Ciencias Matemáticas, Vol. 35, No. 1, 2021, Pag. 41-45
Recibido 11-2020, Aceptado 04-2021

Integración de curvas elípticas criptográficamente seguras al EJBCA
Integration of criptographically secure elliptic curves to the EJBCA

Arlet Ponce Alvarez[1], Teresa B. Pagés López[2], Yessica C. Castaño Sainz[1], Camilo Denis González [3]

Resumen En el presente trabajo se verifica la disponibilidad de una criptografía desarrollada sobre curvas elípticas que permite generar parámetros criptográfcos más efcientes que se integran al software EJBCA para poder generar certifcados digitales autónomos de clave pública más seguros y eficientes, y que tienen como antecedente estudios realizados por el Instituto de Criptografía.

Abstract In the present work the availability of a cryptography developed on elliptic curves is verifed, which allows to generate more eficcient cryptographic parameters that are integrated into the EJBCA software to generate safer and more efficient autonomous public key digital certifcates and which have as background studies carried out by the Cryptography Institute.

Palabras Clave
criptografía asimétrica, curvas elípticas, software EJBCA, biblioteca Bouncy Castle

Keywords
asymmetric cryptography, elliptic curves, EJBCA software, Bouncy Castle library

[1] *Instituto de Criptografía, Universidad de La Habana,La Habana, Cuba, arlet.ponce@matcom.uh.cu*
[2] *Instituto de Criptografía, Universidad de La Habana,La Habana, Cuba, teresa.bernarda@matcom.uh.cu*
[3] *Instituto de Criptografía, Universidad de La Habana,La Habana, Cuba,yessica.castano@matcom.uh.cu*
[4] *Instituto de Criptografía, Universidad de La Habana,La Habana, Cuba, kmilo.denis.glez@gmail.com*

Introducción

En la actualidad las tecnologías constituyen una herramienta imprescindible para el ser humano por lo que se ha impuesto el intercambio constante de información por las redes de computadoras, y ha sido tendencia global que estas y sus sistemas sean cada vez más abiertos y estén interconectados entre sí. Este intercambio, en muchas ocasiones, se realiza sobre canales inseguros de comunicación, por lo que la información está expuesta a ser leída y modificada por intrusos no deseados.

Esta situación ha provocado un llamado de atención sobre la necesidad de implementar y poner en práctica mecanismos que garanticen la seguridad de las redes y los datos, para así poder lograr un empleo óptimo de las tecnologías de la información.

La Criptografía es la ciencia encargada de garantizar la seguridad y resguardo de la información y los datos confidenciales de instituciones y personas. Con la implementación de mecanismos de seguridad que asumen la protección criptográfica es posible asegurar las redes y datos que permiten el empleo óptimo de las tecnologías de la información. Es imprescindible para lograrlo que las claves secretas que los usuarios utilizan para resguardar la información estén protegidas de cualquier tipo de ataque en la red, ya sea convencional, físico, lógico, etc.

La Criptografía, según el manejo de las llaves, se puede dividir en simétrica y asimétrica. Simétrica es la que utiliza la misma llave para cifrar y descifrar; y asimétrica, la que tiene dos llaves, una pública para cifrar y validar firmas y una privada para descifrar y firmar digitalmente. Los métodos criptográficos permiten garantizar la protección de la información y garantizan la confidencialidad, integridad, autenticidad y el no repudio de la comunicación,carácterísticas de la seguridad que se definen a continuación a partir de dos entidades, A y B, que matienen comunicación, y un intruso denominado E [12].

Definición 1 *Confidencialidad.*

La información esté accesible únicamente al personal autorizado: un mensaje enviado por A para B no debería ser leído por E.

Definición 2 *Integridad.*

Prevenir cambios no autorizados e impropios: B debería ser capaz de detectar si lo enviado por A ha sido modificado por E.

Definición 3 *Autenticidad.*

Es la identificación y la garantía de origen de la información: B debería ser capaz de verificar que lo enviado por A realmente proviene de A.

Definición 4 *No repudio.*

Evita que el receptor pueda negar su participación en la comunicación: no solamente B sepa que el mensaje es enviado por A, sino que pueda ser capaz de convencer a una tercera de que el origen del mensaje fue en A, así A no puede negar que envió el mensaje a B.

El problema de investigación a abordar en el presente trabajo es verificar la disponibilidad de una criptografía desarrollada sobre curvas elípticas que permita generar parámetros criptográficos más eficientes y con igual o mayor seguridad que la que ofrece la criptografía asimétrica sobre la aritmética modular. Conjuntamente, se propone integrar esta criptografía al software EJBCA, Enterprise Java Bean Certificate Authority, para generar y autenticar certificados digitales de clave pública. Esta integración propiciará la utilización de estudios realizados previamente en el Instituto de Criptografía, cuyos resultados se quieren testear en la práctica.

A partir del problema planteado se formula la hipótesis que será comprobada en la investigación: la posibilidad de inclusión de las curvas elípticas seguras, obtenidas a partir de los algoritmos propuestos en proyectos previos a esta investigación, en el software EJBCA, para su futuro uso en la generación de certificados digitales criptográficos.

Objetivo General:

Integrar las curvas elípticas propuestas al software EJBCA para tener una herramienta con elementos autónomos con la que se puedan generar certificados digitales.

1. Materiales y métodos

La investigación se desarrolló en el ámbito de la Criptografía, siendo elementos principales los conocimientos relacionados específicamente con la criptografía asimétrica y con la PKI, Public Key Infraestructure [3].

Definición 5 *Public Key Infraestructure: Infraestructura compleja compuesta por hardware, software, bases de datos, redes, procedimientos de seguridad y obligaciones legales necesarias para crear, gestionar, almacenar, distribuir y revocar certificados digitales.*

La generación de nuevas curvas elípticas seguras fue objeto de estudio en investigaciones previas a este trabajo, en el Instituto de Criptografía, cuyos resultados se publicaron en [7]. Los resultados obtenidos en dicho proyecto se utilizaron como fuente directa de información, así como los manuales de usuario del software EJBCA [8].

1.1 Criptografía asimétrica

Dentro de los esquemas criptográficos de mayor interés en la actualidad destacan los asimétricos. La criptografía asimétrica o criptografía de clave pública es el método criptográfico que usa un par de claves: una pública que se emplea para cifrar o validar firmas digitales y que es accesible a cualquier persona receptora del mensaje; ya sea en un directorio público o en un certificado digital de clave pública; y otra privada con la que se descifra la información o se firma digitalmente y que es propiedad exclusiva de la persona emisora y debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

La criptografía de clave pública se caracteriza por el uso de problemas matemáticos computacionalmente difíciles, los más utilizados son el problema de la factorización de números enteros grandes y el problema del logaritmo discreto. Actualmente para ambos casos existen algoritmos de tiempo subexponencial que permiten resolverlos; pero cuando se trabaja con esquemas criptográficos que usan largos de claves muy grandes no es posible romper el cifrado. Esta situación dio lugar a la utilización de las curvas elípticas como plataforma matemática no explorada hasta entonces en el diseño de los protocolos criptográficos.

1.2 Curvas elípticas

Para entender la criptografía de curvas elípticas es preciso primero abordar el tema de curvas elípticas:

Definición 6 *Una curva elíptica E definida sobre un campo Fp, es el conjunto de soluciones (x,y), donde x y y pertenecen a Fp y satisfacen la ecuación de Weierstrass: [Baier, 2002][3][4]*

$$y^2 = x^3 + ax + b(mod\, p) \tag{1}$$

La anterior ecuación es llamada definición de la curva elíptica sobre un campo Fp. Las variables x y y son constantes que también pertenecen al campo Fp y deben satisfacer la ecuación:[6][1][3][5]

$$4a^3 + 27b^2 \neq 0(mod\, p) \tag{2}$$

Además de los puntos que pertenecen a la curva o puntos soluciones, existe un punto extra o punto en el infinito. Este punto se incluye por razones técnicas, ya que resulta necesario para las operaciones matemáticas que se realizan sobre la curva [11].

1.3 Criptografía de curvas elípticas

La Criptografía de Curvas Elípticas es una variante de la criptografía asimétrica que se basa en las matemáticas de las curvas elípticas que fue una propuesta realizada en el año 1985 por sus autores Neal Koblitz y Víctor Miller bajo el argumento de las ventajas que introducen las curvas elípticas en la criptografía asimétrica, referidas a la garantía de la seguridad criptográfica con largos de claves menores y además por la velocidad que se logra alcanzar en las operaciones de cifrado y descifrado, muy superior al RSA[1] [10]. De hecho,

[1] RSA: Rivest, Shamir,Adleman. Sistema criptográfico de llave pública.

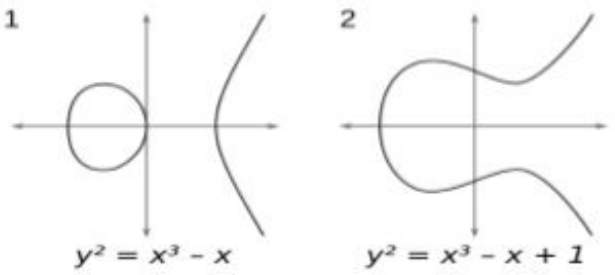

Figura 1. Curvas elípticas

se estima que una clave RSA de 4096 bits da el mismo nivel de seguridad que una clave de 313 bits de un sistema de curva elíptica.

Esta diferencia resulta realmente notable cuando se trabaja con dispositivos móviles, dado que una operación como generar una clave, que tardaría unos pocos segundos mediante un sistema de curva elíptica, podría demorarse varios minutos utilizando un sistema como RSA. El interés en estos sistemas aumenta cada día, tanto en el ámbito académico como en el ámbito empresarial.

Los parámetros de dominio establecen el contexto para realizar las tareas requeridas basándose en la teoría de curvas elípticas. Estos definen una curva E sobre una campo finito Fp, un punto base G que pertenece $E(Fp)$, y su orden n. Usualmente los parámetros de dominio son compartidos por un grupo de entidades, pero en algunas aplicaciones pueden ser específicas para cada usuario.

Estos parámetros en curvas elípticas se componen de la séxtupla [9]:

$$T(p,a,b,G,n,h) \tag{3}$$

p**:** indica el número de elementos del campo finito primario.

a **y** b**:** elementos que pertenecen al campo finito primario y forman parte de la definición de la curva.

G**:** un punto base con coordenadas.

n**:** es el orden de G. Al multiplicar el punto por este número el resultado es el punto en el infinito.

h**:** es el número de puntos del campo finito dividido por el orden del punto.

1.4 Infraestructura de LLave Pública

El uso de la criptografía asimétrica exige de medios y tecnologías para la distribución y administración de la clave pública de sus usuarios, de forma tal que puedan ser garantizados los servicios criptográficos asociados de: cifre, descifre, firma y validación, soportados en la confidencialidad, autenticidad, integridad y no repudio que tienen como base estos sistemas [2]. De igual forma, el uso de la criptografía asimétrica infiere la necesidad de almacenar de manera segura la relación que se establece entre la clave pública y la información personal de los usuarios. Una de las tecnologías más seguras y efectivas para la creación de estas condiciones es la infraestructura de clave pública, conocida en la literatura como Public Key Infrastructure (PKI) por sus siglas en inglés, fundamentada en la generación, almacenamiento y uso de los certificados digitales de clave pública.

Una de las tareas de la PKI es la emisión y distribución de certificados criptográficos, que son mecanismos que contienen los datos necesarios para establecer la comunicación y garantizan formas de verificación de la seguridad e integridad del intercambio de los datos. Un software muy conocido que permite el diseño e implementación de una PKI es el EJBCA, Enterprise Java Bean Certificate Authority [8]. Este es gratis y contiene un paquete de creación y mantenimiento de Autoridad de Certificación. Está diseñado para ser una plataforma independiente y completamente integrable, lo que permite un mayor grado de escalabilidad.

2. Descripción del proceso/software // Máquina virtual (VM)

Se utilizó una máquina virtual (VM) de EJBCA Community 6.3.1.1 EJBCA, Enterprise Java Bean Certificate Authority. Esta máquina virtual está configurada con 2 procesadores y 3GB RAM para correr el software de manera óptima.

Las características del sistema que tiene esta VM son las siguientes: sistema operativo Ubuntu Server 12.04.3 LTS, proyecto EJBCA ce 6.3.1.1, J Boss 7.1.1, MariaDB 5.5, OpenJDK 1.7.0, Apache Ant 1.8.2, x-windowlxde-core. Fue montada con VMware Workstation. El EJBCA ofrece interfaces web, y para acceder por el navegador se pueden utilizar las siguientes vías: EJBCA public Web: https://ejbca.localdomain:8443/ejbca EJBCA admin web: https://ejbca.localdomain:8443/ejbca/ adminweb

2.1 Proceso de integración

Se buscó una manera de modificar el software EJBCA [8] para poder incluirle elementos deseados, en este caso las curvas elípticas. No se encontró forma de hacerlo directamente al EJBCA, pues en este se utiliza la API de Bouncy Castle para realizar todas las operaciones criptográficas que se ofrecen como funcionalidades. Debido a esto, la solución que se halló fue modificar directamente la API para integrarle los elementos.

Este proceso consta de dos etapas: en un primer momento se adiciona las curvas a la biblioteca Bouncy Castle (BC Java) y luego fue necesario agregar las configuraciones necesarias al EJBCA para que reconociera los cambios realizados y presentara entre sus opciones disponibles los nuevos elementos en la interfaz de administración.

En el desarrollo de este proceso fue necesario descargar el código fuente del Bouncy Castle, la misma versión que se utiliza en la máquina virtual del EJBCA, para evitar conflictos. En este se añadieron las curvas elípticas y sus respectivos parámetros.

Estos elementos se crearon en un nuevo paquete. Este paquete se incluyó en otros ficheros para que fueran reconocidos por Bouncy Castle. Estos fueron org.bouncycastle.asn1.x9.ECNamedCurveTable, para incluirlos en la tabla de curvas conocidas, y org.bouncycastle.jcajce.provider.asymmetric.util.ECUtil, para integrarlas al proveedor.

Luego, se compiló el proyecto, y se incluyó este .jar a las bibliotecas que utiliza el EJBCA. O sea, se sustituyó el Bouncy Castle del EJBCA por este, que se modificó con las nuevas curvas.

En la segunda fase, ya integrado este módulo al EJBCA, se compila el proyecto de EJBCA completo para que reconozca los cambios y cargue la interfaz visual modificada.

Se utilizaron los comandos ant-clean, ant-build, ant-deploy y ant-install. Luego se reinició el servidor Jboss. Compilado y cargado el proyecto, ya se logró la integración de las nuevas curvas al software.

3. Resultados

Se confirmó la posibilidad de modificar el software EJBCA para poder integrarle elementos necesarios para el trabajo en el Instituto de Criptografía. Del grupo de curvas elípticas, generadas y disponibles, se validó las que fueran factibles integrar al software mediante la verificación del cumplimiento de los requerimientos de la librería Bouncy Castle para su integración. A continuación, se presentan imágenes que muestran el resultado de verificar si es posible generar claves con la curva a integrar.

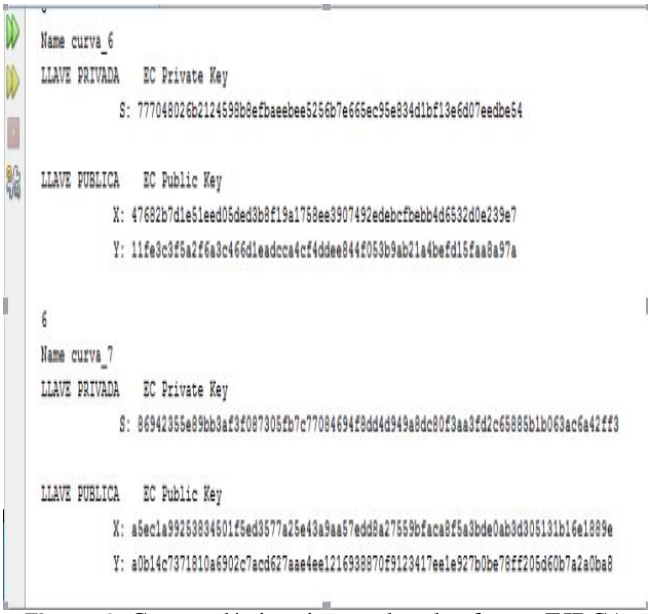

Figura 2. Curvas elípticas integradas al software EJBCA

Las curvas elípticas criptográficamente seguras propias del Instituto de Criptografía que pasaron satisfactoriamente el proceso se integraron al software de forma tal que pueden ser utilizadas para la generación futura de certificados digitales A continuación se presentan las imágenes Figura 3 y Figura 4 que validan la correcta integración de las curvas al EJBCA.

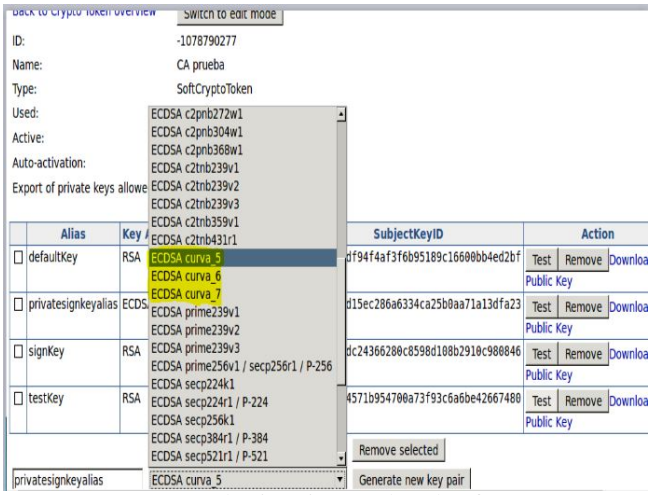

Figura 3. Curvas elípticas integradas al software EJBCA

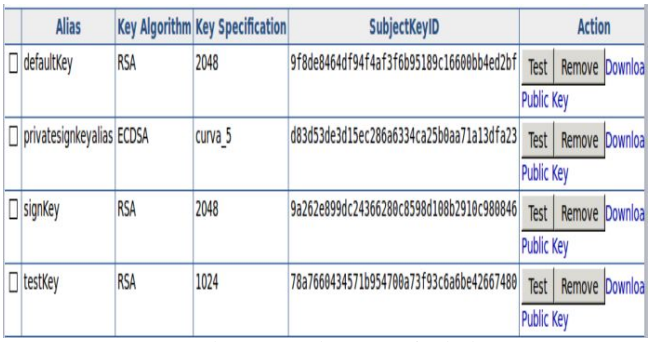

Figura 4. Crypto tokens creados a partir de las curvas elípticas integradas al software EJBCA

Conclusiones

Durante el desarrollo de esta investigación se realizó el estudio de los principales elementos vinculados a la criptografía de curvas elípticas y la base matemática que utiliza. También se profundiza en el conocimiento del software EJBCA como herramienta para el diseño y desarrollo de una PKI, centrándonos en la fase de integrar nuevos elementos al mismo.

A partir de este estudio se logró la integración al software EJBCA de las curvas elípticas seguras, generadas en proyectos anteriores desarrollados en el Instituto de Criptografía. Con la integración de estos elementos se logra que el Instituto pueda erigirse como una Autoridad de Certificación con capacidad de generar certificados digitales de clave pública, basado en curvas elípticas, aspecto novedoso respecto a la PKI que actualmente posee el país.

Se obtuvo una versión del software EJBCA con las curvas elípticas integradas que se puede montar de forma factible en el servidor del Instituto de Criptografía, proporcionando los servicios criptográficos que hoy se necesitan en la informatización de la sociedad.

Esta solución dio lugar a que el Instituto de Criptografía sea independiente en la generación de curvas elípticas seguras, garantizando así elementos criptográficos fuertes que certifican la calidad de este proceso.

Agradecimientos

Agradecer a mi familia, a mis tutores y compañeros de trabajo.

Referencias

[1] Akbani, R. (2018). Elliptic curve cryptosystem and its applications.

[Baier, 2002] Baier, H. (2002). *Efficient Algorithms for Generating Elliptic Curves over Finite Fields Suitable for Use in Cryptography*. PhD thesis, Universidad de Darmstadt.

[2] Franchi, M. (2012). *Algoritmo de encriptación de clave asimétrica*. PhD thesis, Universidad Nacional de La Plata.

[3] Hankerson, D., Menezes, A., and Vanstone, S. (2003). *Guide to Elliptic Curve Cryptography*. Lithuanian Mathematical Society.

[4] Luna, C. (2009). Aplicaciones de las curvas elípticas a la criptografía.

[5] Montiel, G., Hernández, C., and Cortes, Y. (2011). Implementación del criptosistema de curva elíptica en entornos móviles. *Víncuos*, 8.

[6] Naehrig, M. (2015). Selecting elliptic curves for cryptography real worldïssues. Cambridge University Press.

[7] no, Y. C. (2015). *Generación de curvas elípticas con buenas propiedades criptográficas sobre campos primos*. PhD thesis, Universidad de La Habana.

[8] PrimeKey, E. t. o. s. c. (2019).

[9] Robles, A. (2016). *Curvas elípticas en criptografía*. PhD thesis, Universidad de La Habana.

[10] Sánchez, P. (2015). *Análisis de los mecanismos de encriptación para la seguridad de la información en redes de comunicaciones*. PhD thesis, Pontificia Universidad Católica del Ecuador.

[11] SB, T. and RM., C. (2017). Análisis del cifrado elgamal de un módulo con curvas elípticas propuesto para el gnupg.

[12] Willems, W. and García, I. (2010). *Una introducción a la criptografía de clave pública*. Ediciones Uninorte.