4-2 Assignment: Algorithm Ciphers

SNHU

CS-305

Nicholle Caudy

After reviewing Artemis Financials’ needs and what they hope to accomplish, the algorithm cipher I believe would be best is the AES or Advanced Encryption Standard which was established by the NIST back in 2001 and is also used by the U.S. Government for encrypting classified information. AES is used to secure data at rest and in transit. Specifically, the AES-256 algorithm cipher is used for banking and is considered the most secure. This is because of the 256-bit symmetric-key encryption that protects sensitive information and makes it extremely difficult to hack.

The hash function converts the input data into a fixed-length string of bits compressing the value. The bit level is used to determine the length of the encryption, working together these functions keep secure information protected and make it harder to be infiltrated. Using the random number function will create an unpredictable sequence of random numbers making it more difficult for an intruder to guess or figure out the keys for the encryptions and decryptions. Symmetric key encryption uses the same key to encrypt and decrypt the data in transit or at rest. Asymmetric keys, typically used for signing, have two separate keys. One key is to be kept secret and only known by the sender and the other is the public key and can be known by anyone. Keysets are also useful because you can manage the use of several different keyset types (symmetric and asymmetric keys) in your application. The beginning of modern cryptography started in the early 1970s with the Data Encryption Standard or DES until it was cracked in 1997. AES was approved in 2002 and became effective as a U.S. federal government standard. Encryption algorithms are still in use and even more so in today’s world with more and more information being transferred to the cloud and over the internet. The technology field is always looking for better, safer, faster, and more secure ways to protect people’s information whether in transit or being stored in a database.

Reference

* Lake, J. (2023, September 29). *Common Encryption types explained: A guide to protocols and algorithms*. Comparitech. Retrieved March 28, 2024, from <https://www.comparitech.com/blog/information-security/encryption-types-explained/#:~:text=Currently%2C%20the%20gold%20standards%20for%20secure%20yet%20still,symmetric-key%20encryption%202%20RSA-4096%20%E2%80%94%20For%20public-key%20encryption>
* Detlefsen, J., & Kenan, K. (2014). *Iron-Clad Java: Building Secure Web Applications* (pp. chapters 6 and 8). McGraw Hill Computing. <https://learning.oreilly.com/library/view/iron-clad-java/9780071835886/ch01.html>
* Thales (2023, February 1). *A Brief History of Encryption (and Cryptography)*. Retrieved March 30, 2024, from <https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption>