Artemis Financial is seeking to encrypt their archive files in the long term. This means that we need to implement the best practices of the CIA triad (Confidentiality, Integrity, Availability) combined with system efficiency (optimize performance). The most appropriate algorithm cipher to use in this case is Advanced Encryption Standard (AES). AES is a symmetric key block cipher, standardized by NIST and generally regarded as the gold standard for secure encryption; with its high-complexity, 256-bit keys, and no known weaknesses (Portnox, 2025), it is a great choice for Artemis Financial. While AES itself is considered most secure and widely used, there are certain risk factors associated with its use—not due to shortcomings with AES, but from improper implementation and weak key management. In consideration of government regulations, the Gramm-Leach-Bliley Act requires institutions that offer financial products to their customers explain their information sharing practices and safeguard sensitive data(Nguyen, 2025). Article 32 of The General Data Protection Regulation (GDPR) requires the controller and processor of personal data to have appropriate security controls in place to prevent said data from being compromised; while this is an EU standard, it applies to US businesses that may do business internationally (EU, 2016).

This cipher is being used in order to secure store long-term archive files for Artemis Financial—More on justification for this in the following section. When reviewing which ciphers to use, there are *technically* more secure ciphers, for example Post-Quantum Cryptography, which utilizes quantum computing to go to new lengths when it comes to security. However, PQC has not yet been standardized by NIST, tested and implemented in a wide variety of systems, and has huge computational costs associated (Computer Security Division, 2025). For the purposes Artemis Financial seeks, as well as considering current options, AES is the best option moving forward.

AES is the best option for Artemis Financial in this situation. AES offers up to a 256-bit key size and multiple rounds of encryption which makes it resistant to brute-force attacks and helps maintain confidentiality. Hash functions such as SHA-256 are used for integrity verification and authenticity. By using higher-bit algorithms, we are making the keys more complex and therefore more secure. In this instance, we are utilizing the symmetric key AES, which is much better suited for data storage. AES can encrypt large files quickly with low computational power, while asymmetric keys are computationally expensive, *especially* with large data stores. In regard to RNG or random number generation, RNG is extremely important in ensuring that our cipher is secure. RNG allows us to generate keys that are unpredictable and cryptographically random. RNGs are also responsible for Initialization vectors and salting hashes, which further help verify that data integrity and confidentiality are secure (Barker & Kelsey, 2015).

The history of encryption can date back to ancient times (simple transposition cipher, the Caesar cipher) through medieval times as well, but did not see leaps and bounds until the beginning of WWI. The first rotor machines used for cryptography were developed, and during WWII the enigma machine was cracked by allied codebreakers (Schneider, 2024). Modern day cryptography is generally noted as beginning in 1977 with DES, followed by 3DES in and AES in 2001. Post-Quantum Cryptography is the emerging field which many believe will be refined and streamlined enough for application soon (Chen & Scholl, 2022).

**References:**

Barker, E., & Kelsey, J. (2015, June 24). *Recommendation for random number generation using deterministic random bit generators*. CSRC. https://csrc.nist.gov/pubs/sp/800/90/a/r1/final

Chen, L., & Scholl, M. (2022, May 26). *The cornerstone of cybersecurity – Cryptographic Standards and a 50-year evolution | nccoe*. NIST - National Cybersecurity Center of Excellence. https://www.nccoe.nist.gov/news-insights/cornerstone-cybersecurity-cryptographic-standards-and-50-year-evolution

Computer Security Division, I. T. L. (2025). *Post-quantum cryptography: CSRC*. CSRC. https://csrc.nist.gov/projects/post-quantum-cryptography

EU. (2016, August 30). *Art. 32 GDPR – security of processing*. General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-32-gdpr/

Nguyen, S. T. (2025, February 6). *Gramm-Leach-Bliley Act*. Federal Trade Commission. https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

Portnox. (2025). *What is Advanced Encryption Standard (AES)?* https://www.portnox.com/cybersecurity-101/what-is-advanced-encryption-standard-aes/#:~:text=AES%20is%20the%20gold%20standard,importance%20in%20protecting%20sensitive%20data.

Schneider, J. (2024, November 25). *The history of Cryptography*. IBM. https://www.ibm.com/think/topics/cryptography-history