(RSA Algo)

Public key Crypto System

(or)

Assymetric key encryption

Encryption = public key

Decryption = private key

We will see next how to encrypt and decrypt the msg

Algo

1) generate 2 large random prime numbers p & q approx equal size

2) compute $N = p \times q$

3) compute $\phi(N)$ Euler totient func

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

Euler totient :- $\phi(10)$ product 10

1	~~6~~
~~2~~	7
3	~~8~~
~~4~~	9
~~5~~	~~10~~

2

5

$\phi(10) = 4$

4) choose integer E, $1 < E < \phi(N)$ such that $\gcd(E, \phi(N)) = 1$

5) compute D, $1 < D < \phi(n)$, such that $E \times D \equiv 1 \pmod{\phi(n)}$

6) The public key is (N, E) & private key is (N, D)

$D \times E \bmod \phi(n) = 1$

$a \equiv b \pmod{n} \Rightarrow \frac{a}{n} = \frac{b}{n}$

Ift

remainder $(a, n) = \text{rem}(b, n)$

Decrypt

$M = C^{P} \bmod N$

$C = 13$

$m = 13^{7} \bmod 33$

$m = 7$

① $P = 11$ $Q = 3$

② $N = 11 \times 3 \Rightarrow 33$

③ $\phi(N) = (P-1) \times (Q-1)$

$\phi(N) = \phi(33)$

$\phi(33) = (11-1) \times (3-1) \Rightarrow 10 \times 2 \Rightarrow 20$

④ $1 < E < 20$

$GCD(E, \phi(N)) = 1$ $GCD(E, 20) = 1$

$\cancel{1}, 2, 3 \ldots \cancel{20}$ $E = 3$

⑤ $1 < D < 20$

canceled Cancel

$D \times 3 \bmod \phi(20) = 1$ $D = \cancel{1}, 2, 3, 4, 5, 6, 7 \ldots \cancel{20}$

$21 \bmod 20 = 1$

6) $Pk(33, 3)$

7 $Prk(33, 7)$

Encrypt

$C = 13$

Decrypt

$m = 7$

Encr

m plain text

text $M < N$

Cipher = encrypt

C cipher text

$C = M^{E} \bmod N$

$M = 7$

$C = 7^{3} \bmod 33$

$= 343 \bmod 33 \Rightarrow 13$