Page No.
Date:

ASSIGNMENT-1

AIM: Write a program in C++ to implement R algorithm for key generation & cipher verificat

OBJECTIVES: - Concept of public key & private k
- Public key algorithm
- Working of RSA algorithm

THEORY:

- Public key algorithm is used to solve the proble of key distribution in symmetric algorithm.

- It is achieved by using one key for encryption a different but related key for decryption.

- RSA like algorithms use either of the two relat keys for encryption, while the other is used fo decryption.

- Public key encryption scheme has:

i. Plaintext:
Readable message that is fed into algorithm, as input.

ii. Encryption algorithm:
It performs various transformations on plain-te

iii. Public & private key:
This is a pair of keys that have been selecte selected for encryption & decryption process.

iv. Ciphertext:
It is the scrabbled message produced as o/p.

v. Decryption Algorithm:
Accepts ciphertext & matching key & produces the original plaintext.

RSA ALGORITHM:
It is an algorithm for public key cryptography involves 3 steps key generation, encryption & decryption.

It is a block cipher with each block having binary value less than some no. 'n'. Encryption decryption are of the following form, for some plaintext block M & ciphertext block C,

$$C = M^e \bmod n$$
$$M = C^d \bmod n$$
$$= (M^e)^d \bmod n$$
$$= M^{ed} \bmod n$$

Thus public key generated, $PU = \{e, n\}$
& private key generated, $PR = \{d, n\}$

Both sender & reciever must know the value of n. Sender knows the value of e & reciever knows the value of d

i. Key Generation:

a. Choose 2 distinct prime nos. p & q

b. Compute $n = p \cdot q$

c. Compute $\phi(n) = (p-1)(q-1)$

d. Choose an integer e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$, i.e., e & $\phi(n)$ are co-prime

e. Determine $d = (e-1) \bmod \phi(n)$

public key = $\{e, n\}$

private key = $\{d, n\}$

ii. Encryption:

a. $C = M^e \bmod n$

iii. Decryption:

$M = C^d \bmod n$

- Example:

$p = 17$ & $q = 11$

$n = p \cdot q = 17 \times 11 = 187$

$\phi(n) = (p-1)(q-1) = 16 \times 10 = 160$

e should be co-prime to $\phi(n)$, i.e., $e = 7$

d should be modular inverse of e, $\therefore d = 23$

$\therefore PU = \{7, 187\}$

$PR = \{23, 187\}$

CONCLUSION:

Thus, in this assignment, we learnt & understood the RSA algorithm for key generation & cipher verification & successfully implemented it.