Bryce Jensen
CS-305-H7005
4-2 Written Assignment: Algorithm Ciphers
11/16/2023

Algorithm Cipher:

After looking at the options in the Java Security Standard Algorithm Names (Oracle, 2017) page and doing some research on what the best practices are, I found that The AES seems to be the most widely used and accepted encryption standard. (Computer Security Resource Center (CSRC), 2023) I would recommend this for Artemis Financial's software security. One disadvantage to The AES is that it requires storage of its encryption keys. The biggest risk of using the AES algorithm is the mismanagement in storing the keys. Rotating and updating those keys seems to be the best way to maintain security of files. While I couldn't seem to find any regulations for the United States, it seems like the AES-256-bit encryption is trusted by the US government. Often referred to as "military grade" encryption, it seems to be the standard for high security applications. The AES algorithm will be used to encrypt and decrypt the data transferred and stored by Artemis Financial.

Justification:

What is the purpose of the cipher's hash functions and bit levels?

The AES uses various rounds of encryption based on the key length (14 rounds for a 256-bit level length) (Cryptoguiding, 2023). AES uses that key to generate round keys for the encryption process. One generated key for each of the 10 – 14 rounds.

Explain the use of random numbers, symmetric versus non-symmetric keys, and so on.

Random Numbers are used in a lot of types of cryptography. They can be used to generate keys and other parameters that need to be unique. The unpredictability of random numbers is used to ensure that patterns or predictability are not taken advantage of.

Bryce Jensen
CS-305-H7005
4-2 Written Assignment: Algorithm Ciphers
11/16/2023

Symmetric Keys are when the same key is used for both encryption and decryption. If this key is leaked or shared, the security of the encrypted data is compromised. They are quick and efficient and can be used for block data encryption. AES uses symmetrical keys for its process.

With non-symmetrical keys (asymmetrical keys), two keys have a mathematical relationship. The two keys are called the public key and the private key. The public key, as the name suggests, is shared publicly, where the private key is kept secret. Without the private key, the encrypted data cannot be accessed. This is used in RSA encryption methods. (Roeder, 2023)

Describe the history and current state of encryption algorithms.

AES was chosen as the encryption standard by NIST in 2001 after a public competition to select a replacement for the aging Data Encryption Standard (DES). According to AXEL Network, Symmetrical Key Algorithms like AES have become the most widely used and most secure form of encryption so far (AXEL Network, 2021). There are however advancements in quantum computing which would topple that method very quickly. The National Institute of Standards and Technology (NIST) has recently chosen four new methods that are “quantum resistant” (National Institute of Standards and Technology (NIST), 2022). However, the day quantum computers become common is the day quantum security methods will need to be developed.

Bryce Jensen
CS-305-H7005
4-2 Written Assignment: Algorithm Ciphers
11/16/2023

References

AXEL Network. (2021, May 28). *Encryption: The Past, Present, and Future*. Retrieved from axel.org: https://www.axel.org/2021/05/28/history-of-encryption/

Computer Security Resource Center (CSRC). (2023, May 8). *Cryptographic Standards and Guidelines*. Retrieved from csrc.nist.gov: https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development

Cryptoguiding. (2023). *Advantages of AES | disadvantages of AES (2023)* . Retrieved from cryptoguiding-com.ngontinh24.com: https://cryptoguiding-com.ngontinh24.com/article/advantages-of-aes-disadvantages-of-aes

National Institute of Standards and Technology (NIST). (2022, July 5). *NIST Announces First Four Quantum-Resistant Cryptographic Algorithms*. Retrieved from nist.gov: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

Oracle. (2017). *Java Security Standard Algorithm Names*. Retrieved from docs.oracle.com: https://docs.oracle.com/javase/9/docs/specs/security/standard-names.html#cipher-algorithm-names

Roeder, T. (2023). *Asymmetric-Key Cryptography*. Retrieved from cs.cornell.edu: https://www.cs.cornell.edu/courses/cs5430/2021fa/TL04.asymmetric.html