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 cáclulo 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	$6Q$

Procedmemos a su cálculo explícito:

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

$$\begin{aligned} \lambda &= x_1 + y_1 x_1^{-1} = \xi^9 + \xi^{18}\xi^{-9} = \xi^9 + \xi^9 = 0 \\ x_3 &= \lambda^2 + \lambda + a + x_1 + x_2 = \xi^5 + \xi^9 + \xi^9 = \xi^5 \\ y_3 &= \lambda(x_1 + x_3) + x_3 + y_1 = \xi^5 + \xi^{18} = (\xi^2 + 1) + (\xi + 1) = \xi^2 + \xi = \xi^{19} \end{aligned}$$

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

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

$$\begin{aligned} \lambda &= (y_2 + y_1)(x_2 + x_1)^{-1} = (\xi^{18} + \xi^{19})(\xi^5 + \xi^9)^{-1} = (\xi^4 + \xi^3 + \xi^2 + \xi + 1)(\xi^2 + 1)^{-1} = \\ &\quad \xi^5(\xi^{15})^{-1} = \xi^{-10} = \xi^{21} \\ x_3 &= \lambda^2 + \lambda + a + x_1 + x_2 = \xi^{11} + \xi^{21} + \xi^5 + \xi^5 + \xi^9 = \xi^{15} + \xi^9 = \xi^5 \\ y_3 &= \lambda(x_1 + x_3) + x_3 + y_1 = \xi^{21}(\xi^5 + \xi^5) + \xi^5 + \xi^{19} = \xi^{18} \end{aligned}$$

$$3Q = (\xi^2, \xi^{18})$$

$$4Q = 3Q + Q = (\xi^5, \xi^{18}) + (\xi^9, \xi^{18})$$

$$\begin{aligned} \lambda &= (y_2 + y_1)(x_2 + x_1)^{-1} = (\xi^{18} + \xi^{18})(\xi^5 + \xi^9)^{-1} = 0 \\ x_3 &= \lambda^2 + \lambda + a + x_1 + x_2 = \xi^5 + \xi^5 + \xi^9 = \xi^9 \\ y_3 &= \lambda(x_1 + x_3) + x_3 + y_1 = \xi^9 + \xi^{18} = \xi^{25} \end{aligned}$$

$$4Q = (\xi^9, \xi^{25})$$

$$5Q = 4Q + Q = (\xi^9, \xi^{25}) + (\xi^9, \xi^{18})$$

$$\begin{aligned} \lambda &= (y_2 + y_1)(x_2 + x_1)^{-1} = (\xi^{25} + \xi^{18})(\xi^9 + \xi^9)^{-1} = 0 \\ x_3 &= \lambda^2 + \lambda + a + x_1 + x_2 = \xi^5 + \xi^9 + \xi^9 = \xi^5 \\ y_3 &= \lambda(x_1 + x_3) + x_3 + y_1 = \xi^5 + \xi^9 = \xi^{15} \end{aligned}$$

$$5Q = (\xi^5, \xi^{15})$$

$$6Q = 5Q + Q = (\xi^5, \xi^{15}) + (\xi^9, \xi^{18})$$

$$\begin{aligned} \lambda &= (y_2 + y_1)(x_2 + x_1)^{-1} = (\xi^{15} + \xi^{18})(\xi^5 + \xi^9)^{-1} = (\xi^{13})(\xi^{15})^{-1} = \xi^{-2} = \xi^{29} \\ x_3 &= \lambda^2 + \lambda + a + x_1 + x_2 = \xi^{27} + \xi^{29} + \xi^5 + \xi^5 + \xi^9 = \xi + \xi^9 = \xi^{21} \\ y_3 &= \lambda(x_1 + x_3) + x_3 + y_1 = \xi^{29}(\xi^5 + \xi^{21}) + \xi^{21} + \xi^{15} = \xi^{29}\xi^{14} + \xi^{11} = \xi^{12} + \xi^{11} = \xi^{29} \end{aligned}$$

$$6Q = (\xi^{21}, \xi^{29})$$

Los puntos calculados quedan de la siguiente forma:

0	0	$(0,0)$
1	Q	(ξ^9, ξ^{18})
2	$2Q$	(ξ^5, ξ^{19})
3	$3Q$	(ξ^2, ξ^{18})
4	$4Q$	(ξ^9, ξ^{25})
5	$5Q$	(ξ^5, ξ^{15})
6	$6Q$	(ξ^{21}, ξ^{29})

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

$$
\begin{aligned}
7Q &= 6Q + Q = (\xi^{21}, \xi^{29}) + (\xi^{9}, \xi^{18}) \\
\lambda &= (y_2 + y_1)(x_2 + x_1)^{-1} = (\xi^{29} + \xi^{18})(\xi^{21} + \xi^{9})^{-1} = (\xi^{6})(\xi)^{-1} = \xi^{5} \\
x_3 &= \lambda^2 + \lambda + a + x_1 + x_2 = \xi^{10} + \xi^{5} + \xi^{5} + \xi^{21} + \xi^{9} = \xi^{29} + \xi^{9} = \xi^{17} \\
y_3 &= \lambda(x_1 + x_3) + x_3 + y_1 = \xi^{5}(\xi^{21} + \xi^{17}) + \xi^{17} + \xi^{29} = \xi^{5}\xi^{27} + \xi^{9} = \xi + \xi^{9} = \xi^{21}
\end{aligned}
$$

$7Q = (\xi^{17}, \xi^{21})$

$\Rightarrow\ -7Q = (x_3, x_3 + y_3) = (\xi^{17}, \xi^{27})$

$$
\begin{aligned}
2(-7Q) &= (-7Q) + (-7Q) = (\xi^{17}, \xi^{27}) + (\xi^{17}, \xi^{27}) \\
\lambda &= x_1 + y_1 x_1^{-1} = \xi^{17} + \xi^{27}(\xi^{17})^{-1} = \xi^{17} + \xi^{10} = \xi \\
x_3 &= \lambda^2 + \lambda + a + x_1 + x_2 = \xi^{2} + \xi + \xi^{5} = \xi^{18} \\
y_3 &= \lambda(x_1 + x_3) + x_3 + y_1 = \xi(\xi^{17} + \xi^{18}) + \xi^{18} + \xi^{27} = \xi^{5} + \xi^{3} = \xi^{8}
\end{aligned}
$$

$2(-7Q) = (\xi^{18}, \xi^{8})$

$$
\begin{aligned}
3(-7Q) &= 2(-7Q) + (-7Q) = (\xi^{18}, \xi^{8}) + (\xi^{17}, \xi^{27}) \\
\lambda &= (y_2 + y_1)(x_2 + x_1)^{-1} = (\xi^{8} + \xi^{27})(\xi^{17} + \xi^{18})^{-1} = \xi^{19}(\xi^{4})^{-1} = \xi^{15} \\
x_3 &= \lambda^2 + \lambda + a + x_1 + x_2 = \xi^{30} + \xi^{15} + \xi^{5} + \xi^{18} + \xi^{17} = \xi^{8} + \xi^{5} + \xi^{4} = \xi^{21} \\
y_3 &= \lambda(x_1 + x_3) + x_3 + y_1 = \xi^{15}(\xi^{18} + \xi^{21}) + \xi^{21} + \xi^{8} = \xi^{15}\xi^{16} + \xi^{22} = \xi^{7}
\end{aligned}
$$

$3(-7Q) = (\xi^{21}, \xi^{7})$

$$
\begin{aligned}
4(-7Q) &= 3(-7Q) + (-7Q) = (\xi^{21}, \xi^{7}) + (\xi^{17}, \xi^{27}) \\
\lambda &= (y_2 + y_1)(x_2 + x_1)^{-1} = (\xi^{7} + \xi^{27})(\xi^{17} + \xi^{21})^{-1} = \xi^{15}(\xi^{27})^{-1} = \xi^{-12} = \xi^{19} \\
x_3 &= \lambda^2 + \lambda + a + x_1 + x_2 = \xi^{7} + \xi^{19} + \xi^{5} + \xi^{21} + \xi^{17} = \xi^{30} + \xi^{5} + \xi^{27} = \xi^{26} + \xi^{27} = \xi^{13} \\
y_3 &= \lambda(x_1 + x_3) + x_3 + y_1 = \xi^{19}(\xi^{21} + \xi^{13}) + \xi^{13} + \xi^{7} = \xi^{21} + \xi^{3} = \xi^{4}
\end{aligned}
$$

$4(-7Q) = (\xi^{13}, \xi^{4})$

$$
\begin{aligned}
5(-7Q) &= 4(-7Q) + (-7Q) = (\xi^{13}, \xi^{4}) + (\xi^{17}, \xi^{27}) \\
\lambda &= (y_2 + y_1)(x_2 + x_1)^{-1} = (\xi^{4} + \xi^{27})(\xi^{17} + \xi^{13})^{-1} = \xi^{16}(\xi^{23})^{-1} = \xi^{-7} = \xi^{24} \\
x_3 &= \lambda^2 + \lambda + a + x_1 + x_2 = \xi^{17} + \xi^{24} + \xi^{5} + \xi^{17} + \xi^{13} = \xi^{8} + \xi^{5} + \xi^{23} = \xi^{11} \\
y_3 &= \lambda(x_1 + x_3) + x_3 + y_1 =
\end{aligned}
$$

$5(-7Q) = ()$

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

$$(E, Q, cQ) = ((\xi^5, \xi^{16}), (\xi^9, \xi^{18}), 2Q) = ((\xi^5, \xi^{16}), (\xi^9, \xi^{18}), (\xi^5, \xi^{19}))$$

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:

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