Roll no. 43308

Page No.
Date: / /

Assignment No. 1

Aim:
Write a program in C++ or Java to implement RSA Algorithm for key generation cipher & verification.

Objective:

To study:

- Concept of public and private key
- Public key algorithm
- Working of RSA algorithm

Theory:

- Asymmetric/Public Key algorithm

pubic key algorithm were ~~en~~evolved to solve the problem of key distribution in symmetric algorithm. This is achieved by using one key for encryption and different key for description.

- Pubic key algorithm has six ingredients

1) Plaintext :- readble message to send.

ii) Encryption Algorithm

The algorithm performs various transformations on plaintext.

iii) Public and private key.

This is pair of keys that have been selected so that if one is used for encryption and other used for decryption.

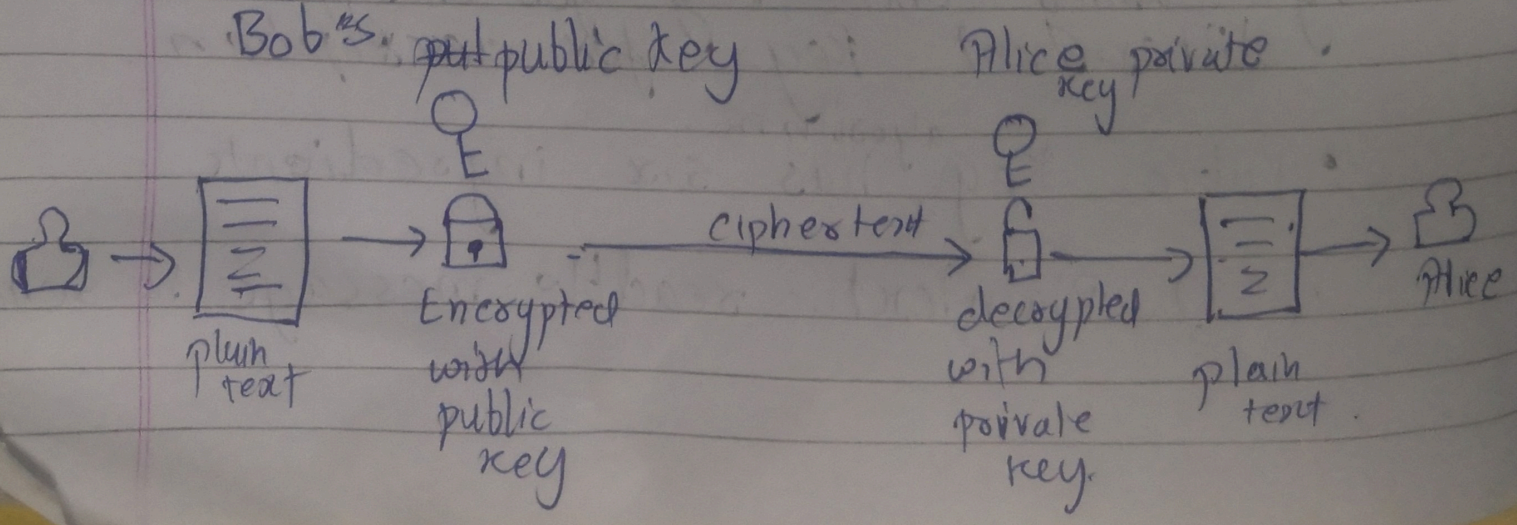
iv) Ciphertext:

This is scrambled message produced as output. It depends on the plaintext and key.

~~v) Decryption~~

v) Decryption algorithm

Accept ciphertext, matching key and produce original plaintext



- RSA Algorithm.

RSA (Rivest, shamir, & Adleman) is an algorithm for public key cryptography which involves 3 steps

i) Key generation
ii) Encryption
iii) Decryption.

- RSA is block cipher with each block having a binary value less than some number n. That is block size must be less than or equal to log (n)

Both sender and receiver must know value of n. sender knows value of e, & only the receiver knows the value of d.

Thus, this is public key encryption algorithm with public key $PU = \{e, n\}$ & private key $PR = \{d, n\}$.

- Algorithm

1) Key generation

2) Encryption

3) They Decryption

Page No.
Date: / /

- Example:

1) Select two 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 $\phi(n) = 160$ & less than $\phi(n)$ (Here e=7)
5) Determine d such that $de = 1 \pmod{160}$ & $d < 160$. The correct value is d=23, because $23 * 7 = 161 = 10 * 160 + 1$: d can be calculated using the extended Euclid's algorithm.

The resulting keys are public key PU = {7, 187} & private key PR = {23, 187}. The example shows use of keys to encrypts M = 88.

Plain text = 88 cipher = 11
Decryption = {23, 187}

Conclusion:
Thus, we successfully implemented RSA algorithm for key generated cipher verification.