UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
SEGURIDAD DE AUTENTICACIÓN DE CLAVE PÚBLICA DE CURVA ELÍPTICA
Línea de Investigación:
Sistemas de Información e Informática
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación (TIC)
Autora:
Jessica Viviana Córdova Moreta
Tutor:
MSc. Pablo Recalde

Quito – Ecuador

2023

APROBACIÓN DEL TUTOR

Yo, MSc. Pablo Recalde con C.I: 1711685055 en mi calidad de Tutor del proyecto de investigación titulado: SEGURIDAD DE AUTENTICACIÓN DE CLAVE PÚBLICA CURVA ELÍPTICA.

Elaborado por Jéssica Viviana Córdova Moreta, de C.I: 1721539516, estudiante de la **Maestría de Seguridad Informática** de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2023

Firmado electrónicamente por:
PABLO MARCEL
RECALDE VARELA

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Jéssica Viviana Córdova Moreta con C.I: 1721539516, autora del proyecto de titulación denominado: AUTENTICACIÓN DE CLAVE PÚBLICA DE CURVA ELÍPTICA. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autora del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., septiembre de 2023

_____

Firma

orcid: 0000-0002-1760-8106

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

A continuación una breve descripción de la problemática que da origen al presente trabajo.

Contextualización del tema

Según afirma (Albuixech, 2016), IOT son dispositivos capaces de controlar toda el área del hogar, el usuario a través de un dispositivo móvil puede configurar las funciones y cambios de seguridad, iluminación, temperatura, entre otras funciones.

Es decir que la evolución de IoT va solventando problemas tanto empresariales como la vida cotidiana de las personas, ya es una realidad y actualmente tiene mucha fama. Las aplicaciones para el uso de estos dispositivos son infinitas. Como por ejemplo: un frigorífico normal de un hogar el mismo que contiene alimentos con fecha de caducidad, en este ejemplo se podría conectar el frigorífico a su teléfono móvil y que mediante la aplicación este anuncie cuando los productos estén a punto de caducar.

Esta tecnología es una serie de soluciones creadas por diferentes fabricantes, la cual sigue evolucionando. Actualmente la seguridad de la información es un tema importante a tratar, algunas empresas ya cuentan con una seguridad de cifrado el cual protege la información de ataques o de secuestros.

El presente documento tiene como objetivo investigar acerca de la autenticación de clave pública de curva elíptica para sugerir en qué ambiente puede ser aplicada esta autenticación de clave pública de curva elíptica.

En el amplio tema del Internet de las cosas se procede a investigar si la aplicación es aceptable sólo a nivel de hardware o a nivel de software también de la misma manera explicar los beneficios de esta seguridad.

Problema de investigación

Si bien es cierto los sistemas informáticos y las redes hoy en día ya cuentan con un tipo de seguridad o autenticación, la autenticación de clave pública de curva elíptica es un nuevo tema que se está acoplando o enlazando en dispositivos.

La autenticación es muy importante al momento de acceder a un sistema o a un dispositivo, para evitar el acceso de personas no autorizadas.

La seguridad de autenticación en una empresa es fundamental ya que la persona que ingresa con sus credenciales es la responsable de las actividades que se realizan con ese usuario.

Uno de los problemas radica también con el mal uso que los empleados hacen con las credenciales por ejemplo prestar su usuario y contraseña para que un compañero de trabajo realice cierta acción.

En la presente investigación se determina los ambientes en los que puede ser aplicada la seguridad de autenticación de clave pública de curva elíptica también responde a la interrogante: ¿Qué garantiza que el acceso a un IoT sea seguro a nivel de hardware y software?

Objetivo general

Analizar los beneficios que otorga esta la seguridad de autenticación de clave pública de curva elíptica.

Objetivos específicos

1. Contextualizar el funcionamiento de la autenticación mediante curva elíptica
2. Establecer el proceso de funcionamiento de la curva elíptica en la encriptación.
3. Proponer esta autenticación como medio seguro para software como para hardware.

Vinculación con la sociedad y beneficiarios directos:

Esta investigación busca democratizar el acceso al conocimiento e inculca la aplicación de seguridad tanto en software como en hardware, mostrando los métodos, procesos de encriptación mediante curva elíptica. Esto implica también la capacitación a personas que manejan el tema, con el fin de aportar a la seguridad informática y de sistemas de información.

Este tema y aplicación es de gran impacto para la sociedad ya que con su aplicación se logrará incrementar la seguridad en los equipos.

Mediante la aplicación de esta seguridad los beneficiarios directos son las personas que adquieran equipos tecnológicos conocidos hoy en día como Internet de las cosas IoT.

Cómo vinculación de manera natural a la sociedad se establece el Objetivo de Desarrollo Sostenible número cuatro donde se asocia el proyecto con la educación de calidad la cual es clave para erradicar la pobreza. Otro objetivo de desarrollo sostenible que se puede asociar al proyecto es el número ocho que trata del trabajo decente y crecimiento económico.

Y por último se puede asociar con el número nueve el cual trata de la industria, innovación e infraestructura, se puede acotar que en la infraestructura de comunicaciones la población está conectada a nivel global con una cobertura de red móvil, la cual sigue avanzando día a día.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

En este apartado se manejan algunos de los conceptos de seguridad informática y curvas elípticas que dan respuesta a la seguridad de hardware y software.

1.1. Contextualización general del estado del arte

En el siguiente apartado se explica de forma detallada las ecuaciones de las cuales se forma la curva elíptica.

Curva

Puede ser utilizada para diferentes funciones como una vía, un dibujo entre otros como menciona (Pérez, 2022) viene “Del latín *curvus*, una curva es una línea (real o imaginaria) que se aparta de la dirección recta sin formar ángulos. Esto quiere decir que su dirección varía de manera paulatina y constante”.

La curva es representada de forma gráfica dependiendo como varían sus valores, la gráfica se realiza en dos ejes conocidos como X eje horizontal y eje Y vertical.

Curva elíptica

Actualmente la curva elíptica es un tema de estudio muy útil como lo menciona el autor de (EcuRed, s.f.). “Curva Elíptica (del inglés: Elliptic curve cryptography, ECC) es una variante de la criptografía asimétrica o de clave pública basada en las matemáticas de las curvas elípticas”.

Funcionamiento de Curva elíptica

En la página web Redacción KeepCoding (2023) se explica que “la curva elíptica se define sobre los números reales, se puede expresar matemáticamente por medio de la siguiente ecuación:$y^2 + axy + by = x^3 + cx^2 + dx + e$

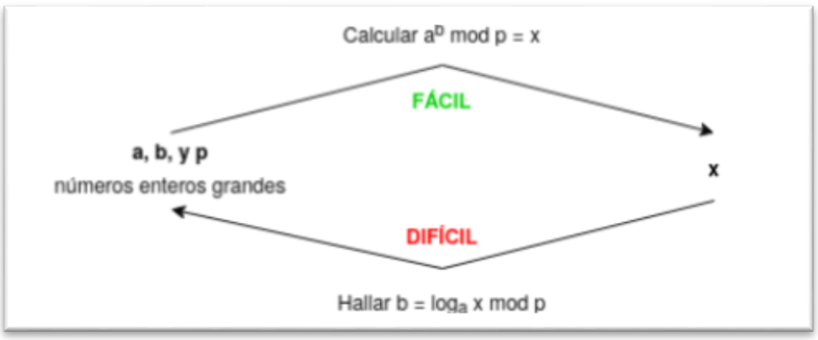
De modo que los puntos infinitos (x, y) de curva elíptica tienen como coordenadas los números reales que, adicionalmente, cuentan con las siguientes condiciones:

- La curva elíptica que representa los valores no se cruza sobre sí misma.
- La curva elíptica no presenta ningún pico.”

Comparando con otros métodos de encriptación se muestra la diferencia como por ejemplo el problema de logaritmo discreto usado en Diffie-Hellman:

Figura 1.

Cifrado de Diffie-Hellman



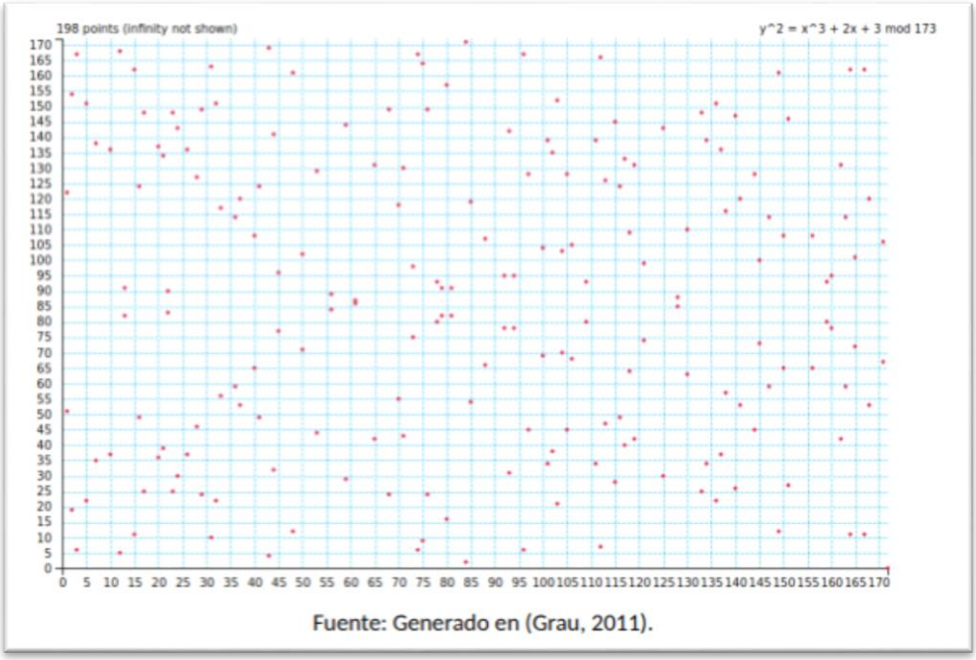
Nota: Figura tomada de (Gallo, 2022)

El cifrado de Diffie-Hellman trata de lograr el intercambio de clave secreta por medio de un canal inseguro como es Internet.

En contra posición al ejemplo anterior se muestra el proceso de curva elíptica en la cual trabaja una serie de operaciones conocidas como multiplicación de puntos, sobre un plano que opera todo el tiempo con puntos de coordenadas:

Figura 2.

Criptografía de curva elíptica



Nota: Figura tomada de la Tesis de Maestría de Software Educativo para Aprendizaje de Cueva Elíptica (Gallo, 2022).

Se evidencia un problema unidireccional en el cual la criptografía de curva elíptica tiene fortaleza y es el llamado logaritmo discreto para curvas elípticas, para esto es necesario comprender las operaciones básicas como son suma y multiplicación, como por ejemplo sumar puntos no equivalentes para puntos en un eje cartesiano.

Si se inicia de un punto racional y se realiza la gráfica de la recta también con pendiente racional, esto significa que solo se necesita un punto racional para encontrar a todos los infinitos en otras palabras uno para gobernarlos a todos, entonces la dificultad para todo es encontrar solo un punto racional, para lo cual se cuenta con algoritmos.

Uso de la curva elíptica en la criptografía

Por el uso importante de criptografía el autor (Villanueva, 2014) menciona que "La criptografía de curva elíptica fue introducida por Neal Koblitz y Víctor Miller en el año de 1985. La razón por la cual es atractiva, es que no se conocen algoritmos eficientes para resolver el problema del logaritmo discreto".

Con el pasar del tiempo la seguridad informática se va convirtiendo en una herramienta necesaria para resguardar los sistemas informáticos.

La curva elíptica se usa con algoritmos de clave pública como por ejemplo firma digital, cifrado de información e intercambio de claves.

Este tipo de cifrado es importante porque protege los datos de ciberataques, prácticamente es un control que autoriza el acceso, esto permite tener un control detallado sobre el acceso y saber a qué información se accedió.

Clave pública

En la página S.L.U (2020) menciona que "el procedimiento de la criptografía asimétrica, el destinatario genera su par de claves y comunica la clave pública a la otra parte, guardándose la clave privada para sí. El proceso de transmisión es sencillo y se lleva a cabo a través de organismos de certificación o mediante los llamados servidores de claves, en los que se puede almacenar la clave. El remitente codifica su mensaje con esta clave pública y puede enviarlo al destinatario como "texto secreto". Desde el momento del cifrado, el destinatario sólo podrá descifrar este mensaje con su clave privada. Por esta razón, en principio, el canal del mensaje puede elegirse libremente: si el mensaje cifrado es interceptado, su contenido permanece oculto para el atacante"

El cifrado en clave pública utiliza un par de claves para cifrar y autenticar la información, este proceso se conoce también como criptografía asimétrica, esto significa que puede distribuirse sin afectar la seguridad.

Clave privada

En el libro Ferro (2020) se menciona que “El cifrado de clave privada o cifrado simétrico se basa en que una clave puede cifrar o descifrar la información. La ventaja de este enfoque es que el proceso es muy rápido y una sola tecla se utiliza para ambos extremos de la cadena de cifrado. La preocupación es la protección de la clave como un punto único de fallo para la seguridad. La gestión de claves es la principal preocupación cuando se utiliza el cifrado de la clave principal”

Se comprueba que la preocupación que se menciona sobre la protección de datos hace que este tipo de cifrado sea el menos usado, ya que el punto objetivo en este tema es la seguridad y protección de datos mediante la aplicación del cifrado correcto, actualmente algunas empresas no toman este punto como primordial cuando sí deberían hacerlo.

Tabla 1.

Clave pública y privada

Diferencias	
Clave pública	Clave privada
Es distribuida entre todos los posibles destinatarios	Se almacena en el equipo del emisor

Nota: Elaboración propia

Cifrado de extremo a extremo

El cifrado de datos es un proceso que utiliza un algoritmo para transformar los caracteres de texto estándar en un formato no legible. Este proceso utiliza claves de cifrado para mezclar los datos, de manera que solo los usuarios autorizados pueden leerlos. El cifrado de extremo a extremo utiliza este mismo proceso, pero va un poco más lejos, ya que protege las comunicaciones desde un punto final a otro (IBM, s.f.).

Se puede tomar como ejemplo a la aplicación más utilizada que es WhatsApp, esta aplicación poco a poco va mejorando su seguridad, hoy en día cuenta con cifrado de extremo a extremo, si bien es cierto la mayoría de usuarios no conocen el dignificado de esta acción siendo la más importante en cuanto a seguridad.

El cifrado de extremo a extremo en este caso, garantiza que si un usuario envía una fotografía esta permanezca cifrada y solo se descifrará cuando llegue al usuario receptor, lo mismo sucede con notas de voz, videos y mensajes.

Como se menciona “Uno de los aspectos más destacados del tipo de cifrado que utiliza ahora WhatsApp es la forma en la que se gestionan las claves de cifrado. En lugar de almacenar esas claves en un servidor centralizado y gestionado por personal de WhatsApp, el cifrado extremo a extremo funciona mediante el almacenamiento de esas claves de cifrado en el dispositivo de cada usuario” (Pastor, 2016).

Esto significa que ni el personal de whatsApp puede tener acceso a descifrar los mensajes enviados por los usuarios, ya que su clave se queda encriptada en el dispositivo del usuario.

Figura 3.

Ejemplo de cifrado

Nota: Tomado de (Pérez, 2022)

Según el paper tomado de López (2023) indica que “el cifrado de extremo a extremo ayuda a proteger el contenido de los mensajes, texto e incluso archivos para que nadie los entienda excepto su destinatario”

Esto prueba que un mensaje no fue alterado o dañado, las herramientas de cifrado de extremo a extremo son las más usadas por sus varias funciones.

1.2. Proceso investigativo metodológico

En el presente trabajo se pretende alcanzar los objetivos mencionados mediante la metodología analítica y deductiva.

Metodología de investigación

Esta metodología es la más usada para trabajos de investigación ya que “La metodología de la bibliografía es el método que utilizarás para resolver un problema de investigación mediante la recopilación de datos utilizando diversas técnicas, proporcionando una interpretación de los datos recopilados y sacando conclusiones sobre los datos de la investigación” (Questionpro, 2023).

Método analítico

Es un método usado frecuentemente ya que en todo tema de investigación se debe analizar, comprobar y de este proceso obtener resultados los cuales son analizados nuevamente para experiencias futuras como menciona el autor “Este método consiste en la aplicación de la experiencia directa (lo propuesto por el empirismo) a la obtención de pruebas para verificar o validar un razonamiento, a través de mecanismos verificables como estadísticas, la observación de fenómenos o la replicación experimental” (Editorial Etecé, 2023).

Es método analítico es aplicado en esta investigación ya que trata de la experiencia directa y razonamiento, en el contenido del documento se puede evidenciar casos reales de encriptación en aplicaciones.

Método deductivo

Se conoce como método o razonamiento deductivo a un tipo de razonamiento lógico que se caracteriza por inferir de manera necesaria una conclusión a partir de una serie de premisas (Enciclopedia Humanidades, 2023).

Con este método se obtienen argumentos válidos referentes a la información obtenida de diferentes autores, este método es importante en este trabajo ya que trata de analizar el pensar de cada autor para deducir sus ideas.

CAPÍTULO II: PROPUESTA

En el siguiente apartado se menciona conceptos básicos de software y hardware, tomando en cuenta también la aplicación de encriptación.

2.1 Fundamentos teóricos aplicados

Para comprender de mejor manera la investigación se parte de conceptos básicos, luego se procede a explicar la aplicación de encriptación con curva elíptica en hardware y en software.

Hardware

Se conoce como hardware como algo físico, tangible y que es parte de algo como lo menciona el autor “aquel dispositivo necesario para iniciar el funcionamiento de la computadora (dispositivos necesarios para el funcionamiento del ordenador), y el complementario, para realizar funciones más específicas” (Hapen Soluciones Informáticas, 2023).

Como se puede apreciar todo parte desde el hardware dependiendo las necesidades y funciones de cada componente del computador.

Los elementos del hardware interno se encargan de almacenar y procesar la información. En cambio, los periféricos son los encargados de ayudar a introducir o extraer información de la computadora (Juliá, 2023).

Cada componente físico del computador es muy importante por su funcionalidad y aporte, en el caso del hardware se menciona a los periféricos de entrada y salida.

Software

En cambio software es todo lo contrario al hardware corresponde a lo que no podemos tocar como es un programa de un computador como menciona el autor “El software es un conjunto de reglas o programas que dan instrucciones a un ordenador para que realice tareas específicas” (Arimetrics, 2022).

El complemento para el funcionamiento de un equipo informático es el software es decir los programas que van a ser utilizados en el ordenador. Una vez tomado en cuenta los conceptos básicos de hardware y software se mención IOT.

IOT

Se refiere a dispositivos inteligentes capaces de resolver un problema humano, como por ejemplo el dispositivo muy conocido actualmente como “Alexa” que identifica

la voz, recibe y ejecuta órdenes, según como van estos dispositivos recibiendo y ejecutando órdenes, van almacenando datos, como movimientos, horario de uso entre otros.

Esta importante evolución ayuda a detectar número de movimientos realizados de ser el caso en un lugar con sensores para análisis de datos, pero en el tema de investigación se investiga la seguridad en estos dispositivos.

Seguridad de software y hardware

Es importante aplicar seguridad a software y hardware, actualmente no es suficiente proteger solo a nivel de software ya que hardware también puede ser atacado para robar datos. Hoy en día IOT es muy utilizado en empresas, hogares y por ende esta información es debe ser resguardada.

A continuación se muestra las diferencias de cifrado entre software y hardware:

Tabla 2.

Diferencias cifrado de hardware y software

Cifrado	
Hardware	Software
Utiliza el algoritmo de dispositivo para el cifrado y descifrado.	Usa criptografía simétrica la cual aplica la misma clave para el cifrado y descifrado.
Se realiza con dispositivos de cifrado integrales.	Ocurre en la copia de seguridad de datos y migración.
Usa un dispositivo aislado por ser más Seguro.	Se lleva a cabo en un dispositivo aislado. Por lo tanto, es la opción más segura
Necesita que use un procesador dedicado separado. Si desea escalar, debe comprar nuevos dispositivos con la misma funcionalidad	Software no necesita ningún dispositivo adicional. Puede copiarlo fácilmente a otros controladores y computadoras cuando necesite ampliar la seguridad.
Un procesador dedicado ubicado en el dispositivo realiza el cifrado de hardware	Utiliza recursos informáticos para operaciones criptográficas.

Nota: Elaboración propia con datos tomados de (GEEKFLARE, 2023)

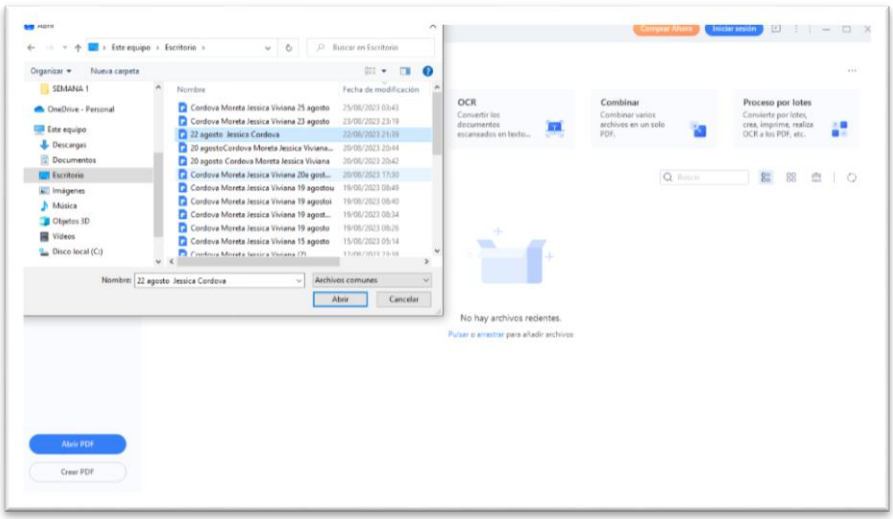
2.2 Descripción de la propuesta

Actualmente existen varias técnicas de realizar cifrado tanto para documentos, como para sistemas, se menciona a continuación un ejemplo muy simple de realizar encriptación en un documento con el software pdfelements:

Una vez instalado el software gratuito, se procede abrir el documento

Figura 4.

Encriptación con software pdfelements

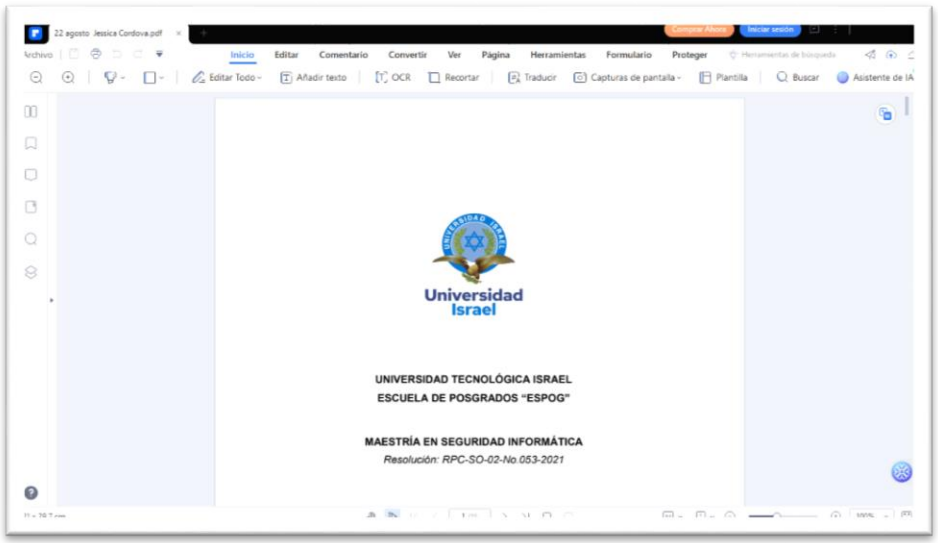


Nota: Elaboración propia

Como siguiente paso dar click en “Proteger”

Figura 5.

Abrir documento en pdfelements

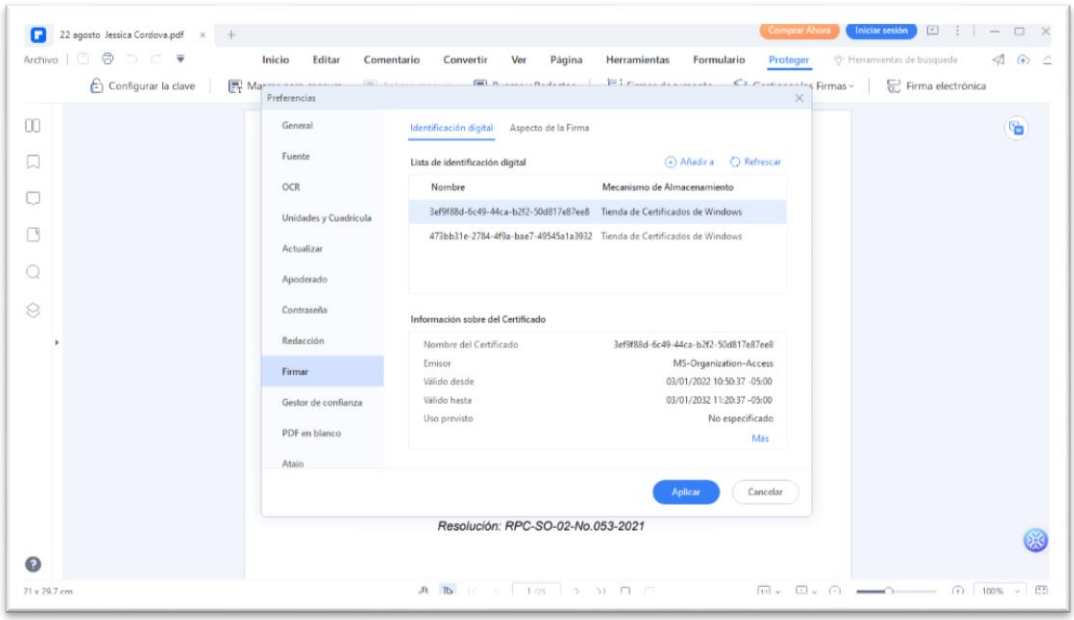


Nota. Elaboración propia

Se procede a gestionar las firmas

Figura 6.

Gestionar firmas para encriptar documento

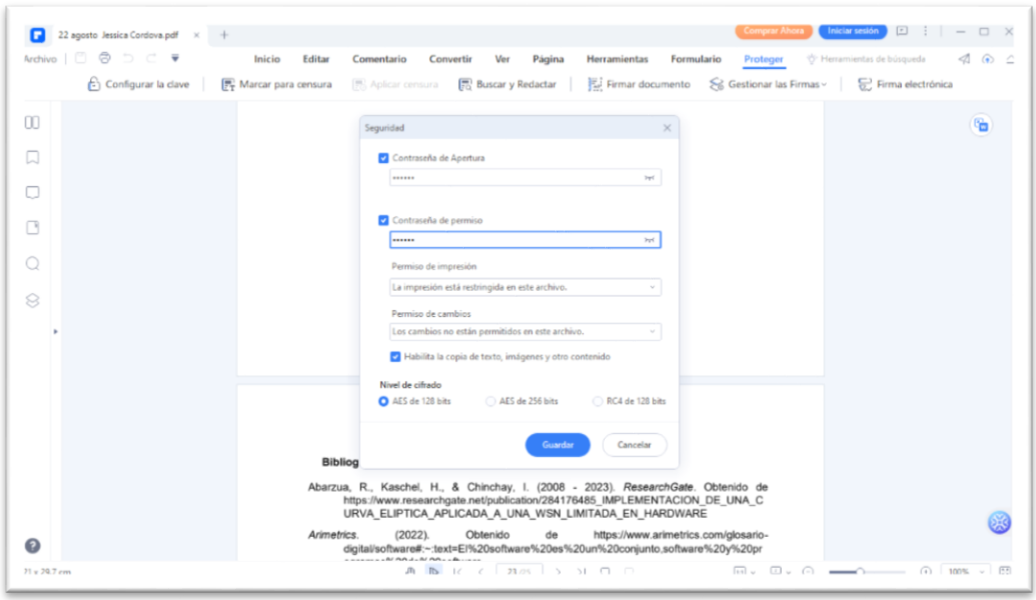


Nota. Elaboración propia

Se selecciona una de ellas y click en aplicar y se procede a ingresar la clave

Figura 7.

Ingresar una clave en pdfelements



Nota: elaboración propia

En la figura 7, se puede observar el nivel de cifrado de seguridad para el documento. Como ejemplo simple se muestra el proceso que puede realizarlo cualquier persona con conocimiento básico en protección de información.

Los algoritmos de curva elíptica el cifrado se basa en problemas matemáticos, en conclusión esta encriptación es la más actual, más segura y confiable por su nivel de complejidad para aplicar. Tomando en cuenta que la información viaja se convierte con lenguaje no comprensible normalmente se conoce como "*****" simbología no traducible humanamente, este tipo de código es generado por el algoritmo de encriptación, al ser de curva elíptica la llave es más pequeña y con un problema matemático sin solución.

La propuesta de uso de encriptación de curva elíptica que se plantea en este documento, trata de mostrar que con este tipo de cifrado proteger los datos de forma robusta es de gran ayuda en todos los ámbitos respecto a giro de negocio, se debe tomar en cuenta que la información es parte fundamental en toda empresa

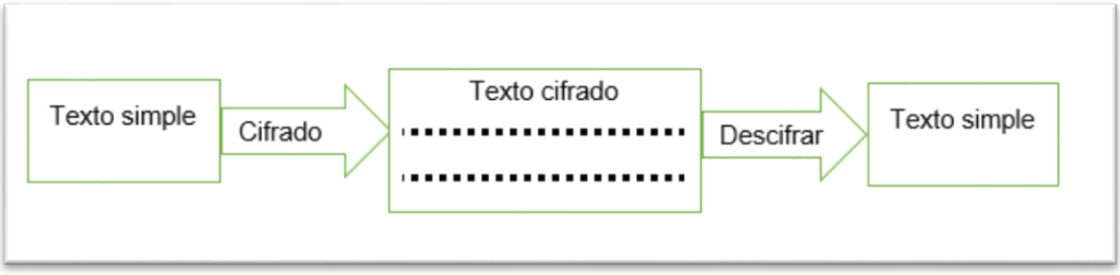
En el proceso de cifrado la curva elíptica siempre pasa en movimiento dependiendo los valores de a y b lo cual hace que los números en punto varíen y para el atacante se vuelve complejo acceder a la información.

Cabe recalcar que la complejidad de buscar solución a ciertos problemas matemáticos, en grupos infinitos de gran tamaño es extensa eso significa que para poder descifrar el atacante tendrá de coincidir en algún punto de movimiento de curvas.

El proceso es el siguiente:

Figura 8.

Proceso de cifrado



Nota: Elaboración propia con datos tomados de (Toro, 2020)

En la figura 8, se visualiza el proceso de cifrado desde que se digita el texto el lenguaje comprensible, al ser enviado el mensaje se convierte en texto con simbología,

llega el mensaje se descifra, se convierte en lenguaje comprensible y finalmente el receptor lo puede ver.

A nivel de hardware se detecta que el beneficio de utilizar encriptación con curva elíptica es que se puede usar llaves más cortas y esto también es beneficioso en cuanto al almacenamiento, por lo tanto no reduce el nivel de seguridad es una técnica muy efectiva y segura.

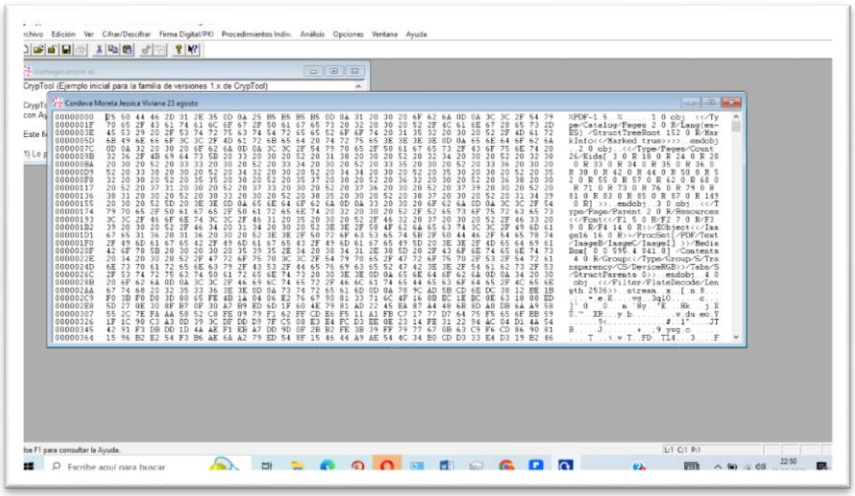
Otro beneficio es que los algoritmos es hardware son reconfigurables, su desempeño es súper bueno y tiene flexibilidad en tiempo de ejecución.

Existen herramientas como CrypTool que contienen funcionalidades para realizar el estudio de curva elíptica, como se mencionó anteriormente usando encriptación de curva elíptica, el uso de operaciones, los algoritmos asociados hace que resulte más difícil la vulnerabilidad.

Al abrir un archivo en CrypTool para encriptarlo se obtiene como resultado

Figura 9.

Encriptación con CrypTool

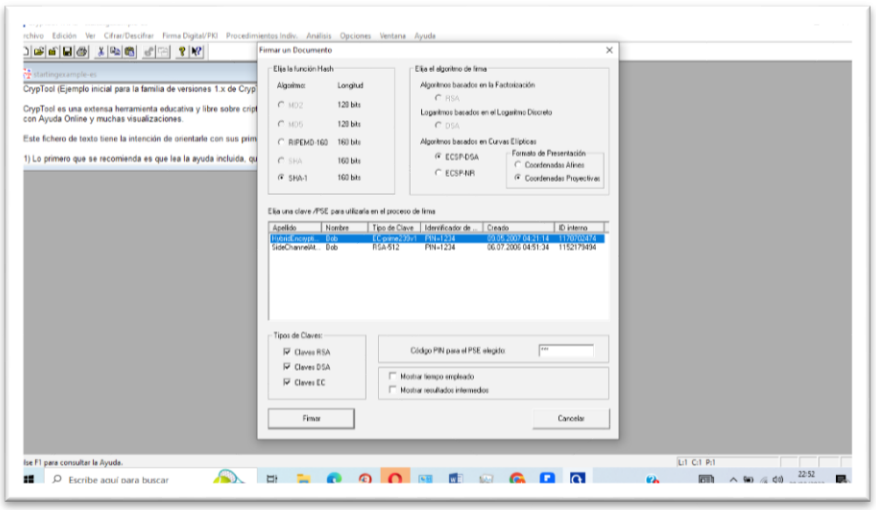


Nota: Elaboración propia

En la Figura 9, se observa prácticamente el resultado de la ejecución del problema matemático y algoritmo aplicado en encriptación de curva elíptica, por lo que la diferencia en la encriptación del ejemplo anterior es clara.

Figura 10.

Firma de documento en CrypTool



Nota: Elaboración propia

En la figura 10 se muestra el proceso de firma de un documento en el cual se puede seleccionar dos tipos de encriptación que son EC-prime y RSA.

2.3 Valoración de la propuesta

El siguiente apartado trata de la aplicación de autenticación de criptografía de curva elíptica.

Autenticación con clave elíptica en hardware

En la página web Rivera (2023) el autor afirma que: “La presencia de un dispositivo criptográfico hardware basado en algoritmos de curvas hiperbólicas.

Las curvas hiperbólicas se conocen y estudian desde hace más de un siglo. Pese a que su aplicación en criptografía tuvo detractores en sus inicios, hoy en día es uno de los campos más prometedores dentro de las modernas técnicas de cifrado asimétrico.

Si bien su complejidad teórica es relativamente elevada, presentan ciertas ventajas respecto a algoritmos tradicionales basados en la factorización, como RSA. Su implementación resulta muy eficiente por la propia aritmética de las curvas elípticas, y sobre todo, logra alcanzar niveles de seguridad óptimos con tamaños de clave muy reducidos. Esta propiedad hace de la criptografía con curvas elípticas ("ECC") la candidata ideal para ser implementada en dispositivos con escasa capacidad de cálculo, como los que nos encontramos en el ecosistema del IoT”

Es recomendable que todos los dispositivos cuenten con seguridad ya que mediante su funcionamiento almacenan datos como detección de movimiento en horarios y esa información es valiosa para poder mediante intuición saber el horario y actividades de una persona o empresa. A continuación se toma como ejemplo el cifrado el SSD y su funcionamiento tomando en cuenta que para personas y empresas es muy importante proteger los datos.

El cifrado aporta una capa de protección reforzada en caso de que se produzcan accesos no autorizados a las redes informáticas o dispositivos de almacenamiento. Con el cifrado, los intrusos no pueden acceder a los datos. En este artículo se explica el cifrado basado en software, las unidades de autocifrado (SED, por sus siglas en inglés) y el mecanismo de cifrado de los discos SSD (Kingstong, 2021).

El cifrado en dispositivos es importante ya que previene el acceso a hackers y por ende el secuestro de información, cabe recalcar que se puede aplicar varios tipos de cifrado, pero en este caso el tema de estudio es cifrado con curva elíptica.

En la página web Abarzua (2023) el autor afirma que “Las Redes de Sensores Inalámbricas (Wireless Sensor Network: WSN), utilizan dispositivos llamados nodos, formados por un hardware y un software con capacidades limitadas, porque su característica principal es el bajo costo, dimensiones pequeñas y de bajo consumo energético. Con este principio, es complicado establecer un esquema de seguridad robusto que asegure un nivel aceptable de seguridad a una aplicación que lo requiera. Por esto se hace necesario implementar un esquema de seguridad que sea ligero y a la vez seguro. Uno de los que la literatura recomienda es el uso de la criptografía en curva elíptica (ECC=Elliptic Curve Cryptography), como base para implementar diferentes esquemas de seguridad”

Se intuye que al contar con un dispositivo encriptado con curva elíptica es más seguro, como se mencionó anteriormente en proceso de generación de ecuaciones en el algoritmo de curva elíptica es el más confiable y seguro.

Puesta en funcionamiento del Algoritmo de una Curva Eliptica en WSN

Las redes de sensores son a menudo bidireccionales, permitiendo configurar los dispositivos, enviar comandos, o actuar sobre el ambiente. En este último caso, se les conoce como WSAN (del inglés Wireless Sensors and Actuator Networks). (Fundación Tekniker, 2023)

Según lo afirma Abarzua (2023) “El módulo Xbee (Xbee), (ZigBee), transportará la información, en forma de un punto de la curva elíptica, como un dato dentro

de su trama. La trama tiene una estructura adecuada para poder identificar las partes del dato. Lo anterior, se logra utilizando la trama tipo API, que maneja el Xbee. El estándar IEEE 802.15.4 define una trama API."

Se conoce como WSN a sensores inalámbricos que monitorean y registran ubicaciones, por lo que en su implementación usa un módulo arduino es decir un tipo de interruptor controlado por un circuito eléctrico, de tal forma que el módulo xbee brinda solución integrada a un medio inalámbrico para conectar dispositivos.

Autenticación con clave elíptica en Software

La página web AWS (2023), indica que "el uso de criptografìa en firma digital, los esquemas de firma digital son un tipo de criptografía de clave pública que garantiza la integridad, autenticidad y no repudio de los datos.

El proceso de firma puede considerarse como el cifrado del archivo mediante la clave privada. Para ello, la persona que firma utiliza su clave privada para producir una "firma" en un documento digital, como un archivo o un fragmento de código.

Esta firma es única para el par documento/clave privada, y puede adjuntarse al documento y verificarse con la clave pública de la persona que firma. Dos algoritmos comunes para las firmas digitales son RSA con el esquema de firma probabilística (RSA-PSS) y algoritmo de firma digital (DSA)"

La firma digital es un archivo muy delicado de tratar ya que es cualquier persona con acceso a un ordenador que tenga almacenada la firma digital puede hacer uso de ella para fines perjudiciales para el dueño de la firma, por eso es importante que al obtener la firma esta sea almacenada en un lugar seguro del computador, no guardar clave en el equipo. Lo indispensable en la criptografía simétrica es proteger la clave privada o contraseña.

Las conexiones HTPPS ofrecen seguridad en las en las páginas webs que frecuentamos diariamente. Hasta hace algunos años, Chrome para Android ha estado utilizando AES-GCM como algoritmo de cifrado simétrico, sin embargo, Google lleva trabajando desde hace muchos años en cifrados más actuales, seguros y rápidos (López A. , 2023)

Un beneficio a nivel de software también es que permite generar claves más cortas que el RSA, su funcionamiento es más eficiente con el cifrado de curva elíptica. Un sistema de encriptación ECC de 256 bits equivale a un sistema RSA de 3072 bits; un sistema cifrado ECC de 384 bits es un sistema RSA de 7680 bits (KeepConding, 2023).

Los algoritmos de cifrado se basan en problemas matemáticos cuya solución es difícil de encontrar, un beneficio es que no permite que esta acción sea reversa, una vez generado o ejecutado el algoritmo se crean una serie de números aleatorios que hacen que la curva elíptica se mantenga en movimiento, de esta forma es difícil compctar con el pico de la curva para poder acceder.

Según lo mencionando en los párrafos anteriores, RSA, SSH proporciona un nivel de seguridad, en cuanto a encriptación como curva elíptica en software y hardware, también se debe tomar en cuenta que con el avance de la tecnología e información, hay considerar que la encriptación es un ámbito importante, es por ello que el este trabajo de investigación aporta como propuesta de uso de cifrado de curva elíptica.

2.4 Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación de la investigación realizado con los sustentos teóricos, metodológicos.

Tabla

Matriz de articulación

Ejes o partes principales del proyecto		Breve descripción de los resultados de cada parte	Sustento teórico que se aplicó en la construcción del proyecto	Tecnología
1	Encriptación	Aplicación de seguridad en clave de acceso	Seguridad según algoritmo aplicado. Mediante Metodología Bibliográfica	Aplicaciones más usadas
2	Algoritmos	Nivel de protección según ejecución de algoritmo y dificultad de acceso indebido.	Ejecución de algoritmos de protección segura como RSA, SSH que mediante fórmulas que dan como resultado números aleatorios difíciles de descifrar.	Investigación de varios algoritmos
3	Ejemplo de encriptación	Alto nivel de seguridad	Ejecución de software CrypTool	Muestra final de documento encriptado Xbee (Xbee), (ZigBee), WSN
4	Curva elíptica	Cifrado seguro	Ejemplo aplicado en encriptación con dos software diferentes	CrypTools, pdfelements

CONCLUSIONES

El funcionamiento de curva elíptica está basado en problemas matemáticos complejos de resolver, cuya complejidad garantiza la seguridad de encriptación ya que estos problemas al ejecutarse hacen que la curva se encuentre en constante movimiento, para de esta forma lograr en los menos posible compactar con el hacker, con el ejemplo aplicado en esta investigación se mostró el nivel de seguridad de un software que no lleva curva elíptica, comparado con un CrypTool el cual consta de un proceso mas amplio.

El uso de curva elíptica es un tema muy amplio a estudiar y llevar a cabo, la complejidad de aplicar curva elíptica para encriptación ha conllevado que se usen otros softwares para encriptar, pero ¿Cuán segura tenemos la información? Se debería plantear el resultado de costo beneficio en cuanto a la encriptación, hoy en día la información es lo más valioso.

La propuesta de uso de encriptación de cura elíptica es la mejor opción, tomando en cuenta que puede ser usada en software y hardware, se mostró en el proceso de investigación que no se puede comprar la seguridad de encriptación de un documento como de una firma electrónica, ya que su uso y funcionalidad son completamente diferentes, lo que conlleva a ver la necesidad de tener un buen método de encriptación, con el fin de evitar que personas que realizan malas prácticas en base a sus conocimientos perjudiquen al dueño del archivo de la firma.

Con el desarrollo de esta investigación se comprende que los algoritmos son importantes y usados por todas las personas todos los días, sin tomar en cuenta las personas realizan una serie de pasos ordenados para lograr un objetivo, lo cual es básicamente la definición de algoritmo, es de esta manera como trabaja encriptación de curva elíptica, donde todo se encuentra relacionado con la Seguridad de la Información.

RECOMENDACIONES

En el ámbito educativo es recomendable ampliar el conocimiento, motivar a los estudiantes en temas de Seguridad Informática, existe mucho potencial por explotar tanto en estudiantes como en investigación, todo lo que abarca Tecnología de la Información, es el futuro de grandes puestos laborales, ya que la Tecnología no solo avanza para fines beneficiosos, sino también existen personas que hacen mal uso del conocimiento, es por eso que se necesita profesionales en el área.

Desarrollo de software que genere encriptación de curva elíptica sería una muy buena opción en el ámbito académico como se mencionó en uno de los ods, tener educción de calidad con temas relevantes para el avance de la seguridad informática.

Es recomendable mediante realizar capacitaciones constantes a empleados a cerca de Seguridad de la información, si bien es cierto en la mayoría de empresas hay grandes profesionales en diferentes ramas, un aporte fundamenta a al conocimiento y en beneficio de la empresa es dar a conocer cómo detectar un archivo malicioso, qué hacer si su red llega se llega a encontrar es espionaje, conocimiento básico sobre la ley de protección de datos, son temas actuales muy básicos los cuales es recomendable empezar por ahí para luego entrar en temas como buscar una encriptación segura como lo es encriptación de curva elíptica.

El uso y aplicación de problemas matemáticos es fundamental ya que con esto se ha logrado encontrar una forma robusta de encriptar información, tomando en cuenta que encriptación de curva elíptica se puede usar en cualquier giro de negocio, se recomienda realizar el uso de esta encriptación, realizar investigaciones que aporten al crecimiento de este tema con el objetivo de hacer más robusta esta seguridad.

BIBLIOGRAFÍA

Abarzua, R., Kaschel, H., & Chinchay, I. (2008 - 2023). ResearchGate. Obtenido de https://www.researchgate.net/publication/284176485_IMPLEMENTACION_DE_UNA_CURVA_ELIPTICA_APLICADA_A_UNA_WSN_LIMITADA_EN_HARDWARE

Albuixech, Á. (2016). Icea. 7. Obtenido de Icea : https://www.icea.es/es-es/formacion/accionesformativas/MemoriasMaster/2016/2016-Internet-de-las-cosas.pdf

Arimetrics. (2022). Obtenido de https://www.arimetrics.com/glosario-digital/software#:~:text=El%20software%20es%20un%20conjunto,software%20y%20programas%20de%20software.

AWS. (2023). Obtenido de https://aws.amazon.com/es/what-is/cryptography/

De Luz, S. (24 de mayo de 2023). Redes Zone. Obtenido de https://www.redeszone.net/tutoriales/seguridad/bitlocker-cifrar-discos-windows/

EcuRed. (s.f.). Obtenido de Curva Elíptica (del inglés: Elliptic curve cryptography, ECC) es una variante de la criptografía asimétrica o de clave pública basada en las matemáticas de las curvas elípticas.

Editorial Etecé. (2013 - 2023). Obtenido de https://concepto.de/metodo-analitico/

Enciclopedia Humanidades. (2023). Obtenido de https://humanidades.com/metodo-deductivo/

Fundación Tekniker. (agosto de 2023). Obtenido de https://www.tekniker.es/es/redes-de-sensores#:~:text=Las%20redes%20de%20sensores%20Inal%C3%A1mbricas,presi%C3%B3n%2C%20movimiento%20o%20agentes%20contaminantes.

Gallo, O. (2022). Software educativo para aprendizaje de criptografía de Curva Elíptica. Unir, https://reunir.unir.net/bitstream/handle/123456789/12792/Gallo%20Haddad%2c%20Omar.pdf?sequence=1&isAllowed=y.

GEEKFLARE. (2023). Obtenido de GEEKFLARE: https://geekflare.com/es/hardware-encryption/

Hapen Soluciones Informáticas. (08 de 2023). Obtenido de https://apen.es/glosario-de-informatica/hardware/#:~:text=El%20hardware%20son%20aquellos%20elementos,elemento%20f%C3%ADsico%20que%20est%C3%A9%20involucrado.

IBM. (s.f.). Obtenido de https://www.ibm.com/es-es/topics/end-to-end-encryption#:~:text=El%20cifrado%20de%20extremo%20a%20extremo%20comienza%20con%20la%20criptograf%C3%ADa,mensaje%20a%20texto%20sin%20formato.

Juliá, S. (08 de 2023). Gadae NetWeb. Obtenido de https://www.gadae.com/blog/hardware/

KeepConding. (2023). Obtenido de https://keepcoding.io/blog/que-es-la-criptografia-de-curva-eliptica/#Ventajas_de_la_criptografia_de_curva_eliptica

Kingstong. (mayo de 2021).

López, A. (18 de 06 de 2023). RZ Redes Zone. Obtenido de https://www.redeszone.net/tutoriales/seguridad/criptografia-algoritmos-clave-simetrica-asimetrica/

López, R. (2023). Scribd. Obtenido de https://es.scribd.com/document/531377938/cifrado-extremo-a-extremo#

Pastor, J. (25 de agosto de 2016). Xataka. Obtenido de https://www.xataka.com/seguridad/como-funciona-el-cifrado-extremo-a-extremo-de-whatsapp-y-que-implicaciones-tiene-para-la-privacidad

Pérez Porto, J. (07 de 10 de 2022). Definicion.de. Obtenido de Definicion.de: https://definicion.de/curva/

Questionpro. (2023). Obtenido de https://www.questionpro.com/blog/es/metodologia-de-la-investigacion/

Rivera, J. (14 de 08 de 2023). Obtenido de https://telefonicatech.com/blog/seguridad-criptografica-en-iot-ii

Toro, E. (29 de 06 de 2020). Obtenido de https://repositorio.espe.edu.ec/bitstream/21000/22406/1/T-ESPE-043761.pdf

Villanueva, R. (2014). Algoritmos Basicos Para La Multiplicacion De Puntos En Una Curva Eliptica. Investigación e Innovación en Ingenierías.

ANEXOS

Valoración problema de investigación y aplicación de encriptación

SEGURIDAD DE AUTENTICACIÓN DE CLAVE PÚBLICA DE

CURVA ELÍPTICA

Evaluador: Maria Gabriela Arcos

MAGÍSTER EN SEGURIDAD

INFORMÁTICA

Registro Senecyt: 1051-2023-2657160

Coordinadora área de QA en la empresa Mobilvendor Software Company

Realizo la siguiente valoración a la problemática planteada en el documento, porque es una realidad que la vulnerabilidad en sistemas no se considera como algo prioritario en la gran cantidad de empresas los recursos son usados para otros fines menos importantes y no pararesguardar la información. Desde mi punto de vista Seguridad de Curva Elíptica es una seguridad más robusta que sería bueno se aplique en empresas que manejan datos sensiblesque son la mayoría en Ecuador.

Observaciones: Es una propuesta muy buena planteada por la Ing. Jéssica Córdova apoyo al tema y por mi área laboral tengo conocimiento como para afirmar que el uso de algoritmos yproblemas matemáticos es un gran aporte al avance de la tecnología y seguridad

Sin ninguna observación adicional, la interesada puede hacer uso de este documento para losfines académicos pertinentes.

Atentamente

Mag. María Gabriela Arcos

CI.725532582

Teléfono: 0983745483

Departamento de QA

Mobilvendor Software Company

Valoración de curva / curva elíptica

SEGURIDAD DE AUTENTICACIÓN DE CLAVE PÚBLICA DE CURVA ELÍPTICA

Evaluador: Cristhian Nahim Cobos

MoralesIngeniero Matemático

Registro Senecyt: 1005-2022-2576523

Analista TI en la empresa Mobilvendor Software Company

Hago la siguiente valoración respecto a lo mencionado en la propuesta de que los problemas matemáticos se utilizan en todas las áreas académicas y son fundamentalespara la seguridad, como lo señala la Ingeniera Jéssica Córdova en su investigación sobre curvas elípticas. Estas curvas no generan picos ni cruces en sí mismas, lo que las hace más seguras en comparación con otros métodos, como RSA.

Observaciones: Dado que la tecnología avanza a pasos agigantados, con la proliferación de dispositivos conectados a Internet, el crecimiento del comercio electrónico, aplicaciones de servicios bancarios, asistentes inteligentes y aplicaciones de compras, nuestra relación y dependencia de estos avances también crece. Esto, a su vez, aumenta significativamente la exposición a posibles vulneraciones de datos como resultado del constante aumento de la ciberdelincuencia. Por lo tanto, considero que esta propuesta es de gran relevancia para la protección de la información. Desde mi punto de vista, es un tema viable y sumamente interesante. La explicación es clara yposee una sólida validez.

Sin ninguna observación adicional, la interesada puede hacer uso de este documento para los fines académicos pertinentes.

Atentamente,

Ing. Mat. Cristhian Cobos
MoralesCI. 1722932637
Teléfono:0996792103
Departamento de TI
Mobilvendor Software
Company

Valoración Autenticación con clave elíptica en Software

SEGURIDAD DE AUTENTICACIÓN DE CLAVE PÚBLICA DE CURVA ELÍPTICA

Evaluador: Samanta Estefania Guayasamín Tituaña

Máster Universitario en Análisis y Visualización de datos masivos.

Registro Senecyt: 7241199344

Data Scientist en la empresa Mobilvendor Software Company

Como se menciona en el documento, la firma digital es un archivo sensible que se puede vulnerar, puedo aportar que la encriptación de curva elíptica es un método muy bueno,ya que incorpora métodos y funciones matemáticas que eleva el nivel de complejidad frente al acceso de personas no autorizadas a la información, como se ha explicado enel documento.

Observaciones: Esta propuesta, realizada por la Ing. Jéssica Córdova está basada en seguridad y autenticación. Lo que da valor al tema, debido a la necesidad de resguardar y proteger la información, es contar con una buena opción de encriptación.

Sin ninguna observación adicional, la interesada puede hacer uso de este documento para los fines académicos pertinentes.

Atentamente

MSc. Samanta Guayasamín

CI. 1723679617

Teléfono:0998239792

Departamento de TI

Mobilvendor Software

Company

Valoración de Seguridad de Software y Hardware

SEGURIDAD DE AUTENTICACIÓN DE CLAVE PÚBLICA DE CURVA ELÍPTICA

Evaluador: Daniel Andretty Soria Badillo

Ingeniero en Sistemas mención

Telemática Registro

Senecyt:1034-2020-2220514

Desarrollador y Segundo a bordo en el área de TI de la empresa Mobilvendor Software Company

He revisado la Seguridad de Software y Hardware que menciona la Ing. Jessica Córdova, puedo mencionar que el tema planteado es muy interesante y realizo la valoración al apartado de Seguridad de Software y Hardware porque con la aplicación de una buena encriptación se evitaría tantos casos de caídas de aplicaciones y servicios bancarios, donde se deduce que la seguridad no es la correcta lo cual conlleva a esos resultados.

Observaciones: Esta investigación sobre el método de encriptación mediante curva elíptica demuestra que la seguridad constituye un elemento esencial debido a la presencia constante de la tecnología en nuestro entorno, esto implica que las organizaciones deban adoptar mayores medidas de protección que en épocas anteriores. Por consiguiente, esta investigación nos confirma que el uso de métodos de cifrado nos proporcionará una mayor seguridad como usuarios al dificultar el acceso no autorizado a nuestros datos y generará una mayor confianza hacia las organizaciones, sobre todo por el auge comercial que han experimentado los dispositivos conectados a Internet (IOT, por sus siglas en inglés).

La interesada puede hacer uso de este documento para sus fines académicos pertinentes.

Atentamente

Ing. Daniel Soria

CI. 1722722392

Teléfono:0960520715

Departamento de TI

Mobilvendor Software Company