PLANTEAMIENTO:

Dados los números primos **p=11, q=13**, y el mensaje **m=7**; usar el algoritmo RSA para encriptar el mensaje(m).

SOLUCIÓN:

1. Hallar n y Φ(n):

   a. **n = p*q = 11*13 = 210 **

   b. **Φ(n) = (p-1)*(q-1) = (11-1)*(13-1) = (10)*(12) = 120 Φ(n) = 120.**

2. Hallar k:

   k = Φ(n)+1 = 120+1 = 121 k = 121

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. **121= e*d = 11*11.**
   b. **Se supone e=11:**
      i. **1 < 11< 120.**
      ii. **MCD (11, 120)) = 1 11 y 120 si son primos relativos.**
   c. **Luego, d = 121/11 = 11.**

d. **En conclusión:**
    i. **Llave pública: (e, n) = (11, 143).**
    ii. **Llave privada: (d, n) = (11, 143).**

5. 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.

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

    $\mathbf{m_c} = (m)^e \ \mathbf{mod}\ n = (7)^{11}\ \mathbf{mod}\ 143 = 1{,}977{,}326{,}743\ \mathbf{mod}\ 143 = 106$;

    con MCD (7, 143) = 1 y 106 < 143 $\Rightarrow$ $\mathbf{m_c} = 106$**.**

7. 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):

    $\mathbf{m} = (m_c)^d\ \mathbf{mod}\ n = (106)^{11}\ \mathbf{mod}\ 143 = 18{,}982{,}985{,}583{,}354{,}248{,}390{,}656\ \mathbf{mod}\ 143 = 7$

<u>Tarea</u>

Dados los números primos **p=7, q=11**, y el mensaje **m=5**; usar el algoritmo RSA para encriptar el mensaje(m).

SOLUCIÓN:

1. Hallar n y $\Phi(n)$:

    a. **$n = p*q = 7*11 = 77$** □**$n= 77$.**

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

2. Hallar k:

    $k = \Phi(n)+1 = 60+1 = 61$ □ **$k= 61$**

3. Factorizar K para hallar e y d:

    c. **$k = e*d$.**

    d. **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.**

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

***No es posible encontrar números para el valor 61(k) ya que este es un número primo y solo es divisible entre el mismo y el 1, y para encontrar e, el valor debe ser mayor a 1 y menor a 60($\Phi(n)$) lo cual no se cumple.**