Diseño y desarrollo de un sistema de cifrado de datos basado en curvas elípticas

Design and development of a data encryption system based on elliptical curves

Juan Manuel Gómez Velásquez[1]
Carlos Andrés Restrepo Restrepo[2]
Luis Reinel Castrillón Osorio[3]

1 Ingeniero Electrónico. Especialista de Infraestructura, Infraestructura tecnológica, Pragma S.A, Medellín, Antioquia, Colombia, juan.gomez@pragma.com.co.

2 Ingeniero Electrónico, La Unión, Antioquia, Colombia, carres123@hotmail.com.

3 Magíster en Ingeniería, Grupo de Investigación GIMU, docente tiempo completo, Facultad de Ingeniería, Universidad Católica de Oriente, Rionegro, Antioquia, Colombia, lcastrillon@uco.edu.co.

Resumen

En este artículo se presenta el desarrollo de un sistema para el cifrado de datos basado en algoritmos ECC, los cuales emplean aritmética modular y teoría de curvas elípticas para asegurar qué información puede viajar a través de un canal de comunicaciones inseguro. Se busca que la información no pueda ser interpretada por un atacante acceda a ella, el cual se debe enfrentar al problema del logaritmo discreto, cuya complejidad matemática garantiza que la información transmitida esté cifrada de manera robusta. Para el desarrollo del sistema criptográfico se implementa un protocolo *Diffie-Hellman* para el intercambio de la llave y se aplica el algoritmo de cifrado de *ElGamal Elíptico,* para la transmisión de la información. La implementación del sistema se hace bajo herramientas de software libre, utilizando un sistema operativo Linux y lenguaje de programación C.

El sistema es probado mediante la implementación de un modelo cliente-servidor que permite el intercambio de la llave, el acceso pseudoaleatorio a los datos, su representación como puntos de una curva y el cifrado-descifrado de la información. El sistema fue probado en el laboratorio donde se realizaron pruebas con diferentes tamaños de trama. Se logran transmitir tramas de hasta 64 bytes, con tiempos promedio de 41 ms y errores del 0 %. Las propiedades que ofrecen los algoritmos ecc permiten el uso de llaves de menor tamaño y con el mismo nivel de seguridad que otros sistemas de seguridad informática de llave pública, lo que los hace ideales para aplicaciones en dispositivos móviles.

Palabras clave

ECC, curvas elípticas, criptografía, cifrado asimétrico, seguridad informática.

Abstract

This article presents the development of a system for data encryption based on ECC algorithms, which employs modular arithmetic and elliptic curve theory to ensure that information can travel through an insecure communications channel. It is sought that the information can not be interpreted by an attacker who accesses it, which must face the problem of the discrete logarithm, whose mathematical complexity guarantees that the information transmitted is encrypted in a robust manner. For the development of the cryptographic system a Diffie-Hellman protocol is implemented for the exchange of the key and the ElGamal Elliptical encryption algorithm is applied for the transmission of the information. The implementation of the system is done under free software tools, using a Linux operating system and programming language C. The system is tested by implementing a client-server model that allows the exchange of the key, the pseudo-random access to the data, its representation as points of a curve and the encryption-decryption of information. The system was tested in the laboratory where tests were carried out with different frame sizes. It is possible to transmit frames of up to 64 bytes, with average times of 41 ms and errors of 0 %. The properties offered by ECC algorithms allow the use of smaller keys with the same level of security as other public key computer security systems, which makes them ideal for applications on mobile devices.

Key words

ECC, elliptic curves, cryptography, asymmetric encryption, computer security

Introducción

Cada vez es más frecuente el uso de sistemas electrónicos para la manipulación de información personal, empresarial y comercial. Gracias al uso masivo de la Internet, la constante evolución tecnológica y las nuevas tendencias del mercado (*big data,* redes sociales, internet de las cosas) el tráfico de datos crece cada día en todo el mundo; estos datos se transmiten por medio de canales públicos que, por definición, son inseguros y en donde posibles atacantes pueden filtrarse y acceder a información de manera no autorizada.

Esto sugiere un reto para la comunidad científica: utilizar los procesos matemáticos para la protección de la información que viaja por medio de redes de computadoras o dispositivos móviles inteligentes de una forma fuerte y eficiente, que permita garantizar la confidencialidad y la integridad de cualquier tipo de dato que se esté transmitiendo.

Dos conceptos matemáticos ayudan a implementar dichos sistemas:

Aleatoriedad: esto significa que a pesar de conocer el conjunto de pasos necesarios que ejecuta un sistema de seguridad, resulte impráctico tratar de predecir su salida. Es decir, que se debe garantizar que no exista ningún patrón o secuencia generatriz que dé lugar a las salidas obtenidas.

Complejidad matemática: se deben utilizar funciones en un solo sentido. Estas son funciones matemáticas fáciles de utilizar para obtener un resultado, pero que son complejas de revertir a partir del conocimiento a priori de dicho resultado. Esto, en términos de máquina, se traduce en un alto uso de recursos de procesamiento y memoria que hace poco viable la ejecución de ataques sobre la información transmitida.

«Una de las técnicas matemáticas más populares para proteger la información digital es la factorización de números primos».

Una de las técnicas matemáticas más populares para proteger la información digital es la factorización de números primos, que resulta en cifrados de alta complejidad cuando se trabaja sobre números considerablemente grandes. Sin embargo, este tipo de técnicas tienden a la obsolescencia debido a que los nuevos ataques informáticos son implementados a partir de procesos paralelos realizados por varias máquinas conectadas a la vez (ataques dirigidos). Surgen entonces nuevas tendencias en la innovación de la seguridad informática, como es el caso de la criptografía basada en curvas elípticas ECC (*elliptic curves*

cryptography) (Hankerson, Menezes y Vanstone, 2006). El uso de la ECC brinda niveles de seguridad iguales a los de los sistemas de factorización de primos, pero con ventajas como menor carga computacional y mayor complejidad matemática en sus algoritmos, lo que se traduce en menores costos de los sistemas de seguridad de datos y mayor complejidad en la elaboración de ataques dirigidos a este tipo de cifrado. El presente trabajo fue desarrollado utilizando curvas elípticas sobre campos finitos.

Campos finitos

La teoría de los sistemas criptográficos se basa en funciones, ecuaciones, demostraciones, teoremas y conceptos matemáticos, por lo tanto, para entender la criptografía basada en curvas elípticas es necesario definir los conceptos ***grupo abeliano*** y ***anillo***:

Grupo abeliano: es un conjunto de elementos sobre los cuales se pueden realizar operaciones para obtener un tercer elemento contenido dentro del mismo grupo; además, todos los elementos del grupo cumplen conmutatividad en sus operaciones, es decir,

$$P \text{ operado } Q = Q \text{ operado } P$$

Anillo: es un grupo abeliano con dos operaciones válidas entre sus elementos: la adición y la multiplicación. A este grupo pertenecen el conjunto de puntos que satisfacen la ecuación de las curvas elípticas, por lo que todo sistema criptográfico implementado parte de estas dos operaciones entre puntos para asegurar que la información que se comparte por una red se hace de una forma robusta y con tiempos de respuesta mucho menores en comparación a otros algoritmos de seguridad informática.

Curvas elípticas

Una curva elíptica E sobre un campo p (donde p es un número primo mayor a 3 lo más grande posible) posee un número determinado de puntos en los cuales se representará cada uno de los datos que se deseen proteger, mediante implementaciones que obedecen a la aritmética de las curvas elípticas para realizar operaciones con puntos y entre puntos. La ecuación que rige las curvas elípticas sobre campos finitos es:

La cual genera el conjunto de soluciones o puntos para una curva determinada una vez establecidos los coeficientes ***a*** y ***b.*** Estos coeficientes deben satisfacer la ecuación:

$$y^2 = x^3 + ax + b \ (mod\ p)$$

Esta condición garantiza que la curva sobre la cual opera un sistema no contenga elementos repetidos, lo que añade un alto grado de seguridad, dificultando la implementación de ataques dirigidos que puedan violar el sistema en tiempos cortos. La base de las operaciones en la criptografía de las curvas elípticas es la multiplicación de un punto P que pertenece a la curva por una constante k, lo que se procesa como la adición de ese punto el número de veces que indique la constante k (Hankerson *et al.*, 2006).

Metodología

A continuación, se describen cada uno de los pasos necesarios para la implementación del sistema criptográfico:

Criptografía asimétrica

También llamada criptografía de llave pública, consiste en un acuerdo secreto que se realiza por medio de un canal inseguro mediante el uso de operaciones matemáticas de una sola vía. El uso de protocolos definidos permite implementar algoritmos capaces de realizar el proceso de intercambio de llave.

Esta estrategia se realizó debido a las restricciones en las distancias que se tienen a través de una red. Antes de que se implementara la criptografía asimétrica, la única forma de intercambiar datos de manera segura era mediante un previo acuerdo, entre transmisor y el receptor, de la llave secreta con la cual se codificaría y decodificaría la información que se deseaba transmitir (criptografía simétrica o de llave secreta), la cual resulta impráctica en redes como Internet o redes locales vulnerables.

La criptografía de llave pública proporciona niveles de seguridad mucho más altos, debido a que no se depende de una única llave para asegurar los datos, además, la llave puede ser generada periódicamente y compartida de forma segura (Lauter, 2004).

El hecho de que los sistemas basados en criptografía asimétrica brindan una mayor seguridad radica en la dificultad comparativa de realizar dos tipos de operaciones: una «hacia adelante» que debe ser manejable y fácil, tanto de implementar como de ejecutar, y otra operación «inversa» que debe ser, en términos prácticos, intratable computacionalmente. El grado de dificultad para la implementación de ataques dirigidos depende también de los tamaños de las llaves escogidas, a mayor tamaño de las llaves mayor es el grado de seguridad. Esta relación se ilustra en la figura 1.

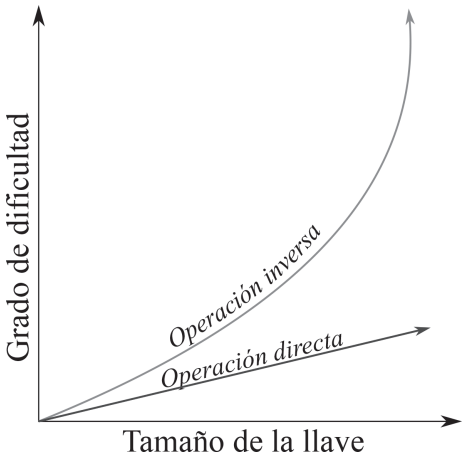

Figura 1. Dificultad de las operaciones en base al tamaño de la llave. Fuente: elaboración propia.

Protocolo para el intercambio de la llave

El desarrollo del sistema criptográfico se basó en el protocolo de intercambio de llave *Diffie–Hellman,* en su variación para las curvas elípticas, (el cual es una función de una sola vía) (Al-Aali, Boneau y Landers, 2000). La seguridad radica en lo que se denomina el problema del logaritmo discreto en las curvas elípticas (ecdlp) (Kar y Majhi, 2009), el cual consiste en determinar un valor entero a partir de un punto *P* y un múltiplo escalar *Q,* tal que:

$$Q = kP$$

Donde *k* es el parámetro para generar la llave pública e iniciar un intercambio seguro

de llave secreta para cifrar la información. El proceso inverso, a simple vista, no representa mucha dificultad, ya que solo bastaría con realizar una división entre *Q* y *P*. Sin embargo, debido a que se trata de una función de tipo anillo, las únicas operaciones válidas para los elementos de la función son la adición y la multiplicación. La división se convierte en una operación impráctica, lo que conlleva al uso de procesos complejos y difíciles de implementar para realizar un ataque dirigido. El protocolo *Diffie–Hellman* parte de la generación de un par de llaves públicas entre quienes desean compartir información de manera segura a través de un canal posiblemente vulnerable. Con este par de llaves y la multiplicación por sus respectivas llaves secretas, se genera un acuerdo secreto compartido de manera segura a través de un medio inseguro.

El protocolo se basa en parámetros públicos, es decir, datos que se van a compartir en la red previamente al envío de la información que se desea proteger, por lo que pueden ser interceptados y visualizados por cualquier atacante; pero a partir de esta información le resulta imposible calcular la llave secreta con la que los datos están siendo cifrados.

Cifrado de datos

Luego de tener acordado un valor en secreto por las dos partes que desean compartir información a través de una red o canal inseguro, se procede al cifrado de los datos, de tal manera que al operarlos con la llave secreta acordada, solo serán entendibles para el receptor que posee la llave de descifrado.

Existen diferentes tipos de cifrado, es decir, diferentes maneras de operar la llave secreta convenida con la información. Un método de uso común es la transposición, que consiste en la reorganización de los caracteres dentro del mensaje. Este tipo de técnicas se utilizan en algoritmos tales como DES y 3DES (Singh y Supriya, 2013) como una etapa inicial de su cifrado. Otra técnica utilizada comúnmente es la sustitución de datos, la cual consiste en reemplazar los caracteres del mensaje o dato con otros caracteres, este tipo de técnica es utilizado por el «algoritmo de Cesar» el cual consiste en desplazar *k* posiciones cada una de las letras del alfabeto; por ejemplo, el mensaje «*ABCD*» cifrado con una llave de tres es «*DEFG*» (Goyal y Kinger, 2013). En cada caso es necesario conocer el valor de la llave y el método de cifrado para obtener la información original.

«Existen diferentes tipos de cifrado, es decir, diferentes maneras de operar la llave secreta convenida con la información».

Para el caso de las curvas elípticas, se tiene inicialmente una llave secreta acordada mediante protocolo de intercambio *Diffie–Hellman* en su variante elíptica, por lo que la llave y la información son representadas como puntos pertenecientes a la curva sobre la cual opera el sistema. Para el cifrado se utiliza el algoritmo de *ElGamal elíptico* que opera la llave secreta adicionada con los datos de información como puntos pertenecientes a la curva elíptica escogida, a partir de la cual se obtendrán otros

puntos resultantes los cuales serán el mensaje cifrado a transmitir a través de la red (Sutikno, Surya y Effendi, 1998). Luego el receptor de los datos tendría que restar la llave secreta acordada del conjunto de puntos cifrados que ha recibido, aunque la resta no es una operación válida dentro del concepto de anillo, la aritmética para las curvas elípticas permite representar el proceso de resta como una adición, negando la ordenada *Y* del punto del sustraendo.

Software libre en el diseño y desarrollo

Toda la implementación del sistema fue enfocada al uso de software libre partiendo del sistema operativo de licencia gnu y herramientas para el modelado —como StarUML— y de desarrollo en lenguaje C —como CodeBlocks—. Además de las ventajas económicas, la política de código abierto contribuye a que personas interesadas en esta línea de desarrollo realicen mejoras al sistema o hagan sus propias aplicaciones. El uso de software libre favorece la distribución del conocimiento y de las aplicaciones sin restricciones a nivel mundial; se fomenta la libre competencia; se obtiene un mejor soporte y en menor tiempo para las aplicaciones, gracias a las grandes comunidades que día a día aportan a los desarrollos y proyectos de investigación. La compatibilidad a largo plazo, debido a la extensión del conocimiento y la estandarización de los programas bajo licencia gnu o alguna de sus modificaciones, también es una ventaja a futuro del diseño y la programación bajo software libre.

Resultados

Se logró implementar exitosamente un modelo cliente–servidor en computadoras tipo estación de trabajo, con procesadores *i5* de 2.8GHz y *4GB* de memoria RAM. El sistema implementado es totalmente escalable para diferentes tipos o tamaños de tramas de datos, con tasas de procesamiento ideales para la manipulación de información en tiempo real y una tasa de error del 0 %, esto debido a la inclusión del protocolo tcp para el intercambio de información por la red. Los resultados de diferentes transmisiones de información se presentan en la tabla 1.

Tamaño de la trama	Tasa de tramas procesadas
16 Bytes	69 Tramas/s
32 Bytes	40 Tramas/s
64 Bytes	24 Tramas/s

Tabla 1. Tasas de procesamiento del sistema criptográfico implementado.

El sistema es totalmente adaptable a un protocolo udp, el cual es un tipo de protocolo en donde no es indispensable la integridad de algunos paquetes de datos que se envíen y por lo que conservar el 0 % en la tasa de error no se hace necesario. Bajo estas circunstancias las tasas de procesamiento aumentarían muy significativamente.

Gracias a las propiedades de la criptografía asimétrica, el sistema contiene un control configurable para la renovación de la llave secreta de manera periódica, lo que aumenta el nivel de seguridad que se puede ofrecer. La renovación de la llave secreta se realiza en intervalos de tiempo muy pequeños, lo que hace poco práctico realizar ataques dirigidos al sistema.

Guía de implementación de algoritmos ECC

Adicionalmente a la implementación del sistema criptográfico en un modelo cliente – servidor, se realiza una guía para el desarrollo e implementación de este tipo de algoritmos que incluye conceptos como: el intercambio de la llave, el acceso pseudoaleatorio a los datos, la representación de estos como puntos de una curva, el cifrado y descifrado de la información, guiando al lector en cada uno de los pasos con las definiciones, ejemplos y conceptos necesarios para la implementación.

La guía es una contribución a la comunidad de habla hispana debido al poco material que se encuentra en este idioma que aborde a profundidad el desarrollo de aplicaciones, y no solo los conceptos involucrados y las ventajas que este tipo de algoritmos ofrece. El lector podrá saber exactamente cómo abstraer, a un lenguaje de programación, cada uno de los pasos descritos en la criptografía asimétrica y en la criptografía de las curvas elípticas, utilizando funciones propias de la interfaz de desarrollo, optimizando procesos y haciendo las validaciones respectivas que son requeridas para garantizar la seguridad de los datos que se van a procesar.

En la guía también se introduce al lector en el área de las comunicaciones seguras, exponiendo la importancia de estas en la actualidad y orientándole sobre cómo utilizar las herramientas de comunicación, a través del código de desarrollo, para transmitir datos por Ethernet, iniciar o detener el flujo de datos a través de un puerto en específico o direccionar datos y paquetes a través de redes de computadoras.

El conocimiento plasmado en la guía permite obtener los fundamentos necesarios para emular el sistema que se implementó o para impulsar el desarrollo de un nuevo sistema con múltiples estrategias, de acuerdo con el tipo de necesidades que se tenga, adaptando la lógica sugerida al problema específico para el cual se requieran este tipo de algoritmos.

Conclusiones

Se diseñó y desarrolló, bajo software libre, un sistema criptográfico basado en curvas elípticas totalmente escalable y adaptable a necesidades y niveles de seguridad requeridas en cualquier área de aplicación, sin restricciones de licenciamiento.

El conocimiento reflejado en la guía de implementación y la lógica propuesta logra ser

adaptable a otros lenguajes de programación, lo que permite la interdisciplinaridad en las aplicaciones que se desarrollen utilizando algoritmos basados en ECC, que van desde sistemas móviles hasta aplicaciones del sector productivo comercial e industrial.

ECC *para el futuro*

La constante evolución tecnológica propone cada día más portabilidad en los dispositivos electrónicos, lo que conlleva al uso de procesadores cada vez más pequeños y potentes, pero aun así limitados; lo que para el desarrollo de aplicaciones se debe tener en cuenta, intentando obtener el mejor rendimiento y el menor uso de recursos posibles. los algoritmos de cifrado basados en ECC son ideales para el uso en este tipo de dispositivos, como lo han demostrado entidades técnicas y científicas dedicadas al estudio y certificación de algoritmos de seguridad (Vanstone, 2004b). Estos algoritmos responden en tiempos menores comparados con otros algoritmos basados en criptografía asimétrica, utilizando llaves de menor longitud, lo que hace que los algoritmos requieran menor uso de memoria, pero sin sacrificar niveles de seguridad. Este tipo criptografía es totalmente aplicable, tanto a sistemas electrónicos móviles como a aplicaciones industriales (Vanstone, 2004a), donde se requiera restringir y proteger la información que se manipula en tiempo real sin generar retrasos significativos en el funcionamiento de todo el sistema.

Las aplicaciones que implementen ecc en dispositivos móviles se ejecutan más rápido, esto implica menor producción de calor, menor uso de memoria y menor consumo energético, características que siempre son una ventaja en cualquier sistema electrónico.

Referencias bibliográficas

Al-Aali, G., Boneau, B. y Landers, K. (2000). Diffie-Hellman Key Exchange. En J. A. Izaguirre, J. Furgeson y Q. Ma (Eds.), *Proceedings of CSE 331, Data Structures* (pp. 67–74). Notre Dame (EE. UU.): University of Notre Dame.

Goyal, K. y Kinger, S. (2013). Modified Caesar Cipher for Better Security Enhancement. *International Journal of Computer Applications, 73*(3), 26–31. http://doi.org/10.5120/12722-9558

Hankerson, D., Menezes, A. J. y Vanstone, S. (2006). *Guide to Elliptic Curve Cryptograph*. Nueva York: Springer.

Kar, J. y Majhi, B. (2009). An Efficient Password Security of Key Exchange Protocol based on ECDLP. IACR Cryptology ePrint Archive. En *12th International Conference on Information Technology* (pp. 1–5). Bhubaneswar (India): College of Engineering and Technology.

Lauter, K. (2004). The advantages of elliptic curve cryptography for wireless security. *IEEE Wireless Communications*, 11(1), 62–67. http://doi.org/10.1109/MWC.2004.1269719

Singh, G. y Supriya. (2013). A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. *International Journal of Computer Applications, 67*(19), 33–38.

Sutikno, S., Surya, A. y Effendi, R. (1998). An implementation of ElGamal elliptic curves cryptosystems. En *IEEE. APCCAS 1998. 1998 IEEE Asia-Pacific Conference on Circuits and Systems. Microelectronics and Integrating Systems. Proceedings (Cat. No.98EX242)* (pp. 483–486). Chiangmai (Tailandia): IEEE. http://doi.org/10.1109/APCCAS.1998.743829

Vanstone, S. (2004a). Public-Key Cryptography: Where is it Going? *Code and Cipher, 1*(3), 2–4.

Vanstone, S. (2004b). The Use of Public-Key Cryptography in BlackBerry. *Code and Cipher, 2*(1), 3–4.