CURVAS ELÍPTICAS APLICADAS A LA CRIPTOGRAFÍA.

COLOQUIO DE ORIENTACIÓN MATEMÁTICA.

14-septiembre-2021.

Manuel Díaz Díaz

mandiaz@ciencias.unam.mx

ANTECEDENTES:

El objetivo principal de la criptografía es la transmisión de información confidencial a través de un canal inseguro. Ya desde la antigüedad una de las preocupaciones era el intercambio de mensajes de forma privada, sobre todo en el contexto de asuntos bélicos, políticos y financieros.

En los 70's aparecen varios algortimos y protocolos para tratar de aumentar la seguridad en el intercambio de información, basados principalmente en ciertos problemas matemáticos considerados difíciles de resolver. Así se comenzaron a adaptar diferentes herramientas matemáticas que en principio no tenían relación con la Criptografía para intentar desarrollar algoritmos, sistemas y protocolos difíciles de comprometer. Un ejemplo de esto es la introducción en los sistemas criptográficos de **curvas elípticas**.

La criptografía de curvas elípticas es un tipo específico de la Criptografía de llave pública (asimétrica), que utiliza diferentes problemas matemáticos para generar una clave pública y otra privada con las que se realizan operaciones. En el caso particular de las curvas elípticas, su utilización en algoritmos Criptográficos fue propuesta por primera vez en 1987 por Victor Miller y Neal Koblitz.

ORIGEN:

Las Curvas Elípticas, aparecen indirectamente en **Aritmética** de Diofanto de Alejandría (Siglo III A.C.) Mucho después, en 1994 Andrew Wiles las empleó para probar el último Teorema de Fermat; hoy en día son el ingrediente fundamental en uno de los problemas más importantes en matemáticas, y también un instrumento básico para la criptografía.

- Las curvas Elípticas no son elipses.

- Tienen Relación con la integral elíptica.

¿QUÉ ES UNA CURVA ELÍPTICA?

Una curva elíptica sobe un campo K es una curva algebraica que esta dada por una ecuación del tipo

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5,\ con\ a_i \in \mathbb{K}\ y\ \triangle \neq 0$$

llamada **ecuación general de Weierstrass** donde $\triangle$ es el discriminante de la ecuación, donde

$$\triangle = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6$$

$$d_2 = a_1^2 + 4a_2$$

$$d_4 = 2a_4 + a_1a_3$$

$$d_6 = a_3^2 + 4a_6$$

$$d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$

FORMA REDUCIDA DE UNA CURVA ELÍPTICA:

Definición: Para un campo K con identidad multipliactiva 1 la **Característica** denotada $Car(K)$ se define como el entero positivo mas pequeño r tal que: $1+1+...+1=0$, r veces.

En consecuencia de la definición los campos $\mathbb{Q}$ (Racionales), $\mathbb{R}$ (Reales), $\mathbb{C}$ (Complejos) tienen característica 0. Para un número primo p, el campo finito $\mathbb{Z}_{p^n}$ tiene característica p.

Si la característica de un campo $\mathbb{F}_p$ es distinta de 2 y 3, usando transformaciones lineales en **la ecuación general de Wierstrass**, la ecuación de la curva se puede reducir a:

$$y^2 = x^3 + ax + b, a\ b\ \in \mathbb{F}_{q.}$$

Llamada **ecuación reducida de Weierstrass**, con discriminante $\triangle = 4a^3 + 27b^2 \neq 0$ para que la curva sea **no singular,** es decir no hay puntos en la curva que tengan 2 o más tangentes distintas.

ALGUNOS EJEMPLOS DE CURVAS:

Singulares: $\triangle = 0$
$y^3 = x^3$
`https://www.desmos.com/calculator/boqqcruvtg`

$y^2 = x^3 - 3x + 2,$
`https://www.desmos.com/calculator/gtwujh46ty`

No singulares: $\triangle \neq 0$

$y^2 = x^3 - 10x + 9$
`https://www.desmos.com/calculator/cf1uji6eho`

$y^3 = x^3 - 2x + 3$
`https://www.desmos.com/calculator/wgrpegzzwe`

ESTRUCTURA DE GRUPO EN CURVAS ELÍPTICAS:

Un detalle interesante sobre las curvas elípticas es que se puede definir sobre ellas una operación $+$ de forma que $(E, +)$ sea un grupo conmutativo, con elemento identidad el punto $\mathcal{O}$. Para definir esta operación, supondremos por un momento que $K = \mathbb{R}$, y entenderemos que el punto del infinito se encuentra al principio y al final del eje Y. Podemos pensar entonces que que una recta vertical siempre interseca a E al menos en el punto $\mathcal{O}$.

Dados dos puntos $P = (x_1, y_1)$ y $Q = (x_2, y_2)$ con $P, Q \in E$, consideramos la recta que los une y llamamos R a la otra intersección de dicha recta con la curva E. Entonces, definimos $P + Q$ como el punto reflejado de R con respecto al eje X, al que llamaremos $-R$.

`https://www.desmos.com/calculator/x8nx6uyol3`

CASOS PARTICULARES DEL MÉTODO:

1. Si $P = \mathcal{O}$ tendremos que la recta que une P y Q es vertical, luego intersecta a la curva en el punto reflejado de Q, es decir, $\mathcal{O} + Q = -(-Q) = Q$. Aquí el punto $\mathcal{O}$ actúa como elemento identidad para la operación $+$.

2. Consideremos $P, Q \neq \mathcal{O}$. Abordamos primero el caso en el que $x_1 \neq x_2$. Entonces, la recta que une P y Q tiene pendiente

$$m = \frac{y_2 - y_1}{x_2 - x_1},$$

   y veremos que corta a la recta en otro punto R que permite aplicar el procedimiento general para calcular $P + Q$.

3. Si $Q = P$ con segunda coordenada no nula, no podemos considerar la recta que los une, pero la aproximamos por la recta tangente a E en el punto P. Es decir, tomando $y = y(x)$ en la expresión de la curva, podemos derivar implícitamente y obtener la pendiente de la recta tangente:

$$2yy' = 3x^2 + a \implies m = \frac{3x_1^2 + a}{2y_1}.$$

   La recta tangente corta a la curva en otro punto y podremos aplicar el procedimiento general, calculando el valor de $P + P$.

4. Si $Q = -P$, como las curvas son simétricas respecto al eje X no hay otra posibilidad. Así, la recta que une P y $-P$ es vertical, corta a la curva en $\mathcal{O}$, y por tanto $P + (-P) = -\mathcal{O} = \mathcal{O}$, obteniendo que el elemento inverso de un punto P es su reflejado $-P$.

CURVAS ELÍPTICAS MÓDULO UN PRIMO:

Las Curvas Elípticas sobre $\mathbb{Z}_p$, se pueden definir de la misma manera que en los reales y la operación de SUMA tambien se puede definir de la misma forma, las operaciones en $\mathbb{R}$ son reemplazadas por las operaciones análogas en $\mathbb{Z}_p$.

Definición: Sea $p > 3$ un número primo, la curva elíptica $E : y^2 = x^3 + ax + b$ sobre $\mathbb{Z}_p$ es el conjunto de soluciones $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$, donde $a,\ b \in \mathbb{Z}_p$ son constantes tal que $4a^3 + 27b^2 \neq 0\ (mod\ p)$ junto con un punto especial $\mathcal{O}$ llamado el punto al infinito.

Dicho de otra forma

$$E(\mathbb{F}_p) = \{(x, y) \in \mathbb{Z}_p^2 | y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

SUMA DE PUNTOS EN E:

La suma de puntos esta definida de la siguiente manera:
Sea $P = (x_1, y_1)$ y $Q = (x_2, y_2)$ puntos sobre E, si $x_2 = x_1$ y $y_2 = -y_1$ entonces $P + Q = \mathcal{O}$, en otro caso $P + Q = (x_3, y_3)$, donde

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

y

$$\lambda = \begin{cases} \dfrac{(y_2 - y_1)}{(x_2 - x_1)}\ si\ P \neq Q. \\ \\ \dfrac{3x_1^2 + a}{2y_1}\ si\ P = Q. \end{cases}$$

- λ es la pendiente correspondiente a los puntos P y Q

PAPEL DE LA NIST:

El Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés, National Institute of Standards and Technology), es una agencia de la Administración de Tecnología del Departamento de Comercio de los Estados Unidos. La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología.

ESQUEMAS CRIPTOGRÁFICOS CON CURVAS ELÍPTICAS:

- $ECDSA$ Firma digital.(Bitcoin, Voto electrónico, Streaming de datos Netflix, HBO.)
- $ECDH$ Intercambio de llaves seguras.
- TLS (Seguridad de la capa de transporte) Para conexiones *https* Proceso de establecimiento de sesión segura.
- $ECIES$ Cifrado y Descifrado.

ESQUEMA DE CIFRADO INTEGRADO DE CURVAS ELÍPTICAS: ECIES

Es un esquema de cifrado híbrido que proporciona seguridad semántica (un criterio para evaluar la seguridad en un cifrado de clave asimétrico) contra texto sin formato y cifrado elegido ataques de texto, ECIES utiliza diferentes tipos de funciones:

1. Función de acuerdo de claves
2. Función de derivación de claves
3. Esquema de cifrado simétrico
4. Función Hash.

La idea de este cripsistema fue propuesto por M. Bellare y P. Rogaway.

OBSERVACIONES:

VENTAJAS.

1. Mayor flujo de datos.
2. Llaves mas cortas por ejemplo RSA(15360 bits) versus CCE (512 bits) y mismo nivel de seguridad.
3. Se conjetura que un cifrado con CE de 224 bits (equivalente a un RSA de 2018 bits) soportaria un ataque cuantico de entre 4,000 y 10,000 qubits.

DESVENTAJAS

1. Difícil de implementar.
2. Aumenta la probabilidad de errores de implementación.

ALGUNOS RESULTADOS IMPORTANTES

TEOREMA DE HASSE.

Este teorema nos permite aproximar el número de elementos que tiene el grupo que forma una curva elítica E.

Sea E una curva elíptica sobre un campo finito $\mathbb{F}_q$, entonces el orden de $E(\mathbb{F}_q)$ satisface

$$|q + 1 - \#\mathbb{F}_q| \leq 2\sqrt{q}$$

EL ORDEN DE UN PUNTO.

El orden de un punto P es el entero positivo k mas pequeño tal que $kP = \mathcal{O}$

EL PLD O LOGARITMO EÍPTICO.

Dados dos puntos P y Q en el Grupo aditivo de la curva E, encontrar un entero k tal que $kP = Q$

• En casos reales k será muy grande y este ataque sera computacionalmente imposible.

*

PUNTO DE COMPRESIÓN:
Esta operación puede ser expresada como sigue:

$$Punto\ Comprimido : E \setminus \{\mathcal{O}\} \to \mathbb{Z}_p \times \mathbb{Z}_2$$

La cual definimos como $Punto\ de\ Compresion(P) = (x, y\ mod\ 2)$, donde $P = (x, y) \in E$.

Esta idea reduce el almacenamiento de los puntos en E y tambien reduce el costo requerido para calcular la coordenada de y de P al menos un 50%.

La operación inversa al punto de compresión, es el **punto de descompresión,** esta nos ayuda a reconstruir el punto $P = (x, y)$ de E a partir de $(x, y\ mod\ 2)$ y para ello usamos el siguiente algoritmo.

Algoritmo Para descomprimir un punto (x, i)
$z \leftarrow x^3 + ax + b\ mod\ p$ si z no es RC mod p
entonces regresa (error)

$$\text{En otro caso} \begin{cases} y \leftarrow \sqrt{z}\ mod\ p \\ Si\ y\ \equiv\ i\ mod\ 2 \\ entonces\ regresa\ (x, y) \\ De\ otro\ modo\ regresa\ (x, p - y). \end{cases}$$

El valor de $\sqrt{z}$ lo podemos calcular como $z^{\frac{p+1}{4}}\ mod\ p$ siempre que $p \equiv 3\ mod\ 4$ y z es un RC $mod\ p$ o $z = 0$.

CRIPTOSISTEMA ECIES SIMPLIFICADO

Sea E una Curva Elíptica sobre $\mathbb{Z}_p$ con $p > 3$ tal que E contiene un subgrupo cíclico $H =< P >$ de orden primo n en el cual el PLD sea dificil de resolver.

Sea $\mathcal{P} = \mathbb{Z}_p^*$, $\mathcal{C} = (\mathbb{Z}_p \times \mathbb{Z}_2) \times \mathbb{Z}_p^*$ y definimos $\mathcal{K} = \{(E, P, m, Q, n) : Q = mP\}$
Los valores P, Q Y n son la llave pública y $m \in \mathbb{Z}_n^*$ es la llave privada.

Para $x \in \mathbb{Z}_p^*$ definimos

$$K = (E, P, m, Q, n)$$

Para un número secreto aleatorio $k \in \mathbb{Z}_n^*$ y para $x \in \mathbb{Z}_p^*$.

Definimos

$$e_k(x, k) = (Punto\ Comprimido(kP), xx_o\ mod\ p)$$

donde $kQ = (x_0, y_0)$ y $x_0 \neq 0$.

Para un texto cifrado $y = (y_1, y_2)$, donde $y_1 \in \mathbb{Z}_p \times \mathbb{Z}_2$ y $y_2 \in \mathbb{Z}_p^*$.

Definimos

$$d_k(y) = y_2(x_0)^{-1}\ mod\ p$$

donde $(x_0, y_0) = m$ es el Punto de Descompresión.

EJEMPLO DE DESCIFRADO ECIES:

Sea E la curva $y^2 = x^3 + x + 14$ definida sobre Z_{31}, con $\#E = 39$ y $P = (8, 21)$ es un elemento de orden $39 \in E$ el cual es un generador del grupo cíclico. El ECIES definido sobre E tiene $\mathbb{Z}_{31}^*$ como espacio de texto plano

ver `https://www.desmos.com/calculator/bmhl0sizpx`
Descifra el siguiente mensaje:

((9, 1), 2), ((19, 0), 10),((29, 1), 24),((12, 1), 24),((0, 1), 19),((24, 1), 13), ((9, 1), 15), ((19, 0), 1),((29, 1), 17),((24, 1), 20),((0, 1), 16),((27, 0), 4),((0, 1), 29).

Suponiendo que llave privada es: $m = 8$.
Si cada texto plano representa un caracter del alfabeto, convertir el texto plano en palabras del español, usando la correspondencia $A = 1, B = 2, ..., Z = 26$.

OPERACONES:
como $m = 8$ y $P = (8, 21)$ primero tenemos que calcular $Q = mP$ o sea $Q = 8(8, 21)$

Cuentitas para $2P$, como $P = P$ usamos la λ correspondiente, así:

$$\lambda = \frac{3x_1^2 + a}{2y_1} = \frac{3(8)^2 + 1}{2(21)} \; mod \; 31 = 26, \text{ luego}$$

$$x_3 = \lambda^2 - x_1 - x_2 = (26)^2 - 8 - 8 \; mod \; 31 = 9$$

$$y_3 = \lambda(x_1 - x3 - y_1) = 26(-1) - 21 = -47 \; mod \; 31 = 15$$

Así $2P = (9, 15)$ Análogo para $4P = 2P + 2P = (29, 29)$.

$$Q = 8P = 4P + 4P = (1, 4).$$

Dado que el mensaje esta cifrado, significa que cada uno de los puntos en el mensaje estan comprimidos, para ello usaremos el algoritmo para descomprimir los puntos.

De la entrada $((9, 1), 2)$ tomamos $(9, 1)$ lo descomprimimos y recuperamos el punto original:
$z = 9^3 + 9 + 14 \; mod \; 31 = 8$ pero buscamos $y = \sqrt{z}$ por lo que hacemos $y = z^{\frac{p+1}{4}} \; mod \; p$ así $y = 8^{\frac{32}{4}} \; mod \; 31 = 16$

ahora como $16 \neq 1 \; mod \; 2$ al descomprimirlo obtenemos $(9, 31 - 16) = (9, 15)$

como $m = 8$ hacemos $8(9, 15) = (6, 9)$

Finalmente usamos la función de descifrado $d_k(y) = y_2(x_0)^{-1} \; mod \; p$

$d_k(y) = 2(6)^{-1} = 2(26) = 52 \; mod \; 31 = 21$

POR LO QUE $((9, 1), 2) = 21$

Aplicamos el mismo procedimiento para cada una de las entradas de mensaje cifrado

((9, 1), 2), ((19, 0), 10),((29, 1), 24),((12, 1), 24),((0, 1), 19),((24, 1), 13), ((9, 1), 15), ((19, 0), 1),((29, 1), 17),((24, 1), 20),((0, 1), 16),((27, 0), 4),((0, 1), 29).

Aplicamos la correspondencia $A = 1, B = 2, ..., Z = 26$. Obteniendo el texto plano:

$\mathcal{xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx}$

$21 \longmapsto U$, $19 \longmapsto S$, $1 \longmapsto A$, $3 \longmapsto C$, $21 \longmapsto U$, $2 \longmapsto B$, $18 \longmapsto R$, $5 \longmapsto E$, $2 \longmapsto B$, $15 \longmapsto O$, $3 \longmapsto C$, $1 \longmapsto A$, $19 \longmapsto S$

U S A C U B R E B O C A S