Matthew Muller

**Module Four Algorithm Ciphers Assignment**

Due to the sensitive nature of the information in Artemis Financial’s long-term archive files, it is extremely important that they be properly encrypted in order to prevent data breaches. Because of this, I believe that the company should deploy the Advanced Encryption Standard (AES) encryption algorithm cipher. AES is a symmetric block cipher developed by the U.S. government that can be implemented using cryptographic keys of 128, 192, or 256 bits. All three of these options will provide the system with security against brute force attacks, as the time required to try all possible key combinations would be too great for even extremely powerful computers. Therefore, it may not be necessary to choose the most secure cipher (the 256-bit) as it will require much more processing power and take longer to execute. Since this is a symmetric cipher, the same key is used for both encrypting and decrypting the data. This is one of the risks of my recommendation because it means that both the sender and the receiver must know the key, which could lead to vulnerabilities if the key is not properly protected. However, this can be guarded against by taking precautions such as implementing multi-factor authentication and deploying firewalls and antimalware software (Bernstein).

AES uses AES-hash, a secure hash function that takes a string input of an arbitrary amount of bits and returns a fixed bit length string as output. This process ensures that each input will provide a unique output as finding two files which hash to the same value should require on average approximately 2^128 operations (Cohen). AES was developed by the National Institute of Standards and Technology (NIST) starting in 1997. This came after it announced that there was a need for an alternative to the currently used Data Encryption Standard (DES) because it was starting to become vulnerable to brute-force attacks. AES was designed to provide effective encryption well into the 21st century in a manner that is easy to implement in hardware and software. It was created with voluntary free use programs that provide encryption services but any nongovernmental organizations that use AES are subject to limitations created by U.S. export control (Bernstein).

**References**

Bernstein, C., &amp; Cobb, M. (2021, September 24). Advanced Encryption Standard (AES).

TechTarget. Retrieved June 5, 2022, from https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard

Cohen, B. (n.d.). AES-hash - csrc.nist.rip. Retrieved June 6, 2022, from

https://csrc.nist.rip/groups/ST/toolkit/BCM/documents/proposedmodes/aes-hash/aeshash.pdf