Universidad Nacional de Loja
Carrera Computación
Facultad de Energía las Industrias y los Recursos Naturales no Renovables

ACTIVIDAD AUTÓNOMA

CURVAS ELÍPTICAS

Estudiante	Melissa Tuza Jiménez		
Paralelo	7mo A		
Professor	Ing. Cristian Narváez G. Mg.Sc.		
Unidad	Criptografía computacional, unidad 2.		
Fecha	29/01/2024	**Plagio:** Si:No	**Calificación:** .....
Observación.:			

Introducción

En el amplio campo de la criptografía, las curvas elípticas manejan conceptos matemáticos que ha permitido a lo largo del tiempo ofrecer un nivel de seguridad robusto, con menos cantidad de recursos y con el mismo nivel de eficiencia en comparación de otros algoritmos. Una curva elíptica trabaja bajo una ecuación, manejando ejes del plano cartesiano (x,y), partiendo de esto es posible realizar operaciones, entre las más comunes es la suma de puntos. Por otro lado, el problema del logaritmo discreto se enfoca directamente en la complejidad que existe al momento de invertir la operación, por ende, se asegura un nivel de seguridad relativamente alto, ya que, se deduce que las curvas elípticas permiten ofrecer seguridad con un menor tamaño de bits dentro de la clave. Como todo sistema, no está libre de riesgos y vulnerabilidades, al momento de la implementación es un ejemplo común, por ello, es recomendable manejar parámetros como la correcta definición del campo finito, con el fin de evitar los diversos ataques. A continuación, se profundiza los conceptos básicos que permiten comprender la matemática aplicada dentro del algoritmo de curvas elípticas, los posibles casos de uso y un análisis a los errores que se suele cometer.

Desarrollo

A continuación, los conceptos fundamentales de las curvas elípticas enfocados en la criptografía serán analizados, comenzando por las operaciones matemáticas que lo componen y que, a partir de ellas, las operaciones que se pueden realizar. Considerando puntos importantes como el logaritmo discreto y realizando un análisis en cuanto al nivel de seguridad que ofrece, las vulnerabilidades a las que está expuesta, con el fin de obtener una idea de forma general del algoritmo en sí, dentro de la criptografía moderna.

0.1. ¿Qué es una curva elíptica ECC?

Una curva elíptica representa varios puntos agrupados en conjuntos que corresponden a una ecuación en un plano, con coordenadas x e y, dentro de un campo finito. Un campo finito tiene características representativas, como lo es al momento de realizar la suma de dos números, se obtiene un valor inesperado, como puede ser un 0. En este campo, se rige mediante la aplicación de una ecuación se describe como:

$$y^2 = x^3 + ax + b$$

Dentro de un enfoque simétrico, se identifica una regla con curvas elípticas que maneja la siguiente ecuación

$$y^2 + cy = x^3 + ac + b$$

Depende radicalmente de cuántas raíces puede tener la ecuación cúbica, es importante mencionar que no es posible obtener dos raíces cúbicas, entonces existen dos casos que una ecuación cúbica puede obtener una única raíz real, con el valor de 0, este tipo de raíz se identifica rápidamente al momento que existe un solo punto en donde la curva se une con el eje de las x en el plano cartesiano, un segundo caso, es al momento de obtener tres raíces reales, en donde existen tres puntos de intersección entre la curva y el eje de las x, esto sucede cuando los valores de x mayor o igual a 0. Por otro lado, otra regla sería

$$y^2 = x^3 + ax^2 + bx + c$$

. Al tomar las reglas, se determina que en todas las representaciones dentro del plano, existe un punto en el infinito. Se refiere a un punto que permite mantener un equilibrio dentro las operaciones, un ejemplo de ello, es la operación de suma de dos puntos.

0.2. ¿Cómo se realiza la Suma de Puntos en una curva elíptica?

Dentro de esta suma, existen factores como el módulo, dos puntos que corresponden a coordenadas en un plano cartesiano (P, Q), para finalmente obtener el valor de un punto R. Este valor es calculado mediante

$$R = P + Q$$

En donde cada punto, representa un valor en el eje de las coordenadas x, y, así como se determina en la siguiente ecuación: [5]

$$P = (x_1, y_1) y Q = (x_2, y_2)$$

0.3. ¿Cómo opera el logaritmo discreto en curvas elípticas ECDLP?

Dentro de este algoritmo se plantea dos puntos, generalmente representados por las variables P y Q, estas variables corresponden a puntos dentro de un plano cartesiano en el que se plasma una curva elíptica, dichos puntos deben ser múltiplos de P. Basándose en los valores que se le otorga a cada variable, permite calcular el valor de Q, al conocer el valor de P y de k. Este algoritmo opera dentro de los protocolos al momento de realizar el intercambio de claves, como en ECDH y ECDSA, pero al momento de hablar a nivel de vulnerabilidades y riesgos, este algoritmo es vulnerable al enfrentarse con otros algoritmos. [5] Dentro de este algoritmo se aplican temas como la aritmética de curvas elípticas, aquí interviene el punto P y Q dentro de la curva, estos puntos corresponden a valores dentro del eje de las coordenadas (x,y) del plano cartesiano, para obtener un nuevo punto llamado R, este punto sería un nuevo punto descubierto de la curva, adicional al valor de P y Q, se maneja un k que corresponde al módulo. Al realizar el cálculo de este último valor, resulta ser sencillo pero al momento de intentar calcular el proceso inverso. Entre los principales usos es en el intercambio de claves dentro del algoritmo de Diffie Hellman, en donde, el emisor y receptor, manejan independientemente sus claves públicas y privadas, partiendo de ellas, se crea una nueva clave compartida, se trata de una clave manejada de forma secreta. Así, es posible fortalecer el nivel de seguridad. Por otro lado, las firmas digitales de curvas elípticas permite verificar la autenticidad de un texto.

0.4. ¿Cuál es el nivel de seguridad que ofrece el algoritmo de curvas elípticas?

La aplicación de conceptos criptográficos fusionados con curvas elípticas permiten plantear criptosistemas con la intervención de claves públicas que se basan en logaritmos discretos, en

la actualidad, un claro ejemplo del tamaño y del nivel de seguridad que ofrece el algoritmo de curvas elípticas es en el nivel de seguridad en el tamaño de bits que maneja una clave de RSA, curvas elípticas permite ofrecer un nivel más alto de seguridad con tan solo 256 bits, mientras que, por otro lado, a una clave de RSA le toma trabajar con un valor de 3072 bits, esta diferencia radica en el alto nivel de complejidad que maneja el algoritmo de curvas elípticas al momento de procesar el logaritmo discreto. Hay que considerar que, a mayor nivel de longitud de una clave, también representa mayor cantidad de procesamiento y recursos para realizar un proceso. En la actualidad, una clave de RSA para que se considere segura, debe ser de una longitud de 2028 bits. [4] La seguridad de este ECC está enfocado en temas como el Problema del Logaritmo Discreto de Curvas Elípticas (ECDLP). Este algoritmo se desarrolla dentro de una multiplicación en forma escalar, punto por punto, va siendo parte de una curva, de esta forma es casi imposible hacer el proceso de izquierda a derecha para descubrir los valores iniciales. Por otro lado, es importante considerar que el concepto de curvas elípticas trabaja sobre un campo finito, al hablar de un campo finito se refiere a números primos. Se deduce que el nivel de seguridad que ofrezca este algoritmo, es proporcional al campo finito que se maneja. Por ende, esta característica, al momento de intentar descubrir una clave, se evalúa el tamaño de la clave y el tamaño del campo finito que se está manejando. [3]

0.5. ¿Qué tipo de vulnerabilidades se presentan en curvas elípticas?

Dentro de la curva, es importante definir los parámetros como elegir el tamaño correcto para un campo finito, tomando en consideración un punto importante, la longitud de la clave. Se deduce que el tamaño de la clave que se maneje dentro del algoritmo será proporcional al nivel de seguridad que ofrezca. Además, para contribuir al nivel de dificultad dentro del algoritmo, se puede manejar la generación de números aleatorios al momento de trabajar las claves privadas. [2] Una vulnerabilidad presente en todos los aspectos, es la mala implementación y en ECC no es la excepción, debido a que un error podría dejar la puerta abierta a muchos ataques, entre ellos es muy común el ataque de canal lateral, básicamente se refiere a diversos tipos de ataques que buscan conocer los tiempos que existen de un extremo a otro para intentar filtrar la información al momento de conocer propiedades de la energía que se está tomando, se analiza la potencia, el voltaje para determinar el tipo de potencia, la variación que representa con el fin de llegar a deducir dichas claves, al identificar un patrón de estos factores, se facilita más aún el proceso de extracción de las claves secretas. [1]

Conclusiones

- Los fundamentos básicos de las curvas elípticas permiten mejorar el nivel de la seguridad de la información. Parte desde conceptos matemáticos y aritméticos que mediante la aplicación de fórmulas y operaciones, permiten realizar un Este algoritmo tiene la capacidad de ofrecer un alto rendimiento a nivel de recursos debido a que maneja claves relativamente cortas y mantiene una rusticidad y resistencia frente a otros sistemas criptográficos. Además, es posible fusionar este algoritmo con las propiedades de Diffie Helman, (ECDH), por otro lado, para trabajar firmas digitales se maneja ECDSA se emplea en los protocolos a nivel de seguridad online, para verificar la autenticidad de los datos.

- Una característica representativa de curvas elípticas es el alto nivel de complijidad que tiene para en el proceso de obtener el valor del logaritmo discreto, el nivel de complejidad de este resultado va a depender de valores como el campo finito, módulo, entre otros elementos

importantes. Hay que tener en consideración, que al realizar una operación como la suma y la curva intercepta más de una vez el eje de las x, significa que el resultado sería mayor o igual que 0, mientras que si el valor es 0, se deduce que existirá una única intersección. Partiendo de esto, no existe un algoritmo en particular que permita resolver el problema del logaritmo como tal, por ende, el atacante tendrá una mayor complejidad.

- El algoritmo de curvas elípticas debido al nivel de complejidad matemática y aritmética ofrece un alto nivel de seguridad, pero no está libre de ataques, vulnerabilidades y riesgos. Definir correctamente los parámetros para reconocer efectivamente la curva es importante, ya que, existen ataques con diferentes enfoques, puede tratarse de un ataque lateral, el que se enfoca en analizar la frecuencia, cantidad de energía que utiliza con el fin de identificar un patrón que le permita hacer operaciones para descubrir o acercarse a la información.

Referencias

[1] *¿Se puede confiar en la Criptografía de Curva Elíptica? Un breve análisis de la seguridad de este popular sistema de Criptografía.* ISACA, 2019. URL: https://www.isaca.org/es-es/resources/isaca-journal/issues/2016/volume-3/can-elliptic-curve-cryptography-be-trusted-a-brief-analysis-of-the-security-of-a-popular-cryptosyste (visitado 29-01-2024).

[2] Criptografía De et al. *Universidad Politécnica de Madrid.* 2018. URL: https://oa.upm.es/56215/1/TFG_SANTIAGO_ALFONSO_RAPOSO_BRICENO.pdf (visitado 28-01-2024).

[3] A. Hernández Estrada et al. "Criptografía de curva elíptica". En: *TecnoCultura* (mar. de 2023), págs. 24-24. URL: https://tecnocultura.org/index.php/Tecnocultura/article/view/186 (visitado 29-01-2024).

[4] Celia Rodríguez Muñoz. "Curvas elípticas: su uso en criptografía". En: *Uvadoc.uva.es* (2022). DOI: https://uvadoc.uva.es/handle/10324/57975. URL: https://uvadoc.uva.es/handle/10324/57975 (visitado 27-01-2024).

[5] Delgado Rosario. "Curvas elípticas en la criptografía | Archivo Digital UPM". En: *Oa.upm.es* (jul. de 2022). DOI: https://oa.upm.es/71038/. URL: https://oa.upm.es/71038/ (visitado 25-01-2024).