4-2: Algorithm Ciphers

Jason Kremhelmer

Southern New Hampshire University

CS 305: Software Security

Sarah North

3/31/2024

# Algorithm Ciphers

After reviewing the needs of Artemis Financial as well as the system, I have come to the conclusion the ideal encryption cipher would be the Advanced Encryption Standard (AES). In my research, I have found the AES is most commonly used for banking and is a 256-bit encryption. AES-256, is one of the best against hackers as even with quantum computing, the time it would take to brute force the system ifs more than a lifetime. “AES protects data from any third parties” (N-able, 2019). Some of the risks that have been taken into consideration are; making sure the system isn’t leaking information, making sure that access is secured in all forms, firewalls, etc. With security being one of, if not the top, priority choosing the most secure cipher only makes sense. As this is the most common cipher among financial institutions, it would seem that it is the way to go in this industry.

Creating hash functions is done so by taking the input value and converting it to a compressed value. This compressed value is known as the hash, or hash value. The length of the encryption is determined by the Bit levels, for instance, an encryption of 256 indicated there are 256 combinations within the encryption. Using a 256-Bit encryption along with a random number makes hacking into the system all but impossible.AES-256 uses Symmetric keys which are better for sending bulk data. "Because the algorithm behind symmetric encryption is less complex and executes faster, this is the preferred technique when transmitting data in bulk. The plaintext is encrypted using a key, and the same key is used at the receiving end to decrypt the received ciphertext. The host in the communication process would have received the key through external means” (Exploring the Differences Between Symmetric and Asymmetric Encryption, 2019). While doing my research It was interesting to learn how far back encryption actually goes. “**Circa 600 BC**: The ancient Spartans used a scytale device to send secret messages during battle. This device consists of a leather strap wrapped around a wooden rod. The letters on the leather strip are meaningless when unwrapped, and the message makes sense only if the recipient has the correctly sized rod.” (A BRIEF HISTORY OF ENCRYPTION (AND CRYPTOGRAPHY), (updated)2023) With the evolution of encryption, it has allowed us to continue protecting our valuable data.

# References

*A BRIEF HISTORY OF ENCRYPTION (AND CRYPTOGRAPHY)*. ((updated)2023, June 10). Retrieved from Thales: https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption

*Exploring the Differences Between Symmetric and Asymmetric Encryption*. (2019, November 30). Retrieved from Cyware Social: https://cyware.com/news/exploring-the-differences-between-symmetric-and-asymmetric-encryption-8de86e8a

N-able. (2019, July 29). *Understanding AES 256 Encryption*. Retrieved from N-ABLE: https://www.n-able.com/blog/aes-256-encryption-algorithm