RSA ALGORITHM

➔ It's an Asymmetric Key Algorithm

➔ In this there are 2 keys

1) Private key
2) Public key

➔ As the name describes that the Public Key is given to everyone and Private key is kept private.

Step-1 :

Select 2 prime numbers P and Q

P = 3

Q = 5

Step-2:

Compute the value of n

N= P * Q

N= 3 * 5

N = 15

Step-3

Find the value of Euler's Totient (φ(n))

Φ(n) = (P-1) * (Q-1)

Φ(n) = (3-1) * (5-1)

= 2 * 4

Φ(n) = 8

Step-4

Find the e value (public key)

e value is random number, but it should satisfy 2 conditions

1) $1 < e < \varphi$
2) Gcd(e, φ(n)) = 1

Consider e values 3,5,7

Then the above 2 conditions will satisfy for the above 3 numbers here I am considering the value of e as 7

e= 7

Step-5

Now we need to find the value d which is a private key value

To find private key

$D = (1+ k \varphi(n)) / e$

Or

$d.e \mod(\varphi(n)) = 1$

by using the first formula

$d = (1+ k \varphi(n)) / e$

here the value of k is a random which is less than the value of e so that the d value should be integer value

if we consider k=6 then the value of d is (1 + 6*8) / 7

so the d = 7

if we consider the d formula as

$$d.e \mod(\varphi(n)) = 1$$

$$d.7 \mod(8) = 1$$

if the value of d is 7 then the above formula is satisfied

To Encrypt data

$$C = t^e \mod n \; [\text{plain-text} < n]$$

T = message

Consider my message as 2

So the cipher text is

$$C = 2^7 \mod(15)$$

$$= 128 \mod 15$$

$$= 8$$

So the cipher text = 8

To Decrypt data

$P = C^d \bmod n$

$= 8^7 \bmod 15$

$= 2097152 \bmod 15$

$= 2$

THANK YOU