Julianne Takaya

CS-305 Software Security

3/29/2025

Artemis Financial handles many users sensitive and confidential financial and personal information, and so they have a duty to ensure that the information they possess is kept confidential. Encrypting the data in the archives is a good way to begin upholding that duty. At the writing of this report, the standard encryption is AES, or Advanced Encryption Standard. The AES algorithm is a symmetric block cypher that can encrypt or decrypt data (National Institue of Standards and Technology, 2023).

A symmetric algorithm refers to an encryption algorithm with only one secret key that encrypts and decrypts the data. The opposite of a symmetric, or secret key algorithm is an asymmetric, or public key algorithm. Public key algorithms are used to sign and validate data. The public key can also be used to encrypt data, which can be decrypted by the private key (Manico & Detlefsen, 2015). A block cypher is a cypher that encrypts blocks or chunks of data at a time. AES was developed by the NIST in 2001 and is widely used today (Geeks for Geeks, 2025).

AES operates in three different key sizes, 128, 192, and 256 bits. AES encrypts input data in blocks of 128 bits and outputs 128 bits of encrypted cypher text. Contrary to a Hash algorithm, which takes a large amount of data and outputs a small sized output. In cryptographic applications, hash functions are used to create secure hash algorithms, such as SHA-256 (Geeks for Geeks, 2025).

For these reasons, I recommend Artemis Financial use the AES algorithm to encrypt their archives as it is secure, fast, and, as the current standard, is widely used.

# References

Geeks for Geeks. (2025, February 3). *Advanced Encyrption Standard (AES)*. Retrieved from Geeks for Geeks: https://www.geeksforgeeks.org/advanced-encryption-standard-aes/

Geeks for Geeks. (2025, March 10). *Hash Functions and Types of Hash Functions*. Retrieved from Geeks for Geeks: https://www.geeksforgeeks.org/hash-functions-and-list-types-of-hash-functions/

Manico, J., & Detlefsen, A. (2015). *Iron-Clad Java.* McGraw-Hill Education.

National Institue of Standards and Technology. (2023). *Advanced Encryption Standard (AES).* Gaithersburg, MD: Department of Commerce. Retrieved from https://doi.org/10.6028/NIST.FIPS.197-upd1