Implementation of RSA Encryption Algorithm

# Abstract

The first public key scheme was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT. Now Rivest-Shamir-Adleman (RSA) is the most widely accepted and implemented public key cryptosystem. The public key system is based on using different keys, one key for encryption and a different but related key for decryption. The whole process involves computing the remainder after exponential and modular operation of large number.

Encryption and decryption have the following form for some plaintext block M and cipher text block C:

**C = M^e mod n.**

**M = C^d mod n.**

Generally, it includes a third party to generate a pair of public key and to distribute keys to transmitter and receiver. Transmitter and receiver should both know the value of n. The transmitter has the knowledge of public key e, and only the receiver knows the private key d. Thus, a public key of (e, n) and secret key (d, n) generated by third party is distributed to transmitter and receiver separately.

# Outcomes

**Key Generation:** Verilog implementation generates RSA key pairs, calculation of modulus, and determination of public and private exponents.

**Encryption:** Verilog design performs the encryption of plaintext messages using the public key.

**Decryption:** Verilog design decrypts ciphertext using the private key to recover the original plaintext.