

## Ejercicio 4

David García Curbelo

Sea  $\mathbb{F}_{32} = \mathbb{F}_2[\xi]_{\xi^5 + \xi^2 + 1}$ . Cada uno de vosotros, de acuerdo a su número de DNI = 45352581 o similar, dispone de una curva elíptica sobre  $\mathbb{F}_{32}$  con una raíz  $x$  y un punto base dados en el Cuadro 6.1.

**Ejercicio 1.** Calcula, mediante el algoritmo de Shank o mediante el Algoritmo 9,  $\log_Q \mathcal{O}$ .

Teniendo el  $DNI = 45352581$ , tenemos que  $DNI \equiv 5 \pmod{32}$ , y por tanto, de acuerdo con el Cuadro 6.1, obtenemos  $E = E(\xi^2 + 1, \xi^4 + \xi^3 + \xi + 1)$  y el punto  $Q = (\xi^3 + \xi^2 + \xi, \xi + 1)$ . Procedemos al cálculo del logaritmo  $\log_Q \mathcal{O}$  mediante el algoritmo de Shank, por lo que para ello procedemos primeramente al cálculo de las potencias de  $\xi$  en base  $\xi^5 + \xi^2 + 1$ .

$$\begin{aligned}
 \xi^0 &= 1 \\
 \xi^1 &= \xi \\
 \xi^2 &= \xi^2 \\
 \xi^3 &= \xi^3 \\
 \xi^4 &= \xi^4 \\
 \xi^5 &= \xi^2 + 1 \\
 \xi^6 &= \xi^3 + \xi \\
 \xi^7 &= \xi^4 + \xi^2 \\
 \xi^8 &= \xi^3 + \xi^2 + 1 \\
 \xi^9 &= \xi^4 + \xi^3 + \xi \\
 \xi^{10} &= \xi^4 + 1 \\
 \xi^{11} &= \xi^2 + \xi + 1 \\
 \xi^{12} &= \xi^3 + \xi^2 + \xi \\
 \xi^{13} &= \xi^4 + \xi^3 + \xi^2 \\
 \xi^{14} &= \xi^4 + \xi^3 + \xi^2 + 1 \\
 \xi^{15} &= \xi^4 + \xi^3 + \xi^2 + \xi + 1 \\
 \xi^{16} &= \xi^4 + \xi^3 + \xi + 1 \\
 \xi^{17} &= \xi^4 + \xi + 1 \\
 \xi^{18} &= \xi + 1 \\
 \xi^{19} &= \xi^2 + \xi \\
 \xi^{20} &= \xi^3 + \xi^2 \\
 \xi^{21} &= \xi^4 + \xi^3 \\
 \xi^{22} &= \xi^4 + \xi^2 + 1 \\
 \xi^{23} &= \xi^3 + \xi^2 + \xi + 1 \\
 \xi^{24} &= \xi^4 + \xi^3 + \xi^2 + \xi \\
 \xi^{25} &= \xi^4 + \xi^3 + 1 \\
 \xi^{26} &= \xi^4 + \xi^2 + \xi + 1 \\
 \xi^{27} &= \xi^3 + \xi + 1 \\
 \xi^{28} &= \xi^4 + \xi^2 + \xi \\
 \xi^{29} &= \xi^3 + 1 \\
 \xi^{30} &= \xi^4 + \xi
 \end{aligned}$$

Tenemos por tanto que  $E = E(\xi^2 + 1, \xi^4 + \xi^3 + \xi + 1) = E(\xi^5, \xi^{16})$  y el punto  $Q = (\xi^3 + \xi^2 + \xi, \xi + 1) = (\xi^{12}, \xi^{18})$ . Ahora procedemos a buscar una cota para  $|E| \leq q + 1 + \lfloor 2\sqrt{q} \rfloor = 32 + 1 + 11 = 44$  (donde  $q = 32$ ). Obtenemos así que  $f = \lceil 44 \rceil = 7$ , por lo que obtenemos los siguientes puntos:

0	0
1	$Q$
2	$2Q$
3	$3Q$
4	$4Q$
5	$5Q$
6	$6Q$

Procedemos a su cálculo explícito:

$$2Q = Q + Q = (\xi^{12}, \xi^{18}) + (\xi^{12}, \xi^{18})$$

$$\lambda = x_1 + y_1 x_1^{-1} = \xi^{12} + \xi^{18} \xi^{-12} = \xi^{12} + \xi^6 = \xi^2$$

$$x_3 = \lambda^2 + \lambda + a + x_1 + x_2 = \xi^4 + \xi^2 + \xi^5 = \xi^7 + \xi^5 = \xi^{10}$$

$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1 = \xi^2(\xi^{12} + \xi^{10}) + \xi^{10} + \xi^{18} = \xi^{17} + \xi^{30} = 1$$

$$2Q = (\xi^{10}, 1)$$

$$3Q = 2Q + Q = (\xi^{10}, 1) + (\xi^{12}, \xi^{18})$$

$$\lambda = (y_2 + y_1)(x_2 + x_1)^{-1} = (\xi^{18} + 1)(\xi^{10} + \xi^{12})^{-1} = \xi \xi^{-15} = \xi^{17}$$

$$x_3 = \lambda^2 + \lambda + a + x_1 + x_2 = \xi^3 + \xi^{17} + \xi^{10} + \xi^{12} = 1$$

$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1 = \xi^{17}(\xi^{10} + 1) + 1 + 1 = \xi^{21}$$

$$3Q = (1, \xi^{21})$$

$$4Q = 3Q + Q = (1, \xi^{21}) + (\xi^{12}, \xi^{18})$$

$$\lambda = (y_2 + y_1)(x_2 + x_1)^{-1} = (\xi^{18} + \xi^{21})(\xi^{12} + 1)^{-1} = \xi^{24}$$

$$x_3 = \lambda^2 + \lambda + a + x_1 + x_2 = \xi^{17} + \xi^{24} + \xi^5 + 1 + \xi^{12} = \xi^{11}$$

$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1 = \xi^{24}(1 + \xi^{11}) + \xi^{11} + \xi^{21} = \xi^{10}$$

$$4Q = (\xi^{11}, \xi^{10})$$

$$5Q = 4Q + Q = (\xi^{11}, \xi^{10}) + (\xi^{12}, \xi^{18})$$

$$\lambda = (y_2 + y_1)(x_2 + x_1)^{-1} = (\xi^{10} + \xi^{18})(\xi^{11} + \xi^{12})^{-1} = \xi$$

$$x_3 = \lambda^2 + \lambda + a + x_1 + x_2 = \xi^2 + \xi + \xi^5 + \xi^{11} + \xi^{12} = \xi^6$$

$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1 = \xi(\xi^{11} + \xi^6) + \xi^6 + \xi^{10} = 1$$

$$5Q = (\xi^6, 1)$$

$$6Q = 5Q + Q = (\xi^6, 1) + (\xi^{12}, \xi^{18})$$

$$\lambda = (y_2 + y_1)(x_2 + x_1)^{-1} = (1 + \xi^{18})(\xi^6 + \xi^{12})^{-1} = \xi^{30}$$

$$x_3 = \lambda^2 + \lambda + a + x_1 + x_2 = \xi^{29} + \xi^{30} + \xi^5 + \xi^6 + \xi^{12} = \xi^9$$

$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1 = \xi^{30}(\xi^6 + \xi^9) + \xi^9 + 1 = \xi^{17}$$

$$6Q = (\xi^9, \xi^{17})$$

Los puntos calculados quedan de la siguiente forma:

0	0	(0, 0)
1	$Q$	$(\xi^{12}, \xi^{18})$
2	$2Q$	$(\xi^{10}, 1)$
3	$3Q$	$(1, \xi^{21})$
4	$4Q$	$(\xi^{11}, \xi^{10})$
5	$5Q$	$(\xi^6, 1)$
6	$6Q$	$(\xi^9, \xi^{17})$

Procedemos a continuación al cálculo de  $-7Q$ :

$$7Q = 6Q + Q = (\xi^9, \xi^{17}) + (\xi^{12}, \xi^{18})$$

$$\lambda = (y_2 + y_1)(x_2 + x_1)^{-1} = (\xi^{17} + \xi^{18})(\xi^{12} + \xi^9)^{-1} = \xi^{28}$$

$$x_3 = \lambda^2 + \lambda + a + x_1 + x_2 = \xi^{25} + \xi^{28} + \xi^5 + \xi^{12} + \xi^9 = \xi^{24}$$

$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1 = \xi^5(\xi^9 + \xi^{24}) + \xi^{24} + \xi^{17} = \xi^{15}$$

$$7Q = (\xi^{24}, \xi^{15})$$

$$\Rightarrow -7Q = (x_3, x_3 + y_3) = (\xi^{24}, 1)$$

$$2(-7Q) = (-7Q) + (-7Q) = (\xi^{24}, 1) + (\xi^{24}, 1)$$

$$\lambda = x_1 + y_1 x_1^{-1} = \xi^{24} + (\xi^{24})^{-1} = \xi^{24} + \xi^7 = \xi^6$$

$$x_3 = \lambda^2 + \lambda + a + x_1 + x_2 = \xi^{12} + \xi^6 + \xi^5 = 1$$

$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1 = \xi^6(\xi^{24} + 1) + 1 + 1 = \xi^{21}$$

$$2(-7Q) = (1, \xi^{21})$$

Hemos encontrado que  $2(-7Q) = (1, \xi^{21})$  pertenece a la tabla y corresponde con  $3Q$ . Por tanto tenemos que

$$2(-7Q) = 3Q \quad \Rightarrow \quad \mathcal{O} = 17Q \quad \Rightarrow \quad \log_Q \mathcal{O} = 17$$

**Ejercicio 2.** Para tu curva y tu punto base, genera un par de claves pública/privada para el protocolo ECDH.

Tomamos una clave privada que llamaremos  $c$  a partir de la cual generaremos una clave pública dada por  $(E, Q, cQ)$ , siendo  $E$  la curva y  $Q$  el punto base considerados en el ejercicio anterior. Tomamos como clave privada  $c = 2$  para simplificar los cálculos (aunque dicho valor puede ser aleatorio), y obtenemos la clave pública

$$(E, Q, cQ) = ((\xi^5, \xi^{16}), (\xi^{12}, \xi^{18}), 2Q) = ((\xi^5, \xi^{16}), (\xi^{12}, \xi^{18}), (\xi^5, \xi^{19}))$$

**Ejercicio 3.** Cifra el mensaje  $(\xi^3 + \xi^2 + 1, \xi^4 + \xi^2)$  mediante el criptosistema de Menezes-Vanstone.

Tomemos, además de la clave privada anterior  $c$ , un nuevo valor para  $k$ , el cual tomaremos como  $k = 2$ . Calculamos el punto  $(x_0, y_0)$  que viene dado por

$$(x_0, y_0) = a \cdot k \cdot Q = 4Q = (\xi^9, \xi^{25})$$

Tomamos el mensaje  $(m_1, m_2) = (\xi^3 + \xi^2 + 1, \xi^4 + \xi^2) = (\xi^8, \xi^7)$  y procedemos al cifrado mediante el algoritmo de Menezes-Vanstone:

$$E(m_1, m_2) = (kQ, x_0 m_1, y_0 m_2) = (2Q, \xi^9 \xi^8, \xi^{25} \xi^7) = ((\xi^5, \xi^{19}), \xi^{17}, \xi)$$

**Ejercicio 4.** Descifra el mensaje anterior.

Para descifrar el mensaje, conociendo la clave privada calculamos  $a((\xi^5, \xi^{19})) = a(kQ) = 4Q = (\xi^9, \xi^{25})$ . Por tanto, el mensaje descifrado quedaría como sigue:

$$D((\xi^5, \xi^{19}), \xi^{17}, \xi) = (\xi^{-9} \xi^{17}, \xi^{-25} \xi) = (\xi^8, \xi^{-24}) = (\xi^8, \xi^7)$$