Philip Trinh

SNHU/ CS-305

03/25/2023

**Module Four Written Assignment Algorithm Cypher**

After reviewing the Artemis Financial requirements, considering that the client is in financial sector and managing many customers account information, the best security protection I would recommend is that they needed to upgrade their current system to include encryptions for all their customers and corporation data to avoid security breech and unauthorized access to these private information. The current best cypher algorithm in the world and has been used as a standard for government data protection since 2000 is known as Advanced Encryption System or AES. The AES uses symmetric algorithm, same key for encryption and decryption, and provides 128-bits block encryption, also support 192 and 256 bits. The 128-bits encryption has never been cracked. However, the strongest is AES 256-bit encryption but the downside is that it takes longer to execute and may slow the network down if processing demands are high. Therefore, I would recommend the client to use the 128-bit or 192-bits version to avoid this slowdown unless the system can handle the AES-256 bits without noticeable delay in network processing. “The AES algorithm uses a substitution-permutation, or SP network, with multiple rounds to produce ciphertext. The number of rounds depends on the key size being used. A 128-bit key size dictates ten rounds, a 192-bit key size dictates 12 rounds, and a 256-bit key size has 14 rounds. Each of these rounds requires a round key, but since only one key is input into the algorithm, this key needs to be expanded to get keys for each round, including round 0” (Anushed, sec 3). AES protected from straightforward, brute-force attacks. However, it has weakness with side-channel attack and related-key attack. A related attack is possible if the attack has some way of linking down the key and able to get through a poorly configure AES system. The side-channel attack work by the attacker attempt to pick up leaked information from the system and reduce the number of possible combinations required to attack AES with brute force. “Side-channel attacks involve collecting information about what a computing device does when it is performing cryptographic operations and using that information to reverse-engineer the device's cryptography system” (Corrinee, sec 8). Currently, all I can find in US is S.4051 - Lawful Access to Encrypted Data Act which “requires certain technology companies to ensure that they can decode encrypted information on their services and products in order to provide such information to law enforcement. It also establishes requirements and procedures for assisting law enforcement agencies in accessing encrypted data” (congress.gov). To meet this bill, the client needs to ensure that they have the key for the data encrypted written somewhere securely using another encryption perhaps in case the current key is missing or forgotten.

Hash Function is a function which is used to map the data according to the hash values which are used to index a fixed size table (Hash Table). Those tables are arbitrary size to fixed size values and help to convert it into a unique ciphertext of a specific length. Bits level refers to the length of the bit in the encryption, for example A 128-bit level of encryption has 2128 possible key combinations, 256-bits encryption has 2256 possible key combinations.

“Symmetric encryption, which uses the same secret key to encrypt and decrypt sensitive information, asymmetric encryption, also known as public-key cryptography or public-key encryption, uses mathematically linked public- and private-key pairs to encrypt and decrypt senders’ and recipients’ sensitive data” (Brit, sec 7). “A Random Number Generator (RNG), also called a Random Bit Generator (RBG), is needed in the key generation process to create a random (strong) key as well as for other cryptographic purposes such as initialization vectors and nonces. Typically, a True Random Number Generator (TRNG) provides a source of randomness or “entropy” to seed a Pseudo-Random Number Generation (PRNG), also called a Deterministic Random Bit Generator (DRBG). RNGs must be capable of generating random numbers at least as quickly as they are consumed” (Peter sec 1).

Some interesting history of cryptography I like is back in WW2 when the unbreakable Enigma code that changed setting everyday would be cracked by the Bombe Machine created by cryptographers Alen Turing. Related to IT cryptography going back to early 1970 when IBM formed a group to design cypher block to protect its customers’ data, the Data Encryption Standard (DES) was born. However, it was cracked in 1977. In the year 2000, the advanced encryption standard (AES) was born to replace DES. In 2005, elliptic-curve cryptography (ECC), an advanced public-key cryptography scheme that allows for shorter encryption key. ECC will be more commonly used in web applications since it is harder to break than RSA or Diffie-Hellman and uses less computing power to make it faster to access data. Currently WhatsApp, Signal, Telegram use ECC for their encryption protocols.

**REFERENCES**

Thales Group. (2016, April 18). A brief history of encryption | Thales Group.

Www.thalesgroup.com. <https://www.thalesgroup.com/en/markets/digital-identity-and->

security/magazine/brief-history-encryption

Scholten (guests), P. S. & U. (n.d.). The Role of Random Number

Generators in HSMs & Key Management. Www.cryptomathic.com. Retrieved March 27,

2023, from <https://www.cryptomathic.com/news-events/blog/the-role-of-random-number-generators-in-relation-to-hsms-key-management#:~:text=The%20role%20of%20RNGs%20in>

Hougen, A. (2021, May 24). What Is AES Encryption & How Does It Work in 2022?

[256-bit vs 128-bit]. Cloudwards. <https://www.cloudwards.net/what-is->

aes/#:~:text=The%20AES%20algorithm%20is%20the

Daniel, B. (2021, May 4). Symmetric vs. Asymmetric Encryption: What’s the Difference?

Www.trentonsystems.com. <https://www.trentonsystems.com/blog/symmetric-vs->

asymmetric-

encryption#:~:text=Unlike%20symmetric%20encryption%2C%20which%20uses

Anusheh, M. What is the AES algorithm? (n.d.). Retrieved 26 March, 2023

Educative: Interactive Courses for Software Developers.

<https://www.educative.io/answers/what-is-the-aes-algorithm>

Graham, L. (2020, June 23). S.4051 - 116th Congress (2019-2020): Lawful Access to Encrypted

Data Act. Www.congress.gov. <https://www.congress.gov/bill/116th-congress/senate->

bill/4051