**Brandon Hobbs**

**CS-305**

**5-27-2022**

**Module 4: Short Paper**

Artemis’ data at rest needs to be protected. As I have conjectured before the data being of financial in original makes for a larger target. To secure the data I would suggest an AES128 encryption utilizing the CTR mode. However, because AES is a symmetric encryption technique the keys need to be secured. RSA should be employed to protect the keys.

I would choose this scheme because as Franklin (2021) says, “...the bulk of the data…is encrypted by the speedy AES algorithm. To get the secret key required to decrypt that data…[the] sender then uses that public key and RSA to encrypt and transmit to each recipient their own secret AES key…”.

This scheme has the advantage of protecting the most vulnerable part of AES with a more rigid encryption mechanism but without subjecting users to the slower performance of RSA.

Moreover, I would choose 128-bit AES strength utilizing the CTR method. CTR has, according to Baeldung (2021), the advantage of being able to parallelize encryption and decryption. If there are large volumes of encrypted data, this would aid user satisfaction. CTR is preferred over the older DES and 3DES. ECB should not be used for any data larger then 128 bits due to the repeating patterns becoming obvious.

128-bit AES is suggested over 256-bits for similar performant reasons. “128 bit key is enough security for most of every use case with the exception of quantum computer protection. Also using 128 bit encrypts faster than 256 bit and the key-schedule for 128 bit keys seems to be better protected against related-key attacks (however this is irrelevant to most real-world uses)” (Baeldung, 2021).

If, at some point, the encrypted data needs to be transmitted then CTR may be swapped for the GCM method. GCM is more complex to implement but signs the data with a hash so that any manipulation, e.g., bit flipping, becomes evident.

Any chosen encryption method, or the choice to not use any, may bring liability. Some countries have different laws pertaining to the use or non-use of data encryption. Within the United States even differing states may have different opinions. For example, California state (California Consumer Privacy Act of 2018) makes any company not taking “reasonable security procedures” liable to consumer lawsuits. The European Banking Authority regulation states that minimum security requirements must be put in place by financial institutions that ensure “secure, end-to-end encryption” (Crane, 2016). Outside legal representation should be sought to ensure compliance within any operating region.

Baeldung. (2021, Nov. 14). *Java AES encryption and decryption.* <https://www.baeldung.com/java-aes-encryption-decryption>

Crane, C. (2019, June 28). *10 data privacy and encryption laws every business needs to know.* TheSSLStore. https://www.thesslstore.com/blog/10-data-privacy-and-encryption-laws-every-business-needs-to-know/

Franklin, R. (2021, Mar. 13). *AES vs. RSA encryption: what are the differences?* Precisely. <https://www.precisely.com/blog/data-security/aes-vs-rsa-encryption-differences>

Townsend, P. (2019, Mar 25). *RSA vs AES encryption - a primer*. TownsendSecurity. <https://info.townsendsecurity.com/rsa-vs-aes-encryption-a-primer>