PLANTEAMIENTO:

Dados los números primos **p=7, q=19**, y el mensaje **m=5**; usar el algoritmo RSA para encriptar el mensaje(m).

SOLUCIÓN:

1. Hallar n y Φ(n):

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

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

0. Hallar k:

k = Φ(n)+1 = 20+1 = 21 □ **k = 21.**

e= 7

0. Factorizar K para hallar e y d:

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

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

. **1 < e < Φ(n)**

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

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

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

a. **21 = e*d = 7*3**

a. **Se supone e=7:**

   . **1 < 7 < 20.**

   . **MCD (7, 20)) = 1 7 y 20 si son primos relativos.**

a. **Luego, d = 21/7 = 3.**

a. **En conclusión:**

   . **Llave pública: (e, n) = (7, 33).**

   . **Llave privada: (d, n) = (3, 33).**

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

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

   Descifrado: $m = m_C{}^d \bmod n$.

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

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

78125÷33

1. Divide 78 entre 33: 78÷33=2 con un resto de 78−(33×2)=78−66=12. Baja el siguiente dígito (1), formando 121.

2. Divide 121 entre 33: 121÷33=3 con un resto de 121−(33×3)=121−99=22. Baja el siguiente dígito (2), formando 222.

3. Divide 222 entre 33: 222÷33=6 con un resto de 222−(33×6)=222−198=24. Baja el siguiente dígito (5), formando 245.

4. Divide 245 entre 33: 245÷33=7 con un resto de 245−(33×7)=245−231=14.

El resto final es 14.

$$\mathbf{m_C} = (m)^e \ \mathbf{mod}\ n = (5)^7 \ \mathbf{mod}\ 33 = 78125 \ \mathbf{mod}\ 33 = 14;$$

con MCD (5, 33) = 1 **y** 2<33 □ **m_c = 14.**

4. Se recibe el mensaje cifrado m_c, y se procede a realizar el procedimiento inverso que implica decifrar m_c, obteniendo el mensaje original (m):

Para calcular 143(mod33), primero calculamos 143:

143=14×14×14 14×14=196 196×14=2744

Ahora, calculamos 2744(mod33):

Podemos realizar la división: 2744÷33

1. **Divide 274 entre 33: 274÷33=8 con un resto de 274−(33×8)=274−264=10. Baja el siguiente dígito (4), formando 104.**

2. **Divide 104 entre 33: 104÷33=3 con un resto de 104−(33×3)=104−99=5.**

El resto final es 5.

Por lo tanto: 143(mod33)=5

m = $(m_c)^d$ **mod** n = $(14)^3$ **mod** 33 = 2744 **mod** 33 = 5