Brian Engel

Module Four Written Assignment

For Artemis Financials internal long-term archive files, there are a few things to consider. Since the information is not being transmitted and will just be at rest, we can use a symmetric-key algorithm because we will be the ones doing both the encryption and decryption of the information. Also, since it is long-term, we will not have to encrypt and decrypt very often, so we can sacrifice speed for extra security. There are also financial records involved so with that there are always government regulations involved. After a little research, I have decided to use AES-256 as the encryption algorithm cipher.

There are a few risks involved with using this cipher. The main one is that you need to generate a secure, random key, and have a secure way of storing it. If your key becomes compromised, anyone can decrypt the information that you have encrypted. To combat this, it is recommended not to keep the key in the database with all the information that is encrypted. Instead, you could keep it on the server that runs the application, or another secure location. It also does not provide any digital signatures to ensure that it has not been modified, but since it is not in transit, there is less of a chance of it being tampered with. If it is a big concern though, you can add another layer to it after encryption to ensure the integrity of the data. Also, while no known attacks have occurred to this point, evolving technologies such as AI might be able to break through the cipher in the future.

The AES-256 cipher is the strongest of the widely recommended ciphers for financial services. The Gramm-Leach-Bliley Act and the update to the FTC Safeguards Rule make financial and insurance institutions encrypt all data in transit whether it is internal or external communication, and all data at rest as well. In this instance, we only need to worry about data at rest, and the AES-256 should be perfect for protecting customers' data. The government uses this encryption to protect classified information, so it should be strong enough to protect our information.

To use AES, you will need to generate a key, and keep the key secure. Then AES will break the data into blocks, then expand the key, then adds the key to the block, and then a whole bunch of steps to mix up the data that I don’t completely understand, but they are byte substitution, shifting rows, and mixing columns, and then adds the key to the data again, and repeats from there. AES-128 does 9 rounds, AES-192 does 11 rounds, and AES-256 does 13 rounds. Then it does one additional round of byte substitution, row shifts, and adding key. Decryption does that same process, but backward. As you can see, it all revolves around the key, which is why it is imperative that it stays secure.

From what I can tell, the best cipher is AES-256. While it is the best, there are reasons not to use it as well. If it was for data that was being accessed frequently, I would only use AES-128, since it is still very secure, but is much faster to encrypt and decrypt information. But since our information is a long-term archive file, we might as well use the best to protect it since we don’t have to access it frequently.

Using AES-256 means that the key is 256 bits, which means that there are 2^256 possible combinations, which is virtually impossible to crack without an enormous amount of time and resources. Using random numbers helps to keep the key unpredictable, which keeps the cipher as strong as it can be. Symmetric keys are used for both encryption and decryption and should be used when you don’t have to transmit data, otherwise you would have to transmit the key as well and that is a huge security concern. Asymmetric keys usually have a public key for encrypting, so anyone can send an encrypted message to the receiver, and then a private key for decrypting, so only the receiver can decrypt the message. This is the case with credit card transactions. All merchants encrypt the card info, but only the credit card company can decrypt it. AES is a trusted encryption algorithm that many organizations and governments around the world use. The thing that surprised me in an industry that technology evolves so quickly, this cipher is old. It was developed in 1998 by two Belgian cryptographers. It is also one of the easiest to use, secure, and fastest, which makes it easy to understand the cipher’s longevity of use.