Matt Tranchina 11/19/2023

CS-305 Software Security 4-2 Algorithm Ciphers

A financial business needs to have security at their physical location, security guards, a vault with impenetrable locks, and an alarm to alert the police, just to name a few. A financial business with online capabilities should be no different, but online threats are very different than physical ones. Sensitive data, such as financial information, can be vulnerable to attacks in transit and at rest. Artemis Financial is looking to encrypt their archive files, which would give them, as well as their clients, the security that the data entrusted to them is protected. When it comes to encryption there are essentially two ways to do it, symmetrically (one key to encrypt and decrypt data) and asymmetrically (one key to encrypt and a different key to decrypt data). Which brings us to two cipher algorithms to choose from, Advanced Encryption Standard (AES) or RSA, which is named for the MIT scientist Rivest, Shamir, and Adleman who first described it in 1977 (Franklin, 2022). After researching both ciphers, I believe AES would be the best cipher algorithm for Artemis Financial, along with the open-source cryptography toolkit Tink.

Advanced Encryption Standard, also known as the Rijndael algorithm by Joan Daemen and Vincent Rijmen, is a 128-bit block cipher supporting keys of 128, 192, and 256 bits. This means that using this algorithm would turn plaintext data into a sequence of 256 bits (digits with values of 0 or 1). AES has become the encryption algorithm of choice for governments, financial institutions, and security-conscious enterprises around the world. The U.S. National Security Agency (NSC) uses it to protect the country’s “top secret” information (Franklin, 2022). When using an AES-256 cipher, there are 2256 different possible key values, meaning even a supercomputer would take over 100 trillion years to penetrate using “brute force”. Granted if the key used to encrypt the data were discovered, it could be used to decrypt the data. This is where Tink comes into play.

Tink is an open-source library provided by Google to encrypt and sign data. Tink can also help rotate, or change, keys or secure keys using external Key Management Systems (KMSs) (Google, 2023). Tink is primarily used for payment companies such as Google, Square, and Citadel. Tink uses keysets, which is essentially a set of keys to encrypt, decrypt, or sign data. Tink can use AES algorithms to develop keysets to encrypt data, exchange data, protect data from tampering, digitally sign data, and then change said keys to keep attacks at bay.

While the AES cipher is the most popular, technically an RSA is more secure. RSA is asymmetrical, meaning one key encrypts the data and a different one decrypts the data. The public key (encryption key) is created by multiplying two large prime numbers. That key is made public and only the one who created the public key knows the numbers that were used to create it, which means only they can generate the private (decryption) key. While this may be the “safer route”, it is much more computationally intensive than AES and thus, a lot slower. Given the time and power needed, typically this cipher is used for small amounts of data.

Artemis Financial is searching for an algorithm cipher for file encryption. A large amount of data needs to be encrypted and secured during transit as well as in storage. The data entrusted should be verified by signed and trusted applicants, to ensure that the data being encrypted and stored is in fact the correct, untampered, data. For these reasons, the AES cipher algorithm used with the Tink toolkit would be the best fit.

**Resources**

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

Google (2023, November 3). Tink Cryptographic Library. Developers.Google. <https://developers.google.com/tink>

Franklin, R. (2022, November 14). AES vs. RSA Encryption: What Are the Differences? Precisely. <https://www.precisely.com/blog/data-security/aes-vs-rsa-encryption-differences#:~:text=how%20they%20compare.-,AES%20encryption,country's%20%E2%80%9Ctop%20secret%E2%80%9D%20information>.