Huan Ai

7/27/2025

CS 305 - Module Four Written Assignment

Given Artemis Financial’s security vulnerabilities, the encryption algorithm cipher to recommend is Advanced Encryption Standard, or AES. AES is a common encryption for the banking industry. AES-256 (256-bit key) provides military-grade encryption against brute-force attacks. It’s also good against eavesdropping, tampering, and replay attacks. The risks of AES-256 may include the possibility of key compromise, which may result in data loss. It’s also vulnerable to quantum threats, as future quantum computers may break AES-256. However, this is not imminent. As for governmental restrictions, they must comply with local governmental regulations because there are international transactions crossing borders every day. The company must comply with stringent regulations like GDPR (for European clients). GDPR will require encryption of archives containing personal data. To use AES, we would first generate a 256-bit secret key using Java's KeyGenerator, encrypt the files, and securely store the encrypted files. AES-256 is the best cipher because it has 2^256 possible keys and is technically unbreakable. It’s also the current U.S. government standard for top-secret data. There is no reason I would not choose the most secure cipher as data security is the number one priority for a banking company.

Hash functions mix up data into a fixed-size fingerprint (like a unique ID) to verify integrity—if the file changes, the hash changes. Bit levels (like AES-256's 256-bit keys) determine strength—higher bits mean more possible combinations, making brute-force attacks more impossible. Together, they ensure data stays secure. Random numbers create unpredictability and make it harder for hackers to obtain information. Symmetric keys (like AES) use one secret key to lock/unlock data—fast for big files, but you must share the key securely. Asymmetric keys (like RSA) use two keys (public + private). They are safer for sharing, but slower, so they're mainly used to send symmetric keys securely. The most ancient encryption algorithms date back to around 600 BC. Modern encryption algorithm - AES was approved in 2001, which still protects top-secret data today.

**APA citation:**

Jeganathan, S. (n.d.). The Issa Journal November 2019: DevSecOps: A systemic approach for secure software development. Content Delivery Platform. https://mydigitalpublication.com/article/DevSecOps:+A+Systemic+Approach+for+Secure+Software+Development/3524379/632044/article.html