**CS 305 Module Four Written Assignment**

Upon reviewing the algorithmic encryption ciphers for Artemis Financial, my best recommendation is that of the Advanced Encryption Standard (AES). AES is the most robust and popular algorithm cipher of today, it is actively employed for professional implementation both by financial institutions and the government. The AES was classified as the best encryption standard set forth and established by the National Institute of Standards and Technology (NIST) (GeeksforGeeks, 2023), it is also employed by the National Security Agency. Therefore, I highly recommend this encryption standard for Artemis Financial that deals with private financial information for high level clients and thus requires extremely robust encryption measures.

**Security Best Practices:** AES is recognized for its resilient security features, even that of quantum decryption. It is highly effective towards thwarting attacks from brute-force attacks and is adopted as the most widely used encryption standard to date. It has withstood constant scrutiny from cryptographers and serves as a reliable choice for Artemis Financial in terms of its protection strength.

**Risk assessment:** While no encryption standard is without risks, the AES is still the most reliable and has been known to withstand any deciphering technique against it. When factoring it its relative strength against other encryption standards like the DES and triple DES (GeeksforGeeks, 2023), it still outperforms other strong standards. This makes it the obvious choice for a financial institution like Artemis Financial when considering the risk with which standard to implement.

**Compliance and Regulation:** The AES cipher is approved by the Federal Information Processing Standard (Dray, 2021), making it an obvious choice for government approved encryption standards. This will allow any company that uses this standard like Artemis Financial to be within governmental regulations and legal standards when implementing cryptographic technology.

**Usage and implementation:** When employing the AES into Artemis Financials system, the encryption technology can be implemented by encrypting hardware and software, as well as file systems that may hold sensitive customer information. AES has a vast amount of usecases but some include “Wireless security, Database encryption, Secure communication, Data storage, Virtual Private Networks, Secure Storage of Passwords, and File and Disk Encryption (GeekforGeeks, 2023)”. It may also be applied to any platforms where the user interacts with or inputs sensitive information like a username, password, or other sensitive financial information for their account.

I recommend AES due to its versatile implementation across various organizations while adhering to governmental standards and regulations. The availability of 128-, 192-, and 256-bit encryption options adds to its versatility. However, it's essential to note some drawbacks, such as multiple rounds of encryption and potential challenges in software implementation, which may impact application performance.

**Justification:** The AES employs what’s called a substitution-permutation network (SPN) structure that utilizes hash functions that creates a complicated cipher of the plaintext. There are various bit levels to choose from including 128-, 192-, and 256-bit encryption, which is in this way purely a show of strength.

The AES is a symmetric key algorithm, meaning the same key is used for both encryption and decryption (GeekforGeeks, 2023). AES uses random numbers in generating secure keys as well through the multiple rounds of encryptions it calculates. It’s especially useful for extremely large quantities of data so can be especially beneficial for archived file encryption.

Regarding the history and current state of AES, it was established by the National Institute of Technology (NIST) in 2001, effectively replacing the antiquated Data Encryption Standard (DES) by its vastly outperforming measures under quantitative testing by cryptologists (GeekforGeeks, 2023). Its widespread use throughout multiple businesses and government organizations demonstrates its adaptability and performance for advanced encryption measures, making it the perfect choice for Artemis Financial to ensure its sensitive client and financial information can remain secure.

Dray, M. J. D. E. B. B. J. R. N. J. F. L. E. B. E. R. J. F., Jr. (2021, March 1). *Advanced Encryption Standard (AES) | NIST*. NIST. https://www.nist.gov/publications/advanced-encryption-standard-aes

GeeksforGeeks. (2023, May 22). *Advanced Encryption Standard AES*. <https://www.geeksforgeeks.org/advanced-encryption-standard-aes/>

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