

## Ejercicio 3

### David García Curbelo

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

Por el enunciado y por mi  $DNI = 45352581$ , obtenemos el criptograma  $(154, \text{dni} \pmod{211}) = (154, 30)$ . Procedemos a aplicar los dos algoritmos vistos en teoría:

#### Paso de Bebé - Paso de Gigante

Sabemos que  $D_\alpha(x, y) = y \cdot x^{-\alpha}$ , por lo que vamos a calcularlo mediante el logaritmo discreto. Por el enunciado, sabemos que la clave pública viene dada por  $3^a = 109 \pmod{211}$ , por lo que tenemos el problema  $\alpha = \log_3 109 \pmod{211}$ . Además conocemos la siguiente información:

- $G = \mathbb{F}_{211}^*$
- $g = 3$
- $h = 109$
- $f = \lfloor \sqrt{p-1} \rfloor = \lfloor \sqrt{210} \rfloor = 15$

Procedemos ahora a la construcción de la tabla de iteraciones:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	3	9	27	81	32	96	77	20	60	180	118	143	17	21

Además tenemos

$$g^{-f} = 3^{-15} = 3^{211-1-15} = 3^{195} = 67 \pmod{211}$$

- $h_0 = 109$  no pertenece a ninguna de las iteraciones de la tabla.
- $h_1 = 109 \cdot 67 = 129$  no pertenece a ninguna de las iteraciones de la tabla.
- $h_2 = 129 \cdot 67 = 203$  no pertenece a ninguna de las iteraciones de la tabla.
- $h_3 = 203 \cdot 67 = 97$  no pertenece a ninguna de las iteraciones de la tabla.
- $h_4 = 97 \cdot 67 = 169$  no pertenece a ninguna de las iteraciones de la tabla.
- $h_5 = 169 \cdot 67 = 140$  no pertenece a ninguna de las iteraciones de la tabla.
- $h_6 = 140 \cdot 67 = 96$  sí pertenece a la tabla, concretamente en la sexta iteración.

Hemos encontrado un  $h_k$  que pertenece a la tabla, obteniendo  $i = 6$  y  $j = 6$ . Obtenemos por tanto el resultado que andábamos buscando, de la forma  $\alpha = \log_3 109 \pmod{211} = 6 + 6 \cdot 15 = 96$ .

$$\begin{aligned}
 D_{96}(154, 30) &= 30 \cdot 154^{p-1-\alpha} \pmod{211} \\
 &= 30 \cdot 154^{211-1-96} \pmod{211} \\
 &= 30 \cdot 154^{114} \pmod{211} \\
 &= 30 \cdot 114 \pmod{211} \\
 &= 44 \pmod{211}
 \end{aligned}$$

Por tanto hemos obtenido el mensaje, el cual es  $m = 48$ .

## Silver - Pohlig - Hellman

Consideremos de nuevo  $p = 211$ ,  $h = 109$  y  $g = 3$  el generador del grupo  $\mathbb{F}_{211}^*$ . Para conocer el número de iteraciones necesarias, factorizamos  $p - 1 = 210 = 2 \cdot 3 \cdot 5 \cdot 7$ , lo que nos informa que el algoritmo necesita de 4 iteraciones.