Ejercicio Tema 4

Ana Buendía Ruiz-Azuaga

May 26, 2022

1 Ejercicio Tema 4

Los parámetros de un criptosistema de ElGamal son p = 211 y g = 3, es decir, el criptosistema está diseñado en el cuerpo $F_{211} = Z_{211}$ y tomamos como generador de F_{211}^* , g = 3. La clave pública empleada es $3^a = 109 \mod 211$**. Descifra el criptograma (154, dni mod 211), donde dni es el número de tu DNI. Para calcular los logaritmos discretos necesarios emplea dos de los métodos descritos en la teoría.**

Comenzamos calculando a. Para ello vamos a usar dos implementaciones distintas del logaritmo discreto: paso de bebé - paso de gigante y el algoritmo de Silver-Pohlig-Hellman.

Una vez calculado a, descifraremos el criptograma.

1.1 Paso de bebé - paso de gigante

Sea $p = 211$ y $g = 3$. Vamos a calcular $a = \log_3(109)$

Comenzamos calculando f como $f = \lceil \sqrt{p-1} \rceil = \lceil \sqrt{210} \rceil = 15$.

Ahora calculamos la tabla, obteniendo:

```
[0, 1], [1, 3], [2, 9], [3, 27], [4, 81], [5, 32], [6, 96], [7, 77],
[8, 20], [9, 60], [10, 180], [11, 118], [12, 143], [13, 7], [14, 21]
```

También calculamos $g^{-f} = g^{p-1-f} = 67 \mod p$.

Empezando por $h_0 = 109$, vamos a calcular parejas (i, h_i), con $h_i = h_{i-1} g^{-f} \mod p$ hasta que alguno de estos h_i pertenezca a la tabla ya calculada.

Las parejas calculadas son: $(0, 109)$, $(1, 129)$, $(2, 203)$, $(3, 97)$, $(4, 169)$, $(5, 140)$, $(6, 96)$.

Obtenemos la pareja $(6, 96)$, donde 96 está en la tabla en la posición 6.

Luego tenemos $a = j + if = 6 + 6 \cdot 15 = 96$.

1.2 Algoritmo de Silver-Pohlig-Hellman

Partimos del mismo planteamiento del apartado anterior: $p = 211$ y $g = 3$. Vamos a calcular $a = \log_3(109)$.

Consideramos $n = p - 1 = 210$.

Tenemos que la descomposición de $n = 210 = 2 \cdot 3 \cdot 5 \cdot 7$.

Comenzamos trabajando con $p_1 = 2$, $e_1 = 1$. Tenemos que:

$r_{1,0} = 1$, $r_{1,1} = 210$.

Y la sucesión de coeficientes:
$y_0 = 109$, $x_0 = 0$.
Calculamos además $y_0^{\frac{n}{p_1^{0+1}}} = 109^{\frac{210}{2}} \equiv 1 \mod p$.
Luego $m_1 = 0$.
En el siguiente paso, con $p_2 = 3$, $e_2 = 1$:
$r_{2,0} = 1$, $r_{2,1} = 196$, $r_{2,2} = 14$.
Y la sucesión de coeficientes:
$y_0 = 109$, $x_0 = 0$.
Calculamos además $y_0^{\frac{n}{p_2^{0+1}}} = 109^{\frac{210}{3}} \equiv 1 \mod p$.
Luego $m_2 = 0$.
Ahora con $p_3 = 5$, $e_3 = 1$:
$r_{3,0} = 1$, $r_{3,1} = 188$, $r_{3,2} = 107$, $r_{3,3} = 71$, $r_{3,4} = 55$.
Y la sucesión de coeficientes:
$y_0 = 109$, $x_0 = 1$.
Calculamos además $y_0^{\frac{n}{p_3^{0+1}}} = 109^{\frac{210}{5}} \equiv 188 \mod p$.
Luego $m_3 = 1$.
Finalmente con $p_4 = 7$, $e_4 = 1$:
$r_{4,0} = 1$, $r_{4,1} = 171$, $r_{4,2} = 123$, $r_{4,3} = 144$, $r_{4,4} = 148$, $r_{4,5} = 199$, $r_{4,6} = 58$.
Y la sucesión de coeficientes:
$y_0 = 109$, $x_0 = 5$.
Calculamos además $y_0^{\frac{n}{p_4^{0+1}}} = 109^{\frac{210}{7}} \equiv 199 \mod p$.
Luego $m_4 = 5$.
Por tanto el sistema de congruencias es:

$$\begin{aligned} m &\equiv 0 \mod 2 \\ m &\equiv 0 \mod 3 \\ m &\equiv 1 \mod 5 \\ m &\equiv 5 \mod 7 \end{aligned} \tag{1}$$

Resolvemos este sistema de congruencias con ayuda de software y obtenemos que $m = 96$.

Dado que la solución obtenida por los dos algoritmos es la misma, procedemos a descifrar el criptograma.

1.3 Descifrando el criptograma

Mi DNI es 77770080, y $77770080 \mod 211 \equiv 122$, luego el criptograma que vamos a descifrar es $(154, 122)$.

Tenemos que $D_a(x, y) = yx^{-a}$, sustituyento $D_{96}(154, 122) = 122 \cdot 154^{-96} = 193$.

Luego el mensaje original es 193.