Alex Surprenant

CS 305

11/27/2024

Algorithm Ciphers

Given the electronic data transfer nature of Artemis Financials’ platform, I would recommend the Advanced Encryption Standard(AES) as the encryption method of choice. This cipher was designed with the intention of encryption and decryption of electronic data using keys from lengths of 128, 192 and 256 bits, while encrypting and decrypting in 128 bit blocks. This cipher is intended for use in both federal, as well as non-federal private organizations, which would be perfect for a private banking system

In order to defend from a large variety of security attacks, many layers of defense against such attacks are necessary. Practices that should be in place include multifactor authentication, strong user input sanitization and password protection. In order to defend from a well-rounded variety of security attacks, many layers of data protection must be used. The Advanced Encryption Standard provides reevaluation by NIST every five years to make sure the technology behind the algorithm remains up to date and useful.

Though the AES is a well backed solution, there are potential risks. Implementation of the code can introduce human error into the system. Code must always be reviewed by piers to make sure that solid code is being written. The cipher also relies on keys that are possessed by the sending and receiving end of the system. If these keys are mis-managed, this can lead to potentially compromised data.

In implementing this cipher, regulations from the federal export controls must be considered. Usage of cryptographic modules must comply with the Bureau of Export Administration of the U.S. Department of Commerce. Specific controls are laid out under the Export Control section of the AES document. Through using this cipher and the security it provides, I believe this would supply Artemis financial with the best cipher solution.