

**SSN College of Engineering,
Department of Computer Science and Engineering
IT8761 Security Laboratory**

Exercise 6:

To implement the Rivest-Shamir-Adleman (RSA) Algorithm.

Programming Language: Java

Hints:

Key Generation

1. Generate two large random primes, p and q , of approximately equal size such that their product $n = pq$.
2. Compute $n = pq$ and $(\phi) \phi = (p-1)(q-1)$.
3. Choose an integer e , $1 < e < \phi$, such that $\gcd(e, \phi) = 1$.
4. Compute the secret exponent d , $1 < d < \phi$, such that $ed \equiv 1 \pmod{\phi}$.
5. The public key is (n, e) and the private key (d, p, q) .
- 6.

Encryption Procedure for RSA:

Sender does the following:-

1. Obtains the recipient B's public key (n, e) .
2. Represents the plaintext message as a positive integer m , $1 < m < n$.
3. Computes the cipher text $C = m^e \bmod n$.
4. Display the cipher text C .

Decryption Procedure for RSA:

1. Use the cipher text as input.
2. Uses his private key (n, d) to compute $m = C^d \bmod n$.
3. Extracts the plaintext from the message representative m .
4. Display the plain text.