Introducción Matemática a la Criptografía

Yiseth Karina Rodríguez Cáceres
Cesar David Del Real Lario

4 de mayo de 2023

INTRODUCCIÓN

La criptografía es una disciplina que existe desde tiempos remotos con el propósito de ocultar información a observadores no deseados. Desde el cifrado por sustitución, como el cifrado César y el algoritmo de cifrado de Augusto, hasta el cifrado de Vigenère, los métodos criptográficos han evolucionado y perfeccionado a lo largo de los siglos. Con la llegada de los nuevos medios de comunicación, como el telégrafo, la criptografía tomó una mayor importancia y se empezaron a buscar nuevos métodos criptográficos.

Los métodos criptográficos conocidos como "cifrados simétricos o cifrado de clave privada"presentan una gran desventaja dado que en estos cifrados, la clave utilizada para cifrar y descifrar la información debe ser compartida por ambas partes. Visto de otra manera, si dos personas necesitan comunicarse de manera privada y utilizan un cifrado simétrico, ambas personas comparten la misma clave secreta para cifrar y descifrar sus mensajes. El problema radica en que ambas personas necesitan ponerse de acuerdo en la misma clave antes de poder utilizarla, lo cual puede ser difícil y riesgoso en situaciones donde la seguridad no está garantizada. Los cifrados simétricos pueden no ser la mejor opción en estas situaciones, ya que si alguien descubre la clave, puede leer todos los mensajes cifrados.

En 1976, Whitfield Diffie y Martin Hellman introdujeron el concepto de criptografía de clave pública en su artículo titulado "Nuevas direcciones en criptografía". Este sistema utiliza dos claves diferentes, una pública y otra privada, lo que permite que la información pueda ser cifrada por cualquier persona que tenga la clave pública, pero solo pueda ser descifrada por la persona que posee la clave privada correspondiente. Una característica útil y esencial de los criptosistemas de clave pública es que solo se necesita una clave pública compartida para que cualquier persona pueda enviar mensajes cifrados al propietario de la clave privada. Además, no es necesario que el propietario proporcione una clave privada separada para cada persona que desee comunicarse con él. Esto aumenta significativamente la seguridad de la comunicación y ha permitido el

desarrollo de numerosos sistemas criptográficos que se utilizan ampliamente en la actualidad.

En este texto expositivo, presentamos un estudio de los algoritmos criptográficos Diffie-Hellman y ElGamal, tanto en el campo $\mathbb{F}_p$ como en curvas elípticas, y discutimos el Problema del Logaritmo Discreto, un problema matematico sobre el cual se basa la seguridad de ambos algoritmos.

1. Algoritmos criptográficos Diffie-Hellman y Elgamal

Los algoritmos criptográficos Diffie-Hellman y ElGamal son dos ejemplos de algoritmos criptográficos que utilizan clave pública para establecer un canal seguro de comunicación entre dos partes y son utilizados ampliamente en la actualidad para garantizar la seguridad en la comunicación electrónica, como en la transmisión segura de información en internet, entre otras aplicaciones. A continuación detallamos en qué consiste cada uno de estos criptosistemas.

1.1. Algoritmo Diffie-Hellman

El algoritmo de intercambio de claves Diffie-Hellman proporciona una solución ingeniosa al problema criptográfico de cómo compartir una clave secreta de forma segura entre dos partes que solo pueden comunicarse a través de un canal inseguro, tarea que parecía imposible hasta 1976 que Diffie y Hellman publicaron su trabajo, en el que incluían el hoy conocido Algoritmo Diffie-Hellman. Este algoritmo nos permite intercambiar una clave secreta de manera segura para poder usarla en un cifrado simétrico.

Ahora bien, supongamos que Alice y Bob quieren intercambiar de manera segura una clave privada, pero su único medio de comunicación no es seguro, ya que su adversario, Eva, puede interceptar cada mensaje. ¿Cómo podrían Alice y Bob intercambiar dicha clave sin que fuese interceptada por Eva?.

Alice y Bob deben elegir un primo p grande, y un entero g no nulo módulo p. Para una mayor seguridad es más conveniente elegir g tal que su orden en $\mathbb{F}_p^*$ sea un primo grande. Presentamos el algoritmo en la siguiente tabla:

Creación de parámetros públicos	
Un partido de confianza elige y publica un primo p (grande) y un entero g que tiene gran orden primo en $\mathbb{F}_p^*$	
Cálculos privados	
Alice	Bob
Elige un entero secreto a Computa $A \equiv g^a (\text{mód} p)$.	Elige un entero secreto b Computa $B \equiv g^b (\text{mód} p)$.
Intercambio público de valores	
Alice envía A a Bob $\longrightarrow A$ $B \longleftarrow$ Bob envía B a Alice	
Otros cálculos privados	
Alice	Bob
Computa el número $B^a (\text{mód} p)$.	Computa el número $A^b (\text{mód} p)$.
El valor secreto compartido es $B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \text{ mód } p$	

Ejemplo 1. *Alice y Bob han acordado intercambiar una clave secreta para comunicarse. Han elegido el primo* $p = 941$ *y la raíz primitiva* $g = 627$. *Alice elige su clave secreta* $a = 347$ *y calcula* $A = 390 \equiv 627^{347} (\text{mód} 941)$. *De igual forma, Bob elige su clave secreta* $b = 781$ *y calcula* $B = 691 \equiv 627^{781} (\text{ mód } 941)$. *Alice envía a Bob el* 390 *y Bob envía a Alice el* 691. *Como se están comunicando por un canal inseguro, puede considerarse que los valores* $A = 390$ *y* $B = 691$ *están comprometidos. Pero los numero* $a = 347$ *y* $b = 781$ *no se transmiten, por lo que permanecen en secreto. Por lo tanto, Alice y Bob calculan el número*

$$470 \equiv 627^{347 \cdot 781} \equiv A^b \equiv B^a (\text{mód} 941),$$

así el número secreto de ambos será 470.

El cifrado Diffie-Hellman es un método criptográfico de intercambio de claves de manera segura en un canal de comunicación inseguro. Constituye un algoritmo de clave pública dado que utiliza una clave pública para el intercambio de claves, pero a diferencia de otros algoritmos de clave pública, no se utiliza para cifrar los datos en sí. En cambio, se utiliza para establecer una clave compartida que luego se utiliza en un cifrado simétrico para cifrar los datos.

1.2. El criptosistema de clave pública Elgamal

Aunque el algoritmo de Diffie-Hellman nos permite compartir una clave privada usando un canal inseguro, no logra ser un criptosistema de clave pública, ya que no nos permite el intercambio de información. El desarrollo más natural de un sistema criptográfico usando el documento de Diffie-Hellman es el sistema descrito por Taher Elgamal en 1985. Mostramos el algoritmo en la siguiente tabla:

Creación de parámetros públicos	
Un partido de confianza elige y publica un primo p (grande) y un elemento g mód p que tiene orden primo grande.	
Alice	Bob
Creación de claves	
Elige clave privada $1 \leq a \leq p-1$. Computa $A \equiv g^a(\mod p)$. Publica la clave pública A.	
Cifrado	
	Escoja el texto plano m. Escoja un elemento aleatorio k. Use la clave pública A de Alice Compute $c_1 = g^k(\mod p)$ y $c_2 = mA^k(\mod p)$. Envíe a Alice el texto cifrado (c_1, c_2).
Descifrado	
Compute $(c_1^a)^{-1} \cdot c_2(\mod p)$. El cual es igual al mensaje m.	

Ejemplo 2. *Alice y Bob eligen el primo* $p = 467$ *y la raíz primitiva* $g = 2$. *Alice elige como su llave privada a* $a = 153$, *y calcula*

$$A \equiv g^a \equiv 2^{153} \equiv 224(\text{mód}467).$$

Bob quiere enviar a Alice el mensaje $m = 331$. *El elige el número aleatorio* $k = 197$ *y calcula*

$$c_1 \equiv 2^{197} \equiv 87(\text{mód}467) \quad y \quad c_2 \equiv 331 \cdot 224^{197} \equiv 57(\text{mód}467).$$

Por lo que el par, $(c_1, c_2) = (87, 57)$ *es el mensaje cifrado que se envía a Alice.*
Alice, usando su llave privada calcula

$$x \equiv (c_1^a)^{-1} \equiv c_1^{p-1-a} \equiv 87^{313} \equiv 14(\text{mód}467).$$

Y para calcular el mensaje, calcula

$$c_2 x \equiv 57 \cdot 14 \equiv 331(\text{mód}467).$$

En este criptosistema el mensaje que se quiere cifrar es un entero m entre 2 y $p-1$, mientras que el texto cifrado son dos enteros c_1 y c_2 del mismo rango.

2. Seguridad de los criptosistemas

Ya conocemos el funcionamiento de estos criptosistemas, pero ¿qué tan seguros son? ¿Cuál es el fundamento de su seguridad? La seguridad de estos sistemas

criptográficos se basa en la complejidad computacional de ciertos "problemas matemáticos", cuya resolución resulta difícil en la práctica, específicamente, el problema del logaritmo discreto.

2.1. El Problema del Logaritmo Discreto

La primera construcción de clave pública, publicada por Diffie y Hellman en 1976, se basa en la dificultad de resolver el problema del logaritmo discreto en un campo finito $\mathbb{F}_p$, donde p es primo, y $\mathbb{F}_p$ es un campo finito con p elementos.

Definición 2.1. *Sea g una raíz primitiva para $\mathbb{F}_p$ y $h \in \mathbb{F}_p$ un elemento no nulo. El Problema del Logaritmo Discreto (DLP) es el problema de encontrar un exponente x tal que*

$$g^x \equiv h(\text{mód}p).$$

El número x es llamado el logaritmo discreto de h de base g y es denotado por $\log_g(h)$.

Recordemos que se llama raíz primitiva g a aquel elemento tal que cada elemento no nulo de $\mathbb{F}_p$ es generado por una potencia de g, en particular $g^{p-1} = 1$, por el Pequeño Teorema de Fermat. Este elemento primitivo siempre existe y lo podemos ver en el teorema 1.30 de [1]. A partir de g podemos listar todos los elementos no nulos de $\mathbb{F}_p$:

$$1, g, g^2, \cdots, g^{p-2} \in \mathbb{F}_p.$$

Notemos que si existe una solución para el DLP, i.e existe x tal que $g^x \equiv h(\text{ mód } p)$, entonces existen infinitas soluciones. Ya que por Pequeño Teorema de Fermat tenemos que $g^{p-1} \equiv 1(\text{mód}p)$, y si x es una solución de DLP, entonces

$$g^{x+k(p-1)} \equiv g^x \cdot (g^{(p-1)})^k \equiv h \cdot 1^k \equiv h(\text{mód}p),$$

entonces las soluciones son de la forma $x = x_0 + k(p-1)$ para $k \in \mathbb{Z}$, por lo que $\log_g(h)$ está definido en módulo $p-1$.

Hasta el día de hoy, no se conocen algoritmos que nos permitan resolver el DLP sobre $\mathbb{F}_p$ en un tiempo razonable, es decir, en tiempo polinomial. Y se considera que este problema es aún más difícil de resolver si lo tratamos en otro grupo, el grupo de curvas elípticas.

2.2. Problema de Diffie-Hellman (DHP)

Ahora, siguiendo con el ejemplo 1. Note que si Eva puede interceptar la comunicación de Alice y Bob, para descifrar la clave compartida de estos, ella necesitaría resolver

$$627^a \equiv 390(\text{mód}941) \quad \text{ó} \quad 627^b \equiv 691(\text{mód}941),$$

y así ella podrá conocer uno de los exponentes secretos. Hasta donde se sabe, esta es la única manera para que Eva pueda descifrar la clave secreta.
Los números del ejemplo anterior eran demasiado pequeños para poder brindar una seguridad real, ya que le tomaría muy poco tiempo a Eva calcular todas las potencias posibles de 627 módulo 941. Actualmente, se sugiere que se elijan primos que tengas más de 1000 bits o de aproximadamente 2^{1000}, y g cuyo orden es primo de aproximadamente $p/2$. En este caso. Eva si se enfrentará a una tarea difícil.
Entonces, la dificultad de Diffie-Hellman depende de resolver:

Definición 2.2. *Sea p un número primo y g un entero. El problema de Diffie-Hellman (DHP), es el problema de calcular el valor de $g^{ab}(\text{mód}p)$ conociendo los valores $g^a(\text{mód}p)$ y $g^b(\text{mód}p)$.*

Note que si Eva puede resolver el DLP, entonces ella puede calcular los exponentes secretos de Alice y Bob. Pero si Eva puede resolver el DHP, no se conoce si podrá resolver el DLP.

2.3. Problema de Elgamal

Ahora, ¿Es el criptosistema Elgamal tan difícil de atacar para Eva como el problema Diffie-Hellman?. Podemos ver en la proposición 2.10 de [1] que si Eva puede romper Elgamal, entonces puede romper el problema DHP, y también podemos probar, que si Eva logra romper el problema de DHP, entonces puede romper el Elgamal. Por lo que, la seguridad del criptosistema de clave pública Elgamal también depende de la dificultad de resolver el problema de Diffie-Hellman, y, por lo tanto, de la dificultad que implique el DLP.

Proposición 1. *Si se fija un p como número primo y una base g para el cifrado Elgamal, y se supone que Eva tiene acceso a un oráculo que descifra textos cifrados arbitrarios utilizando claves públicas también arbitrarias, entonces podría resolver el problema de Diffie-Hellman. Por otro lado, si Eva pudiera resolver el problema de Diffie-Hellman, también podría romper el criptosistema de clave pública de Elgamal.*

Demostración. Supongamos que Eva es capaz de resolver el problema de Diffie-Hellman. Más precisamente, asuma que si Eva tiene dos potencias g^a y $g^b \mod p$ entonces Eva puede computar $g^{ab} \mod p$. Veamos que Eva puede romper el criptosistema de clave pública Elgamal.

Eva conoce los valores $A \equiv_p g^a$ (clave pública de Alice), y los valores $c_1 \equiv_p g^k$ y $c_2 \equiv_p mA^k$, donde m es el texto plano y k es el elemento aleatorio de Bob. Ahora, Eva puede computar $g^{ak} \mod p$, entonces también puede computar $(g^{ak})^{-1}$. Además, nótese que $g^{ak} \equiv A^k \mod p$. Por tanto, Eva puede conocer el mensaje m computando $c_2 \cdot (g^{ak})^{-1} \mod p$.

Ahora, supongamos que Eva puede romper el criptosistema de clave pública Elgamal. Por el algoritmo de Diffie-Hellman Eva conoce los valores de p y g, además también tiene conocimiento de $A \equiv g^a \mod p$ y $B \equiv g^b \mod p$, Eva necesita calcular g^{ab}, sin conocer los valores privados a y b.

Dado que se conoce $A \equiv g^a \mod p$ y $B \equiv g^b \mod p$, y como Eva puede romper el criptosistema de clave pública Elgamal, Eva conoce $(c_1^a)^{-1} \cdot c_2 \equiv m \mod p$, donde (c_1, c_2) es un supuesto texto cifrado. Ahora, sí consideramos $c_1 = B \equiv g^b \mod p$, entonces Eva conoce

$$(B^a)^{-1} \cdot c_2 \equiv (g^{ab})^{-1} \cdot c_2 \equiv m \mod p$$

por lo que Eva fácilmente puede computar

$$(g^{ab}) \equiv m^{-1} \cdot c_2 \mod p.$$

□

3. Criptografía sobre curvas elípticas

El grupo $\mathbb{F}_p$ no es el único grupo sobre el cual podemos definir estos métodos criptográficos. Las curvas elípticas son también grupos de gran importancia en el mundo de la criptografía. Antes de pasar a los criptosistemas sobre estos grupos, veamos una breve introducción a este interesante grupo.

3.1. Curvas Elípticas

Definición 3.1. *Una curva elíptica es el conjunto de soluciones a una ecuación de la forma:*

$$Y^2 = X^3 + AX + B$$

mejor conocida como "Ecuaciones de Weierstrass".

La figura 1 es un ejemplo de la gráfica de una curva elíptica.

Algo sorprendente de las curvas elípticas es que hay una forma natural de tomar dos puntos sobre la curva elíptica, y por medio de estos llegar a un tercer punto, es decir, por medio de una operación, que en este caso es análoga a la suma. La forma más natural de describir esta operación es por medio de la geometría

3.1.1. Operación

Sea P y Q dos puntos en una curva elíptica E, trazamos la recta L que pasa a través de P y Q. Esta recta intercepta a E en tres puntos, los puntos P, Q y otro punto R. Tomamos este punto R y lo reflejamos a través del eje x (i.e,

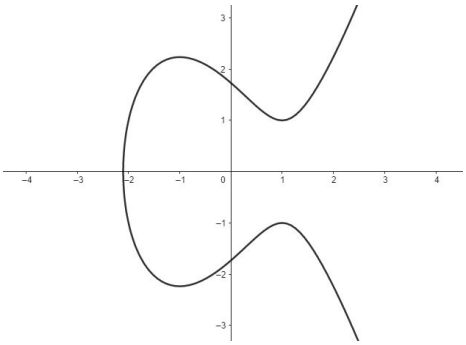

Figura 1: $E : Y^2 = X^3 - 3X + 3$

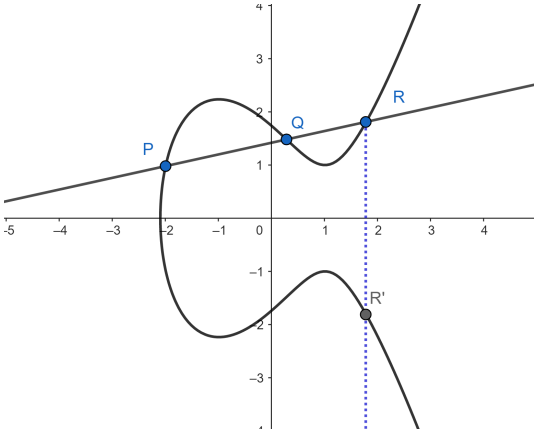

Figura 2: $P \oplus Q = R'$

multiplicamos la coordenada y por -1) para obtener un nuevo punto R'. Este punto R' se llama suma de P y Q. Por ahora, lo representamos con $\oplus$. Esto lo podemos escribir como

$$P \oplus Q = R'.$$

Ejemplo: Sea E la curva elíptica

$$Y^2 = X^3 - 15X + 18 \tag{1}$$

y sean $P = (7, 16)$, $Q = (1, 2)$ puntos sobre la curva E. La recta que pasa por los puntos P y Q es $L : Y = \frac{7}{3}X - \frac{1}{3}$. Entonces

$$\left(\frac{7}{3}X - \frac{1}{3}\right)^2 = X^3 - 15X + 18,$$
$$\frac{49}{9}X^2 - \frac{14}{9}X + \frac{1}{9} = X^3 - 15X + 18,$$
$$X^3 - \frac{49}{9}X^2 - \frac{121}{9}X + \frac{161}{9} = 0.$$
$$X^3 - \frac{49}{9}X^2 - \frac{121}{9}X + \frac{161}{9} = (X-7)\cdot(X-1)\cdot\left(X + \frac{23}{9}\right).$$

Por lo que el tercer punto de intersección de L y E es $X = -\frac{23}{9}$, con lo cual tenemos que $R = \left(-\frac{23}{9}, -\frac{170}{27}\right)$. Así que

$$P \oplus Q = \left(-\frac{23}{9}, \frac{170}{27}\right).$$

Con esta definición de suma, hay varios casos que debemos tratar, el primero sería cuando operamos $P \oplus P$. Imaginemos lo que le sucede a la recta L que pasa por P y Q si el punto Q se desliza a lo largo de la curva y se acerca cada vez más a P. En el límite, a medida que Q se acerca a P, la recta L se convierte en la recta tangente a E en P. Así, para sumar P a sí mismo, simplemente tomamos la recta L como la recta tangente a la curva E en L.

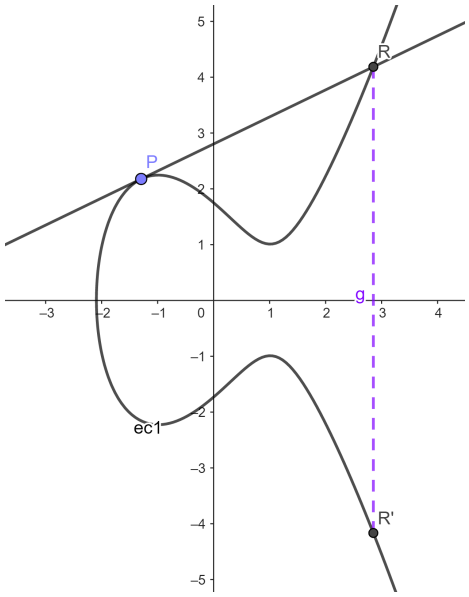

Figura 3: $P \oplus P = 2P = R'$

Nuestro segundo problema se presenta cuando queremos sumar $P = (a, b)$ con su simétrico respecto al eje x, $P' = (a, -b)$. En este caso, si lo hacemos con la definición que mencionamos anteriormente, no vamos a tener ningún punto de intersección, por lo que para este caso debemos definir un punto extra, el $\mathcal{O}$ que vive «en el infinito.» Más precisamente, el punto $\mathcal{O}$ no existe en el plano XY, pero pretendemos que se encuentra en cada recta vertical, por lo que

$$P \oplus P' = \mathcal{O}.$$

Y por último

$$P \oplus \mathcal{O} = \mathcal{O}.$$

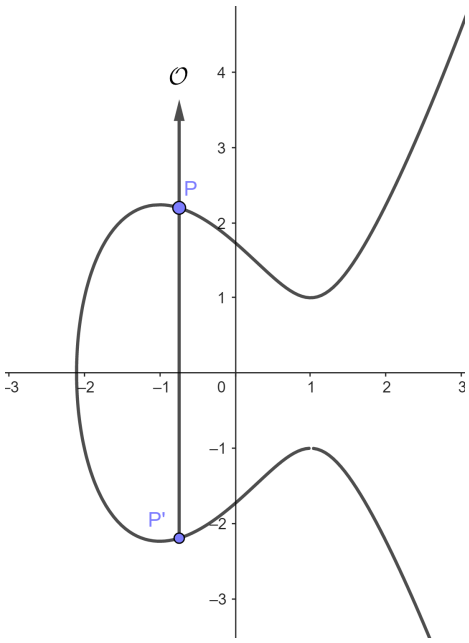

Figura 4: $P \oplus P' = \mathcal{O}$, donde $P = (a, b)$ y $P' = (a, -b)$

El algoritmo que nos permite sumar dos puntos sobre E es el siguiente:

Algoritmo de adición de curva elíptica

Sea

$$E : Y^2 = X^3 + AX + B$$

una curva elíptica y sean $P1$ y $P2$ puntos en E.

1. Si $P_1 = \mathcal{O}$, entonces $P_1 + P_2 = P_2$.
2. De lo contrario, si $P_2 = \mathcal{O}$, entonces $P_1 + P_2 = P_1$.

3. De lo contrario, escribimos $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$.
4. Si $x_1 = x_2$ y $y_1 = -y_2$, entonces $P_1 + P_2 = \mathcal{O}$.
5. De lo contrario, defina λ por

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{si } P_1 \neq P_2, \\ \frac{3x_1^2 + A}{2y_1} & \text{si } P_1 = P_2, \end{cases}$$

y sea

$$x_3 = \lambda^2 - x_1 - x_2 \quad \text{y} \quad y_3 = \lambda(x_1 - x_3) - y_1.$$

Entonces $P_1 + P_2 = (x_3, y_3)$.

Con todo esto claro, entonces definimos

Definición 3.2. *Una curva elíptica E es el conjunto de soluciones a una ecuación de Weierstrass*

$$E : Y^2 = X^3 + AX + B,$$

junto con un punto adicional $\mathcal{O}$, donde las constantes A y B deben satisfacer

$$4A^3 + 27B^2 \neq 0.$$

Y E con la operación definida anteriormente es un grupo abeliano aditivo.

3.2. Curvas elípticas sobre campos finitos

Ahora, para aplicar la teoría de curvas elípticas a la criptografía, necesitamos mirar las curvas elípticas cuyos puntos tienen coordenadas en un campo finito $\mathbb{F}_p$.

Definición 3.3. *Sea $p \geq 3$ un primo. Una curva elíptica sobre $\mathbb{F}_p$ es una ecuación de la forma*

$$E : Y^2 = X^3 + AX + B \text{ con } A,\ B \in \mathbb{F}_p \text{ tal que } 4A^3 + 27B^2 \neq 0.$$

El conjunto de puntos en E con coordenadas en $\mathbb{F}_p$ es el conjunto

$$E(\mathbb{F}_p) = \{(x, y) : x, y \in \mathbb{F}_p : y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$$

Ejemplo 3. *Sea*

$$E : Y^2 = X^3 + 3X + 8 \text{ sobre el campo } \mathbb{F}_{13}$$

Podemos encontrar todos los valores de $E(\mathbb{F}_p)$ sustituyendo X en E todos los valores de $\mathbb{F}_p$ y comprobando para que valores de X la cantidad $X^3 + 3X + 8$ es un cuadrado módulo 13. Por ejemplo, $X = 0$ nos da 8, y 8 no es un cuadrado módulo 13. En cambio, si $X = 1$ nos da 12, y 12 es una raíz módulo cuadrado 13. De hecho, tiene dos:

$$5^2 \equiv 12(\text{mód}13) \text{ y } 8^2 \equiv 12(\text{mód}13)$$

por lo que los puntos $(1, 5)$ y $(1, 8) \in E(\mathbb{F}_{13})$. Los elementos de $E(\mathbb{F}_{13})$ son

$$E(\mathbb{F}_{13}) = \{\mathcal{O}, (1, 5), (1, 8), (2, 3), (2, 10), (9, 6), (9, 7), (12, 2), (12, 11)\}.$$

$E(\mathbb{F}_p)$ es un grupo finito, y es sobre este grupo que trabajaremos y definiremos los algoritmos criptográficos.

3.3. Diffie-Helman sobre curvas elípticas

Finalmente, es el momento de trabajar los algoritmos criptográficos sobre curvas elípticas. Empezamos mostrando el de Diffie-Hellman, que es análogo a la forma como lo definimos sobre $\mathbb{F}_p$

Ahora, supongamos que Alice y Bob eligen una curva particular, trabajando así sobre el campo $E(\mathbb{F}_p)$ y también eligen un punto $P \in E(\mathbb{F}_p)$. Entonces, si desean ponerse de acuerdo en una clave privada, para usarla en un criptosistema de clave pública, pueden hacerlo realizando el procedimiento expuesto en la siguiente tabla:

Creación de parámetros públicos	
Un partido de confianza elige y publica un primo p (grande) Una curva elíptica E en $\mathbb{F}_p$ y un punto P en $E(\mathbb{F}_p)$.	
Cálculos privados	
Alice	Bob
Elige un entero secreto n_A Computa $Q_A = n_A P$.	Elige un entero secreto n_B Computa $Q_B = n_B P$.
Intercambio público de valores	
Alice envía Q_A a Bob $\longrightarrow Q_A$ $Q_B \longleftarrow$ Bob envía Q_B a Alice	
Otros cálculos privados	
Alice	Bob
Computa el punto $n_A Q_B$.	Computa el número $n_B Q_A$.
El valor secreto compartido es $n_A Q_B = n_A(n_B P) = n_B(n_A P) = n_B(n_A P) = n_B Q_A$	

Ejemplo. Alice y Bob deciden usar Diffie-Hellman elíptico con el siguiente primo, curva y punto:

$$p = 3851, \qquad E : Y^2 = X^3 + 324X + 1287, \qquad , P = (920, 303)$$

Alice y Bob eligen sus respectivos valores secretos $n_A = 1194$ y $n_B = 759$. Entonces
Alice calcula $Q_A = 1194P = (2067, 2178) \in E(\mathbb{F}_{3851})$,
Bob calcula $Q_B = 1759P = (3684, 3125) \in E(\mathbb{F}_{3851})$.
Alice envía Q_A a Bob, y Bob envía Q_B a Alice, y finalmente
Alice calcula $n_A Q_B = 1194(3684, 3125) = (3347, 1242) \in E(\mathbb{F}_{3851})$
Bob calcula $n_B Q_A = 1759(2067, 2178) = (3347, 1242) \in E(\mathbb{F}_{3851})$.
Así, Alice y Bob tienen el mismo punto secreto.

De esta misma manera, y análogamente a $\mathbb{F}_p$ podemos definir el Problema de Diffie-Hellman sobre curvas elípticas.

Definición 3.4. *Sea $E(\mathbb{F}_p)$ una curva elíptica sobre un campo finito, y sea $P \in E(\mathbb{F}_p)$. El problema de Diffie-Hellman sobre la curva elíptica, es el problema de calcular el valor de $n_1 n_2 P$ a partir de los valores conocidos $n_1 P$ y $n_2 P$.*

3.4. Criptosistema Elgamal

Análogamente, como Elgamal descrito para $\mathbb{F}_p$, si se desea implementar una comunicación segura sobre curvas elípticas, se podría utilizar Elgamal sobre este grupo $E(\mathbb{F}_p)$. Por lo que, si Alice y Bob desean comunicarse utilizando este criptosistema, deben elegir un primo p lo suficientemente grande, una curva elíptica E y un punto $P \in E(\mathbb{F}_p)$. El proceso es descrito en la siguiente tabla:

Creación de parámetros públicos	
Un partido de confianza elige y publica un primo p (grande) una curva elíptica E en $\mathbb{F}_p$ y un punto P en $E(\mathbb{F}_p)$.	
Alice	Bob
Creación de claves	
Elige clave privada n_A. Computa $Q_A = n_A P$ en $E(\mathbb{F}_p)$. Publica la clave pública Q_A.	
Cifrado	
	Escoja el texto plano $M \in E(\mathbb{F}_p)$. Escoja un elemento aleatorio k. Use la clave pública Q_A de Alice Compute $C_1 = kP \in E(\mathbb{F}_p)$. y $C_2 = MQ_A \in E(\mathbb{F}_p)$ Envíe a Alice el texto cifrado (C_1, C_2).
Descifrado	
Compute $C_2 - n_A C_1 \in E(\mathbb{F}_p)$. El cual es igual al mensaje M.	

3.5. El problema del logaritmo discreto en curvas elípticas (ECDLP)

Así como en $\mathbb{F}_p$ la seguridad dependía de la dificultad de resolver el DLP, en curvas elípticas, la seguridad de estos criptosistemas también está basada en este problema. ¿Pero como se define el Problema del Logaritmo Discreto sobre curvas elípticas?

La definición que presentamos anteriormente del DLP nos pedía que g fuese una raíz primitiva módulo p, pero esto no es estrictamente necesario. También podríamos definir el DLP de manera más general, para un grupo cualquiera con

operación " $*$ " de la siguiente manera:

Definición 3.5. *Sea G un grupo con operación "$*$". El Problema del Logaritmo Discreto es determinar para cualesquiera $g, h \in G$, un entero x tal que*

$$\underbrace{g * g * \cdots * g}_{x \quad veces} = h.$$

Ya pudimos observar que el grupo de curvas elípticas sobre $\mathbb{F}_p$ es un grupo abeliano aditivo, por lo que podemos definir el Problema del Logaritmo Discreto, sobre este grupo utilizando la definición anterior.

Definición 3.6. *Sea E una curva elíptica sobre el campo finito $\mathbb{F}_p$ y sea P y Q en $E(\mathbb{F}_p)$. El problema del logaritmo discreto en curva elíptica (ECDLP) es el problema de encontrar un entero n tal que $Q = nP$. Por analogía con el problema del logaritmo discreto para $\mathbb{F}_p$, denotamos este entero n por $n = \log_P(Q)$ y llamamos a n el logaritmo discreto elíptico de Q con respecto a P.*

Note que

$$h = \underbrace{g * g * \cdots * g}_{x \quad veces}$$

que sobre $E(\mathbb{F}_p)$ sería

$$Q = \underbrace{P + P + \cdots + P}_{x \quad veces} \text{ con } P, Q \in E(\mathbb{F}_p)$$

Ejemplo. Sea $E : Y^2 = X^3 + 8X + 7$ sobre $\mathbb{F}_p$, los puntos $P = (32, 53)$ y $Q = (39, 17)$ están en $E(\mathbb{F}_p)$ y es fácil verificar que

$$Q = 11P \text{ entonces } \log_P(Q) = 11.$$

La ventaja que se tiene al trabajar criptosistemas de curvas elípticas (Elliptic Curve Cryptosystems - ECC) es que, ofrecen un nivel de seguridad comparable a los sistemas criptográficos basados en campos finitos, pero con claves más cortas sin comprometer la seguridad. Además, dada la complejidad matemática de las curvas elípticas, hace que sean más difíciles de atacar mediante técnicas criptoanalíticas, dado que los ataques a estos sistemas requieren mucho más tiempo y recursos computacionales que los sistemas criptográficos tradicionales. Al tener una llave pequeña, las operaciones criptográficas puede realizarse más rápido, lo que implica mayor velocidad, y menores necesidades de memoria, es decir, los ECC son muy eficientes en términos de consumo de recursos computacionales.

Por otro lado, el problema del Logaritmo Discreto es considerado un problema computacionalmente difícil. El mejor algoritmo conocido para resolver este problema toma aproximadamente $\sqrt{\#E(\mathbb{F}_p)}$ pasos, y como $\#E(\mathbb{F}_p) \approx p$, si consideramos p lo suficientemente grande, por ejemplo si $p \approx 2^{256}$ entonces se requiere 2^{128} operaciones en resolver el problema del Logaritmo Discreto. Y se estima que la capacidad de cálculo de todo el planeta disponible actualmente

no podría vulnerar un esquema con una seguridad superior a 2^{100} pasos. En particular, si el grupo de curvas elípticas se elige cuidadosamente, entonces el mejor algoritmo conocido requiere tiempo exponencial para resolver el problema del logaritmo discreto de la curva elíptica (ECDLP).

Referencias

[1] Hoffstein, J., Pipher, J., y Silverman, J. H. (2014). An Introduction to Mathematical Cryptography. In Undergraduate texts in mathematics. Springer Science+Business Media.

[2] Morales, M. (2003). Notas sobre Criptografía.