Abdulrahman Al-Nachar

CS305 / 4-2

After reviewing the different ciphering options we have and considering Artemis Financial's needs I believe the best ciphering method to implement for Artemis Financial’s project would be the AES algorithm cipher, AES complex ciphering and encryption process will protect data from being accessed by unwanted actors, However, even with AES, we should still apply other security methods to protect against injection attacks and data leaks. We have to make sure that AES’s key is protected and isn’t shared with any unauthorized actor, because if someone has access to the key they can access protected data, AES will help us comply with government regulations like the Federal Information Processing Standards FIPS140 for using cryptography that is certified by FIPS for file encryption and Gramm-Leach-Bliley Act that requires to protect by encryption all data that is held or transmitted thru a financial institution, AES will be used to encrypt archives and customer information and all data held or transmitted thru Artemis Financial’s program, AES is the best cipher for its strong encryption of using 128 to 256 block sizes and keys to cipher the data, and AES is used by multiple government institutions and financial institutions nationwide for its security and compliance with different regulations, there are several reasons why some would not choose the best cipher technology some don’t because the intended program they have is small, some because of the costs , but for this project it’s imperative that Artemis Financial has the best cipher used in its program.

Hash Functions takes data input and puts it in a set-sized string, Hash works in conjunction with AES and is used mainly to ensure data isn’t changed in storage or when transmitted by comparing the original computed hash to it.

AES has three different lengths for bits like 128, and 256, AES protocol has a unique key, 128 bits or 256 bits is the length of the encryption key so the larger it is the harder it is for hackers to crack.

Random numbers and characters in encryption are used to avoid showing a pattern that hackers can use to figure out the underlying calculations used to encrypt. In general, it makes it harder for hackers to find the key. Symmetric keys are one key that is used for both data encryption and decryption, and asymmetrical keys are two keys: one is only used for encryption, and one private key is used for decryption.

Ciphering and Encryption have come a long way over the centuries. In the past, people used to cipher their letters so no one could understand the letter’s contents but the intended recipient. Ciphering is now mostly digital and, on the computer, since everything is being done and stored on computers.