PLANTEAMIENTO:

Dados los números primos **p=11, q=23**, y el mensaje **m=3**; usar el algoritmo RSA para encriptar el mensaje(m).

SOLUCIÓN:

1. Hallar n y Φ(n):

a. **n = p*q = 11*23 = 253** → **n = 253.**

b. **Φ(n) = (p-1)*(q-1) = (11-1)*(23-1) = (10)*(22) = 220** → **Φ(n) = 220.**

2. Hallar k:

k = Φ(n)+1 = 220+1 = 221 → **k = 221.**

3. Factorizar K para hallar e y d:

a. **k = e*d.**

b. **Para hallar e, se deben tener en cuenta las siguientes características:**

i. **1 < e < Φ(n)**

ii. **MCD (e, Φ(n)) = 1** → **e y Φ(n) sean primos relativos.**

c. **Se despeja d (d = k/e).**

4. Según lo anterior se procede de la siguiente manera:

a. **221= e*d = 13*17.**

b. **Se supone e=13:**

i. **1 < 13< 221.**

ii. **MCD (3, 220)) = 1 ⍰ 13 y 220 <u>si son</u> primos relativos.**

c. **Luego, d = 221/13 = 17.**

d. **En conclusión:**

i. **Llave pública: (e, n) = (13, 253).**

ii. **Llave privada: (d, n) = (17, 253).**

5. Una vez se tienen las llaves, se puede pasar a encriptar (cifrar) / desencriptar (descfirar) el mensaje:

Cifrado: mc = m^e mod n; con MCD (m, n) = 1 y m < n.

Descifrado: m = mc^d mod n.

Es importante decir que para efectuar estos cálculos se necesita de un computador y se requiere manejar los números con altísima precisión.

1. Se cifra el mensaje m (mc) y se lo envía, de acuerdo al siguiente procedimiento:

mc = $(m)^e$ **mod** n **=** $(3)^{13}$ **mod** 253 **=** 1594323 **mod** 253 **=** 170;

con MCD (3, 253) = 1 **y** 3<253 ⍰ **mc = 170.**

2. Se recibe el mensaje cifrado mc, y se procede a realizar el procedimiento inverso que implica descifrar mc, obteniendo el mensaje original (m):

m = $(mc)^d$ **mod** n = $(170)^{17}$ **mod** 253= 3.8621687291664*10^36 **mod** 253 = 3 (p, q, m) = (3, 11, 14)

1. Hallar n y Φ(n):

a. **n = p*q = 3*11 = 33** **n = 33.**

b. **Φ(n) = (p-1)*(q-1) = (3-1)*(11-1) = (2)*(10) = 20** **Φ(n) = 20.**

2. Hallar k:

k = Φ(n)+1 = 20+1 = 21 **k = 21.**

3. Factorizar K para hallar e y d:

a. **k = e*d.**

21= 3*7

b. **Para hallar e, se deben tener en cuenta las siguientes características:**

e= 3 1<e< Φn

se cumple que 1<3<20

ii) MCD (e, Φ, (n)) = 1

MCD(3, 20) = 1 son primos relativos

C. **Se despeja d**

K= e*d

d= k/e

d= 21/3 por lo tanto d= 7

4) **a) 21 = e*d**

21 = 3*7

Entonces e= 3

1<3<20 3 y 20 son primos relativos

Luego d= 21/3 = 7

En conclusión

i. Llave pública: (e, n) = (3, 33).

ii. Llave privada: (d, n) = (7, 33).

5. Una vez se tienen las llaves, se puede pasar a encriptar (cifrar) / desencriptar (descifrar) el mensaje:

Cifrado: $mc = m^e \bmod n$; con MCD (m, n) = 1 y m < n.

Descifrado: $m = mc^d \bmod n$.

Es importante decir que para efectuar estos cálculos se necesita de un computador y se requiere manejar los números con altísima precisión.

6. Se cifra el mensaje m (mc) y se lo envía, de acuerdo al siguiente procedimiento:

mc = $(14)^3$ **mod (**33)

mc = 2744 mod 33

mc= 5

7. Se recibe el mensaje cifrado mc, y se procede a realizar el procedimiento inverso que implica descifrar mc, obteniendo el mensaje original (m):

m = $(mc)^d$ **mod** n =

m = $(5)^7$ **mod** (33) =

m = 78125 **mod** 33 =

m = 14

Explicación porque no da $p=7$, $q=11$, $m=5$

c. **$n = p*q = 7*11 = 77$ ⍰ $n = 77$.**

d. **$\Phi(n) = (p-1)*(q-1) = (7-1)*(11-1) = (6)*(10) = 60$ ⍰ $\Phi(n) = 60$.**

3. Hallar k:

$k = \Phi(n)+1 = 60+1 = 61$ ⍰ $k = 61$.

4. Factorizar K para hallar e y d:

a. **$k = e*d$.**

b. **Para hallar e, se deben tener en cuenta las siguientes características:**

i. **$1 < e < \Phi(n)$**

ii. **MCD $(e, \Phi(n)) = 1$ ⍰ e y $\Phi(n)$ sean primos relativos.**

c. **Se despeja d ($d = k/e$).**

$61 = e*d = 1*61$.

61 es un número primo, solo es divisible entre 1 y el mismo número, por lo tanto para este caso no existe e que cumpla la condición $1 < e < \Phi(n)$

Es decir: $1 < e < 61$