Michael Martin

5/29/22

CS 305

SNHU

Algorithm Ciphers

Given that Artemis Financial needs to encrypt archival data, which is data that will not be accessed often, I recommend the AES algorithm for encrypting their archival data, specifically the 256 bit cipher. This algorithm has yet to be cracked, as the weakest link would be considered the key. This is because the key is typically user chosen and can vary in length. Using the algorithm will protect from most types of attacks, such as man in the middle or brute force attempts. A man in the middle attack will only see the encrypted data, while a brute force attack would take 2.29\*10^32 years to crack the key. The only attack that may have an effect on the data is a ransomware attack that encrypts data, which offsite backups would nullify.

While 128 bit AES has not been cracked, I chose to recommend 256 bit due to

the data not being actively used. For archival data the read and write speeds are not typically the priority. In this instance, security is the top priority, and the AES algorithm with the 256 bit cipher provides the best security without using multiple algorithms. AES uses a symmetric cipher, which means that the encryption and decryption keys are the same. This algorithm is used by government agencies to encrypt active and archival data, as well as communications. This has been the standard for the US Government since May 26th, 2002.

*FIPS 197, Advanced Encryption Standard (AES) - CSRC*. (n.d.). Retrieved May 29, 2022, from https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf

Tobias, E. (2021, February 15). *128 or 256 bit encryption: Which should I use?* Ubiq. Retrieved May 29, 2022, from https://www.ubiqsecurity.com/128bit-or-256bit-encryption-which-to-use/

Wikimedia Foundation. (2022, May 17). *Advanced encryption standard*. Wikipedia. Retrieved May 29, 2022, from https://en.wikipedia.org/wiki/Advanced\_Encryption\_Standard