CS-305-T1168 Software Security

Module Four Assignment

Eric Wallace

Sep. 23, 2022

The best algorithm to use in this situation is the Advanced Encryption Standard (AES). It is the most widely used encryption method for securely encrypting data and securing data connections. The National Institute of Standards and Technology (NIST) assisted with the creation of the algorithm which was created for the government. Despite it being 20 years old this year, to date, no cryptanalytic attacks have been successful at breaking the encryption. The only successful attacks have come from incorrect implementations of the algorithm.

AES is a symmetric block cipher consisting of 3 key lengths, 128, 192 and 256. It can encrypt all three levels of government classifications. While Confidential and Secret levels can be encrypted with all three lengths of AES, highly classified requires either AES-192 or AES-256 (Advanced Encryption Standard: AES Encryption Algorithm Guide, 2022) (Advanced Encryption Standard: AES Encryption Algorithm Guide, 2022). All of this means that this algorithm is perfectly capable of encrypting any data needing transmitted by Artemis Financial.

AES executes computation processes the 128-bit plaintext structure as 16 bytes and arranging them into 4x4 matrices. It uses a variable number of rounds which is dependent on the length of the key. The encryption process is conducted in a series of round which involves sub-steps, shifting rows and mixing columns.

Since the algorithm is the stand used by the government and most widely known there are no reasons as to why I would not use this algorithm for the Artemis Financial project. Even though there are attacks out there such as side-a-channel, brute-force, and the man-in-the-middle, the only proven vulnerability is the failure to follow standard guidelines and practices.

AES was created because the then standard cipher used by the government was the Data Encryption Standard (DES) was found to be insecure. The government had been using it since 1977 but in 1999 the government started looking for a more secure method of encrypting data. The process took 5 years and was a very stringent process (Villanueva, 2022). During the selection process the National Security Agency (NSA) experts performed tests and discussion to find vulnerabilities and weaknesses. The criteria tested during the process included speed, versatility, and computation, but the most influential criteria were how the algorithm stood up against attacks. While other algorithms were good, they did not meet the governments requirements of not only being impenetrable, but it has to be fast, versatile and reliable. The only algorithm that fit those requirements was AES which was declared a Federal Information Processing Standard (FIPS) by NIST in 2001.

Stated above, AES is a symmetric block cipher, a block cipher is an algorithm that encrypts data on a per-block basis (Advanced Encryption Standard: AES Encryption Algorithm Guide, 2022). Symmetric key encryption uses a single key for both ends of the connection and Asymmetric uses two keys, one for each end. Given that AES does not currently suffer from the most advanced attacks its use in the future is almost guaranteed.

# Bibliography

*Advanced Encryption Standard: AES Encryption Algorithm Guide*. (2022, August 7). Retrieved from Software Testing Help: https://www.softwaretestinghelp.com/aes-encryption-algorithm/

Villanueva, J. C. (2022, Aug 25). *What Is AES Encryption And How Does It Work?* Retrieved from JSCAPE: https://www.jscape.com/blog/aes-encryption