Matthew Trembley

1/30/2022

Southern New Hampshire University

CS-305

After reviewing some of the Java Security Standard Algorithms, I’ve decided the most useful one to Artemis Financial will be AES, or Advanced Encryption Standard. The AES standard uses either a 128, 192, or 256 bit keys. This standard has not identified any weak or semi-weak keys, therefore would do a fantastic job for Artemis Financial and securing their information. There is no regulation in the U.S., but as AES is considered a standard it must be followed correctly.   
 The longer the key, the stronger it becomes as a result – like any real passcode. Because AES uses 128, 192, or 256 bit keys, the potential for uncrackable keys is incredibly real. The best way to enact this standard is by use of hashing. The increased bit levels of the cipher and the hash function work together to make a practically impenetrable, secure key that will not allow any feasible attempt to crack. The use of random numbers makes each key unique, and the fact that AES uses a symmetric key means that the same key is used for encryption and decryption.

Historically, encryption has been used widely since World War II. More now than ever, it runs through almost every software to maintain safe and secure connections. AES is currently used by the United States government as it has proven to be effective and secure.