

Ejercicio 3

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 ξ 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 $Q = (\xi^3 + \xi^2 + \xi, \xi + 1) = (\xi^9, \xi^{18})$. 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:

$$2Q = Q + Q = (\xi^9, \xi^{18}) + (\xi^9, \xi^{18})$$

$$\lambda = x_1 + y_1 x_1^{-1} = \xi^9 + \xi^{18} \xi^{-9} = \xi^9 + \xi^9 = 0$$

$$x_3 = \lambda^2 + \lambda + a + x_1 + x_2 = \xi^5 + \xi^9 + \xi^9 = \xi^5$$

$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1 = \xi^5 + \xi^{18} = (\xi^2 + 1) + (\xi + 1) = \xi^2 + \xi = \xi^{19}$$

$$2Q = (\xi^5, \xi^{19})$$

$$3Q = 2Q + Q = (\xi^5, \xi^{19}) + (\xi^9, \xi^{18})$$

$$\lambda = (y_2 + y_1)(x_2 + x_1)^{-1} = (\xi^{18} + \xi^{19})(\xi^5 + \xi^9)^{-1} = (\xi^4 + \xi^3 + \xi^2 + \xi + 1)(\xi^2 + 1)^{-1} = \xi^{15}(\xi^5)^{-1} = (\xi^4 + \xi^3 + \xi^2 + \xi + 1)\xi^2 = \xi^6 + \xi^5 + \xi^4 + \xi^3 + \xi^2 = \xi^4 + \xi + 1 = \xi^{17}$$

$$x_3 = \lambda^2 + \lambda + a + x_1 + x_2 = \xi^2 + \xi^{17} + \xi^5 + \xi^5 + \xi^9 = \xi^2 + (\xi^4 + \xi + 1) + (\xi^4 + \xi^3 + \xi) = \xi^3 + \xi^2 + 1 = \xi^8$$

$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1 = \xi^{17}\xi^3 + \xi^8 + \xi^{19} = \xi^{19} + \xi^8 + \xi^{19} = \xi^8$$

$$3Q = (\xi^8, \xi^8)$$

$$4Q = 3Q + Q = (\xi^8, \xi^8) + (\xi^9, \xi^{18})$$

$$\lambda = (y_2 + y_1)(x_2 + x_1)^{-1} = (\xi^{18} + \xi^8)(\xi^8 + \xi^9)^{-1} = (\xi^{12})(\xi^{26})^{-1} = (\xi^4 + \xi^3 + \xi^2 + \xi + 1)\xi^2 = \xi^6 + \xi^5 + \xi^4 + \xi^3 + \xi^2 = \xi^4 + \xi + 1 = \xi^{17}$$

$$x_3 = \lambda^2 + \lambda + a + x_1 + x_2 = \xi^2 + \xi^{17} + \xi^5 + \xi^5 + \xi^9 = \xi^2 + (\xi^4 + \xi + 1) + (\xi^4 + \xi^3 + \xi) = \xi^3 + \xi^2 + 1 = \xi^8$$

$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1 = \xi^{17}\xi^3 + \xi^8 + \xi^{19} = \xi^{19} + \xi^8 + \xi^{19} = \xi^8$$

$$4Q = (\xi^8, \xi^8)$$

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

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

Ejercicio 4. *Descifra el mensaje anterior.*