**4-2 Written Assignment: Algorithm Ciphers**

Winnie Kwong

Southern New Hampshire University

CS-305 Software Security

Professor Foultz

September 23rd, 2023

**Algorithm Cipher**

The best practice to defend against various security attacks would be using the Advanced Encryption Standard (AES) algorithm, also known as the Rijndael algorithm. According to Nagaraj, the most significant risks of AES are having “the same key is used for encryption and decryption, slow on low-end devices, and vulnerable to side-channel attacks,” (Nagaraj, 2022, para 13). Therefore, the biggest concern is that if keys are not done carefully, it can cause a cryptanalytic attack. The government, nongovernmental organizations, and the National Institute of Standards and Technology (NIST) widely recognized AES as the most secure option. Bernstein and Cobb states, “AES was created for the U.S. government with additional voluntary, free use in public or private, commercial or noncommercial programs that provide encryption services. However, nongovernmental organizations choosing to use AES are subject to limitations created by U.S. export control.” (Bernstein et Cobb, 2021, Para 4). AES is a symmetric block cipher that can encrypt keys using 128,192, and 256 bits to form a ciphertext. The algorithm cipher has a flexible key size that can expand using multiple rounds, including substitute bytes, to help prevent known attacks. AES would be the best cipher because of its option to choose between 128,192, or 256 bits, which is much more efficient than the original successor Data Encryption Standard (DES) algorithm, which only uses 56 bites. AES is known to be the most secure encryption used in government and military applications and business operations. However, even though the AES-256 bit is the best decision, Idera argues, “AES 256-bit encryption is harder to crack than AES 128-bit encryption, AES 128-bit encryption has never been cracked. Furthermore, it would take many, many years to cover all of the possibilities generated by 128-bit encryption, so it is not likely to be cracked in the near future,”.” (Aes-256-Bit-Encryption, n.d., para 3). Also, using 256 bits may take more processing power than some computers cannot handle.

**Justification**

Using hash functions will aid Artemis Financial because it helps improve authentication by being able to process large volumes of data while preventing attacks from hackers. Hash functions can transform given data sets into a bit string of fixed size. Investopedia says, “Cryptographic hash functions add security features to typical hash functions, making it more difficult to detect the contents of a message or information about recipients and senders.” (Frankenfield, 2023, para 4). The cipher’s hash function’s purpose is to ensure data integrity to ensure data has not been tampered with after it’s been signed. Random numbers generate keys, encrypt messages, and verify authenticity, which makes it ideal for generating passwords that meet security requirements and are a barrier to entry. With symmetric keys in a hash function, it uses a single cryptographic key for encryption and decryption that can convert data. In contrast, asymmetric keys must use two different keys (private and public) for encryption and decryption. Depending on one’s preference, symmetric is best for bulk encryption, whereas asymmetric is more secure because of its separate keys. According to Thales, encryption dates back to Circa 600 BC when the ancient Spartans used a scytale device to send secret messages during battle. (Thales, 2023, para 2). Spartans would use leather steps with letters on them, but the message could be read with the correct rod inserted. Modern data encryption has progressed, making it more suitable for communication security and the key to acquiring an advanced computer.

**References**

*Aes-256-bit-encryption*. (n.d.). IDERA. <https://www.idera.com/aes-256-bit-encryption/#:~:text=AES%20256%2Dbit%20encryption%20is>

Bernstein, C. et Cobb, M. (2021, September). *DEFINITION Advanced Encryption Standard (AES)*. TechTarget. <https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard#:~:text=The%20Advanced%20Encryption%20Standard%20(AES)%20is%20a%20symmetric%20block%20cipher,government%20to%20protect%20classified%20information>.

Frankenfield, J. (2023, August 19). *Cryptographic Hash Functions: Definition and Examples*. Investopedia. <https://www.investopedia.com/news/cryptographic-hash-functions/#:~:text=Cryptographic%20hash%20functions%20add%20security>

Nagaraj, K. (2023, March 7). *Advanced Encryption Standard (AES): A Secure and Efficient Symmetric Encryption Algorithm*. Medium. <https://infosecwriteups.com/advanced-encryption-standard-aes-a-secure-and-efficient-symmetric-encryption-algorithm-319eedb49905>

Thales Group. (223, June 10). *A brief history of encryption | Thales Group*. Www.thalesgroup.com. <https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption>