• Consider security protection best practices to defend against various types of security attacks.

⁃ Avoid suites with ANON authentication,contain NULL or EXPORT, RCA, DES, or 3DES

⁃ Choose ECDHE or DHE for key agreement. These offer the forward secrecy feature.

⁃ Choose bulk ciphers with key sizes of 128 bits or larger.

• Consider and identify all of the risks in your recommendation.

⁃ Lots of data at rest. Financial information, possible CPNI or corporate secrets.

⁃ Could need methods for securing user account info

⁃ File upload security could be needed

• Consider the most current government regulations and how they will be met.

⁃ Data needs to be protected according to regulations put in place by the FTC for financial institutions like Artemis. This includes regulations such as the Financial Privacy rule, the Safeguards rule, and those specified in the Gramm-Leach-Bliley Act

• How will this algorithm cipher be used?

⁃ This algorithm will be used to encrypt any data that will need to be protected. It will be incorporated into our Java server processes.

• What is the best cipher and why?

⁃ RSA is the preferred cipher because it is impossible to break break without the paired public key (asymmetric) and is considered the most secure by many industry professionals.

• What are the reasons why you might not choose the most secure cipher?

⁃ A different cipher may be used for different purposes. For example, RSA is usually slower and more computationally intensive than AES, which is also an excellent cipher. Depending on the application a developer may need something that is faster than the most secure.

For our purposes with Artemis Financial, we will be using RSA encryption in our application.

• What is the purpose of the hash functions and bit levels of the cipher?

⁃ RSA bit sizes are customizable, but common bit sizes are 1024, 2048, and 4096 bits

⁃ These bit sizes essentially make the ciphered text more secure because it makes a brute-force attack more infeasible.

• Explain the use of random numbers, symmetric vs non-symmetric keys, and so on.

⁃ RSA is an asymmetric cipher. This means that the same key cannot be used to decrypt ciphered information that was used to encrypt it. This is a big reason why RSA is considered better than some other leading ciphers.

• Describe the history and current state of encryption algorithms.

⁃ Methods of encryption have been around since ancient times. The Romans had the “Caesar cipher” which just shifted letters down a certain number of spaces. This evolved into methods such as the “Jefferson Disk” which involved plates arranged in a certain order that could be used to encrypt messages and only decrypted with a Disk in the same format as the one used to encrypt. Today we have even more such complex methods of encryption that are are essentially unbreakable today without the proper keys. Any method can be brute forced, however the amount of computations this would take with current technology would make the timeframe to crack longer than any would deem feasible.