**Algorithm Ciphers**

Matthew A Keaton

Southern New Hampshire University

CS305: Software Security

Professor Inshan Singh

February 02, 2025

**Algorithm Cipher**

Artemis Financial is looking for advice from their security expert to recommend an appropriate algorithm cipher for encrypting long-term archive files. The recommended encryption algorithm to use is Advanced Encryption Standard 256 (AES-256). This encryption is the best to use because it is a “FIPS-approved” (Federal Information Processing Standards) algorithm, which is issued by the National Institute of Standards and Technology (NIST) after it has been approved by the Secretary of Commerce (National Institute of Standards and Technology, 2001). This verifies that AES is a trusted and reliable encryption algorithm used by federal agencies. A regulation that must be considered is the Gramm-Leach-Bliley Act (GLBA) that requires financial institutions to protect the privacy of consumers personal financial information (Federal Trade Commission, n.d.). Since AES is a FIPS approved encryption algorithm, this ensures the GLBA regulation will be met, and consumers can trust their information will be safe. There are several security best practices to consider when protecting data and one of the most critical is key management. “A common saying in cryptography is that cryptography turns the problem of protecting a lot of information—your data—into the problem of protecting a little information: the keys” (Manico & Detlefsen, 2014). Losing an encryption key poses a serious risk, especially if it falls into the wrong hands. To mitigate this risk, it is important to have strong key management and regular key rotation to maintain security. Although there are more secure algorithms to choose from, AES is highly efficient against all known attacks and remains the industry standard for finance and government data protection, ensuring that Artemis Financial will meet all regulatory requirements.

**Justification**

AES-256 is a popular symmetric encryption algorithm used for securing data where 256 refers to the key size in bits. AES supports three key sizes of 128, 192, and 256 bits. As the key size increases the more secure the encryption is, making it harder for brute force attacks to break the encryption. AES-256 uses random numbers to ensure that each encryption is unique even if it encrypts the same plaintext. Since AES is a symmetric encryption algorithm, it uses the same key to encrypt and decrypt as compared to asymmetric encryption algorithms uses a public and private key for encryption and decryption. Symmetric encryption is fast which makes it better to use to encrypt large amounts of data, however distribution of the key must be secure since anyone can encrypt and decrypt data with it. Cryptography has been used for a long time dating back to ancient times being used by Spartans to scramble military communications and Julius Caesar using what is known today as the Caesar Cipher (IBM, 2024). Through the years cryptography has evolved, adapting to new threats, technological advances, and the needs of security. AES encryption is today’s standard of encryption security that has evolved over time from a simple Caesar Cipher into using a modern algorithm to protect data. Although there are many more encryption algorithms to choose from today, the purpose remains the same to protect the confidentiality, integrity, and authenticity of data.

**References**

Federal Trade Commission. (n.d.). *Gramm-Leach-Bliley Act* (Report No. 106-102, 113 Stat. 1338). Federal Trade Commission. <https://www.ftc.gov/legal> library/browse/statutes/gramm-leach-bliley-act

IBM. (2024, January 5). *A brief history of cryptography: Sending secret messages throughout time.* IBM.https://www.ibm.com/think/topics/cryptography-history

Manico, J. & Detlefsen, A. (2014, September). *Iron-Clad Java: Building Secure Web Applications*. O’Reilly. <https://learning.oreilly.com/library/view/iron-clad> java/9780071835886/ch01.html#ch01lev1sec15

National Institute of Standards and Technology. (2001, November 26). *FIPS PUB 197: Advanced Encryption Standard (AES)*. U.S. Department of Commerce. https://csrc.nist.gov/files/pubs/fips/197/final/docs/fips-197.pdf