**Jennifer Swinton**

**2/2/25**

**CS 305 Software Security**

**S. North**

Algorithm Ciphers

To defend against the security attacks that exist, we have to look at a number of factors. These include the best practices of first, ensuring data integrity, that the data is not altered in the process of storing and transmitting. We need to ensure confidentiality is maintained and users are authenticated when accessing the information. Finally, we need to have a method of tracking and maintaining a history of transactions. (*NIST …Mechanisms*, 2020)

The existing risks include things like performance, encryption can slow down processing and cause delays. We need a means of managing the encryption keys that is not going to endanger the data stored. And lastly, we need to ensure adherence to any state, federal and even international regulatory standards.

Some of the existing regulations to consider include the Federal Information Security Modernization Act (FISMA), which sets security standards to secure government information. As we don’t know what contracts Artemis Financial holds, we should make sure to follow to these. We can do this by conducting routine assessments for potential vulnerabilities and apply continuous monitoring for active incidents, as well as implementing a process of documenting and reporting. (*NIST …Mechanisms*, 2020). We should also plan to utilize the NIST Guidelines, as they help to provide guidelines for the basic standards of cryptography. We should make sure to adhere to these standards by using approved algorithms and implementing secure key management processes including storage and disposal (*NIST …Mechanisms*, 2020)

We can use the algorithm cipher to encrypt our files and ensure they are stored using appropriate security and are only accessed by authorized users. For this I recommend that Artemis Financial use AES (Advanced Encryption Standard)-256, which is considered the most secure encryption standard, even being used to protect US government classified information (DocuWare Europe GmbH, n.d.). The risk for using the most secure method is that the more security that is applied, the slower the performance can be due to increasing complexity. This, however, does not outweigh the peace of mind of customers knowing their financial data is secure. The trust in company is critical.

Further justification for the use of the AES-256 is that is uses a block cipher with a 256-bit key, providing the highest level of security. It has hash functions that take data and transforms it into an unreadable cipher of a standard size, so that it is indistinguishable from other data transmissions larger or smaller. This makes it difficult to reverse by attackers. It uses the same key for both encryption and decryption making it a symmetric key encryption, which is less secure than non-symmetric which requires two different types of keys however, random numbers being used help ensure the encryption can’t be easily broken.

Encryption algorithms have evolved greatly over the years. Some of the earliest algorithms include DES (Data Encryption Standard) that was found to be insecure because of the short key length. This was eventually replaced by AES with the longer key lengths and has become the most trusted encryption algorithm today. (Ward, 2025)

References:

DocuWare Europe GmbH. (n.d.). *4 Keys to Secure Digital Archiving | Best Practices | DocuWare*. https://start.docuware.com/digital-archiving/the-4-keys-to-secure-digital-archiving?form=MG0AV3

*NIST SP 800-175B Revision 1--Guideline for using Cryptographic standards in the Federal Government: Cryptographic Mechanisms*. (2020, March 31). NIST. https://www.nist.gov/news-events/news/2020/03/nist-sp-800-175b-revision-1-guideline-using-cryptographic-standards-federal?form=MG0AV3

Ward, T. (2025, January 8). The evolution of encryption: past, present, and future - Spyrus. *Spyrus*. https://spyrus.com/the-evolution-of-encryption-past-present-and-future/?form=MG0AV3