Universidad Nacional Autónoma de México

Facultad de Ciencias

Criptografía y Seguridad

Tarea 3

Curvas elípticas y seguridad

Profesor:

Manuel Díaz Díaz

Integrantes:

Lázaro Pérez David Jonathan

Licona Gómez Aldo Daniel

Marín Parra José Guadalupe de Jesús

1. Dada la curva $y^2 = x^3 + x + 1 \ mod\ 103$ y el punto $(6, 29)$ aplique el teorema de Hasse o el teorema con que se obtiene el orden del grupo, para obtener el orden del grupo de puntos de la curva y obtenga todos sus puntos.

   Solución.

x	$x^3 + x + 1 \ mod\ 103$	R.C	y
$x = 0$	1,0	si	$(\sqrt{1,0}, 103 + (-\sqrt{1,0})$
$x = 5$	28,0	si	$(\sqrt{131,0}, 103 + (-\sqrt{131,0})$
$x = 6$	17,0	si	$(\sqrt{223,0}, 103 + (-\sqrt{223,0})$
$x = 9$	18,0	si	$(\sqrt{739,0}, 103 + (-\sqrt{739,0})$
$x = 11$	4,0	si	$(\sqrt{1343,0}, 103 + (-\sqrt{1343,0})$
$x = 12$	93,0	si	$(\sqrt{1741,0}, 103 + (-\sqrt{1741,0})$
$x = 14$	81,0	si	$(\sqrt{2759,0}, 103 + (-\sqrt{2759,0})$
$x = 18$	83,0	si	$(\sqrt{5851,0}, 103 + (-\sqrt{5851,0})$
$x = 19$	81,0	si	$(\sqrt{6879,0}, 103 + (-\sqrt{6879,0})$
$x = 21$	13,0	si	$(\sqrt{9283,0}, 103 + (-\sqrt{9283,0})$
$x = 25$	98,0	si	$(\sqrt{15651,0}, 103 + (-\sqrt{15651,0})$
$x = 26$	93,0	si	$(\sqrt{17603,0}, 103 + (-\sqrt{17603,0})$
$x = 27$	38,0	si	$(\sqrt{19711,0}, 103 + (-\sqrt{19711,0})$
$x = 29$	8,0	si	$(\sqrt{24419,0}, 103 + (-\sqrt{24419,0})$
$x = 31$	56,0	si	$(\sqrt{29823,0}, 103 + (-\sqrt{29823,0})$
$x = 35$	63,0	si	$(\sqrt{42911,0}, 103 + (-\sqrt{42911,0})$
$x = 36$	34,0	si	$(\sqrt{46693,0}, 103 + (-\sqrt{46693,0})$
$x = 37$	15,0	si	$(\sqrt{50691,0}, 103 + (-\sqrt{50691,0})$
$x = 41$	56,0	si	$(\sqrt{68963,0}, 103 + (-\sqrt{68963,0})$
$x = 45$	16,0	si	$(\sqrt{91171,0}, 103 + (-\sqrt{91171,0})$
$x = 48$	19,0	si	$(\sqrt{110641,0}, 103 + (-\sqrt{110641,0})$
$x = 50$	9,0	si	$(\sqrt{125051,0}, 103 + (-\sqrt{125051,0})$
$x = 52$	66,0	si	$(\sqrt{140661,0}, 103 + (-\sqrt{140661,0})$
$x = 54$	32,0	si	$(\sqrt{157519,0}, 103 + (-\sqrt{157519,0})$
$x = 56$	58,0	si	$(\sqrt{175673,0}, 103 + (-\sqrt{175673,0})$
$x = 62$	49,0	si	$(\sqrt{238391,0}, 103 + (-\sqrt{238391,0})$
$x = 65$	93,0	si	$(\sqrt{274691,0}, 103 + (-\sqrt{274691,0})$
$x = 69$	9,0	si	$(\sqrt{328579,0}, 103 + (-\sqrt{328579,0})$
$x = 70$	81,0	si	$(\sqrt{343071,0}, 103 + (-\sqrt{343071,0})$
$x = 71$	58,0	si	$(\sqrt{357983,0}, 103 + (-\sqrt{357983,0})$
$x = 72$	49,0	si	$(\sqrt{373321,0}, 103 + (-\sqrt{373321,0})$
$x = 73$	60,0	si	$(\sqrt{389091,0}, 103 + (-\sqrt{389091,0})$
$x = 74$	97,0	si	$(\sqrt{405299,0}, 103 + (-\sqrt{405299,0})$
$x = 75$	63,0	si	$(\sqrt{421951,0}, 103 + (-\sqrt{421951,0})$
$x = 78$	7,0	si	$(\sqrt{474631,0}, 103 + (-\sqrt{474631,0})$
$x = 79$	58,0	si	$(\sqrt{493119,0}, 103 + (-\sqrt{493119,0})$
$x = 80$	68,0	si	$(\sqrt{512081,0}, 103 + (-\sqrt{512081,0})$
$x = 82$	92,0	si	$(\sqrt{551451,0}, 103 + (-\sqrt{551451,0})$
$x = 83$	15,0	si	$(\sqrt{571871,0}, 103 + (-\sqrt{571871,0})$
$x = 86$	15,0	si	$(\sqrt{636143,0}, 103 + (-\sqrt{636143,0})$
$x = 87$	9,0	si	$(\sqrt{658591,0}, 103 + (-\sqrt{658591,0})$
$x = 96$	63,0	si	$(\sqrt{884833,0}, 103 + (-\sqrt{884833,0})$
$x = 99$	36,0	si	$(\sqrt{970399,0}, 103 + (-\sqrt{970399,0})$

Por lo que esos serian los puntos de la curva siendo x el valor x del punto e y uno de los valores de y por ejemplo cuando x = 0 tenemos los puntos (0,1) y (0,102) y asi con todas las x de la tabla, por lo que tenemos que la curva tien 86 puntos.

Entonces aplicando el terema de hasse tenemos que el orden de la curva esta entre $83 \leq \#E(103) \leq 124$
y como el numero de puntos es 86 tenemos que el orden es 86 que cumple con $83 \leq 86 \leq 124$

2. Dada la curva $y^2 = x^3 + x + 1 \ mod\ 10403$, encuentre el factor de 10403.

   Solución. Para encontrar el factor, tomemos el punto $P(1, 1)$. La pendiente de la recta tangente en algún punto $A = (x, y)$ es $s = \frac{3x^2+1}{2y(mod\ 10403)}$, utilizando s podemos calcular 2 A. Si el valor de s es de la forma a/b donde $b>1$ y $mcd(a, b) = 1$, tenemos que encontrar el inverso modular de b. En caso de que no exista, entonces el $mcd(n, b)$ es un factor no trivial de n.

   Ahora calculamos $2P$, en donde tenemos $s(P) = s(1, 1) = 4$ y cuyas coordenadas de $2P = (x', y')$ son $x' = s^2 - 2x = 14 y y' = s(x - x') - y = 4(1 - 14) - 1 = -53$ en los cuales se entienden todos los números de mod 10403. Para comprobar que $2P$ esté en la curva $(-53)^2 = 2809 = 14^3 + 5 \cdot 14 - 5$ haremos lo siguiente.

   Calculando $3(2P)$ tenemos que $s(2P) = s(14, -53) = \frac{-593}{106(mod\ 10403)}$. Usando el algoritmo euclidiano tenemosque $10403 = 101 \cdot 103$, después para $101 = 101$ y para $103 = 103$. Por lo tanto el $mcd(10403, 101) = 101$.

   Por lo que da como resultado la factorización de la curva en el factor 10403.

3. Dada la curva $y^2 = x^3 + x + 4 \ mod\ 53$ y la curva $y^2 = x^3 + 16x + 11 \ mod\ 53$, muestre que son isomorfas y dé el isomorfismo.

   Solución. Por las curvas tenemos que la isogenía es de la forma $\phi = (u(x), v(x) + \lambda y)$ con polinomios de grado un y con λ una constante.

   Como las curvas son isomorfas, entonces existe una isogenía invertible de la forma $\phi : E_1 \to E_2$ de la forma $\phi(x, y) = (u(x), v(x) + \lambda y)$ con u y v de grado 1. Dado que se produce lo anterior entonces decimos que v es nulo, por lo que queda $\phi(x, y) = (u(x), \lambda y)$. De igual manera la inversa de ϕ digamos $\psi : E' \to E$ toma la forma $\psi(t, s) = (U(t), \sigma s)$ en donde U es un polinomio de primer grado y por tanto $\phi : E_1 \to E_2$ como isomorfismo.

4. Sea la curva $y^2 = x^3 + x + 1 \ mod\ 71$ y el punto $P = (18, 61)$ encuentre m tal que $mP = (59, 6)$.

   Dado el cifrado de Ecies con parámetros $E(y^2 = x^3 + x + 1, (18, 61), m, (59, 6), 71)$, descifre el siguiente mensaje. Los caracteres son tomados módulo 26, es decir, $a = 0 = 26$, $b = 1, ...,\ z = 25$:
   $((23, 0)52), ((4, 0)44), ((58, 1)13), ((65, 0)11), ((9, 1)63), ((41, 0)55), ((30, 0)21)$.

   Solución.

5. Describa tres ataques cibernéticos y en qué consiste el computo forense.

   Solución.

   - XSS. Un ataque Cross Site Scripting se da gracias a una vulnerabilidad de seguridad en la cual un atacante puede inyectar código malicioso en un sitio web. El código inyectado es ejecutado por las víctimas y permite eludir los controles de acceso haciéndose pasar por usuarios.

- SQL Injection. Realizado por medio de una Aplicación Web mediante los campos de formularios de acceso, registro o búsqueda que explota los errores y vulnerabilidades de una página web. Comúnmente es utilizado para acceder a las bases de datos y robar, manipular o destruir la información.
- Whaling. Ataques dirigidos a perfiles C-Level (CEO, CMO, CFO, CIO y demás) con el objetivo de robarles credenciales de alto nivel, información crítica o clonar sus identidades para Phising, entre otros fines maliciosos.

El cómputo forense es la aplicación de técnicas informáticas que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal en contra de un ciber atacante. El cómputo forense sirve para.

- La persecución y procesamiento judicial de los criminales.
- La creación y aplicación de medidas para prevenir casos similares.
- Asegurar la protección adecuada de los datos.
- Minimizar las pérdidas de las organizaciones o individuos relativas a incidentes de seguridad.