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

Christine R. Emerson

Department of Computer Science, Southern New Hampshire University

CS-305: Software Security

Dr. Alan Spencer

March 20, 2023

Advanced Encryption Standard (AES) 128 bits and above is the recommended algorithm cipher for Artemis Financials’ archive files. In, Why Is AES Encryption One of The Best Encryption Algorithms, they went over that, "AES is the strongest encryption available; it was selected by NIST as a Federal Information Processing Standard in November 2001 (FIPS-197). Further on, in June 2003, the U.S. Government (NSA) gave way to the AES as a standard to be used for all Top Secret and classified information protection” (2023). AES is a block cipher which means it encrypts data blocks instead of individual characters. As a result of this method, identical text receives a different encryption every time it is displayed. Those variances are an extra layer of protection against hackers who may somehow gain access to your data. Encryption and decryption of data are performed using symmetric keys in block ciphers. For the data to be packaged and viewed, the sender and recipient must share the same private encryption key. When the incorrect key is used, the information remains chaotic, with illogical characters. Applying the correct key enables legibility to be restored.

Across the globe, AES is the most widely used encryption standard for securing network traffic, personal information, and corporate IT infrastructures. Data and information critical to businesses and individuals are now accessible to anyone with access to the internet and cloud computing. Thus, using a more secure encryption standard such as AES becomes even more essential. Many ciphers are available, but AES is among the most secure. As a result of its very complex algorithm and larger key size, it is more secure than other algorithms. As a result, AES is a fantastic choice for applications such as Artemis Financial that require high levels of security. The most secure AES algorithm is AES-256, which has 256 bits of encryption. This cipher is used daily for many applications, such as financial services and online transactions.

AES remains virtually uncrackable currently. Cryptographers are constantly devising how it could happen despite recording no successful attacks.The main risk associated with AES is its implementation. In the case of an incorrect implementation, there might be security holes that can be exploited. Cybercriminals may use side-channel attacks to attempt brute force entry by intercepting leaks of system data.Related-key could reveal the relationship between two different encryption keys as an additional attack method, providing an attack vector against the encryption itself. Additionally known-key, if a malicious user knew the key, they could crack the code*.*Plaintext transformation into ciphertext occurs randomly, making this scenario implausible*.*Furthermore, key recovery requires the hacker to possess a pair or more plaintext messages and their corresponding ciphertexts. These attacks clearly require some parts of the encryption key to be known by the cybercriminal.Hence, AES encryption will protect your data.

To fully justify why AES is the right choice, I will go into more detail about what is involved with ciphers and why it is the right choice for protecting Artemis Financial. Making a hash function consists of taking the input value and converting it into a compressed one. In essence, a hash function transforms regular data into an unreadable cipher that is difficult to crack even by the most advanced hackers. Encryption algorithm ciphers have bit levels based on the number of characters in their keys. As the AES key length increases, so does the number of encryption rounds it undergoes. AES provides multiple security levels, including 128, 192, and 256 bits.

The AES encryption cipher uses symmetric keys. Basically, the same key is used to encrypt and decrypt data. The keys can be cracked with ease if they are easy to remember, as opposed to if they are random. For this reason, random keys are necessary to ensure security. Nevertheless, this presents a challenge. What is the best way to send the key securely? According to Crawford, "Asymmetric encryption systems solve this problem by securing data using a public key which is made available to everyone. It can only be decrypted by an intended recipient who holds the correct private key” (2018).

Since asymmetric encryption does not require the sender to know the recipient's private key, it is more effective at securing data in transit. Therefore, the security of data stored on your hard drive is superior when encrypted using symmetric ciphers like AES because of their low computational requirements for this application. As a result, symmetric encryption makes it much quicker to encrypt and decrypt data. In addition, symmetric ciphers are much faster and ideal for encrypting large volumes of data in bulk. Therefore, using asymmetric encryption, such as RSA, is only sensible for a minimal amount of data, such as keys for symmetric cryptography. A hard drive full of data of little use in today's connected world. By using asymmetric encryption, remote key exchanges can be handled securely over the internet, allowing it to be transferred safely over the web. An asymmetric TLS key exchange is advisable to establish a secure connection between your PC and the VPN server to transfer encrypted data securely.

A gold standard in cryptography for AES was DES (Data Encryption Standard), which was developed in the 1970s. Due to its high level of security, it was adopted by the U.S. government. Despite its suitability for the 70s and 80s, this block cipher cannot be used today due to technological advances. The 56-bit key can now be brute-forced within hours thanks to modern computers; after being hacked in the 1990s, it was replaced in the early 2000s with AES**.**With AES, DES is significantly improved and makes the algorithm substantially safer. As discussed earlier, it has variants that feature 128-bit, 256-bit, and 512-bit keys, although, as Axel pointed out, "AES 256-bit encryption is the official standard for U.S. government agencies such as the NSA” (2018). A brute force attack would likely take billions of years. So you can rest assured that AES is the right choice to secure Artemis Financials’ archive files.

**REFERENCES**

*Why Is AES Encryption One of The Best Encryption Algorithms*. (2023, January 30).

Newsoftwares.  [https://www.newsoftwares.net/blog/why-is-aes-encryption-one-of-the-best-encryption-algorithms/#:~:text=AES%20is%20the%20most%20popular%20encryption%20algorithm%20because,key%20is%20used%20for%20both%20encryption%20and%20decryption.)](%20https://www.newsoftwares.net/blog/why-is-aes-encryption-one-of-the-best-encryption-algorithms/#:~:text=AES%20is%20the%20most%20popular%20encryption%20algorithm%20because,key%20is%20used%20for%20both%20encryption%20and%20decryption.))

Crawford, D. (2018). *How does AES encryption work*. ProPrivacy.

[https://proprivacy.com/guides/aes-encryption](https://proprivacy.com/guides/aes-encryption%20).

*Encryption: The past, present, and future*. (2021). AXEL.

[https://www.axel.org/2021/05/28/history-of-encryption/](https://www.axel.org/2021/05/28/history-of-encryption/%20)