CS 305 Software Security  
Algorithm Ciphers

Sergio Mateos

Southern New Hampshire University

Algorithm Ciphers

Artemis Financial want to encrypt their customer personal information with the best practices and prevent any leaking of information in a long term. As a developer and security expert, my job is to advise on the best and most secure cipher encrypt that will meet the Artemis Financial goal. In my research based on the Java Security Standard and Algorithm Names, I decide to select Advanced Encryption Standard (AES). AES, also known as Rijndael, was developed by Joan Demean and Vicent Rijmen, two Belgian cryptographers. The way that AES work is by linking mathematical operations using a block cipher algorithm. The AES converts input to output of the same size, which in other words could be described as encryption and It will require a secret key to decrypt.

Artemis Financial web application will handle a lot of sensible information about their customers and the implementation of AES will prevent the leaking of information in the long term. Malicious user has problems trying to decrypt AES, since it has large key sizes, from 128-, 192-, or 256-bits keys. Also, AES can be applied to hardware and software.

In June 2003, the US Government announced that AES would be adapted into their system to classified information. The stipulation was "The design and strength of all key lengths of the AES algorithm (i.e., 128, 192, and 256) are sufficient to protect classify information up to the SECRET level. TOP SECRET information will require the use of either the 192 or 256 key lengths." The implementation of AES will adjust and modify the efficiency of exporting process.

AES has proved to be the best cipher algorithm that companies, businesses, government agencies, and users can implement for their security issues. AES has proven to be complicated, if not impossible, for malicious users to decrypt and have access to that information. AES is one of the most used cipher algorithms for many companies like Google, Amazon, Pfizer, etc. Understanding that companies are getting hacked and leak information, they decide to implement the best security for this type of issue.

On the other hand, AES is an incredible cipher algorithm, but it has its problems, the first issue is that hard to implement with software, which means that it takes more time and effort to add into the system. Even is the best cipher algorithm, the encrypting process used a simple algebraic structure that it is broke it its is easy to decrypt. And every block is encrypted in the same way, so if a malicious user is capable to decrypted one box, all the boxes can be decrypted.

Considering both sides of the AES, the result will maintain the same since it will be the best choice for the cipher algorithm based on Artemis Financials’ criteria and goals.

Reference

*Java Security Standard Algorithm Names*. Java security standard algorithm names. (n.d.). Retrieved January 24, 2023, from https://docs.oracle.com/javase/9/docs/specs/security/standard-names.html#cipher-algorithm-names

*Use the U.S. Government approved algorithm for storing classified information*. Use the U.S. government approved algorithm for storing classified information. (n.d.). Retrieved January 24, 2023, from https://www.east-tec.com/kb/safebit/protecting-your-confidential-information/what-is-the-aes-standard/#:~:text=The%20Advanced%20Encryption%20Standard%20%28AES%29%2C%20also%20known%20as,standard%20for%20commercial%20transactions%20in%20the%20private%20sector.

Corporation, T. A. E. S. (2020, July 29). *AES ranked among the top US Companies for Innovators*. AES Ranked Among the Top US Companies for Innovators. Retrieved January 24, 2023, from https://www.prnewswire.com/news-releases/aes-ranked-among-the-top-us-companies-for-innovators-301102212.html

Advantages of AES | disadvantages of AES. (n.d.). Retrieved January 24, 2023, from https://www.rfwireless-world.com/Terminology/Advantages-and-disadvantages-of-AES.html#:~:text=Following%20are%20the%20disadvantages%20of%20AES%3A%20%E2%9E%A8It%20uses,the%20same%20way.%20%E2%9E%A8Hard%20to%20implement%20with%20software.