PQC - Test Vectors

Test vectors are to be provided that can be used to determine the correctness of an implementation. These files come in two types: Known Answer Tests (KAT) files and Intermediate files. The KAT files are for general use to determine an implementation's correctness. The Intermediate values are useful for debugging an incorrect implementation. KAT files shall be provided to test different aspects of the algorithm, e.g., key generation, encryption, decryption.

As an example, suppose one were to look at RSA encryption using the OAEP padding scheme. See IETF RFC 3447 Section 7.1.1 Encryption operation (February 2003) for the specification. For this operation, given a fixed key, the message and label are the other variable inputs. As such, two separate KAT files should be included. Samples for Variable Message Test and Variable Label Test are provided. Additionally, Intermediate Values for the steps in section 7.1.1 are provided. NOTE: For these samples, the hash function is SHA3-256() and the MGF is SHAKE128().

Other sample intermediate values files for various algorithms can be found on the *CryptoToolkit Examples* page.