prime numbers, **p** and **q**.

**n** is called the modulus for encryption and decryption.

C = chipper text

M= plain text.

e = public key

d= private key

**Important Theorem**

- $n = p \times q$
- $\varphi (n) = (p - 1) \times (q-1)$
- $d = (1 + k.\varphi (n))/e$
- $e= (1 + k.\varphi (n))/d$
- $C = m^e \mod n$
- $m = c^d \mod n$

# Example 1:

In an RSA cryptosystem, a particular A uses two prime numbers, 13 and 17, to generate the public and private keys. If the public of A is 35. Then the private key of A is ……………?.

**Explanation:**

**Step 1:** in the first step, select two large prime numbers, **p** and **q**.

p = 13

q = 17

**Step 2:**

$\boldsymbol{\varphi (n) = (p - 1) \times (q-1)}$

$\varphi (n) = (13 - 1) \times (17 - 1)$

$\varphi (n) = 12 \times 16$

$\varphi (n) = 192$

**Step 3:**

$\boldsymbol{d = (1 + k.\varphi (n))/e}$ [let k =0, 1, 2, 3………………]

**Put k = 0**

d = (1 + 0 x 192)/35

d = 1/35

**Put k = 1**

d = (1 + 1 x 192)/35

d = 193/35

**Put k = 2**

d = (1 + 2 x 192)/35

d = 385/35

d = 11

The private key is <d, n> = (11, 221)

Hence, private key i.e. d = 11

## Example 2:

A RSA cryptosystem uses two prime numbers 3 and 13 to generate the public key= 3 and the private key = 7. What is the value of cipher text for a plain text=5?

**Explanation:**

**Step 1:** In the first step, select two large prime numbers, **p** and **q**.

p = 3

q = 13

**Step 2:** Multiply these numbers to find **n = p x q,** where **n** is called the modulus for encryption and decryption.

First, we calculate

**n = p x q**

n = 3 x 13

n = 39

**Step 3:**

To find ciphertext from the plain text following formula is used to get ciphertext C.

**$C = m^e \bmod n$**

$C = 5^3 \bmod 39$

C = 125 mod 39

C = 8

**Hence, the ciphertext generated from plain text, C = 8.**

## Example 3:

In an RSA cryptosystem, a particular A uses two prime numbers, 3 and 11, to generate the public and private keys. If the private key of A is 7. Then the public key of A is ……………?.

**Explanation:**

**Step 1:** in the first step, select two large prime numbers, **p** and **q**.

p = 3

q = 11

**Step 2:**

**φ (n) = (p - 1) x (q-1)**

φ (n) = (3 - 1) x (11 - 1)

φ (n) = 2 x 10

φ (n) = 20

**Step 3:**

**e = (1 + k. φ (n))/ d** [let k =0, 1, 2, 3………………]

**Put k = 0**

e = (1 + 0 x 20) / 7

e = 1/7

**Put k = 1**

e = (1 + 1 x 20) / 7

e = 21/7

e = 3

The public key is <e, n> = (3, 33)

**Hence, public key i.e. e = 3**