Academic Year 2023-24 (Even Sem.)

EXPERIMENT NO. 2

RSA ALGORITHM

AIM: Develop a program to implement RSA algorithm for encryption and decryption.

OBJECTIVE: Able to implement RSA algorithm for encryption and decryption.

OUTCOMES: Implemented RSA algorithm for encryption and decryption.

THEORY:

The RSA cryptosystem is one the initial system. It remains most employed cryptosystem even today. The system was invented by three scholars **Ron Rivest, Adi Shamir,** and **Len Adleman** and hence, it is termed as RSA cryptosystem. The two aspects of the RSA cryptosystem, firstly generation of key pair and secondly encryption-decryption algorithms

ALGORITHM DESCRIPTION:

Generation of RSA Key Pair

- Each person or a party who desires to participate in communication using encryption needs to generate a pair of keys, namely public key and private key.
- The process followed in the generation of keys is described below –
- Generate the RSA modulus (n)

  Select two large primes, p and q.

  Calculate n=p*q. For strong unbreakable encryption, let n be a large number, typically a minimum of 512 bits.
- Find Derived Number (e)

  Number e must be greater than 1 and less than (p – 1)(q – 1).

  There must be no common factor for e and (p – 1)(q – 1) except for 1. In other words two numbers e and (p – 1)(q – 1) are coprime.
- Form the public key

  The pair of numbers (n, e) form the RSA public key and is made public. Interestingly, though n is part of the public key, difficulty in factorizing a large prime number ensures that attacker cannot find in finite time the two primes (p & q) used to obtain n. This is strength of RSA.
- Generate the private key

  Private Key d is calculated from p, q, and e. For given n and e, there is unique number

d.

Number d is the inverse of e modulo (p - 1)(q – 1). This means that d is the number less than (p - 1)(q - 1) such that when multiplied by e, it is equal to 1 modulo (p - 1)(q - 1).

- This relationship is written mathematically as follows $ed = 1 \bmod (p-1)(q-1)$
- The Extended Euclidean Algorithm takes p, q, and e as input and gives d as output.

CONCLUSION: