Universidad Nacional Autónoma de México

Facultad de Ciencias

Criptografía y Seguridad

Tarea 8: Curvas Elípticas

Fecha de entrega: 30/11/2023

Equipo:

Criptonianos

Acosta Arzate Rubén - 317205776

Bernal Marquez Erick - 317042522

Deloya Andrade Ana Valeria - 317277582

Marco Antonio Rivera Silva - 318183583

1. Escoge parámetros a y b adecuados para definir la curva elíptica $E_{17}(a, b)$

Para la curva E_{17} los a, b deben cumplir:

$4a^3 + 27b^2 \ncong 0 \bmod 17$

Por lo que tomamos $a = 5$ y $b = 4$

$4(5)^3 + 27(4)^2$

$4(125) + 27(16)$

$500 + 432 = 932$

$932 \bmod 17 \cong 14 \bmod 17$

$\therefore 4a^3 + 27b^2 \ncong 0 \bmod 17$

Nuestros parametros son adecuados

$y^2 = x^3 + 5x + 4 \pmod{17}$

2. Da todos los puntos de la curva anterior.

Con ayuda del siguiente colab obtuvimos los siguientes puntos

{(0,2), (0,15), (5,1), (5,16), (7,5), (7,12), (9,8), (9,9), (10,0), (10,17), (11,8), (10,9), (14,8), (14,9), (16,7), (16,10)}

3. Cifra un mensaje con dicha curva y dichos puntos.

Nuestra curva es: $E_{17}(a, b) = E_{17}(5, 4)$

Además vamos a tener nuestro punto $G = (0, 2)$, y $k = 2$.

El mensaje a cifrar es $P_m = (0, 15)$ y la llave publica como $P_p = (5, 1)$

Ahora sustituimos en: $\{kG, P_m + kP_p\} = \{2(0, 2), (0, 15) + 2(5, 1)\}$

Con ayuda del siguiente colab obtuvimos que el cifrado es: $\{(9, 8), (16, 7)\}$

4. Construye el campo finito con 8 elementos. Reporta sus tablas de suma y resta. Utiliza este polinomio: $x^3 + x + 1$.

Sea el campo $GF(2^3)$ cambiamos α como raíz, por lo que tenemos $\alpha^3 + \alpha + 1$, cuyos elementos son: $0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1$

La tabla de la suma

+	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
1	1	0	$\alpha+1$	α	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$
α	α	$\alpha+1$	0	1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1
$\alpha+1$	$\alpha+1$	α	1	0	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2
α^2	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	0	1	α	$\alpha+1$
α^2+1	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	1	0	$\alpha+1$	α
$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1	α	$\alpha+1$	0	1
$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2	$\alpha+1$	α	1	0

Figura 1: Tabla de la suma

La tabla de la resta

-	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
1	1	0	$\alpha+1$	α	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$
α	α	$\alpha+1$	0	1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1
$\alpha+1$	$\alpha+1$	α	1	0	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2
α^2	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	0	1	α	$\alpha+1$
α^2+1	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	1	0	$\alpha+1$	α
$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1	α	$\alpha+1$	0	1
$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2	$\alpha+1$	α	1	0

Figura 2: Tabla de la resta

Como podemos notar ambas tablas son idénticas, esto se debe a la congruencia sobre $\mathbb{Z}_2$

5. Escoge parámetros a y b adecuados para definir la curva elíptica $E_{2^3}(a, b)$.

Para que la curva $E_{2^3}(a, b)$ sea valida se debe cumplir:

$4a^3 + 27b^2 \ncong 0 \text{ mod } 2^3$

Por lo que con $E_{2^3}(3, 5)$ tenemos:

$4(3)^3 + 27(5)^2$

$4(27) + 27(25)$

$108 + 675$

$783 \text{ mod } 2^3$

$783 \text{ mod } 8 = 7$

$\therefore$ a=3 y b=5 son validos