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*** $m = 0xCAFE$***.***

Usamos la siguiente función de cifrado:

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

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

$$textRSA_{11781277,11}(51966) = 51966^{11} \pmod{11781277} = 9088323 \pmod{11781277}$$

Donde el mensaje queda cifrado de la siguente 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:

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

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

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

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*** $b=8$***.***

Tratemos de factorizar n en 8 pasos como máximo. Para ello, vamos a utilizar el método $P-1$ de Polard. Usaremos como base el 2, que sabemos que es primo relativo con n. Comencemos con las iteraciones.

$b=1$

$$2^{1!} \equiv 2 \pmod{n}, \quad \text{con} \quad \text{mcd}(2-1,n)=1$$

$b=2$

$$2^{2!} \equiv 4 \pmod{n}, \quad \text{con} \quad \text{mcd}(4-1,n)=1$$

$b=3$

$$2^{3!} \equiv 64 \pmod{n}, \quad \text{con} \quad \text{mcd}(64-1,n)=1$$

$b=4$

$$2^{4!} \equiv 4995939 \pmod{n}, \quad \text{con} \quad \text{mcd}(4995939-1,n)=1$$

$b=5$

$$2^{5!} \equiv 3564251 \pmod{n}, \quad \text{con} \quad \text{mcd}(3564251-1,n)=1$$

$b=6$

$$2^{6!} \equiv 1811135 \pmod{n}, \quad \text{con} \quad \text{mcd}(1811135-1,n)=1$$

$b=7$

$$2^{7!} \equiv 9030003 \pmod{n}, \quad \text{con} \quad \text{mcd}(9030003-1,n)=1$$

$b=8$

$$2^{8!} \equiv 9730811 \pmod{n}, \quad \text{con} \quad \text{mcd}(9730811-1,n)=1$$

En este caso no ha sido posible factorizar n en 8 pasos.

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

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