Alexandria Marbury

Professor Foultz

Project 2

AES would likely be the best algorithm cipher for Artemis financial. This is the most secure algorithm. The reason that this would be the best algorithm cipher is because this is a financial company. Many time financial institutes require user to give their social security and this information could ruin its customer’s lives if it were exposed. This cipher is a great choice regarding the United States’ regulation on data security. This algorithm cipher will be used to encrypt and decrypt customer data. This will keep hackers from stealing valuable information. I chose the most secure cipher in this case because Artemis will be holding information that could destroy people’s lives if it is exposed. This requires high level security that will be as impenetrable as possible. Otherwise, a hacking for this company could result in mistrust and lead to a loss of business.

The purpose of AES’s hash functions is to create secure hashing. “AES uses a 128-, 192-, and 256-bit level to encrypt and decrypt messages” (Raul, A. et al, 2024). Random numbers make it harder for the hacker to discover the data held by an application. Symmetric and non-symmetric keys are different types of encryption methods. AES uses symmetric encryption. The key used to encrypt this data is required to decrypt it, therefore requiring the key to be shared (Poggi, 2021). Asymmetric encryption was created to resolve the issue of having to share the encryption key (Poggi, 2021). This therefore uses two keys to encrypt and decrypt (Poggi, 2021). Encryption can be traced back to “ancient Egypt, and Greek and Roman military culture” (Tresorit Team, 2022). They used encryption to preserve religious and military documents and information. Today it is used on the internet to secure data, or transactions (Tresorit Team, 2022).

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

By refactoring this code, I attempted to secure client/server, cryptography, and APIs. Throughout the process of enhancing this software application, I had to add a hash function, and an API. The hash function created cryptography. The API allowed for interaction with the customer, but a Certificate Authority had to be created to secure this creation. This allows for users to ensure that they are working with Artemis.

When trying to maintain the software application’s current security, I implemented data security enhancers such as a Certificate Authority and cryptography. This ensures that Artemis is secure regarding their data, which is a requirement in the United States. This also helps with trust between the company and its clients.

References

*Poggi, N. (2021, June 15). Types of Encryption: Symmetric or Asymmetric? RSA or AES? | Prey Blog. Preyproject.com.* <https://preyproject.com/blog/types-of-encryption-symmetric-or-asymmetric-rsa-or-aes#:~:text=Symmetric%20encryption%20involves%20using%20a>

*Tresorit Team. (2022, January 14). The history of encryption: the roots of modern-day cyber-security. Tresorit Blog.* <https://tresorit.com/blog/the-history-of-encryption-the-roots-of-modern-day-cyber-security/>

*Raul, A., Bernstein, C., & Cobb, M. (2024, February) What is the Advanced Encyption Standard (AES)? Definition from SearchSecurity. (n.d.). SearchSecurity. What is the Advanced Encryption Standard (AES)? Definition from SearchSecurity. (n.d.). SearchSecurity.* <https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard#:~:text=AES%20includes%20three%20block%20ciphers>