Victor Feight

SNHU CS-305

Algorithm Ciphers

Encryption scenario: long-term archive files need encrypting.

Data security necessary: highest, since Artemis holds financial documents and records of the utmost important nature.

Chosen Algorithm: AES\_128

AES is commonly used for data at rest, which will be great for storage encryption, utilizing symmetric encryption.

Security practices against security attacks:

* Use a secure and trusted library and services for user authentication, using multi-factor authentication (password + key) and asymmetric cipher for key agreement
  + Use only POST requests to transmit authentication credentials, as per OWASP standards.
* Utilize symmetric algorithm for bulk encryption of archived files for fast speed.

According to OWASP, consider additional security requirements:

* + Principle of least privilege: disable default passwords and user accounts
  + Utilizing re-authentication
  + Enforce password complexity, and only send passwords over encrypted connection; prevent re-using passwords, and enforce password changes
  + Log authentication failures, and any unsuccessful logon attempts
  + Logging out should fully terminate session and connection
* Store data in a couple places in case of data loss.

Possible risks in algorithm:

Risks include implementation:

256-bit encryption is more difficult to brute-force or guess than a 128-bit key. However, a 128-bit key is still incredibly difficult to crack; since we are storing archived files over a network, latency is a concern, therefore 128 keys are chosen as they take less processing power. Ensure archived file protection is implemented securely.

Another risk includes encryption key security – even if properly implemented, the encryption keys still need to be stored and protected from hackers.

Current government regulations:

Gramm-Leach-Bliley Act – as a financial institution, there must be policies to protect user information from data breaches or threats in security. Using time-proven libraries and security standards in addition to AES for archiving and

Reasons not to choose the most secure cipher: Speed and resource usage (cpu, ram) would increase in proportion to the cipher bit levels. Asymmetric is going to be more secure but also slower, and should be used for authentication rather than storage of archives.

**Justification**: You have been asked to **provide a brief overview of the encryption algorithm cipher, its advantages, and its disadvantages to justify your reasoning to Artemis Financial**. Consider the following:

* What is the purpose of the hash functions and bit levels of the cipher?
* Explain the use of random numbers, symmetric vs non-symmetric keys, and so on.
* Describe the history and current state of encryption algorithms.

**Purpose of hash functions and bit levels:** Also known as a “compression function”, a hash function is a math function that converts an input value into another, more compressed output value of fixed length (Cryptography hash functions, 2021). Hash functions with n-bit outputs are called “n-bit hash functons”, for example 512-bit (Cryptography hash functions, 2021).

**Use of random numbers, symmetric vs non-symmetric keys**:

Asymmetric encryption uses two unique keys, a public and a private; the public encrypts data, the private decrypts it on the recipient’s end. When creating a key, a sequence of pseudo-random numbers are needed to generate the key. Symmetric encryption only uses one secret key, both sender and recipient having identical copies (allowing encryption of large amount of data).

**History:** Modern cryptographers emphasize a need to depend on secrecy of the keys; they mustn’t be revealed when comparing plaintext and ciphertext (Cryptography, 2021). Keys themselves can be encrypted; modern cryptography algorithms must be executed by computers and are based on mathematically challenging problems involving prime numbers usually (Cryptography, 2021). AES replaced DES as a standard, royalty-free algorithm approved by the US government.

Works Cited

What is GLBA compliance? Understanding the data protection requirements of the Gramm-Leach-Bliley act in 2019. (2019, July 15). Retrieved March 27, 2021, from <https://digitalguardian.com/blog/what-glba-compliance-understanding-data-protection-requirements-gramm-leach-bliley-act>

Cryptography defined/brief history. (n.d.). Retrieved March 27, 2021, from https://www.laits.utexas.edu/~anorman/BUS.FOR/course.mat/SSim/history.html

Cryptography hash functions. (n.d.). Retrieved March 27, 2021, from https://www.tutorialspoint.com/cryptography/cryptography\_hash\_functions.htm