Artemis Financial Algorithm Cipher Review

Encryption has been used since far before the invention of computers. It has evolved from methods involving wrapping leather around varied rod sizes in 600 BC to the first cypher with an encryption key in 1553 AD to the modern Advanced Encryption Standard (AES) developed at the turn of the 20th century (A Brief History of Encryption (And Cryptography), 2023). As technology develops so do methods of cracking encryptions, so there is inevitably going to continue to be advancements in encryption methods well into the future.

In the case of Artemis Financial, I recommend using AES with a 256-bit key as the cipher algorithm for encrypting files. AES came to be after the National Institute of Standards and Technology, or NIST, set out to create a new standard for encryption in 1997. The goal was for protection of government and commercial data. It was not until the end of 2001 when the standard was finally published. This was around the time that computers were becoming more and more able to recover keys from a previous standard, Data Encryption Standard (DES). Although some agencies tried improving DES by increasing the number of encryption keys, this was not an efficient solution because it caused encryption to consume about triple the time that encryption with a single key took (Smid, 2021).

AES uses symmetric encryption, meaning the key used to encrypt the data is used to decrypt as well. Conversely, in asymmetric cryptography, two keys are used. One key is known only by the sender (a private key), while the other one can be used by anyone (a public key). The sender’s private key signs the data, and then the public key validates the signature created by the private key (Manico & Detlefsen, 2015). Both types of encryptions have benefits and downsides. While symmetric encryptions are typically much faster than asymmetric, they are unable to validate data’s authenticity the way asymmetric algorithms do (Arampatzis, 2023). In the case of this application, I believe it is an appropriate risk to sacrifice some security for speed because AES is inherently difficult to crack when implemented without error.

For AES, this key can be 128, 192, or 256 bits. While a larger key may lead to more secure encryption, it is not always the best choice. The larger the key, the more resources it will take to perform the encryption/decryption cycle. That said, in the case of Artemis Financial, I still recommended the 256-bit key because the modern computer makes handling a larger key much more manageable than it has in the past. AES uses multiple rounds of encryption (depending on the key length) to make data extremely safe. 128-bit, 192-bit, and 256-bit keys undergo 10, 12, and 14 rounds of encryption, respectively. While a DES key can be recovered in just over 6 minutes, it can take up to 36 quadrillion years for a 128-bit AES key to be recovered (Rimkiene, 2022).

# References

*A Brief History of Encryption (And Cryptography)*. (2023, June 10). Retrieved September 22, 2023, from Thales: https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption

Arampatzis, A. (2023, July 25). *When Should You Use Symmetric vs. Asymmetric Encryption*. Retrieved from Venafi: https://venafi.com/blog/what-are-best-use-cases-symmetric-vs-asymmetric-encryption/

Manico, J., & Detlefsen, A. (2015). Chapter 6: Protecting Sensitive Data. In *Iron-Clad Java.* McGraw-Hill Education.

Rimkiene, R. (2022, 08 29). *What is AES encryption and how does it work?* Retrieved 09 21, 2023, from Cybernews: https://cybernews.com/resources/what-is-aes-encryption/

Smid, M. E. (2021, August 23). Development of the Advanced Encryption Standard. *Journal of Research of the National Institute of Standards and Technology, 126*, 1-18.