CS305

Alex Zelaya

Module 4 written assignment

For Artemis Financial’s long-term file storage, I recommend using the AES-256 (Advanced Encryption Standard) cipher. AES-256 is the most trusted and secure option available today because it uses a 256-bit key, making it nearly impossible to break with brute force. It’s a symmetric cipher, meaning the same key is used to encrypt and decrypt the data, which makes it faster and easier to manage for large archives. This algorithm also meets strict government standards such as FIPS 197 and FIPS 140-3, keeping Artemis Financial compliant with financial regulations. To stay protected from attacks, the company should also follow best practices like using unique encryption keys, securing those keys in a key-management system, and using TLS 1.3 for data in transit. The main risk to avoid is poor key management, since losing or exposing the key could compromise all encrypted data.

AES-256 also includes features that make it a smart long-term choice. It uses random numbers (initialization vectors) so no two encryptions are ever the same, and hash functions like SHA-256 can verify data integrity, making sure no files are tampered with. Over time, older algorithms like DES and Triple DES became outdated because computers got faster and could break them, but AES replaced them for being stronger and more efficient. While some newer ciphers exist, AES-256 is still the best overall choice because it’s secure, widely supported, and optimized for performance. In short, AES-256 gives Artemis Financial the perfect mix of speed, strength, and reliability to keep sensitive financial records safe.