

(RSA Algo)

Public Key Crypto System

(or)

Asymmetric key encryption

Encryption = public key

Decryption = private key

We will see next how to encrypt and decrypt the msg

Algo

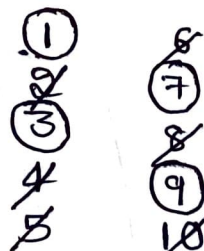
1) generate 2 large random prime numbers p & q
approx equal size

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 $\frac{10}{2}$
 $\frac{5}{5}$

$$\phi(10) = 4$$

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) $\left\{ \begin{array}{l} D \times E \pmod{\phi(N)} = 1 \end{array} \right.$

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

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

$$① \quad p = 11 \quad q = 3$$

$$② \quad N = 11 \times 3 \Rightarrow 33$$

$$③ \quad \phi(N) = (p-1) \times (q-1)$$

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

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

$$④ \quad 1 < E < 20$$

$$\text{GCD}(E, \phi(N)) = 1$$

$$\text{GCD}(E, 20) = 1$$

$$\overset{\times}{1}, 2, 3, \dots, \overset{\times}{20}$$

$$E = 3$$

$$⑤ \quad 1 < D < 20$$

$$D \times 3 \pmod{\phi(20)} = 1$$

$$D = \overset{\text{cancel}}{\overset{\times}{1}}, 2, 3, 4, 5, 6, 7, \dots, \overset{\text{cancel}}{\overset{\times}{20}}$$

$$21 \pmod{20} = 1$$

$$6) \quad \text{pk}(33, 3)$$

$$7) \quad \text{prk}(33, 7)$$

Encrypt

$$C = 13$$

Decrypt

$$M = 7$$

Encr

M plain text

$$\text{text } M < N$$

C Cipher text

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

$$M = 7$$

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

$$= 343 \pmod{33} \Rightarrow 13$$

Cipher = encrypt