Written Assignment 4-2: Algorithm Ciphers

Dhiraj Gurung

Southern New Hampshire University

CS305

Wayne Morris

March 26, 2025

**Algorithm Ciphers**

The algorithm cipher that I would recommend using would be the Advanced Encryption Standard (AES) because it provides a high level of security during data transmission, and it is an industry-standard. The AES encryption works by sending data between two users but preventing access between the two users until the correct key is used to decrypt the data. The data remains encrypted until a key is used to decrypt it. When designing a system to defend against various types of security attacks we must be weary of data falling into the wrong hands. AES encryption utilizes a symmetric encryption algorithm that ensures the data “can't be understood by anyone who does not possess the secret key to decrypt it” (Cryptomathic, 2020). This means that the hackers would need the original key to access the data being transferred from one device to another. While the key does help prevent unauthorized access to data, it is also one of the weak points of AES encryption as without proper key management software there can be key leaks. These leaks can allow hackers to piece together the security key and access data that they shouldn’t be allowed to. However, this is an issue that can be mitigated by using key hierarchies to prevent master keys from being unnecessarily used and using good key management software to ensure that the keys are being managed securely to prevent data leaks. There are privacy and confidentiality laws in place to protect customer privacy and using data encryption software for sensitive information would help the company abide by these laws. While the best cipher is a subjective matter AES-256 bit is widely regarded as one of the best encryption algorithms for enterprise-level applications. However, compared to a lower-bit cipher like AES-128 bit it is slower. The higher-bit cipher will be more secure but at the cost of performance speeds. In situations where speed is more important than security developers might choose to go with a lower-bit encryption method, particularly when they are handling large amounts of data.

The purpose of a cipher’s hash function is two-fold one is to ensure data integrity and also identity verification (Crane, 2024). Data integrity means making sure the data is kept secure and away from hackers, or other unwanted users. The different bit levels of an encryption algorithm denote the size of the key. AES-128 uses a 128-bit encryption key and AES-256 uses a 256-bit encryption key. The rule of thumb is that the higher the bit count the more secure the encryption because you need more resources to hack a 256-bit encryption through brute force methods. AES uses a symmetric key which means that the same key is used for both the encryption and decryption, whereas an asymmetric algorithm would use two separate keys. The purpose of having keys is to control access of data and prevent unauthorized access. The first standardized cipher used was called DES and it later evolved to what’s now known as 3DES which are all generally not recommended for use. This is mainly due to new technological innovations and the speed and processing power of modern computers being more powerful than they used to be. Currently, the AES encryption standard is the most commonly used and is considered more secure than 3DES.

**Citations:**

Crane, C. (2024, November 5). *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/#:~:text=Hash%20functions%20are%20a%20way,a%20means%20of%20identity%20verification.

Cryptomathic. (2024, December 5). *Symmetric Key Encryption: Uses in banking explained*. Symmetric Key Encryption: Uses in Banking Explained. https://www.cryptomathic.com/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking#:~:text=crypto%2Dagile%20infrastructure.-,AES,in%20U.S.%20FIPS%20PUB%20197.

*Java Security Standard Algorithm Names*. Oracle. (n.d.). https://docs.oracle.com/javase/9/docs/specs/security/standard-names.html#cipher-algorithm-names

Manico, J., & Detlefsen, A. (2015). *Iron-Clad Java: Building Secure Web Applications*. McGraw Hill Education.