# Ejercicio Tema 5

Ana Buendía Ruiz-Azuaga

June 9, 2022

## 1 Ejercicio Tema 5

**Sea $\mathbb{F}_{32} = \mathbb{F}_2[\xi]_{\xi^5+\xi^2+1}$. Cada uno de vosotros, de acuerdo a su número de DNI o similar, dispone de una curva elíptica sobre $\mathbb{F}_{32}$ y un punto base dados en el Cuadro 6.1.**

Mi dni es 77770080, luego tenemos que $77770080 \mod 32 \equiv 0$, por lo que de acuerdo al cuadro 6.1 la curva elíptica con la que vamos a trabajar es $E(\xi^3, \xi)$ y el punto $Q = (\xi^4 + \xi + 1, \xi^4 + \xi^2 + \xi)$.

## 2 Apartado 1

**Calcula, mediante el algoritmo de Shank o mediante el Algoritmo 9,** $\log_Q O$

Vamos a usar el algoritmo de Shank.

Acotamos $|E| \leq q + 1 + \lfloor 2\sqrt{q} \rfloor = 32 + 1 + \lfloor 2\sqrt{32} \rfloor = 44$.

Luego $f = \lceil \sqrt{44} \rceil = 7$.

Construimos la tabla usando sagemath:

| | |
|---|---|
| 0 | 0 |
| $Q$ | $(\xi^4 + \xi + 1, \xi^4 + \xi^2 + \xi)$ |
| $2Q$ | $(1, \xi^4 + \xi^3 + \xi^2 + 1)$ |
| $3Q$ | $(\xi^4 + \xi^2 + 1, \xi^4 + \xi^3)$ |
| $4Q$ | $(\xi + 1, \xi + 1)$ |
| $5Q$ | $(\xi^4 + \xi^3 + \xi^2 + \xi, \xi^4 + \xi^3 + \xi^2 + 1)$ |
| $6Q$ | $(\xi^4 + \xi^3 + \xi, \xi^3 + \xi)$ |

Ahora calculamos $-7Q = (\xi^3 + \xi^2, \xi^2)$, que no está en la tabla, por lo que calculamos $2(-7Q) = (\xi^4 + \xi^2 + 1, \xi^4 + \xi^3)$, que se encuentra en la tabla, pues coincide con $3Q$, luego $2(-7Q) = 3Q \Rightarrow O = 17Q \Rightarrow \log_Q O = 17$.

## 3 Apartado 2

**Para tu curva y tu punto base, genera un par de claves pública/privada para un protocolo ECDH.**

Partimos de nuestra curva elíptica y el punto base asignados.

Comenzamos calculando el orden de la curva elíptica, que es $|E| = hn$ con $h$ pequeño y $n$ primo. Tenemos que $|E| = 34 = 2 \cdot 17$ luego $h = 2$ y $n = 17$.

Ahora, Alice toma un número aleatorio $a$ con $2 \leq a < n$ y calcula $P_a = aQ$ y envía a Bob $P_a$.

$$a = 13$$

$$P_a = (\xi + 1, 0)$$

Ahora, Bob toma un número aleatorio $b$ con $2 \leq b < n$ y calcula $P_b = bQ$ y envía a Alice $P_b$. También calcula $bP_a$.

$$b = 10$$

$$P_b = (\xi^3 + \xi^2, \xi^2)$$

$$bP_a = (\xi^4 + \xi^3 + \xi, \xi^4)$$

Finalmente Alice calcula $aP_b$:

$$aP_b = (\xi^4 + \xi^3 + \xi, \xi^4)$$

La clave compartida es $(ab)Q = aP_b = bP_a = (\xi^4 + \xi^3 + \xi, \xi^4)$. Alice hace pública $(E, Q, P_a)$ y, análogamente, Bob hace pública $(E, Q, P_b)$.

# 4 Apartado 3

**Cifra el mensaje $(\xi^3 + \xi^2 + 1, \xi^4 + \xi^2) \in \mathbb{F}_{32}^2$ mediante el criptosistema de Menezes-Vanstone**

Vamos a usar la clave de Alice $a$. Comenzamos seleccionando aleatoriamente $k$ con $2 \leq k < n$.

Calculamos $kQ$ y definimos $(x_0, y_0) = k(aQ)$. Si $x_0 y_0 = 0$ tomamos otro $k$.

El cifrado es:

$$E(m_1, m_2) = (kQ, x_o m_1, y_0 m_2)$$

.

En este caso $k = 2$, luego tenemos

$$kQ = (1, \xi^4 + \xi^3 + \xi^2 + 1)$$

$$(x_0, y_0) = k(aQ) = 2 \cdot (13 \cdot (\xi^4 + \xi + 1, \xi^4 + \xi^2 + \xi) = (\xi^3 + \xi^2 + \xi, \xi^4 + \xi^3 + 1)$$

Esto es válido ya que $x_0 \cdot y_0 = \xi^3 + \xi$.

El mensaje a cifrar es $(m_1, m_2) = (\xi^3 + \xi^2 + 1, \xi^4 + \xi^2)$, luego tenemos que:

$$E(m_1, m_2) = ((1, \xi^4 + \xi^3 + \xi^2 + 1), \xi^3 + \xi^2, \xi)$$

# 5 Apartado 4

**Descifra el mensaje anterior.**

Para descifrar un criptograma $(C_1, c_2, c_3)$ Alice debe calcular $a(C_1) = a(kQ) = k(aQ) = (x_0, y_0)$ y

$$D(C_1, c_2, c_3) = (x_0^{-1}c_2, y_0^{-1}c_3)$$

.

Tenemos que $a(C_1) = (x_0, y_0) = (\xi^3 + \xi^2 + \xi, \xi^4 + \xi^3 + 1)$.

Luego

$$D(C_1, c_2, c_3) = (\xi^3 + \xi^2 + 1, \xi^4 + \xi^2)$$

.