Exp No: 6

RSA algorithm

Aim

To implement RSA encryption and decryption

Description to Implement

The general structure of the RSA consists of key generation and encryption/decryption algorithm.

Key Generation

Select p, q prime numbers.

Compute n=pxq

Compute φ(n)=(p-1) *(q-1)

Select Integer e such that gcd(e, φ(n))=1 and 1<e< φ(n)

Calculate d such that d. e≡1 (mod φ(n)).

Public key: (e, n) and private key: (d, n)

Encryption and Decryption

$$\textbf{Ciphertext } C = M^{e} mod\, n$$

$$\textbf{Plaintext } M = C^{d} mod\, n$$

Example:

Select p=3 and q=11.

Plaintext M=4.

Implement RSA algorithm