4-2 Algorithm Ciphers

SNHU

CS-305

1. Algorithm Cipher

* *Consider security protection best practices to defend against various types of security attacks.*

I believe that AES (Advances Encryption Standard) should be utilized by Artemis Financial to prevent a multitude of different types of security attacks. AES is currently the standard used by many large companies as well as small companies, the United States Government, and the United States Military. AES utilizes 128-bit, 196-bit, and 256-bit key combinations that are considered unbreakable by the U.S. Government and other entities. A brute force attack that is trying to break AES utilizing a 128-bit key would take 13.75 billion years with current computing abilities and this increases exponentially when using 196-bit and 256-bit keys (Kryptall Secure Communication Services, n.d.). This means all data being transmitted, stored, etc. is safe and cannot be accessed by unauthorized users or entities. This would be the ideal method for Artemis Financial to protect their financial information as well as users PII (personal identifiable information) and financial information.

* *Consider and identify all the risks in your recommendation.*

The biggest risk that the AES encryption algorithm has is key size. If a large enough key is not used, then the key may be vulnerable to being cracked. This can be prevented by using a key size that is impossible to crack with modern computing. These key sizes are 128-bit, 196-bit, and 256-bit. Utilizing these key sizes will render the key uncrackable. AES does use symmetric encryption. This means that the same key is used for both encryption and decryption and is known as a secret key (Manico & Detlefsen, 2014). This means that users or organizations that are sharing data, accessing data, or modification of data need to have this secret key. If the key were to become compromised (shared on an unsecure network) this would pose a huge security risk. The key may fall into a potentially bad actor’s hands allowing for the decryption of data. This is unlikely if the network is secured and maintained properly to protect the key.

* *Consider the most current government regulations and how they will be met.*

There are many Government regulations that apply to Financial Institutions such as Artemis Financial. The first of these regulations is the Gramm-Leach-Bliley Act (GLBA). “The Gramm-Leach-Bliley Act requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data” ((Gramm-Leach-Bliley Act, 2022b). Financial institutions must be transparent in how they transmit and safeguard the users’ sensitive and private information. This regulation can also be met by using AES block cipher and using a 128-bit key or higher. The next Government regulation that applies to Artemis Financial is the PCI DSS. “The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment” (PCI Compliance Guide, 2017). This standard will also be met by using the AES block cipher with a 128-bit key or higher to protect the users’ data and sensitive banking information such as credit cards, bank accounts, routing numbers, etc. while in transit or storage.

* *How will this algorithm cipher be used?*

The AES block cipher will be used to safely and securely send and receive files, documents, banking information, bank accounts or any other information needed by Artemis Financial to provide their services to the users. Both the sending and receiving side will have the required secure key to unencrypt the data on each end of the transmission. This will prevent any packet sniffers or intercept attacks. The information will be rendered unreadable even if it is intercepted because when using the proper bit key (128-bit or higher) the information is unbreakable with the current known computation methods.

* *What is the best cipher, and why?*

I personally believe that AES is the best cipher that is currently available for use. It is used by the U.S. Government, the financial industry, private companies (large and small) to protect sensitive information. With the use of a properly sized bit key and proper network security practices (so the key cannot be compromised) AES is considered unbreakable and is the best choice for Artemis Financial because of the sensitivity of the information Artemis Financial will be working with as well as the Government regulations regarding the financial industry.

* *What are the reasons why you might not choose the most secure cipher?*

One of the main reasons that we may not be able to choose the most secure cipher is the ability to be used on our systems. The larger the bit key the longer the process takes to encrypt and unencrypt the data and information. If the hardware is outdated, we may not be able to use the most secure cipher strictly because of system limitations. This means that a less secure cipher will need to be used and would be chosen based on a mix of security and usability on the current system we have in place.

1. Justification

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

The hash function takes raw data input of any size and produces a fixed-length enciphered text. Hash functions are used to ensure data integrity, verify digital signatures, and facilitating secure password storage (Mehta, 2020). An example of this is a password that has been stored using a hash value. Securing a plane text password for users would be unsecure. Once the password is created the hash value, not the plain text, is stored and the only way to replicate that hash value is to have the exact same input. If just one character is off a different hash value will be created and the password will not be accepted. Bit levels are used to describe the order of magnitude of the resources required to break the security (Staff, 2020). AES with a bit level of 256 would require a potential attacker to do computations to reverse engineer the cipher text into plain text (Staff, 2020). The main difference between hash functions and bit levels is that hash functions cannot be reverse engineered back into plain text and can only be replicated by inputting the exact same string whether that is one word or entire paragraphs. Bit levels can be unencrypted with the use of a secure key and are a way to transmit data securely.

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

The use of random numbers or random number generators (RNG) is needed in the key generation process to create secure and random keys (Scholten, n.d.). This ensures that the keys being used are truly random and cannot be simply guessed by potential attackers leaving information being stored or transmitted vulnerable. Symmetric keys use the same secure key (secret key) to encrypt and decrypt the data being transmitted or stored (Manico & Detlefsen, 2014). Non-symmetric keys on the other hand use public key cryptography. This is essential to the signing process. Non-symmetric or public key cryptography uses two different keys. The private key is known only to the sender and is kept private. This key is used to sign the data being transmitted. The public key is known by anyone and is used to validate the signature of the private key. There is no known way to obtain the private key from the public key currently with modern computing abilities (Manico & Detlefsen, 2014).

* *Describe the history and current state of encryption algorithms.*

The first known evidence of cryptography was found in an inscription from ancient Egypt and was believed to be transcribed around the year 1900 BC (*A Brief History of Cryptography*, 2023). This was not used to hide the message but was used to make the message appear more dignified. If we fast forward around 1800 years to the time of the roman empire and Julies Caesar forms of encryption were used to send secret messages across the battlefield to his generals with orders and directions. This and different forms of written cypher texts were used to secretly transmit information all the way until around the 19th century. This is when rotor machines such as the Herbern rotor machine and Enigma machines were used to transmit secret messages through radios. A specific key was needed to encrypt and decrypt the message (A Brief History of Cryptography, 2023). Modern day computer encryption was started in 1973 with a cipher called Lucifer and was created by IBM. The NIST (Nation Bureau of Standards) then put out a request for proposals for a national standard block cipher and would later adapt the Lucifer encryption method to DES (Data Encryption Standard) (A Brief History of Cryptography, 2023). DES was eventually broken because of the increase in computing power and the NIST once again put out a request for a new proposal. “It received 50 submissions. In 2000, it accepted Rijndael, and christened it as AES or the Advanced Encryption Standard. Today AES is a widely accepted standard used for symmetric encryption” (A Brief History of Cryptography, 2023).

**Citations**

*A Brief History of Cryptography*. (2023, January 12).

https://www.redhat.com/en/blog/brief-history-cryptography

*Gramm-Leach-Bliley Act*. (2022a, February 11). Federal Trade Commission.  https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

Kryptall Secure Communication Services. (n.d.). *How Safe is AES Encryption?* https://www.kryptall.com/index.php/information/how-safe-is-aes-encryption

Manico, J., & Detlefsen, A. (2014). *Iron-Clad Java: Building Secure Web Applications*. McGraw-Hill Education.

Mehta, M. (2020, December 4). *Hash Function in Cryptography: How Does It Work?* InfoSec Insights. https://sectigostore.com/blog/hash-function-in-cryptography-how-does-it-work/

PCI Compliance Guide. (2017, September 5). *PCI FAQs*. https://www.pcicomplianceguide.org/faq/

Scholten, U. S. P. &. (n.d.). *The Role of Random Number Generators in Relation to HSMs & Key Management*. https://www.cryptomathic.com/news-events/blog/the-role-of-random -number-generators-in-relation-to-hsms-key-management

Staff, W. (2020, June 6). *The Bit-Security of Cryptographic Primitives*. AWS Wickr. https://wickr.com/the-bit-security-of-cryptographic-primitives-2/