The internet of things is becoming more and more ubiquitous in our everyday lives, from our TVs and dishwashers to even our refrigerators. Every device is connected to the internet gathering and storing data about us and our habits. This data is highly coveted by companies and even more so by potential thieves, which is why it is becoming increasingly important to protect it from prying eyes. Artemis Financial is looking to encrypt their archive files and has asked GLOBALRAIN for their recommendations on the best and most secure ciphers to fit their needs.

Before recommending solutions to Artemis Financial we must first understand what a cypher algorithm is and how they work. Cryptography, the art of writing or solving codes, dates back as far back as 600BC in ancient Sparta. (*A Brief History of Encryption (and Cryptography)*, 2023) Modern cryptography, however, is much more sophisticated, using complex mathematical formulas to hide information. A cypher algorithm is one such formula designed to obscure the value and content of data by generating a key that is used to encrypt the data, the original key or a complementary key is then needed to decrypt the data back its original form. (*IBM Documentation*, n.d.)

Cipher algorithms can be broken down into three main types-Symmetric, Asymmetric, and Hashing. Symmetric Encryption, also called private-key cryptography or secret key algorithm, requires the sender and receiver to have access to the same key. (Simplilearn, 2023) This type of encryption is fast and works best in a closed system, but it requires that both parties have the key stored securely and available only to the software that needs to use it. (Simplilearn, 2023) Asymmetric Encryption, also called public-key cryptography, makes use of two keys for the encryption prosses, a public and a private key, that are mathematically linked. This type of encryption can commonly be found in blockchain crypto currencies. (Brush et al., 2021) Finally, we have hashing which generates a unique mathematical signature called a “hash value” of fixed length for a data set or message. Each message has its own unique hash, and changes to the message can be easily traced by looking at the differences in hash values. (Simplilearn, 2023).

These are the five most common types of encryption algorithms available today.

AES- Considered invulnerable to all but brute force attacks. Uses 192- and 256-bit keys.

Triple DES- Symmetric encryption. Applies DES algorithm three times. Commonly used for UNIX passwords and ATM PINs

RSA- Standard asymmetric algorithm for encrypting internet transmitted information. Creates massive amounts of useless information to frustrate hackers.

Blowfish- Symmetric tool that breaks messages into 64-bit blocks and encrypts them individually. Common use cases are e-commerce platforms, securing payments, and password management tools.

Twofish- Symmetric encryption that deciphers 128-bit data blocks. Always encrypts data into 16 rounds. Many of today’s files and folder encryption software solutions use this method.

Rivest-Shamire-Adleman- Asymmetric encryption that works off the factorization of the product of two large prime numbers. Digital signatures commonly use RSA, but it slows down when given large data sets.

Now that we know about cypher algorithms it is time to discuss the proper course of action for Artemis Financial. One of the simplest things the company can do to protect their archived files is to lock access to them behind a username and password, the user can then be granted access to the all the files or even a subset based on their privilege levels. Password based encryption should be used- PBEWith<digest>And<encryption>-where each angle bracket is replaced with a different algorithm that will generate keys for the password, one example of this would be PBEWithSHA256withAES. (Stackoverflow) Additionally, Artemis should encrypt the files themselves using AES-256, which is a symmetric encryption algorithm that uses 256-bit keys to convert plain text into a cipher. AES-256 uses quite a few steps when encrypting data, these include dividing the data into 4x4 columns of 16 bytes, multiple rounds of key generation, byte substitution, shifting rows of the 4x4 array, then a pre-established mixing of the 4x4 array, and finally more rounds of key generation. (Kananda, 2022)

The proposed implantations for data security at Artemis Financial should be more than adequate to secure their archive files, I would however suggest yearly employee training on phishing schemes, because if an outside entity were to gain access it would more than likely come from human error within the company (i.e. divulging of personal information)

**References**

*A brief history of encryption (and cryptography)*. (2023, February 1). Thales Group. https://www.thalesgroup.com/en/markets/digital-identity-and-security/magazine/brief-history-encryption

*IBM documentation*. (n.d.). https://www.ibm.com/docs/en/ztpf/1.1.0.15?topic=concepts-cipher-algorithms-keys

Simplilearn. (2023). What is data encryption: types, algorithms, techniques and methods. *Simplilearn.com*. <https://www.simplilearn.com/data-encryption-methods-article>

Brush, K., Rosencrance, L., & Cobb, M. (2021). asymmetric cryptography (public key cryptography). *Security*. <https://www.techtarget.com/searchsecurity/definition/asymmetric-cryptography?Offer=abt_pubpro_AI-Insider>

*Java Security Standard Algorithm Names*. (n.d.). <https://docs.oracle.com/javase/9/docs/specs/security/standard-names.html#cipher-algorithm-names>

*What is PBEWithMD5AndDes?* (n.d.). Stack Overflow. <https://stackoverflow.com/questions/54143361/what-is-pbewithmd5anddes>

Kananda, V. (2022, July 8). Why You Should Use AES 256 Encryption to Secure Your Data. *Progress*. https://www.ipswitch.com/blog/use-aes-256-encryption-secure-data