

Universidad Nacional
Autónoma de México

Alumno
Cova Pacheco Felipe de Jesús

Profesor
Manuel Díaz Díaz

Ayudante
Gerardo Rubén López Hernández

Tarea
No. 3

Materia
Criptografía y Seguridad

Fecha de entrega
Viernes 30 de Noviembre de 2018

1. Sea la curva elíptica $E: y^2 = x^3 + x + 9$ definida sobre \mathbb{Z}_{17}

i) Calcula y muestra todos los puntos de E .

Los puntos son $\{(2,6), (2,11), (4,3), (4,14), (7,6), (7,11), (8,6), (8,11), (9,4), (9,3), (10,4), (10,13), (11,5), (11,12), (12,7), (12,10), (13,3), (13,14), (14,8), (14,9), (15,4), (15,13), (0,3), (0,14), 0\}$ $\Rightarrow |E| = 25$

Obtenidos ejecutando el código que

hice en R:

```
for (i in 0:16) {  
    w ← j^3 + j + 9  
    for (j in 1:17) {  
        u ← j^2  
        if (u % 17 == w % 17) {  
            print(c(i,j))  
        }  
    }  
}
```

3

ii) Alicia desea enviar el siguiente mensaje $C = (a, b) = ((12, 7)(11, 12))$ a Bob, los parámetros públicos de Bob son $\alpha = (0, 3) \in E$ una raíz primitiva y $B = (13, 3)$, donde $B = s\alpha$ y s su llave privada

Dem: Alicia eligió $M \in E$ como un punto en E tal que represente su mensaje; luego eligió un $k \in \{1, \dots, 16\}$ tal que $M_1 = (12, 7) = k(0, 3)$

$$\text{Después calculó } (11, 12) = M_2 = M + kB = M + k(13, 3)$$

$$\text{Como la curva elíptica es } y^2 = x^3 + x + 9 \Rightarrow \text{si } P = (x_1, y_1)$$

$$\Rightarrow P + P = \left(\frac{(3x_1^2 + a)^2}{2y_1} - 2x_1, -y_1 + \left(\frac{3x_1^2 + a}{2y_1} \right) \left(x_1 - \left(\frac{3x_1^2 + a}{2y_1} - 2x_1 \right) \right) \right)$$

Si la curva elíptica esté dada por $y^2 = x^3 + ax + b$ Donde

$$\therefore \text{Si } x_3 = \left(\frac{3x_1^2 + a}{2y_1} \right)^2 - 2x_1 \quad y_3 = -y_1 + \left(\frac{3x_1^2 + a}{2y_1} \right) (x_1 - x_3)$$

$$\frac{1}{2y_1} \equiv (2y_1)^{-1} \pmod{17}$$

en nuestra curva elíptica $a = 1 \Rightarrow$ si $P + P = (x_3, y_3) \Rightarrow$ como $|E| = 25 \Rightarrow \sqrt{25} = 5$, así por el algoritmo Baby step Giant St. sea $m = 5 \geq \sqrt{5}$, ahora calculemos $n(0, 3)$ para $n \in \{0, 1, \dots, 5-1=4\}$ primero encontremos los inversos de $r \in \mathbb{Z}_{17}^*$ i.e. r^{-1} , para eso ejecutamos el código en R:

```
for(n in 1:16) {
  for(r in 1:16) {
    if ((n*r) %/% 17 == 1) {
      print(c(n,r))
    }
  }
}
```

Así $1^{-1} \equiv_{17} 1$, $2^{-1} \equiv_{17} 9$, $3^{-1} \equiv_{17} 6$, $4^{-1} \equiv_{17} 13$, $5^{-1} \equiv_{17} 7$, $6^{-1} \equiv_{17} 3$, $7^{-1} \equiv_{17} 5$, $10^{-1} \equiv_{17} 16$
 $8^{-1} \equiv_{17} 15$, $9^{-1} \equiv_{17} 2$, $10^{-1} \equiv_{17} 12$, $11^{-1} \equiv_{17} 14$, $12^{-1} \equiv_{17} 10$, $13^{-1} \equiv_{17} 4$, $14^{-1} \equiv_{17} 11$, $15^{-1} \equiv_{17} 8$

$$\text{como } 0(0,3) = (0,3) - (0,3) = 0$$

$$1(0,3) = (0,3)$$

$$2(0,3) = (0,3) + (0,3) \quad y \text{ como } 2(3) = 6 \Rightarrow (2(3))^{-1} = 3$$

$$\text{así } \frac{3(0)^2 + 1}{2(3)} \equiv_{17} (3(0)^2 + 1)(6)^{-1} \equiv_{17} 3 \Rightarrow 2(0,3)(9, -3 + (3)(0 - 9)) = (9, -13) \\ (3)^2 - 2(0) = 9 \quad = (9, 4)$$

Ahora como dada $E := y^2 = x^2 + ax + b$ y si $P = (x_1, y_1)$, $Q = (x_2, y_2)$ con $x_1 \neq x_2$.

$$\Rightarrow \text{si } P+Q = (x_3, y_3) \Rightarrow x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2 = \left[(y_2 - y_1)(x_2 - x_1)^{-1} \right]^2 - x_1 - x_2$$

$$y \quad y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1} \right) (x_1 - x_3) = -y_1 + \left[(y_2 - y_1)(x_2 - x_1)^{-1} \right] (x_1 - x_3)$$

$$\therefore 3(0,3) = (0,3) + (9,4), \text{ como } [(4-3)(9-0)^{-1}]^2 - 0 \cdot 9 = [(1)(9)^{-1}] \cdot 9 = 4 \cdot 9 \equiv_{17} 12$$

$$y \quad -3 + [(4-3)(9-0)^{-1}] (0-12) = -3 + 2(-12) \equiv_{17} -3 + 2(5) = 7 \Rightarrow 3(0,3) = (12, 7)$$

$$\Rightarrow 4(0,3) = (7, 6) \quad (\text{usando la función adjunta})$$

De hecho usando la función vemos que $\boxed{k=3}$ ahora calculemos

$$kB = k(13, 3) \text{ vemos que } kB = 3B = (7, 11), \text{ así } M = (11, 12) - (7, 11)$$

$$\Rightarrow M = (11, 12) + (7, -11) = (14, 9) \text{ así } M = (14, 9)$$

De hecho se encontró que $s=7$ pues $7(0,3) = (13, 3)$

iii) A partir de la información encontrada en ii) Descifra el mensaje enviado a Bob.

De acuerdo a la información encontrada, y usando ElGamal el mensaje es:

$$\begin{aligned} M &= (11, 12) - s(12, 7) = (11, 12) - 7(12, 7) \\ &= (11, 2) - (7, 11) = (11, 12) + (7, 6) \\ &= \underline{\underline{(14, 9)}} \end{aligned}$$

∴ El mensaje original era $M = (14, 9)$

2. Sea $E: y^2 = x^3 - 20x + 21 \pmod{35}$ y sea $P = (15, -4) \in E$

i) Factoriza 35 tratando de calcular $3P$.

Para poder empezar con el procedimiento, primero se tiene que calcular $2P$, como sigue:

$$m = \frac{3(15^2) - 20}{2(-4)} = \frac{25}{27} = 25(13) = 10 \pmod{35}$$

$$x = 10^2 - 30 = 0 \pmod{35}$$

$$y = 10(15) + 4 = 14 \pmod{35}$$

$$\therefore \underline{2P = (0, 14)}$$

Así entonces, ahora es posible comenzar con el cálculo de $3P$. Se puede ver de la siguiente manera:

$$3P = 2P + P$$

$$\text{y tenemos que } m = \frac{14 - (-4)}{-5} = \frac{18}{20}$$

Aquí hay un detalle notable, ya que al tratar de calcular el inverso multiplicativo de $20 \pmod{35}$, no es posible, debido a que el máximo común divisor entre $(20, 35) = 5$. Lo que queremos decir es que no son primos relativos, por lo tanto no podemos calcular su inverso, pero así lo que hicimos fue obtener un factor de 35, el cual fue 5.

ii) Factoriza 35 tratando de calcular 4P duplicándolo

Si lo que queremos es calcular 4P, lo podemos ver de la siguiente manera: $4P = 2P + 2P$.

Recapitulando el ejercicio anterior, obtuvimos que $2P = (0, 14)$ y así $m = \frac{-20}{2(14)} = \frac{15}{28}$

De una manera similar a la del ejercicio anterior, sucede que en el intento de calcular el inverso multiplicativo de 28 mod 35, surge el inconveniente de que 28 y 35 no son primos relativos, debido a que el máximo común divisor de $(28, 35) = 7$.

De esta forma se hace evidente otro factor de 35

iii) Calcula ambos $3P$ y $4P$ sobre $E(\text{mod } 5)$ y sobre $E(\text{mod } 7)$ explica porqué el factor 5 se obtiene calculando $3P$ y el factor 7 se obtiene calculando $4P$.

3. Alicia quiere firmar un mensaje utilizando el esquema ElGamal elíptico con los siguientes parámetros: $p=314159$, $a=217$, $b=2006$, $P=(123456, 43989)$, $n=314423$. Su clave privada es $d=223344$ y su clave pública es $Q=(216438, 187612)$.

i) Si el mensaje que quiere firmar es $m=6500$ (cantidad de pesos que quiere retirar de su cuenta mediante una transferencia bancaria) ¿Cuál es la firma digital de m ? Supongamos que el entero aleatorio k tal que $1 \leq k \leq n-1$ que se tiene que esoger es igual a 666.

R. Sabemos que $k=666$ y que es primo relativo con 314423 entonces obtenemos $R=(2939, 140788)=666P$

Enseguida, hacemos el cálculo de s , que es:

$$s = (666)^{-1} * (6500 - 217f(R)) \bmod 314423$$

Por lo tanto, la firma queda como $(6500, (2939, 140788), 205063)$.

ii) ¿Qué computos tiene que hacer el banco para verificar la firma de Alicia?

Lo que el banco tendría que hacer, sería calcular V_1 y V_2 y verificar si $V_1 = V_2$, entonces la firma es correcta.

Donde V_1 y V_2 son:

$$\begin{aligned} V_1 &= f(R)Q + sR = 2939Q = (203478, 24120) + (99360, 230917) \\ &= (283710, 77429) \end{aligned}$$

$$V_2 = 6500P = ((283710, 77429))$$

Por lo tanto, la firma es correcta.

4. Sea $E: y^2 = x^3 + 333x + 2$ sobre \mathbb{F}_{347} y sea $P = (110, 136)$

(a) Si sabemos que $|E| = 358$. ¿Podemos decir que E es criptográficamente útil? ¿Cuál es el orden de P ? ¿Entre qué valores se puede escoger la clave privada?

• No tomaría esta curva como criptográficamente útil, debido a que el número de elementos en ella es muy pequeño, lo cual claramente haría que utilizando cualquier sistema criptográfico, solo se necesitarían 358 operaciones para romperlo, tomando en cuenta lo mencionado en clase, que calcular el múltiplo de cada punto nos toma tiempo constante, de ahí se obtienen las 358 operaciones.

• El orden de P debe dividir el orden de 358 (del grupo), así tomado en cuenta del teorema de Lagrange donde nos dice que "el orden de P debe dividir al orden del grupo". Así se sigue que el orden n de P debe ser 1 o 2 o 179. Debido a que 358 se factoriza como $2(179)$.

Pero es más que evidente que P no es el neutro del grupo, y por el orden, no es 1.

Por otra parte, $2P = (260, 260)$, así que tampoco es el neutro. Así que en consecuencia, el orden de P es $n=179$ y la clave privada puede ser libre a escoger en el intervalo $[2, 178]$

(b) Si tu clave privada es $d=101$ y algún conocido te ha enviado el mensaje cifrado ($C_1 = (232, 278)$, $C_2 = (135, 214)$) ¿Cuál era el mensaje original?

$$\begin{aligned} \text{Se tiene que } C &= C_2 - sC_1 = (135, 214) - 101(232, 278) \\ &= (135, 214) - (275, 176) \\ &= (135, 214) + (275, 171) \\ &= (74, 87) \end{aligned}$$

∴ El mensaje original
era $(74, 87)$

□

5. Sea $\mathbb{E} : y^2 = x^3 + 2x + 7$ sobre \mathbb{Z}_{31} con $\#\mathbb{E} = 39$ y $P = (2, 9)$ es un punto de orden 39 sobre \mathbb{E} , el ECIES simplificado definido sobre \mathbb{E} tiene \mathbb{Z}_{31}^* como espacio de texto plano, supongamos que la clave privada es $m = 8$

(a) Calcula $Q = mP$

$$Q = mP = 8(2, 9) = (8, 15)$$

~~✓~~

(b) Descifra la siguiente cadena de texto cifrado

$$(18, 1, 2), ((3, 1), 18), ((17, 0), 19), ((28, 0), 8)$$

Dividamos la cadena de texto cifrado para su mayor comprensión. Empecemos con:

• $(18, 1, 2)$

$$\text{Se calcula } 18^3 + 2(18) + 7 \equiv 16 \pmod{31}$$

$$\Rightarrow z = 4 \text{ ó } z = -4 \equiv 27 \pmod{31}$$

sabemos que $27 \equiv 1 \pmod{2}$, entonces dado que $z = 27$

así obtenemos el punto $(18, 27)$ y $8(18, 27) = (15, 8)$

$$\therefore x = 15, \text{ además } 21(15)^{-1} \equiv 21(29) \equiv 20 \pmod{31}$$

Así obtenemos que el primer carácter es 20.

• $((3, 1), 18)$

$$\text{Se calcula } 3^3 + 2(3) + 7 \equiv 9 \pmod{31}, \text{ entonces}$$

$$z = 3 \text{ ó } z = -3 \equiv 28 \pmod{31}, \text{ y como } 3 \equiv 1 \pmod{2},$$

tengemos que $z = 3$. De esta manera, el punto es $(3, 3)$ y asimismo, obtenemos que $8(3, 3) = (2, 9)$.

$\therefore x = 2$, por lo que conseguimos que

$$18(2^{-1}) \equiv 18(16) \equiv 9 \pmod{31}, \text{ es decir,}$$

el segundo carácter es 9.

- $((17,0), 19)$

Se calcula $17^3 + 2(17) + 7 = 25 \pmod{31}$

por lo que $z=5$ o $z=-5 = 26 \pmod{31}$, y como $26=0 \pmod{2}$ obtenemos que $z=26$. De esta forma el punto obtenido es $(17, 26)$ y de aquí sacamos que $8(17, 26) = (30, 29)$ así $x=30$, por lo que $19(30^{-1}) = 19(30) = 12 \pmod{31}$ así concluimos que el tercer carácter es 12.

- $((28,0), 8)$

Calculamos $28^3 + 2(28) + 7 = 5 = 36 \pmod{31}$, así $z=6$ ó $z=-6 = 25 \pmod{31}$, y como $6=0 \pmod{2}$, obtenemos que $z=6$

De esta forma, el punto obtenido es $(28, 6)$ y de aquí sacamos que $8(28, 6) = (14, 19)$, por lo que $x=14$
 $\therefore 8(14^{-1}) = 8(20) = 5 \pmod{31}$

y así el último carácter es 5

\therefore El mensaje quedaría $(20, 9, 12, 15)$

c) Supongamos que cada texto plano representa un carácter alfabético, convierte el texto plano en una palabra en inglés.
 Usa la asociación $(A \rightarrow 1, \dots, Z \rightarrow 26)$ en este caso, O no es considerado como un texto plano o un par ordenado.

B. Usando la asociación brindada, el mensaje obtenido sería "Tite" que significa azulejo.