MAHEK CHHABRIA
C12-31

EXPERIMENT 6

Aim: Implementation of RSA algorithm.

Theory:

1) RSA is an algorithm used by modern computers to encrypt & decrypt messages. It is an asymmetric cryptography algorithm.
2) Asymmetric means that there are two keys used for encryption & decryption. This is also called public key cryptography because one of the keys can be given to anyone. The other key must be kept private.
3) The algorithm is based on the fact that finding the factors of a large composite no is difficult when the factors are prime no, the problem is called prime factorization. It is also a key pair (public & private key) generator.

RSA Key Setup:

1) Select two large prime nos p & q. (max val could be 1024)
2) $n = p \times q$ (n is modulus for public & private key)
3) $\phi(N) = (p-1)(q-1)$
4) $\gcd = (e, \phi(n)) = 1$ where $1 < e < \phi(n)$
5) $e \cdot d \equiv 1 \bmod \phi(n)$ where $0 \leq d \leq n$
6) publish public key (for encryption) $KU = \{e, n\}$
7) keep secret private key (for decryption) $KR = \{d, p, q\}$

Encryption: To encrypt message m,

1) obtain public key of recipient $KU = \{e, n\}$
2) compute cipher text c

$C = m^e \bmod n$ where $0 \leq m < n$

where e is public key

Decryption: To decrypt cipher text C,

1) Use private key $KR = \{d, p, q\}$
2) compute message m

$m = c^d \bmod n$

where d is private key

Example:

$p = 23,\ q = 19,\ e = 283,\ m = 25$

$N = p \times q = 23 \times 19 = 437$

$\phi(N) = (p-1)(q-1)$

$\phi(N) = 22 \times 18 = 396$

$ed = 1 \bmod \phi(N)$

$283(d) = 1 \bmod 396$

$283d \bmod 396 = 1$

d	283d	283d mod 396
1	283	283
2	566	170
3	849	57
4	1132	340
5	1415	227
6	1698	114
7	1981	1

$\therefore d = 7$

Encrypting $m = 25$

$C = 25^{283} \bmod 437$

$(283)_{10} \rightarrow (100011011)_2$

$25^1 = 25 \bmod 437 = 25$

$25^2 = 25^2 \bmod 437 = 188$

$25^4 = 188^2 \bmod 437 = 384$

$25^8 = 384^2 \bmod 437 = 187$

$25^{16} = 187^2 \bmod 437 = 9$

$25^{32} = 9^2 \bmod 437 = 81$

$25^{64} = 81^2 \bmod 437 = 6$

$25^{128} = 6^2 \bmod 437 = 36$

$25^{256} = 36^2 \bmod 437 = 422$

$C = (25 \times 188 \times 187 \times 9 \times 422) \bmod 437$

$\therefore C = 118$

Decrypting cipher $C = 118$

$m = c^d \bmod n$

$m = 118^7 \bmod 437$

$(7)_{10} \rightarrow (0111)_2$

$118^1 = 118 \bmod 437 = 118$

$118^2 = 118^2 \bmod 437 = 377$

$118^4 = 377^2 \bmod 437 = 104$

$\therefore m = (118 \times 377 \times 104) \bmod 437$

$\therefore m = 25$