PRÁCTICA: CIFRADO RSA

Objetivo: Implementar el cifrado de clave pública RSA.

Desarrollo:

1. Implementa el cifrado RSA de forma que:
   - El programa debe solicitar el texto del mensaje a cifrar, los parámetros p, q y d, comprobar que p y q son números primos (con el **test de Lehman-Peralta**) y que d es primo con φ(n) (con el **algoritmo de Euclides extendido**).
   - El programa debe mostrar la traza completa del algoritmo, es decir, el parámetro e obtenido con el algoritmo de Euclides extendido, y los números correspondientes al mensaje cifrado, obtenidos utilizando el algoritmo de **exponenciación rápida**.

   Nota: Para la **codificación numérica** del texto considerar alfabeto sin Ñ en base 26 (A…Z: 0…25), y dividir en bloques de tamaño j-1 según el valor de n, de forma que $26^{j-1}<n<26^{j}$. Así, por ejemplo, si j-1=4, ABCD equivale a 0*26^3+1*26^2+2*26+3=731. Si el último bloque resultante para cifrar no es de tamaño j-1, se añade una letra nula, la X por ejemplo.

   Ejemplos:

   Entrada:

   Texto original: MANDA DINEROS, p=421, q=7 y d=1619.

   Salida:
   - Se comprueba que p y q son primos
   - Se comprueba que d es primo con ϕ (n)=2520
   - Se calcula e=179
   - Como n=2947, se divide el texto en bloques de 2 caracteres
   - Se pasa cada bloque a decimal para poder cifrar, obteniendo 312, 341, 3, 221, 121, 382,
   - Se calcula en decimal el texto cifrado: 2704, 2173, 0404, 2340, 1789, 2333

   Entrada:

   Texto original: AMIGO MIO, p=2347, q=347 y d=5:
   - Se comprueba que p y q son primos
   - Se comprueba que d es primo con ϕ (n)= 811716
   - Se calcula e= 649373,
   - Como n=814.409, se divide el texto en bloques de 4 caracteres
   - Se pasa cada bloque a decimal para poder cifrar, obteniendo 8326, 254398
   - Se calcula en decimal el texto cifrado: 587813, 526359