**Encryption Algorithm Recommendation for Artemis Financial**

**1. Recommended Algorithm**

After reviewing Artemis Financial’s needs, I recommend using AES (Advanced Encryption Standard) to secure their archive files. AES is a well-known and trusted encryption method. It uses keys of 128, 192, or 256 bits, with AES-256 being the most secure. This method is used by both businesses and the government because of its strong protection.

**2. Security Best Practices**

To protect against common security attacks, there are a few things to keep in mind:

* **Brute force attacks**: AES-256 makes brute force attacks nearly impossible because it would take too long to guess the key.
* **Side-channel attacks**: Implementing AES properly, like handling keys securely, reduces the risk of this kind of attack.
* **Quantum computing**: AES-256 offers good protection against future attacks by quantum computers.

**3. Risks of Using AES**

* **Weak implementation**: If AES isn’t used correctly (like poor key management), it can be vulnerable.
* **Slower performance**: AES-256 might be slower than smaller key sizes, but it’s worth it for the added security.

**4. Government Regulations**

AES meets important regulations such as:

* **FIPS 140-2**: A standard required for U.S. government data.
* **GDPR**: Ensures data protection in Europe. By using AES, Artemis Financial will follow these rules.

**5. How the Algorithm Will Be Used**

AES will be used to:

* **Encrypt the archive files**: AES is fast and can handle large amounts of data, which is great for storing files long-term.
* **Decrypt the files using the same key**: A strong system for managing the keys will make sure only the right people can access the data.

**6. Why AES Is the Best Choice**

AES is the best choice because:

* **Widely trusted**: It’s recommended by the U.S. government and has been proven to be secure.
* **Efficient**: It provides a good balance between security and speed, making it ideal for encrypting large archives.

**7. Why Not Use the Most Secure Cipher?**

Some other ciphers, like RSA (which uses two different keys), are very secure but much slower. For large archives, AES is faster and more efficient. RSA is more useful for smaller tasks, like sending keys, but not for encrypting huge files.

**Justification for Using AES**

**1. Hash Functions and Bit Levels**

* **Hash functions**: These are used to make sure no one has changed the encrypted data. When using AES, adding a hash function like **SHA-256** can ensure data integrity.
* **Bit levels**: Higher bit levels, like the 256-bit key in AES-256, provide stronger security against attacks.
* **Random numbers**: Random numbers are critical for generating secure encryption keys and initialization vectors (IVs). These numbers ensure that the encrypted data is unique and unpredictable each time it's encrypted, even if the same data is used. Without strong randomness, patterns could form, making it easier for attackers to guess the key and break the encryption.

**2. Symmetric vs. Asymmetric Keys**

* **Symmetric encryption (AES)**: This uses the same key for both encryption and decryption. It’s faster and better for large files.
* **Asymmetric encryption (RSA)**: Uses two different keys but is slower and usually used for things like sending keys, not big data encryption.

**3. History and Current Use of Encryption Algorithms**

* **AES** was introduced in 2001 and replaced **DES** (Data Encryption Standard), which had become weak over time.
* **Today**, AES is still one of the strongest and most widely used encryption methods.

In conclusion, AES-256 is the best choice for Artemis Financial’s file encryption because it is secure, efficient, and meets all necessary regulations for protecting long-term archive files.

**References:**

Daemen, J., & Rijmen, V. (2002). The Design of Rijndael: AES - The Advanced Encryption Standard. Springer Science & Business Media.

Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C (20th ed.). Wiley.

NIST. (2001). Announcing the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197. https://doi.org/10.6028/NIST.FIPS.197

Singh, S. (1999). The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Anchor Books.

Oracle. (2023). Java Cryptography Architecture (JCA) Reference Guide. Oracle Documentation. <https://docs.oracle.com/javase/9/docs/specs/security/standard-names.html>