Criptografía y Seguridad - Tarea 3

Rivera González Damián
Tadeo Guillén Diana G

November 27, 2019

Ejercicio 1

Sea la curva $y^2 = x^3 + 7x + 2$ en Z_{11}

a) Mostrar que el punto P =(7, 3) $\in E(Z_{11})$ dada por la ecuación y $y^2 = x^3 + 7x + 2$
Como $y^2 = x^3 + 7x + 2$ entonces siendo x = 7 tenemos

$$y^2 = (7)^3 + 7(7) + 2 = 343 + 49 + 2 = 394 mod 11 = 9$$

Así

$$y^2 = 9 \Rightarrow y = 3$$

Por lo tanto (7,3) $\in E(Z_{11})$

b) dar el orden de (7, 3).
Su orden es de 7, puesto que 7(7, 3) = ∞

c) Usar el teorema de Hasse y el orden de (7, 3) para encontrar el orden de $E(Z_{11})$.
El teorema dice que

$$q + 1 - 2\sqrt{q} \leq \#E(F_q) \leq q + 1 + 2\sqrt{q}$$

Entonces

$$11 + 1 - 2\sqrt{11} \leq \#E(Z_{11}) \leq 11 + 1 + 2\sqrt{11}$$

Así

$$5 \leq \#E(Z_{11}) \leq 18$$

Como debe ser un múltiplo del orden del punto (7, 3), entonces este puede ser 7 o 14.

d) Verificar que la cardinalidad de E es igual a $q + 1 + \sum_{x \in Z_{11}} (\frac{x^3+7x+2}{11})$ donde $\frac{x^3+7x+2}{11}$ es el símbolo de Lengendre y q = 11.
Tenemos que

$$q + 1 + \sum_{x \in Z_{11}} (\frac{x^3 + 7x + 2}{11})$$

y así

$$\begin{aligned}\#E(Z_{11}) &= 11+1 \\ &\quad + \left(\frac{2}{11}\right) + \left(\frac{10}{11}\right) + \left(\frac{24}{11}\right) + \left(\frac{50}{11}\right) + \left(\frac{94}{11}\right) + \left(\frac{162}{11}\right) \\ &\quad + \left(\frac{260}{11}\right) + \left(\frac{394}{11}\right) + \left(\frac{570}{11}\right) + \left(\frac{794}{11}\right) + \left(\frac{1072}{11}\right) \\ &= 12 + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + (-1) + 1 + 1 + (-1) + 1 \\ &= 12 + (-5) \\ &= 7\end{aligned}$$

Ejercicio 2

Sea la ecuación $y^2 = x^3 + x + 1$ en Z_{77} y sea el punto P = (0, 1) que satisface la ecuación anterior, calcule 5P sumando de P en P y así encontrar un factor de 77.

$$\begin{aligned}2P = P + P = (0,1) + (0,1) \\ \Rightarrow \lambda = \frac{3(0)^2+1}{2(1)} = \frac{1}{2} mod 77 = 39 \\ \Rightarrow (x_3, y_3) = ((39)^2 - 2(0) mod 77, 39(0-58) - 1 mod 77) \\ 2P = (58, 47) \\ 3P = 2P + P = (58,47) + (0,1) \\ \Rightarrow \lambda = \frac{1-47}{0-58} = \frac{23}{29} mod 77 = 30 \\ \Rightarrow (x_3, y_3) = ((30)^2 - 58 - 0 mod 77, 30(58-72) - 47 mod 77) \\ 3P = (72, 72) \\ 4P = 3P + P = (72,72) + (0,1) \\ \Rightarrow \lambda = \frac{1-72}{0-72} = \frac{71}{72} mod 77 = 32 \\ \Rightarrow (x_3, y_3) = ((32)^2 - 72 - 0 mod 77, 32(72-28) - 72 mod 77) \\ 4P = (28, 27) \\ 5P = 4P + P = (28,27) + (0,1) \\ \Rightarrow \lambda = \frac{1-27}{0-28} \Rightarrow ...\end{aligned}$$

Como necesitamos calcular el inverso de 28, no existe en Z_{77}, puesto que mcd(28, 77) = 7, no son primos entre si, además $1 < 7 < 77$, por lo cual 28, es un factor de 77.

Ejercicio 3

Sea la curva elíptica E dada por$y^2 = x^3 + 13x + 16$ en $\mathbb{Z}_{17}$ hacer:

a) Cálcula y muestra todos los puntos de E

Para poder saber cuantos puntos hay en E, buscamos $\#E(\mathbb{F}_{17})$. Sea el punto (0,13) en la curva, al calcular su orden N obtenemos que $N = 25$. Entonces, de acuerdo al Teorema de Hesse:

$$q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_{17}) \leq q + 1 + 2\sqrt{q}$$

Tenemos entonces

$$17 + 1 - 2\sqrt{17} \leq \#E(\mathbb{F}_{17}) \leq 17 + 1 + 2\sqrt{17}$$

$$18 - 2\sqrt{17} \leq \#E(\mathbb{F}_{17}) \leq 18 + 2\sqrt{17}$$

Donde $\#E(\mathbb{F}_{17})$ debe de ser un múltiplo de N. Por lo tanto, después de resolver la desigualdad:

$$\#E(\mathbb{F}_{17}) = 25$$

Al calcular los puntos obtenemos los siguientes

x	$x^3 + x + 1$	y	Puntos
∞	-	-	∞
0	5	± 4	$(0, 4), (0, 13)$
1	13	± 8	$(1, 8), (1, 9)$
2	16	± 4	$(2, 4), (2, 13)$
4	13	± 8	$(4, 8), (4, 9)$
5	2	± 6	$(5, 6), (5, 11)$
6	4	± 2	$(6, 2), (6, 15)$
7	8	± 5	$(7, 5), (7, 12)$
12	13	± 8	$(12, 8), (12, 9)$
13	2	± 6	$(13, 6), (13, 11)$
14	1	± 1	$(14, 1), (14, 16)$
15	16	± 4	$(15, 4), (15, 13)$
16	2	± 6	$(16, 6), (16, 11)$

Table 1: Tabla de los puntos en E

b) Alicia desea enviar el siguiente mensaje $c = (a, b) = ((6, 2), (14, 1))$ a Bob, los parámetros públicos de Bob son $\alpha = (0, 13) \in E$ una raíz primitiva y $\beta = (15, 13)$ donde $\beta = s\alpha$ y s es su llave privada. Usar cualquier algoritmo mencionado en la sección 5.2 del libro "Elliptic Curves Number Theory and Cryptography de Lawrence C. Washinton" Para resolver el problema del logaritmo discreto.

Usando el método de "**Baby step, Giant Step**".

Sea dentro del algoritmo $G = E(\mathbb{F}_{17})$, P=(0,13), Q=(15,13) y N=25 a lo más de acuerdo a Hesse. Obtenemos:

$$m = 6$$

Enseguida calculamos iP para $1 \leq i < 6$ y obtenemos la lista de puntos.

$$(0, 13), (13, 6), (6, 2), (12, 9), (7, 12)$$

Después calculamos $Q - jmP$ para j=0,1,2,3,4,5

$$j = 0 \Rightarrow Q - 0 = (15, 13)$$
$$j = 1 \Rightarrow Q - 6P = (15, 13) - (1, 9) = (15, 13) + (1, -9) = (0, 13)$$

Donde encontramos que el punto (0,13) coincide con el primer punto de la liste, por lo tanto obtenemos los valores $i = 1$ y $j = 1$. A partir de esto resolvemos $Q = kP$ con $k \equiv i + jm \pmod{N}$ de la forma que $k \equiv 7 \pmod{25}$ y de ahí obtenemos que:

$$(15, 13) = 7P$$

Donde $k = s = 7$

c) A partir de la información encontrada en b) descifra el mensaje.

Para descifrar el mensaje solo tenemos que resolver $x = y_2 - ky_1$ donde $k = s$ que ya habíamos encontrado. Entonces

$$x = (14, 1) - 7(6, 2)$$
$$x = (14, 1) - (12, 8)$$
$$x = (14, 1) + (12, 9)$$

Y el mensaje descifrado es **(7,5)**

Ejercicio 4

Sea E la curva elíptica dada por los puntos que satisfacen la ecuación $y^2 = x^3 + 7x + 19$ en Z_{31} y P = (18, 26) un punto en E de orden 39, el ECIES simplificado definido sobre Z_{31}^* como espacio de texto plano, supongamos que la clave privada es m = 8

a) Calcula Q=mP
Tenemos $m = 8$

$$2P = (28, 23)$$
$$4P = (11, 30)$$
$$8P = (10, 2)$$

Por lo tanto $Q = (10, 2)$

b) Descifra la siguiente cadena de texto cifrado.

$$((4, 1), 1); ((11, 0), 18); ((27, 1), 17); ((28, 1), 29); ((23, 0), 26)$$

Para el primer punto, descomprimimos (4,1).

$$z = (4)^3 + 7(4) + 19$$
$$z = 64 + 28 + 29 = 111 \equiv 18 \pmod{31} \; z = 18$$

Pero nosotros buscamos y que es $\sqrt{z}$ por lo tanto hacemos

$$y = z^{\left(\frac{p+1}{4}\right)} \pmod{p}$$
$$y = z^{\left(\frac{32}{4}\right)} \pmod{31}$$
$$y = 7$$

Como $7 \equiv 1 \pmod 2$, entonces al descomprimirlo es (4,7). Si lo multiplicamos por m, tenemos $8(4,7) = (2,17)$
Al tener este punto, podemos realizar su descifrado como:

$$d_k(y) = y_2(x_0)^{-1} \pmod{31} = 1(2)^{-1} \pmod{31} = 16$$

Si realizamos el mismo proceso para cada punto, al descomprimirlos y descifrarlos, tenemos:

* Para ((11,0), 18) el punto descomprimido es ((11,30),18), el punto a descifrar es (23,3) y el valor obtenido al descifrar es **21**
* Para ((27,1), 17) el punto descomprimido es ((27,19),17), el punto a descifrar es (18,26) y el valor obtenido al descifrar es **13**
* Para ((28,1), 29) el punto descomprimido es ((28,23),29), el punto a descifrar es (29,20) y el valor obtenido al descifrar es **1**
* Para ((23,0), 26) el punto descomprimido es ((23,28),26), el punto a descifrar es (3,25) y el valor obtenido al descifrar es **19**

c) Supongamos que cada texto plano representa un carácter alfabético, convierte el texto plano en una palabra. Usa la asociación (A→1,..z→26) no es considerado como un texto plano o un par ordenado.
De acuerdo a los valores obtenmidos anteriormente, tenemos

$$16 = P$$
$$21 = U$$
$$13 = M$$
$$1 = A$$
$$19 = S$$