Ejercicio en clase:

1. Seguir la plantilla de word para implementar a mano RSA con sus propios valores

CRIPTOGRAFÍA: CIFRADO DE LLAVE PÚBLICA

Cifrado con Algoritmo RSA

EJERCICIO

Desarrollado por: **Marino Bastidas Rosero**

Presentado a: **Andrés Felipe Escallón Portilla**

Mayo de 2025

PLANTEAMIENTO:

Dados los números primos **p=17, q=23**, y el mensaje **m=6**; usar el algoritmo RSA para encriptar el mensaje(m).

SOLUCIÓN:

1. Hallar n y Φ(n):

   a. **n = 17*23 = 17*23 = 391** **n = 391**

   b. **Φ(n) = (p-1)*(q-1) = (17-1)*(23-1) = (16)*(22) = 352** **Φ(n) = 352**

2. Hallar k:

   d*e ≡1 mod Φ(n)

   a. **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.**

Si e = 3
→ 1 < 3 < 352
→ MCD (3, 352) = 1

d*3 ≡ 1 mod 352

Algoritmo extendido de Euclides
e*x + Φ(n)*y = MCD(e,Φ(n))=1

Reemplazando:
3*x+352*y = 1

División Euclidiana:
352/3 → 352 = 3*117+1

Reorganizando se obtiene:
1=352*(1)-3*117

Comparando con 3*x+352*y = 1
x = -117
y = 1

x = -117 md 352 =
x = 352 -117 = 235

Pero d = x → d = 235

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

   a. **En conclusión:**
      i. **Llave pública: (e, n) = (3, 391).**
      ii. **Llave privada: (d, n) = (235, 391).**

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

   Cifrado: $m_C = 6^3 \bmod 391 = 216 \bmod 391 = 216$; con MCD (6, 391) = 1 y 6 < 391.

   Descifrado: $m = 216^{235} \bmod 391$.