Module Four Written Assignment: Algorithm Ciphers

Alexis Prazak

7/28/2025

It can be difficult to determine the best security measures. Every algorithm has its own advantages and disadvantages. To decide on the best algorithm for Artemis Financial, let's look at the requirements. They will need a high level of security, at least 128-bit encryption. Since these are archived files they don't need the fastest encryption method. This allows us to pick a cipher that'll take longer to run. Some algorithms break information up into smaller pieces and makes one key being decrypted less risky. Any algorithm used should have this feature.

Based on those facts, I suggest implementing the Advanced Encryption Standard (which this paper will refer to as AES). This algorithm is Federal Information Processing Standards-approved, making it ideal for complying with American banking regulations. It can generate keys in 128, 192, and 256 bits. This is a useful feature if the minimum recommended bits for encryption increase. AES uses a symmetric key system, meaning the same key is used to encrypt and decrypt data. Even so, it's still one of the safest algorithms used today.

Using AES can be justified further by its long history of use by the US federal government. Fun fact, it was first used in 2001 and many government agencies were required to transition to this algorithm over DES! Even with its long history, attacks are rarely successful. The computing power needed to break a 256-bit key is massive. I predict AES will be in use for a long time.

References

*Transition to Advanced Encryption Standard (AES)*, Cybersecurity and Infrastructure Security Agency, May 2024, www.cisa.gov/sites/default/files/2024-05/23\_0918\_fpic\_AES-Transition-WhitePaper\_Final\_508C\_24\_0513.pdf.

*FIPS 197, Advanced Encryption Standard (AES)*, 2001, csrc.nist.gov/files/pubs/fips/197/final/docs/fips-197.pdf.