DATE __/__/____
PAGE NO _____

Assignment - 01

43304

myCOMPANION

* **Aim →** Write a program in C++ or Java to implement RSA algorithm for key generation and cipher verification

* **Objective →** To study :- 1. Concept of public and private key
2. Public key algorithm
3. Working of RSA algorithm

* **Theory →**

- **Asymmetric / Public key Algorithm :**

Public-key algorithms were evolved to solve the problem of key distribution in symmetric algorithms. This is achieved by using different keys for encryption and decryption.

A public key encryption scheme has 6 components :-

1. Plaintext - Readable message or data that is fed as input
2. Encryption algorithm - Performs various transformations on the plaintext
3. Public and private key - Pair of selected keys, One is used for encryption, and the other for decryption
4. Ciphertext - Scrambled message produced as output of plaintext and the key.
5. Decryption algorithm - Accepts cipher text and the matching key and produces the original plaintext.

- **RSA Algorithm :**

RSA stands for Rivest, Shamir and Adleman, who first publically described it. RSA involves 3 steps - key generation, encryption and decryption.

RSA is a block cipher with each block having a binary value less than some number n, i.e → block-size $\leq \log_2(n)$

Encryption → $C = M^e \bmod n$

Decryption → $M = C^d \bmod n$

where →

C - ciphertext M - plaintext block

1. Both sender and receiver know the value of n.
2. Only the sender knows the value of e
3. Only the receiver knows the value of d.

- Algorithm :

1. Choose 2 distinct prime numbers p and q.
2. Compute $n = pq$
3. Compute $\phi(n) = (p-1) * (q-1)$, where ϕ is Euler's totient function
4. Choose an integer e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$ → i.e, e and $\phi(n)$ are co-prime
5. Determine $d = e^{-1} \bmod \phi(n)$, i.e, d is the multiplicative inverse of e mod $\phi(n)$

Public key - PU = {e, n}

Private key - PR = {d, n}

Encryption → $C = M^e \bmod n$

Decryption → $M = C^d \bmod n$

- Example :

1. Select 2 prime numbers → p = 17 and q = 11
2. Calculate $n = pq = 17 * 11 = 187$
3. Calculate $\phi(n) = (p-1)(q-1) = 16 * 10 = 160$
4. Select e such that relatively prime to $\phi(n) = 160$ and less than $\phi(n)$; we choose e = 7
5. Determine d such that $de \equiv 1 \pmod{160}$ and $d < 160$.

The correct value of d is 23. → because $23 * 7 = 161 = 160 + 1$

∴ The resulting keys are :-

Public key = {7, 187}

Private key = {23, 187}

Input →

p = 17 , q = 11

e = 7

plaintext = 88

Output →

PU = 7, 187

PR = 23, 187

ciphertext = 11

* Conclusion → Thus in this assignment, we learnt about the working of RSA algorithm and implemented a program to demonstrate the same.