PAGE NO.
DATE / /

Assignment - 02

RollNo :- 43236

Aim :- write a program to implement RBA algorithm for key generation and linear verification

objective :- study the concept of public and private key and working of RSA algorithm

Theory :-

The two important parts of the plain text & encryption algorithm where plain text is the original message encryption algorithm performs transformation on the plain text

The pair of key public and private or called for the encryption & decryption.

The plain text is encrypted using an encryption algorithm to for cip text

• encryption :-

plain text + encryption Algorithm + public key → encrypted text

• decryption :-

encrypted text + decryption Algorithm + private key → plain text

RSA Algorithm:-

Begin

1) Choose 2 preme numbers p & q
2) compute $n = p * q$
3) calculate phi = $(p-1) * (q-1)$
4) choose an integer such that
   $1 < e < \text{phi}(n)$ and $\gcd(e, \text{phi}(n)) = 1$
5) calculate $d = (d = e^{-1} \pmod{\text{phi}(n)})$
   d is modular multiplicative inverse of e mod phi(n)

6) for encryption $c = m^e \bmod n$ where n = original message
7) for decryption message
8) for decryption $m = c^d \bmod n$

ex

$m = 88 \quad p = 17, \; e = 11$

$n = p * q = 187$

phi $= 16 \times 10 = 160$

$e = 7$

$d = e^{-1} (\text{mod}(\text{phi}(n)))$

$\therefore d = 23$

$e = 11 \quad m = 88$

public key = (7, 781)

private key = (23, 187)

PAGE No.
DATE / /

Conclusion :-

Thus we studied and implemented the RSA algorithm