Date ___/___/___

Roll no 43320

Assignment 1

Aim : Write a program to implement RSA algorithm for key generation and cipher verification

Objective: 1. Study the concept of public & private keys & working of RSA algorithms.

Theory:

The two important parts are the plain text & encryption algorithm. where plaintexts is the original message encryption algorithm performs transformations on the plaintext.

The pair of key public & private are used for encryption and decryption

The plaintext is encrypted using an encryption algorithm to form cipher text.

Encryption:

Plaintext + encryption algorithm + public key → cipher text

Roll no: 43320

Date __/__/____

Saathi

Decryption:

Cipher text + decryption algorithm + private key → plain text

RSA algorithm

Begin

1. choose 2 prime numbers p & q
2. compute $n = p * q$
3. calculate phi = $(p-1)*(q-1)$
4. Choose an integer such that $1 < e < phi(n)$ and gcd(e, phi(n))=1 i.e. and phi(n) are co prime.
5. Calculate d: as $d = e^{-1} \pmod{phi(n)}$ d is modular multiplications inverse of e modulo phi(n)
6. For encryption $c = m^e \bmod n$ where m = original message
7. For decryption $m = c^d \bmod n$.

Public key is formed as {e, n}
Private key is formed as {d, n}

Example-

m = 88 p = 17 q = 11
n = p*q = 187
phi = 16 * 10 = 160

Date __/__/____

Saathi

$e = 7$

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

$\therefore d = 23$

$e = 11 \quad m = 88$

public key = (7, 187)

private key = (23, 187)

Conclusion -

Thus, we studied & implemented the RSA algorithm.