

Ejercicio 2

David García Curbelo

Partimos de nuestro dni= 45352581. Dividimos dicho número en dos bloques, 4535 y 2581. Sean $p = 4547$ y $q = 2591$ los primeros primos mayores o iguales que los bloques anteriores. Sea $n = pq = 11781277$ y e el menor primo mayor o igual que 11 que es primo relativo con $\varphi(n)$. Sea $d = e^{-1} \pmod{\varphi(n)}$.

Tenemos así $\varphi(n) = 11774140$, $e = 11$ y $d = 8563011$.

Apartado I. *Cifra el mensaje* $m = 0xC AFE$.

Usamos la siguiente función de cifrado:

$$\text{RSA}_{n,e}(m) = m^e \pmod{n}$$

Pasando m a decimal y aplicando la función anterior, obtenemos el siguiente resultado:

$$\text{textRSA}_{11781277,11}(51966) = 51966^{11} \pmod{11781277} = 9088323 \pmod{11781277}$$

Donde el mensaje queda cifrado de la siguiente manera: $9088323 = 0x8AAD43$.

Apartado II. *Descifra el criptograma anterior.*

Procedamos a continuación a descifrar el criptograma $c = 0x8AAD43 = 9088323 \pmod{11781277}$.

Usamos la siguiente función de descifrado:

$$\text{RSA}_{n,e}^{-1}(c) = c^d \pmod{n}$$

Por tanto procedemos a descifrar el mensaje pedido y el criptograma queda:

$$\text{textRSA}_{11781277,11}^{-1}(9088323) = 9088323^{8563011} \pmod{11781277} = 51966 \pmod{11781277}$$

Donde $51966 = 0xCAFE$ es el mensaje que buscábamos.

Apartado III. *Intenta factorizar n mediante el método $P - 1$ de Polard. Para ello llega, como máximo a $b = 8$.*

Apartado IV. *Intenta factorizar n a partir de $\varphi(n)$.*

Apartado V. *Intenta factorizar n a partir de e y d .*