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.

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

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

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

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

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

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

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

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

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

Apartado IV. ***Intenta factorizar n a partir de $\varphi(n)$.***
Hayar una factorización en nuestro caso consiste en obtener p y q (ya que $n = pq$). Para ello, tenemos la siguiente ecuación:

$$(x-p)(x-q) = x^2 - (n+1-\varphi(n)) \cdot x - n$$

Tratemos de resolverla. Sabemos que p y q son las soluciones de $b \pm \sqrt{b^2-n}$, donde sabemos que $p+q = 2b = n - \varphi(n) + 1 = 7138$, luego obtenemos que $b = 3569$. Ahora resolviendo tenemos

$$b \pm \sqrt{b^2-n} = 3569 \pm \sqrt{956484} = 3569 \pm 978 \quad \Rightarrow \quad p = 4547, \quad q = 2591$$

Apartado V. ***Intenta factorizar*** n ***a partir de*** e ***y*** d***.***
Partimos de $n = 11781277$, $e = 11$ y $d = 8563011$. Tratemos de factorizar n. Para ello calculemos previamente $k = e \cdot d - 1 = 94193120$ y por tanto $k/2 = 47096560$. Calculamos ahora $a^{k/2^i} \pmod n$ para $i = 1, 2, 3, 4, 5$ y $a = 2, 3, 5, 7, 11$.

$$k/2 : \begin{cases} 2^{47096560} \pmod{11781277} = 1 \\ 3^{47096560} \pmod{11781277} = 1 \\ 5^{47096560} \pmod{11781277} = 1 \\ 7^{47096560} \pmod{11781277} = 1 \\ 11^{47096560} \pmod{11781277} = 1 \end{cases}$$

$$k/4 : \begin{cases} 2^{23548280} \pmod{11781277} = 1 \\ 3^{23548280} \pmod{11781277} = 1 \\ 5^{23548280} \pmod{11781277} = 1 \\ 7^{23548280} \pmod{11781277} = 1 \\ 11^{23548280} \pmod{11781277} = 1 \end{cases}$$

$$k/8 : \begin{cases} 2^{11774140} \pmod{11781277} = 1 \\ 3^{11774140} \pmod{11781277} = 1 \\ 5^{11774140} \pmod{11781277} = 1 \\ 7^{11774140} \pmod{11781277} = 1 \\ 11^{11774140} \pmod{11781277} = 1 \end{cases}$$

$$k/16 : \begin{cases} 2^{5887070} \pmod{11781277} = 1 \\ 3^{5887070} \pmod{11781277} = 1 \\ 5^{5887070} \pmod{11781277} = 1 \\ 7^{5887070} \pmod{11781277} = 1 \\ 11^{5887070} \pmod{11781277} = 1 \end{cases}$$

$$k/32 : \begin{cases} 2^{2943535} \pmod{11781277} = 2541772 \end{cases}$$

Hemos obtenido que $2^{k/32} \pmod n = 2541772 \neq 1$, por tanto obtenemos la factorización como sigue:

$$p = \text{mcd}(n, 2541772 + 1) = 4547 \qquad q = \text{mcd}(n, 2541772 - 1) = 2591$$