# RSA Algorithm

RSA -> Revest - Shavier - Aldeman

RSA developed in 1978

-> It is an (asymmetric cryptographic) algorithm (2 keys)

1. Public key
2. Private key

**Public key**

Known to all the users in Network

**Private key**

kept secret, not sharable to all

-> If public key of user A is used for encryption we have to use the private key of same user for decryption

-> The RSA scheme is a block cipher in which plain text and cipher text are integers b/w 0 and n-1 for some value n.

# RSA Algorithm

## (1) Key Generation

(i) Select 2 large prime number 'p' and 'q'

(ii) calculate $n = p * q$

(iii) calculate eulers toitient function

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

$\phi(n)$ → eulerstoitient function

(iv) chose value of e

(i) $1 < e < \phi(n)$ } condition

(ii) $gcd(\phi(n), e) = 1$

(v) calculate

$$d \equiv e^{-1} \bmod \phi(n)$$

$$ed \equiv 1 \bmod \phi(n)$$

$$ed \bmod \phi(n) = 1$$

(vi) public key = $\{e, n\}$

(vii) private key = $\{d, n\}$

(viii) Encryption :

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

(ix) Decryption

$$M = C^d \bmod n$$

let $p = 3, q = 11$

**Step 1**

Two prime numbers $p, q$

$p = 3, q = 11$

**Step 2**

$n = p \times q$

$n = 3 \times 11$

$\boxed{n = 33}$

**Step 3**

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

$\phi(n) = (3-1) \times (11-1)$

$= 2 \times 10$

$\boxed{\phi(n) = 20}$

**Step 4**

The value of e will be given in question

If not we need to choose

$\boxed{e = 7}$ as $1 < 7 < 20$

$\gcd(7, 20) = 1$

Steps

$ed \bmod \phi(n) = 1$

$(7 \times d) \bmod 20 = 1$

hit & run method

$7 \times 3 \bmod 20 = 1$

$\boxed{d = 3}$

Step 6

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

$= \{7, 33\}$

Step 7

~~privat~~

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

$= \{3, 33\}$

Encryption

Abhi -> (4) -> As the letter in Abhi is (4)//

Encryptim.

plain text $= m < n$

c -> cipher text

$$\boxed{C = m^e \bmod n}$$

$C = m^e \bmod n$

$C = 31^7 \bmod 33 = 4$

$\boxed{\text{Let } m = 31}$

$\boxed{C = 4}$

## Decryption

$$m = c^d \bmod n$$

$$= 4^3 \bmod 33$$

$$\boxed{m = 31}$$