When it comes to security everyone needs to take the utmost precautions and see what is available for what conditions. Artemis Financial is included in how security is needed at its max. Due to this, it is suggested to avoid the DES algorithm and proceed with AES instead. After some research, we can rule out DES because of how easy it has become to break into in recent years. AES is more than twice as secure with the 128, 192, and 256 bit compared to DES’s 56 bit. Being this secure will help to protect against algebraic, cryptanalysis, and linear cryptanalysis-type attacks.

Even though AES is an excellent choice for security purposes, everything has both pros and cons. Besides the pros, one of the cons is there is always a possibility of using a weak or easy key. Side Channel attacks are another vulnerability AES has. After research AES is currently considered the government’s standard for software security. The government considers AES to be impenetrable and because of this is also used across multiple agencies.

Once everything is set up, Artemis Financial will end up having a database that will store all sensitive data. AES will be used to help encrypt and protect the sensitive data in this database. AES is a block-style cipher that will be used to help jumble up the bits and help hide sensitive data that can only be seen if using a correct key. Being in finance there is a great chance that the company will be a heavy target for attacks. For this reason, the most secure option should be used as a cipher. If the most secure cipher wasn’t needed, it shouldn’t be used due to memory space.

Within a cipher, hash functions are the key to security. Hashing will allow it to encrypt the data by scrambling it up into unreadable nonsense. The only possible way someone out there could read the data is if they had the key to decrypt the encrypted data. Bit levels all data to be broken up into different bits and then scrambled. The higher the bit level the more secure it is. A simple way of putting that is if it was only 2 bits there are only 2 possible combination orders the bits be in, while 3 has 6. This example is not an actual example but I’m using it to illustrate how complex it will get as the bit level grows.

Although both are considered secure there are some differences between symmetric and non-symmetric keys. The first thing to know is symmetric keys is it is the most widely used style of key because it being a little less complex and easier to use. The symmetric key are used to encrypt and decrypt on both ends therefore both sides of the server use the same key. Non-symmetric keys are the opposite and need different keys for encrypting and decrypting. Encryption was around for a very long time. There is some estimation of it possibly starting in Egypt back around 1900 BC. This tells us that different types of encryption were used well before the technical world we live in now.

**Citations**

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

Blog, W. (n.d.). *Articles*. WinZip Enterprise Blog. https://winzip.com/blog/enterprise/aes-encryption-explained/#:~:text=AES%20was%20developed%20to%20provide,to%20its%20extensive%2C%20impenetrable%20protection.

GeeksforGeeks. (2023, May 22). *Advanced encryption standard (AES)*. GeeksforGeeks. https://www.geeksforgeeks.org/advanced-encryption-standard-aes/

Govindraj Basatwar, G. B. H. (2023, June 5). *How AES encryption is used in cybersecurity and why it matters*. AppSealing. https://www.appsealing.com/aes-encryption/#:~:text=In%20addition%20to%20its%20large,linear%20cryptanalysis%2C%20and%20algebraic%20attacks.

*Java Security Standard Algorithm Names*. Java security standard algorithm names. (2017). https://docs.oracle.com/javase/9/docs/specs/security/standard-names.html#cipher-algorithm-names

Jena, B. K. (2023, February 9). *What is AES encryption and how does it work? - simplilearn*. Simplilearn.com. https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption

Manico, J., & Detlefsen, A. (n.d.). *Iron-clad Java*. O’Reilly Online Learning. https://learning.oreilly.com/library/view/iron-clad-java/9780071835886/?sso\_link=yes&sso\_link\_from=SNHU