks.

Hash functions can be utilized by ciphers. They essentially grab plain text and then turn them into a fixed length hashed text which was determined by the bit level. No matter how long the plain text is the hash text will always be the same bit level length. Generally speaking the longer or higher the bit level the stronger the encryption will be due to the increase in potential possible encryptions. This entire process is known as hashing which is different than encryption. Encryptions will process plain text differently.

Random numbers is where all numbers usually exclusively single digits have a equal chance of being chosen and are picked out at random. This creates an unpredictable outcome that can be used within ciphers and greatly strengthen them. Symmetric Keys refers to ciphers where encryptions and decryptions have the same key. Both the sender and receiver will have the same key when accessing the cipher. Asymmetric keys refers to a scenario where there are two separate keys in a cipher. One is public and can be accessed by many but can only encrypt data. The other is private and only specific people can access it which can decrypt the data.

Ciphers has been used all throughout history. Although during the older days ciphers were simpler and primitive. Ciphers became more structured and effective during the medieval times. Modern cryptography seemed to have generally started around the early 20th century around World War 1. Ciphers were much more prevalent and we see the first encryption system machines being invented such as the Enigma machine. Encryptions and ciphers remained in use throughout world war 2 and in 1975 the first block cipher was developed and used by the U.S government. As technology rapidly developed so did ciphers. Symmetric keys were first developed and then Asymmetric keys followed. Ciphers became more prevalent and more important with the introduction of the internet and advanced computers. Today they are used regularly and are a core part of computers today.

**Summary**

API: Spring boot was utilized. An TLS API is utilized and secures connections between the client and server. Hashing functions and Client Server area of security were implemented and focused which strengthen this area.

Cryptography: Hashing function was implemented. The SsServerController class was created and SHA-256 hashing algorithm was utilized. Hashing function was properly utilized and bytes to hex functions were implemented within this class.

Client/Server: Mapping function were created in the SsServerController class. Through spring boot by running SsServerApplication the server is created and specific content and access is needed to access the server so this prevents unauthorized access.

Code quality: Error handling, proper implementation uses of message digest are some of the examples of proper code quality. These inclusions bolster the effectiveness of other areas of security and were considered.

The basis and necessities of the base code were considered first. Asking questions like did the code run properly, what was needed and what information would be helpful were considered first. This then naturally led to clear requirements such as proper certification, The addition of the SsServerController class with its hashing function and the use of the OWASP dependency check tool. It was then a matter of how to implement them into the code and developing these requirements out.

**Industry Standard**

Industry standard can be seen within the code. There were comments helping identify what line does what and functions variables and classes were properly named to represent what they did and their role within the project. Lines were kept consistent and functions correctly corresponded with the right files or classes. The code was kept organized and easy to follow.

Its important to follow the industry standard to maintain core non-functional requirements and ensure the effectiveness of the code moving forward. Due to the nature of this company and the state of the code and the quality of it will have a large impact. By following industry standard cooperative efforts are greatly improved and everything is kept organized clean and easy to follow. This in turn makes the code more maintainable. By making it more maintainable it then helps non-functional requirements like scalability, usability, performance, security etc.

**Screenshots**

Certificate generation

A screenshot of a computer

Description automatically generated

Deploy Cipher

A screenshot of a computer

Description automatically generated

Secure Communication A screenshot of a computer

Description automatically generated

Secondary TestingA screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

Functional Test

**A screenshot of a computer

Description automatically generated**

**Sources**

Crane, C. (2021, January 25). *What is a hash function in cryptography? A beginner’s guide*. Hashed Out by The SSL StoreTM. https://www.thesslstore.com/blog/what-is-a-hash-function-in-cryptography-a-beginners-guide/

Schneider, J. (2024, January 5). *A brief history of cryptography: Sending secret messages throughout time*. IBM Blog. https://www.ibm.com/blog/cryptography-history/#

José, L. (2023, February 14). *Symmetric encryption vs asymmetric encryption: How it works and why it’s used*. Device Authority Ltd. https://www.deviceauthority.com/blog/symmetric-encryption-vs-asymmetric-encryption/#:~:text=Symmetric%20encryption%20uses%20the%20same,data%20can%20be%20easily%20decrypted.