Rationale

RSA with OAEP padding was used for our key transport protocol while RSA with SHA256 was used for signing.

AES-128 was used for symmetric encryption because there are no currently known practical attacks. AES-128 is also a recommended encryption scheme by NIST.

HmacSHA256 keyed-hashing algorithm was used to generate MAC. This method allows us to hash messages with a key, which makes the hash function even more reliable.

For the configuration that uses both MAC and Encryption, we are using “Encrypt then MAC” method because it is currently the most secure of the options available. We are also able to detect whether MAC fails or not without wasting energy to decrypt.

Specification:

External Libraries:

Bouncy Castle was used to implement RSA with OAEP padding.

Known Problems: