Name: Anish Kulkarni

Roll number: 43227

Assignment 1

Implementation of RSA

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

Objective:

To study:

Concept of public and private key

Public key algorithm

Working of RSA algorithm.

Theory:

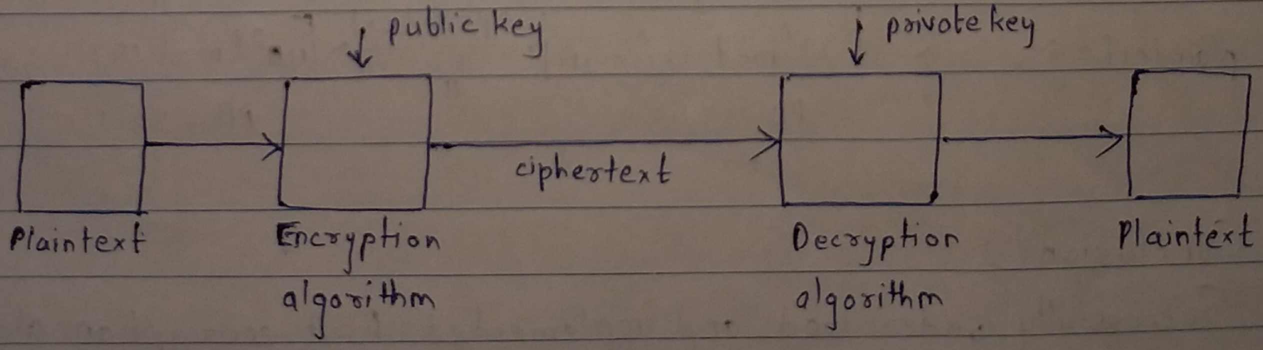
Plaintext: User readable message, input.

Encryption algorithm: Performs transformations on plaintext.

Public and Private key: Pair of keys for encryption and decryption.

Ciphertext: Plaintext after encryption.

Decryption algorithm: Decrypting plaintext from ciphertext.



Public key cryptography

Name: Anish Kulkarni
Roll Number: 43227

Page No.________
Date: / /

RSA algorithm:
Named after Rivest, Shamir, Adleman.

Key generation:

1. Choose two distinct prime numbers p & q.
2. $n = pq$
3. $\phi(n) = (p-1)(q-1)$ - Euler's totient function.
4. Choose e, $1 < e < \phi(n)$ & $\gcd(e, \phi(n)) = 1$.
   e is public key exponent.
5. $d = e-1$ ~~Ao~~ $\bmod (\phi(n))$
   d is private key exponent.

Public key - $\{e, n\}$ Private key - $\{d, n\}$

Encryption - $C = M^e \bmod n$.
Decryption - $M = C^d \bmod n$.

Example:

1. Select $p = 17$, $q = 11$
2. $n = pq = 187$
3. $\phi(n) = (p-1)(q-1) = 160$
4. select $e = 7$
5. $d = 23$ as $23 * 7 = 161 = 10 * 160 + 1$

Encrytion Decryption

$$\text{plaintext} = 88 \rightarrow \boxed{88^7 \bmod 187 = 11} \xrightarrow[11]{\text{ciphertext}} \boxed{11^{23} \bmod 187 = 88} \rightarrow \text{plainte}$$

PU = 7,187 PR = 23,187

Conclusion:
Successfully understood and implemented RSA encryption algorithm.