|  |
| --- |
| CS 305 Software Security |
| 4-2 Written Assignment: Algorithm Ciphers |
| Emily Wood |

|  |
| --- |
| emily.wood7@snhu.edu  3-23-2023 |

Artemis Financial wishes to encrypt their long-term archive files.

1. **Algorithm Cipher**

Based on their need to encrypt static archive files, the AES using the Rjindael cipher would be my recommendation. AES is a block cipher using symmetric encryption. Symmetric encryption uses a single key for both encryption and decryption. It was originally created as a replacement for DES within the United States government. AES has become the most popular algorithm because of its successful use within the US government.

So far, only theoretical attacks have been proposed by researchers. One of which is quantum computing which has never been realized.  
While AES-256 would be considered the most secure, it requires a lot of computing power and cost. AES-128 is considered sufficient for commercial use.

1. **Justification**

Different encryption algorithm ciphers that exist today include:

* AES – Advanced Encryption Standard – symmetric encryption, widely used for protecting data at rest. Can use 128-bit, 192-bit, or 256-bit key lengths.
* DES – Data Encryption Standard – previously used by the government until it was determined that the 56-bit key lengths were too small. Found to be vulnerable to brute force attacks. Was the foundation for many subsequent encryption algorithms.
* RSA – Rivest-Shamir-Aldeman – asymmetric algorithm primarily used in the transmission of data. Relatively slow, so it is not commonly used to encrypt user data. Primarily used to transmit shared keys for other bulk encrypted data.
* ECIES- Elliptic Curve Integrated Encryption Scheme – the elliptic curve equivalent of RSA. Also used to transmit data and establish keys with parties that have never spoken before. Used by Android Pay and Apple iMessage

The different bit lengths available for keys give different levels of security options and CPU usage. It is also able to work well with existing systems. Each size of the AES block ciphers encrypts data in blocks of 128 bits using keys of 128, 192, and 256 bits. The data is put into an array which the cipher then transforms over multiple rounds. 10 rounds are used in AES-128, 12 rounds in AES-192, and 14 rounds in AES-256.

**References:**

Oracle. (n.d.). *Java Security Standard Algorithm Names*. Java security standard algorithm names. Retrieved March 23, 2023, from https://docs.oracle.com/javase/9/docs/specs/security/standard-names.html#cipher-algorithm-names

Bernstein, C., & Cobb, M. (2021, September 24). *What is the Advanced Encryption Standard (AES)? definition from searchsecurity*. Security. Retrieved March 23, 2023, from https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard#:~:text=The%20Advanced%20Encryption%20Standard%20(AES)%20is%20a%20symmetric%20block%20cipher,cybersecurity%20and%20electronic%20data%20protection.

Simplilearn. (2022, November 18). *What is DES (data encryption standard)? DES algorithm and operation [updated]*. Simplilearn.com. Retrieved March 23, 2023, from https://www.simplilearn.com/what-is-des-article

*ECIES – sec.1 and ISO/IEC 18033*. wolfSSL. (2021, August 20). Retrieved March 23, 2023, from https://www.wolfssl.com/ecies-sec-1-isoiec-18033/#:~:text=Unlike%20RSA%20encryption%2C%20ECIES%20can,encrypt%20any%20amount%20of%20data.

*What is AES? how does it work?* Encryption Consulting. (2022, August 17). Retrieved March 23, 2023, from https://www.encryptionconsulting.com/education-center/what-is-aes/