Name : Adwait Purao Batch : CSS - V

UID : 2021300101

BECOMPS B

PAGE NO.:

RSA Algo. overview:

RSA is named after Rivest, Shamir, Adleman is a widely used asymmetric cryptography technique. It relies on the mathematical difficulty of factoring large prime nos. making it a secure method for encrypting & decrypting data.

Key Concepts:

→ Asymmetric Cryptography : RSA uses a pair of key.

Public key : Used for encryption & can be shared openly

Private key : Used for decryption, kept secret

→ Key Generation :

Select 2 large prime nos p & q

Compute $n = p * q$

Calculate $\phi(n) = (p-1) * (q-1)$

Choose e such that $1 < e < \phi(n)$ & $GCD(e, \phi(n)) = 1$

Determine d such that $d \times e = 1 \bmod \phi(n)$

→ Encryption : Convert plaintext message (M) into integer

Compute the ciphertext using $C = M^e \bmod(n)$

→ Decryption :

Compute M using $M = C^d \bmod(n)$

Applications : 1) Secure data transmission

2) Digital Signatures & key exchange protocols.