Criptografía: una tecnología antigua en aplicaciones modernas de alto impacto

Miguel Morales Sandoval
José Antonio Molina de la Fuente*
Héctor Alán de la Fuente Anaya*
Cinvestav Tamaulipas
Victoria, Mexico
miguel.morales@cinvestav.mx

RESUMEN

La criptografía es una técnica que se inventó y ha usado desde tiempos antiguos. Su uso se remonta a hace más de 4,000 años, y ha evolucionado desde entonces hasta nuestros días, pero sin perder la esencia de su funcionamiento. Actualmente, la criptografía se encuentra en amplio uso en varias aplicaciones del día a día de la sociedad, como las compras en línea, el uso de tarjeta bancarias, mensajería instantánea desde teléfonos móviles, entre muchos otros. En este artículo se presenta, de manera simple pero completa, una introducción al fascinante tema de la criptografía, y mediante ilustraciones y ejemplos, se describen las principales técnicas dentro de esta rama de las matemáticas que permiten garantizar confidencialidad, integridad, autenticación, entre otros servicios de seguridad, de los datos sensibles que a diario se usan en las operaciones por medios electrónicos. Se presenta un panorama de las principales aplicaciones donde encontramos el uso de la criptografía, y el impacto que su uso ha tenido en ellas. Se discuten también los retos que afronta la criptografía y las líneas de trabajo que sobre esta área se desarrollan en el Cinvestav Tamaulipas.

PALABRAS CLAVE

Seguridad de datos, criptografía, ciberseguridad, cifrado, firmas digitales, seguridad informática.

Citar como:
Miguel Morales Sandoval, José Antonio Molina de la Fuente, and Héctor Alán de la Fuente Anaya. 2022. Criptografía: una tecnología antigua en aplicaciones modernas de alto impacto. En Miguel Morales Sandoval, José Gabriel Ramírez Torres y Javier Rubio Loyola (Eds.), *Ciencia e Ingeniería en Tecnologías Computacionales*, capítulo 10, 8 páginas. Cinvestav Unidad Tamaulipas, Ciudad Victoria, Mexico, ISBN: 978-607-9023-65-2.

1. INTRODUCCIÓN

La escritura es un sistema gráfico creado por la humanidad con el objetivo de conservar y transmitir información. En distintas etapas de la historia de la humanidad, ha sido necesario proteger la información, escrita, para que ésta solo sea accedida por entidades autorizadas. Este requerimiento de "confidencialidad" de la información fue el primero en demandarse, y la criptografía surgió para satisfacer este requerimiento.

Suponga un conflicto bélico en la antigüedad entre dos reinos. El reino A y sus aliados se distribuyen geográficamente en una región, de la misma forma que lo hace el reino B. Las comunicaciones entre los aliados de cada reino debe protegerse, ya que en dichas comunicaciones se puede encontrar información sensible, tal como estrategias, tácticas, mensajes personales, tomas de decisiones, datos estratégicos, entre otros. Si esta información es interceptada por el enemigo, puede suponer un resultado catastrófico para el propietario de los datos. Aún al interior de los aliados, cierta información podría estar restringida a ciertas entidades. Fue principalmente en este contexto bélico que la criptografía apareció y resolvió los problemas de privacidad y confidencialidad, que fueron los primeros en demandarse en la comunicación de mensajes sensibles (estrategias, tácticas) por medios inseguros (caminos, rutas).

La criptografía tiene su origen en la Grecia antigua. Se conforma de los vocablos *krypto* que significa *oculto*, y *graphos*, que significa *escribir*, es decir, significa *ocultar la escritura*. La criptografía tuvo un antes y un después durante la Segunda Guerra mundial, donde el bloque liderado por Alemania usó un dispositivo criptográfico, la máquina Enigma, para proteger las comunicaciones con sus aliados. Se considera que el triunfo del grupo opositor y la caída de los alemanes se debió en gran medida a la capacidad de poder descifrar los mensajes de Enigma. Este hecho derivó en el inicio de la computación, de la criptografía moderna y de la inteligencia artificial, teniendo como principal precursor a Alan Turing.

Mediante la criptografía se pueden realizar dos operaciones usando una clave secreta k:

1. **CIFRAR**. Consiste en tomar una pieza de información D, entendible para todos, y *transformar* esa pieza D usando k para convertirla en otra pieza de datos, denotada como $CT = CIFRAR(D, k)$. D se le conoce como *texto en claro* y a CT como *texto cifrado*. La transformación debe ser tal que CT pierde significado, ya no es entendible, y no revela ningún indicio sobre el contenido original D. Así, alguien que obtenga CT, no entenderá su contenido, y no podrá a partir de CT tratar de adivinar cuál era el contenido original D.
2. **DESCIFRAR**. Consiste en tomar un texto cifrado CT, y usando la misma clave que fue utilizada durante el cifrado, transformar CT para recuperar el contenido original D,

*Estudiante del Programa de Maestría en Ciencias en Ingeniería y Tecnologías Computacionales, en el Cinvestav Unidad Tamaulipas.

Jornadas de Divulgación - TopTamaulipas 2021, Noviembre 9–18, 2021, Ciudad Victoria, TAMPS

ISBN 978-607-9023-65-2.

Concepto	Descripción	Notación
Clave	Secreto usado para la transformación del texto claro al texto cifrado o viceversa.	k
Cifrar	Transformar texto en claro a texto cifrado, usando una clave.	$CT = CIFRAR(D, k_c)$
Descifrar	Transformar texto cifrado a texto en claro. Requiere de la misma clave que se uso para crear el texto cifrado.	$D = DESCIFRAR(CT, k_d)$

Tabla 1: Principales conceptos y notación en criptografía simétrica.

denotado como $D = DESCIFRAR(CT, k)$. La transformación será exitosa si y solo si la clave de descifrado es la misma que la clave de cifrado. Esto se denota como $D = DESCIFRAR(CIFRAR(D, k), k)$.

La clave usada en el cifrado y en el descifrado tiene una papel fundamental en la seguridad: solo el que posea la clave puede descifrar una pieza de información cifrada. La clave debe tener propiedades que no permitan a un atacante poder adivinar la clave, ya que si se revela u obtiene por el atacante, la seguridad se vulnera; el atacante podría descifrar y acceder al texto en claro. Debido a ello generalmente se requiere de un algoritmo especial encargado de generar la clave de cifrado y de descifrado, llamada **GEN**. Un *criptosistema* es un sistema criptográfico que tiene claramente definidos los tres algoritmos {**GEN, CIFRAR, DESCIFRAR**}.

Se tiene conocimiento de cifradores usados en la guerra entre Sparta y Atenas (hacia el siglo IV A.C). En nuestro país, durante la revolución mexicana, también se usaron cifradores. Desde su creación, los cifradores han funcionado transformando texto legible en algo ilegible, mediante una clave secreta. En la guerra de Sparta y Atenas, la clave era un bastón, donde se enrollaba un material donde se escribía el mensaje. Al desenrrollarlo, los caracteres aparecían en un orden diferente, lo que dificultaba su interpretación. Para leer el mensaje, se debía enrollar nuevamente en un bastón de las mismas características de aquel usado cuando el mensaje cifrado se creó. En la revolución mexicana por ejemplo, se usaron tablas de sustitución. El abecedario se ordenaba en una tabla, de varios renglones y columnas. Los renglones se etiquetaban con letras o números al igual que las columnas. Entonces, un mensaje se codificaba letra por letra, remplazando dicha letra por el número o carácter del renglón y columna donde ese carácter se localizaba en la tabla. El mensaje podría descifrarse solo si se contaba con las mismas etiquetas en renglones y columnas usadas durante la creación del mensaje cifrado. En la segunda guerra mundial, la máquina Enigma tenía un funcionamiento muy similar al de una máquina de escribir. Cuando se tecleaba una letra, la máquina escribía una letra diferente. La máquina se configuraba mediante rotores para que el reemplazo de teclas por otras se realizará de manera aleatoria. La configuración de la máquina era lo que constituía la clave secreta del cifrador.

La Tabla 1 resume los principales conceptos relacionados con criptosistemas y un ejemplo de algunos criptosistemas usados para ocultamiento de la escritura. Note que en el cifrado se ha indicado a la clave como k_c y en el descifrado como k_d. Se ha hecho así para indicar que cualquiera puede intentar descifrar un texto cifrado en su posesión, intentando usar cualquier clave, pero el descifrado solo funcionara si y solo si $k_c = k_d$. Cuando esto ocurre, al criptosistema se le llama *simétrico*.

La criptografía surgió creando cifradores simétricos, desde su invención hace más de 4000 años. Los criptosistemas simétricos han evolucionado desde ese tiempo hasta los más modernos que hoy se usan, pero todos siguen el mismo modelo descrito en la Tabla 1. La principal desventaja de los criptosistemas simétricos es cómo establecer la clave de cifrado entre el emisor que cifra y el receptor que descifra, ya que ambos deben poseer la misma clave.

El problema de establecimiento de claves para cifradores simétricos se acentuó con la llegada de la redes de computadoras y el intercambio de información por medios digitales. Para resolver esta problemática, en 1976 se inventó un protocolo de establecimiento de secretos entre dos entidades, a partir de datos públicos. Este fue el famoso protocolo de establecimiento de claves Diffie-Hellman, aún usado en la actualidad. El protocolo debe su nombre a sus inventores, Withfield Diffie y Martin Hellman, ambos de la Universidad de Stanford. El protocolo hace uso del álgebra abstracta y de la teoría de números para que a partir de datos públicos, dos entidades A y B ejecuten una serie de pasos, intercambien valores públicos, y obtengan cada uno por su cuenta un valor que es el mismo en el lado de A y en el lado de B. Este valor es el que ambos A y B pueden usar como clave de un criptosistema simétrico.

El protocolo Diffie-Hellman tiene relevancia no solo por resolver el problema de establecimiento de claves, sino que sentó las bases de lo que sería conocido como *criptografía asimétrica*. En este caso, se usa una función f con propiedades especiales, de tal forma que f es fácil de calcular pero f^{-1} no lo es. Hay muy pocas funciones que tienen esta propiedad, pero existen, y en ellas se fundamentan los criptosistemas asimétricos. En un criptosistema asimétrico, cada entidad tiene dos claves: una privada denotada como k, que debe salvaguardarse y no revelarse a nadie, y una pública, conocida por cualquiera que se obtiene a partir de k mediante f, denotada como $f(k)$. La propiedad de f de ser difícil de invertirse es lo que hace que a partir de la clave pública no se pueda obtener la clave privada.

En la Tabla 2 se redefinen los conceptos de clave, cifrar y descifrar para el caso de los criptosistemas asimétricos. En el cifrado, las claves que intervienen son solo las del receptor, no las del emisor. Cualquiera puede enviar datos cifrados a una entidad receptora con par de claves $\{k_r, f(k_r)\}$. Para ello solo se requiere conocer $f(k_r)$, la cual es pública. Una vez cifrados los datos, nadie más que el receptor con la correspondiente clave privada k_r asociada a $f(k_r)$ podrá realizar el proceso de descifrado. Particularmente, al cifrado asimétrico se le conoce como *sobre digital*, por la analogía de que los datos se colocan en un sobre para un destinatario particular, y nadie más que dicho destinatario podrá abrir el sobre y extraer los datos de interés. Mediante sobres digitales se puede realizar el transporte seguro de las claves que se usan en los criptosistemas asimétricos, realizando los siguientes pasos. Se asume que el secreto lo genera una entidad A y lo envía a una entidad B.

Concepto	Descripción	Notación
Par de claves	Clave pública y clave privada, relacionadas entre ambas, asignadas a un usuario en el criptosistema	$\{k_u, f(k_u)\}$
Cifrar	Transformar texto en claro a texto cifrado, usando la clave pública del receptor.	$CT = CIFRAR(D, f(k_r))$
Descifrar	Transformar texto cifrado a texto en claro. Requiere de la misma clave que se uso para crear el texto cifrado.	$D = DESCIFRAR(CT, k_r)$

Tabla 2: Principales conceptos y notación en criptografía asimétrica.

1. A genera una clave simétrica usando el algoritmo **GEN**. $k = GEN()$.
2. A obtiene la clave pública de B, $f(k_B)$.
3. A genera un sobre digital de k usando cifrado asimétrico. $CT = CIFRAR(k, f(k_B))$.
4. A envía CT a B.

Por su parte, cuando B recibe CT, procede a realizar la apertura del sobre digital mediante los siguientes pasos:

1. Accede a su clave privada k_B, por ejemplo, desde un dispositivo que el solo posee o usando un mecanismo seguro.
2. Abre el sobre. $k = DESCIFRAR(CT, k_B)$.

Además de hacer posible el concepto de sobres digitales para intercambio seguro de datos hacia un destinatario específico, un criptosistema asimétrico también hace posible la implementación del concepto de *firmas digitales*.

Una firma digital es el análogo a las firmas manuscritas, y tienen el objetivo de garantizar el servicio de autenticación. Note que en el sobre digital, no hay certeza en que el texto cifrado haya sido generado por una entidad particular, ya que cualquiera puede cifrar siempre que cuente con la llave pública del receptor. Con la firma digital, se puede determinar si un cifrado fue realizado por una entidad particular, y vincular dicha operación a esa entidad. De esta forma, el emisor o creador de un cifrado no puede negar haberlo realizado, tal como ocurre cuando alguien firma un documento. Para las firmas digitales, se usan las operaciones de cifrado y descifrado asimétrico, pero se invierte el uso de las claves: se cifra con la clave privada y se descifra con la clave pública. En este caso, al cifrado se le llama *generación de firma* y al descifrado se le llama *verificación de firma*.

En la actualidad, se usan tanto criptosistemas simétricos como asimétricos. Sin embargo, estos algoritmos no son suficientes, se requieren de algoritmos auxiliares pero indispensables para implementar servicios de seguridad basados en criptosistemas. Estas funciones reciben el nombre de *primitivas criptográficas*. Ejemplos de estas funciones son las funciones hash, las funciones de generación de códigos de autenticación, las funciones de derivación de claves, entre otras.

El resto de este documento se encuentra organizado de la siguiente forma. En la Sección 2 se presenta aplicaciones representativas donde se usan criptosistemas y primitivas criptográficas para garantizar confidencialidad, autenticación e integridad en las comunicaciones. En la Sección 3 se presenta un panorama de los principales retos actuales de la criptografía, principalmente por la amenaza de computadoras cuánticas. En la Sección 4 se describen las líneas de trabajo actuales sobre criptografía en el Cinvestav Tamaulipas y finalmente en la Sección 5 se presentan las conclusiones de este trabajo de divulgación.

2. ALGUNAS APLICACIONES MODERNAS DONDE ACTUALMENTE SE USA LA CRIPTOGRAFÍA

La criptografía actualmente tiene muchas aplicaciones, en beneficio de la sociedad para proteger los datos que se almacenan o transmiten por medios digitales. En esta sección se describen aquellas de mayor uso por los ciudadanos, que incluyen mensajería cifrada, criptomonedas y compras en línea.

2.1. Intercambio de mensajes seguros en WhatsApp

La aplicación WhatsApp lanzada en 2009 y adquirida por la empresa Facebook en 2014, lidera el servicios de mensajería instantánea móvil con más usuarios activos al mes (datos de 2019 [1]). Esta aplicación permite enviar y recibir mensajes, compartir imágenes, vídeos, audios y documentos, así como realizar llamadas y videollamadas. Todas estas funciones son realizadas entre un emisor y un receptor usando teléfonos inteligentes a través de Internet.

Hoy en día, la mayoría de los ciudadanos cuentan con un teléfono inteligente y comparten información como nunca antes, por lo que preservar la privacidad de los usuarios ante criminales informáticos se ha vuelto imprescindible. Afortunadamente, WhatsApp incorporó en 2016 un protocolo de comunicación basado en *end-to-end encryption* (E2EE), también llamado cifrado de extremo a extremo. Este mecanismo asegura que el mensaje enviado solo podrá ser leído o escuchado por la persona o chat en grupo al que va dirigido. Ningún tercero podrá ver el contenido del mensaje, esto incluye al personal de WhatsApp o su empresa matriz Facebook.

Gracias al cifrado de extremo a extremo, el contenido del mensaje que se envía va totalmente cifrado desde su origen hasta su destino. Es decir, el mensaje se cifra dentro del dispositivo del emisor antes de ser enviado, y se descifra solamente en el dispositivo del receptor, justo antes de ser desplegado en la pantalla. El receptor del mensaje es el único que cuenta con la clave privada necesaria para descifrar el mensaje. Lo anterior asegura que cualquier entidad que pudiera interceptar el envío o tener acceso legítimo al mensaje, no sea capaz de leerlo. Esto incluye al proveedor del servicio de comunicación.

La seguridad en E2EE es posible gracias a la *criptografía asimétrica*, con la que se crea un par de claves por usuario (teléfono inteligente). La *clave pública* del usuario es almacenada en el servidor y su *clave privada* es almacenada en su propio dispositivo. Si el usuario A desea enviar un mensaje al usuario B (ver Figura

1), primero tendrá que cifrar el texto en claro con la *clave pública* de B y enviarlo. Cuando B reciba el mensaje cifrado, tendrá que usar su *clave privada* almacenada en su dispositivo para descifrar el mensaje de A. Si B quiere responder, debe repetir el proceso, cifrando el mensaje con la *clave pública* de A.

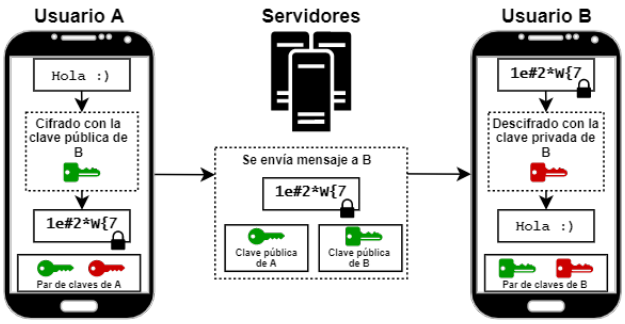

Figura 1: Cifrado de extremo a extremo.

Al usar WhatsApp, cada llamada o mensaje que sea enviado desde el dispositivo emisor será cifrado de extremo a extremo de forma automática y solo el dispositivo receptor lo podrá descifrar. El tipo de criptografía utilizada es el de curvas elípticas (ECC), el cual es un criptositema asimétrico fundamentado en la teoría de grupos y de campos finitos. Como se detalla en [2], WhatsApp hace uso de tres pares de claves ECC generadas en el dispositivo tras la instalación. La primera, I, se crea para identificar al dispositivo; otra, S, se genera periódicamente y es firmada digitalmente usando la clave I; la tercera, O, es remplazada por cada uso de la aplicación. Además de las tres claves previas, se usa una clave raíz R, producida por un procedimiento de establecimiento de clave (protocolo Diffie-Hellman); una clave cadena C que se generada de R y es actualizada con cada ida y vuelta; y una clave de mensaje M que es dividida en tres partes y usadas respectivamente para: el uso en un *criptosistema simétrico*, para la generación de un código de autenticación y para un vector de inicialización usado como parámetro del cifrado.

El sistema para el intercambio de mensajes seguros de WhatsApp cuenta con tres etapas (ver Figura 2):

1. **Registro de cliente**: Un cliente transmite sus claves públicas I_k, S_k y O_k al servidor de WhatsApp, el cual las almacena asociándolas al identificador del usuario.
2. **Configuración de la sesión**: Para comunicarse con otro usuario, el usuario emisor primero necesita establecer una sesión con el usuario receptor. Esto se logra solicitando al servidor las claves públicas del receptor I_{k_r}, S_{k_r} y O_{k_r}. El servidor las regresa y remueve de su almacenamiento a O_{k_r}, ya que es clave de un solo uso. El emisor guarda las claves públicas del receptor y genera un par de claves ECC efímeras E_k, $E_{f(k)}$. Enseguida, se hace uso del protocolo Diffie-Hellman de curva elíptica (ECDH), el cual permite el establecimiento de claves a dos partes usando cada uno un par de claves de curva elíptica. El protocolo ECDH es ejecutado cuatro veces dando de entrada una clave privada del emisor y una clave pública del receptor, como se muestra en la Figura 2. Después, sus salidas son concatenadas para crear la clave maestra MS y darla como entrada a una función de derivación de clave basada en un código de autenticación de mensaje (HKDF). Esta función crea una clave raíz R_k, para generar una clave cadena C_k. Luego de haber generado las claves de sesión, el emisor envía E_k al receptor para que pueda generar MS usando sus propias claves privadas. El receptor también genera R_k y C_k a partir de MS.
3. **Intercambio de mensajes**: Una vez que la sesión se haya establecido entre los dos usuarios, el emisor del mensaje generará una clave de mensaje M_k derivada de C_k con una función HMAC. M_k es utilizada para cifrar simétricamente el mensaje en claro D y enviar el texto cifrado CT al receptor para que pueda descifrarlo con las claves producidas desde su dispositivo.

El proceso hace uso de una cola de claves de un solo uso O_k las cuales se van eliminando y rellenando a medida que se van ocupando. Al utilizar E2EE, WhatsApp no puede leer los mensajes ni los almacena en sus servidores. Esta característica lo hace incluso más seguro que Telegram, debido a que éste almacena en sus servidores una copia de texto plano de cada mensaje que se envía o recibe.

2.2. Criptomonedas

Las criptomonedas [3] son el equivalente digital de las monedas físicas. Tienen un valor y se pueden usar como cualquier otra divisa en transacciones financieras digitales. A diferencia de las monedas físicas, que son principalmente administradas por una entidad central (Banco), las criptomonedas se rigen por mecanismos de consenso, bajo un enfoque de procesamiento descentralizado dentro de una estructura de datos abstracta llamada *cadena de bloques*. La criptografía permite construir los mecanismos para que las transacciones con estas monedas digitales se realicen de forma segura y se puedan garantizar las condiciones que eviten fraudes. La descentralización se consigue mediante el establecimiento de un red de participantes (red *peer to peer*, abreviada P2P), todos ellos registrando y validando las operaciones financieras.

La primera criptomoneda surgió en 2009 con el nombre de *Bitcoin*. Bitcoin [4] se ha convertido en una de las principales criptomonedas que actualmente se usa para realizar pagos electrónicos con criptomonedas de forma segura. La tecnología central detrás de Bitcoin es la cadena de bloques. La cadena de bloques es una unión entre criptografía, mecanismos de consenso y redes P2P.

La cadena de bloques [5] es un registro público distribuido en una red P2P. Cada nodo de la red tiene una copia actualizada de la cadena de bloques que contiene todas las transacciones válidas realizadas. La cadena de bloques permite el seguimiento de las transacciones y asegura la integridad, autenticación y no repudio de las mismas mediante *criptografía asimétrica* y *primitivas criptográficas*.

Los nodos de la red verifican las transacciones mediante firmas digitales y funciones hash. De esta forma, los participantes de la red no necesitan confiar entre ellos para realizar operaciones debido a que las transacciones son firmadas. La cadena de bloques se considera una estructura de datos inmutable debido a que solo permite agregar nuevas transacciones. La estructura de datos de la cadena de bloques es una lista de bloques enlazados mediante el valor hash del bloque anterior. El hash de una pieza de información representa

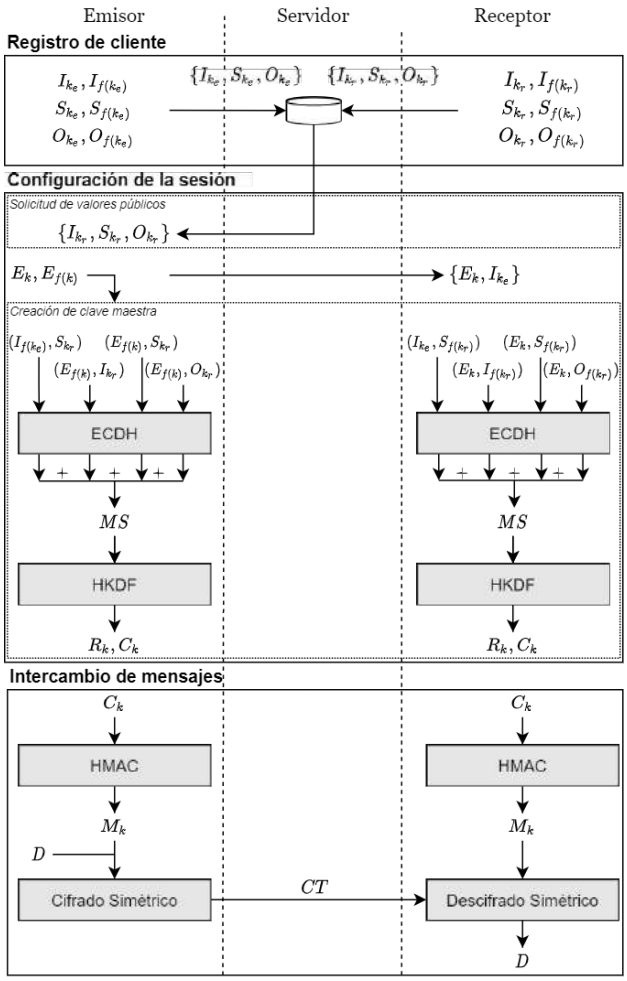

Figura 2: E2EE de WhatsApp.

la huella digital de dicha información. El hash de un bloque i depende de las transacciones del bloque, su información de cabecera y del hash del bloque $i-1$. De esta forma, si se altera un bloque j en la cadena, todos los bloques posteriores a j existentes en la cadena tendrán un hash distinto. Esto indicaría que la información contenida en la cadena de bloques fue manipulada y por lo tanto, la cadena de bloques sería descartada.

Para asegurar que todos los nodos en la red tienen la misma información y que no se generen bloques de forma descontrolada, se utiliza un mecanismo de consenso. En Bitcoin se utiliza la prueba de trabajo como mecanismo de consenso, particularmente el algoritmo *Hashcash* [6]. Hashcash consiste en resolver un acertijo matemático computacionalmente difícil, pero que es fácil de comprobar por un tercero.

2.2.1. Funcionamiento de Bitcoin. Para realizar transacciones, los usuarios de Bitcoin utilizan una billetera digital. Una billetera digital utiliza criptografía asimétrica, es decir, contiene el par de claves criptográficas utilizadas para firmar y verificar transacciones. La clave privada es conocida únicamente por su propietario y es utilizada para firmar transacciones. La clave pública es conocida por todos y es utilizada para verificar transacciones. Ambas claves están relacionadas entre sí. La posesión de la clave privada permite el control de las criptomonedas en la cadena de bloques, por lo tanto, una billetera digital está asociada a un balance en criptomonedas. La Figura 3 muestra el diagrama (basado en [7]) del funcionamiento del protocolo de Bitcoin.

El escenario es el siguiente. La billetera X quieren enviar *1 BTC* a la billetera Y. Esto genera una transacción la cual es propagada a los nodos de la red P2P. Los nodos de la red verifican que la transacción sea correcta y la propagan a los demás nodos. Si la transacción es correcta, los nodos agregan la transacción válida al bloque actual. Después de 10 minutos aproximadamente, los nodos compiten por realizar la prueba de trabajo. El primer nodo que resuelva la prueba de trabajo gana un incentivo en BTC y distribuye el bloque minado a algunos nodos de la red, quienes verifican que el bloque sea correcto. Si el bloque es correcto, los nodos propagan el bloque y lo agregan a su copia de la cadena de bloques. Las transacciones contenidas en el bloque se vuelven parte del registro de forma permanente y por ende, la transacción es reflejada.

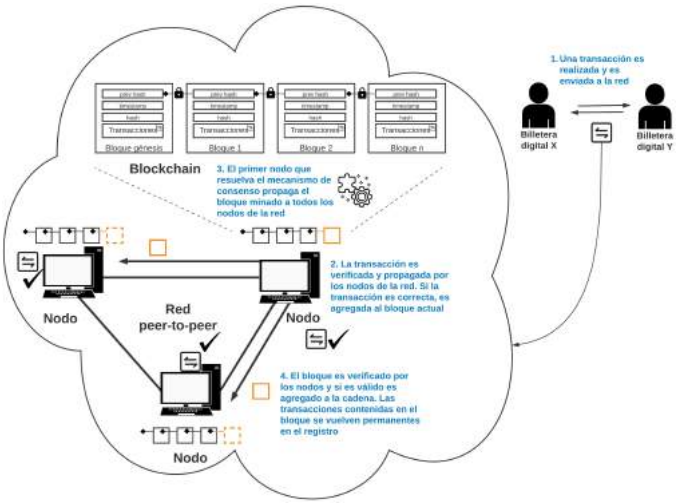

Figura 3: Funcionamiento general de Bitcoin [7].

2.2.2. Tendencias de criptomonedas. Con el paso de los años, las cadenas de bloques han sido mejoradas en distintos aspectos como escalabilidad, seguridad y descentralización. Por ejemplo, Ethereum[1] es una cadena de bloques que puede ser programada mediante contratos inteligentes. Los «contratos inteligentes» son programas definidos por el usuario que son ejecutados de forma descentralizada, heredando todas las características de la cadena de bloques. Los contratos inteligentes permiten el desarrollo de aplicaciones descentralizadas. Además de Bitcoin, existen otras criptomonedas[2] como Litcoin, Binance Coin, Tether, XRP, DogeCoin, etc.

[1] https://ethereum.org/en/whitepaper/
[2] https://coinmarketcap.com/

Las criptomonedas se caracterizan por su gran volatilidad. Las Figuras 4 y 5 muestran el valor de Bitcoin y Ethereum respectivamente al día de hoy en pesos mexicanos, así como una gráfica de sus valores en función del tiempo. Con el paso del tiempo, han surgido nuevas criptomonedas como las *stablecoins* para mitigar la volatilidad. Estas criptomonedas están asociadas al valor de una moneda de curso legal, bienes materiales, otras criptomonedas e incluso algunas son controladas por algoritmos para mantener un valor estable. Algunas stablecoins actuales son Tether, USD Coin y Dai. Recientemente, el país de El Salvador ha presentado la Ley Bitcoin[3] en donde se regula Bitcoin como moneda de curso legal. Esto permite a las personas físicas o morales realizar transacciones con esta criptomoneda, dándole poder liberatorio ilimitado.

Figura 4: Valor de 1 BTC en pesos mexicanos (25 Agosto 2021) según datos de Coinbase.

Figura 5: Valor de 1 ETH en pesos mexicanos (25 Agosto 2021) según datos de Coinbase.

2.3. Compras en línea y uso de tarjetas bancarias

El uso de tarjetas bancarias, de crédito o débito, han sido promovidas desde ya varios años, con el fin de evitar el manejo de dinero físico. Esto, además de resultar benéfico para los bancos, también es benéfico para las personas quienes pueden usar un solo medio para realizar compras o pagos. Las compras en línea tienen también estas premisas, al permitir a las personas realizar compras aún sin estar presente de forma física en los establecimientos. Ambos, el uso de tarjetas bancarias y las compras en línea se acentuaron recientemente con la situación de la pandemia COVID19 que surgió en 2020.

[3]https://www.asamblea.gob.sv/sites/default/files/documents/dictamenes/27F0BD6F-3CEC-4F52-8287-432FB35AC475.pdf

Figura 6: Tecnología chip EVM.

Figura 7: Protocolo HTTPS para intercambio seguro de datos en la web.

A pesar de los beneficios, las amenazas a la privacidad y autenticidad de las transacciones cuando se hace uso de una tarjeta bancaria o compra en línea es mucho mayor. Los datos como el número de tarjeta y el código de seguridad de las tarjetas bancarias deben protegerse, ya sea cuando una transacción se realiza desde una terminal bancaria o desde un portal de internet. Es por ello que tanto la privacidad como la autenticidad actualmente se implementan mediante algoritmos criptográficos.

En el proceso de compra en línea. Cuando el comprador captura los datos bancarios de su tarjeta de crédito, estos son cifrados en su dispositivo usando una *clave pública* antes de ser enviados, y el vendedor es el único que posee la *clave privada* para descifrar la información y concluir la transacción. Además del uso de *cifrado asimétrico* para ocultar la información que se comparte durante una transacción, también se hace uso de la *firma digital* para autentificar al dueño de la información que se comparte y mantener la integridad de dichos datos asegurando que no hayan sido manipulados durante el viaje.

El uso de criptografía en las tarjetas bancarias es conseguido debido al “chip” que se integra en las tarjetas bancarias y que es "leído"por la terminal bancaria (ver Fig. 6, Fuente: https://es.bokfinancial.com). Esto se conoce como tecnología chip EVM.

El chip ya integra una pareja de llaves pública y privada desde su fabricación, y se personaliza cuando dicha tarjeta se asigna a una persona en particular.

Si las compras se realizan en línea, una herramienta de seguridad de amplio uso es el protocolo https. Este protocolo se usa sin que el usuario tenga que realizar ninguna acción más que realizar su

compra desde su aplicación web. El protocolo https se identifica como ''en uso" cuando en la barra de direcciones web aparece un candado y el nombre explícito https, tal como se muestra en la Fig 7. Cuando se accede a la página web, el dispositivo del usuario y el servidor de la tienda en línea ejecutan una serie de pasos ordenados (por eso se llama protocolo) y acuerdan una *ciphersuite*, esto es, un conjunto de algoritmos criptográficos que incluyen:

- Un algoritmo de establecimiento de claves secretas
- Diversos datos secretos a usarse durante la sesión
- Un cifrador simétrico, para cifrar todo el contenido que intercambien el dispositivo y la tienda en línea.
- Un cifrador asimétrico, encargado del transporte seguro de secretos entre el dispositivo y la tienda en línea, y para la generación y verificación de firmas digitales.
- Primitivas criptográficas a usar, tales como funciones hash, u tras basadas en funciones hash, como funciones HMAC o de derivación de claves.

La ciphersuite acordada es usada durante toda la sesión, y es por ello que la comunicación se asegura con los servicios de confidencialidad, integridad y autenticación. Los datos que principalmente se protegen son los inicios de sesión del usuario en la tienda (nombre de usuario y contraseña), y los datos bancarios para hacer los pagos (números de tarjetas de crédito y claves de seguridad). Dado que todos los datos que se intercambian entre el dispositivo y el servidor de la tienda están cifrados, se garantiza la privacidad.

3. RETOS ACTUALES DE LA CRIPTOGRAFÍA

En la opinión de los autores, la criptografía tiene dos grandes retos en el corto y mediano plazo. Uno de ellos es el relacionado con criptografía ligera, la cual tiene el objetivo de proveer construcciones criptográfica eficientes que puedan implementarse en dispositivos con muy pocos recursos computacionales, como los sensores inalámbricos. El otro reto es el relacionado con la criptografía postcuántica [8], la cual se enfoca en proveer construcciones eficientes en los actuales modelos de cómputo pero resistentes a ataques a través de computadoras cuánticas. Los algoritmos criptográficos son demandantes computacionalmente. Esto dificulta su implementación en entornos de cómputo con limitadas capacidades, por ejemplo, en dispositivos con poca memoria, bajo poder de procesamiento y alimentados por baterías, lo que implica que el uso de energía debe ser eficiente. En el paradigma del Internet de las Cosas [9], la mayoría de los dispositivos que producen, almacenan, procesan o transmiten información, son pequeños y no cuentan con las capacidades de cómputo que tiene, por ejemplo, una computadora de escritorio. En algunas aplicaciones, como las militares, de salud o industriales, la información generada de las aplicaciones IoT es sensible y debe salvaguardarse. Es en estos entornos donde la criptografía ligera debe satisfacer requerimientos de alta seguridad y baja sobrecarga de cómputo, almacenamiento y transmisión.

La mayoría de los algoritmos de seguridad basados en criptografía fundamentan su seguridad en la dificultad de ejecutar un algoritmo de ataque usando las computadoras actuales, incluso las más potentes. Por ejemplo, se sabe que las claves que usan los cifradores simétricos son difíciles de adivinar mediante fuerza bruta, esto es, intentar todos los posibles valores de la clave. Si una clave criptográfica es de 112 bits, un atacante requiere probar todas las posibles llaves en el espacio de 2^{112} claves, lo cual es un espacio muy grande que ni con la computadora más potente se puede explorar. Actualmente, el poder de cómputo se ha ponderado y establecido que el tamaño de claves de los algoritmos criptográficas simétricos debe ser al menos de 112 bits para resistir un ataque de fuerza bruta. Lo recomendable es usar claves de al menos 128 bits.

En el caso de los algoritmos criptográficos asimétricos, su seguridad no se fundamenta en la dificultad de realizar un ataque por fuerza bruta, sino en resolver un problema matemático. Los algoritmos asimétricos más representativos en actual uso basan su seguridad en el problema de factorizar un número entero grande (de más de 2048 bits) o en encontrar el número entero x tal que dado un número y y un número g, se cumpla que $y = g^x$. En este último caso se trata de resolver el problema de logaritmo discreto, siendo $\{x, y, g\}$ números grandes, de más de 2048 bits. Ambos problemas, el de factorización de enteros y el del logaritmo discreto se consideran difíciles e infactibles de resolverse aún usando la computadora convencional más potente. Lo anterior debido a que el mejor algoritmo que resuelve dicho problema tiene complejidad exponencial en el tamaño de los números involucrados. Si se usan números como los comentados, de al menos 2048 bits, no existe una computadora con la capacidad de cómputo que pueda ejecutar el algoritmo de ataque.

Sin embargo, se ha demostrado que el algoritmo de Shor [10], si se ejecuta en una computadora cuántica, puede resolver ambos problemas sin ninguna dificultad. Siendo el algoritmo de Shor un algoritmo con complejidad polinomial, el incremento en el tamaño de los números no representa un incremento considerable en la dificultad del problema. Por ello, es innegable que ante la aparición de una computadora cuántica, los algoritmos criptográficos asimétricos como los conocemos, dejarán de ser seguros. De ahí la necesidad de idear nuevos esquemas criptográficos resistentes a ataques de computadoras cuánticas.

4. LÍNEAS DE TRABAJO ACTUALES DE CRIPTOGRAFÍA EN EL CINVESTAV

En torno a los retos descritos en la sección anterior, en el Cinvestav Tamaulipas se han venido desarrollando líneas de trabajo en los dos frentes, tanto de criptografía ligera como de criptografía postcuántica (PQC por su siglas en inglés).

En el primer caso, se han desarrollado y se siguen explorando algoritmos ligeros para cálculo de funciones hash [11], cifradores simétricos ligeros [12, 13], módulos críticos para cifradores asimétricos [14] y realizaciones hardware/software de esquemas híbridos, como el establecimiento de secretos compartidos [15].

En el segundo caso, se ha iniciado trabajo para abordar el problema desde dos perspectivas. La primera es para proveer implementaciones eficientes y evaluar el impacto del uso de algunos algoritmos PQC [16], particularmente para la aplicación de firmas digitales postcuánticas [17, 18].

Actualmente se siguen proponiendo nuevos esquemas de criptografía postcuántica, por ejemplo, el NIST (National Institute of Standards and Technology) inició una competencia en diciembre del 2017 con el propósito de encontrar los nuevos algoritmos más atractivos resistentes a ataques cuánticos, donde se recibieron 82 algoritmos candidatos: solo 69 fueron aceptados como completos y

apropiados [19]. Al momento de escribir este artículo, dicha competencia sigue en curso en busca de encontrar los algoritmos criptográficos más convenientes. Sin embargo, en la actualidad no se conoce o existe muy poco estudio de cómo construir un sistema criptográfico post-cuántico, el cual requiere mucho más que solo algoritmos de criptografía que cifran, descifran, firman o verifican, resitentes a ataques de computadoras cuánticas. En el Cinvestav Tamaulipas se estudia la pertinencia de usar algoritmos PQC en aplicaciones donde actualmente se utilizan algoritmos criptográficos convencionales. Un ejemplo de ello es SIKE (Supersingular Isogeny Key Encapsulation) [20], el cual es una familia de mecanismos de criptografía poscuántica para el establecimiento de llaves, basada en el protocolo de intercambio de llaves SIDH (Supersingular Isogeny Diffie-Hellman). Los desarrollos realizados en torno a SIKE y PQC se pueden consultar en [16]. Una línea de trabajo en este sentido, en progreso, es el de PQC ligera.

5. CONCLUSIONES

La criptografía se inventó hace más de 4,000 mil años. Inicialmente, se creó para garantizar la confidencialidad de las comunicaciones, por medios escritos, en entornos bélicos. En la actualidad, los cifradores modernos usan los mismos principios de permutaciones y sustituciones, que inicialmente se usaron en los cifradores de la antigüedad, para convertir texto legible en ilegible y viceversa, usando una clave secreta. Los principios son los mismos, pero los algoritmos son más sofisticados, por ejemplo, usando funciones matemáticas más complejas para realizar las transformaciones, y para garantizar que aún con las computadoras más potentes en la actualidad, no es posible atacar dichos sistemas, ni siquiera intentando adivinar la clave secreta que permita descifrar datos. Son estos cifradores los que actualmente han hecho posible contar con aplicaciones del día a día, como las compras en línea o el intercambio seguro de mensajes en nuestros teléfonos inteligentes. Estos mismos algoritmos han hecho posible contar con tecnología disruptiva como las criptomonedas y la cadena de bloques.

La criptografía es una herramienta poderosa y crucial para la ciberseguridad. Generalmente usada para el bien, esto es, proteger nuestros datos de atacantes que quieran sacar algún provecho de ellos. Sin embargo, también se le puede dar un uso inadecuado, como lo han sido los recientes ataques de ransomware [21]. El ransomware es un tipo de código malicioso que realiza un secuestro de los datos de la víctima, al cifrarlos todos con una clave que solo conoce el atacante. Si la víctima desea obtener la clave para descifrarlos, debe pagar un rescate por sus datos.

La formación de recursos humanos en criptografía, y por tanto en ciberseguridad, es uno de los retos más importantes en México y en el mundo, pero necesario para transitar a un entorno de digitalización y acelerar su implantación.

AGRADECIMIENTOS

Gran parte del trabajo de investigación sobre criptografía ha sido realizada gracias al proyecto apoyado por el Fondo Sectorial de Investigación para la Educación, Ciencia Básica SEP-CONACyT, número 281565, titulado *Desarrollo de nuevos algoritmos y arquitecturas de cómputo para criptografía ligera*. El proyecto estuvo a cargo del Dr. Miguel Morales Sandoval.

REFERENCIAS

[1] App annie state of mobile 2020 report, 2020. URL www.appannie.com/en/go/state-of-mobile-2020/.
[2] Whatsapp encryption overview - technical white paper. 10 2020. URL https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf.
[3] Monia Milutinović. Cryptocurrency. 2018.
[4] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2009.
[5] David Berdik, Safa Otoum, Nikolas Schmidt, Dylan Porter, and Yaser Jararweh. A survey on blockchain for information systems management and security. *Information Processing & Management*, 58(1):102397, 2021. ISSN 0306-4573. doi: https://doi.org/10.1016/j.ipm.2020.102397. URL https://www.sciencedirect.com/science/article/pii/S030645732030892X.
[6] Adam Back. Hashcash - a denial of service counter-measure. 2002.
[7] Emanuel Regnath and Sebastian Steinhorst. Smaconat: Smart contracts in natural language. pages 5–16, 09 2018. doi: 10.1109/FDL.2018.8524068.
[8] Daniel J. Bernstein and Tanja Lange. Post-quantum cryptography. *Nat.*, 549 (7671):188–194, 2017. doi: 10.1038/nature23461.
[9] Samuel Greengard. *The Internet of Things*. The MIT Press, 2015. ISBN 0262527731.
[10] Peter W. Shor. Polynominal time algorithms for discrete logarithms and factoring on a quantum computer. In Leonard M. Adleman and Ming-Deh A. Huang, editors, *Algorithmic Number Theory, First International Symposium, ANTS-I, Ithaca, NY, USA, May 6-9, 1994, Proceedings*, volume 877 of *Lecture Notes in Computer Science*, page 289. Springer, 1994. doi: 10.1007/3-540-58691-1_68. URL https://doi.org/10.1007/3-540-58691-1_68.
[11] Carlos Andres Lara-Nino, Miguel Morales-Sandoval, and Arturo Diaz-Perez. Small lightweight hash functions in FPGA. In *2018 IEEE 9th Latin American Symposium on Circuits & Systems (LASCAS)*, pages 1–4, Puerto Vallarta, Mexico, February 2018. IEEE. doi: 10.1109/LASCAS.2018.8399948. URL https://ieeexplore.ieee.org/document/8399948.
[12] Carlos Andres Lara-Nino, Arturo Diaz-Perez, and Miguel Morales-Sandoval. Fpga-based assessment of Midori and GIFT lightweight block ciphers. In *20th International Conference on Information and Communications Security*, pages 745–755, Lille, France, October 2018. URL https://doi.org/10.1007/978-3-030-01950-1_45.
[13] Carlos Andres Lara-Nino, Arturo Diaz-Perez, and Miguel Morales-Sandoval. Energy and area costs of lightweight cryptographic algorithms for authenticated encryption in WSN. *Security and Communication Networks*, pages 1 – 15, 2018. ISSN 1939-0114. URL https://doi.org/10.1155/2018/5087065.
[14] Miguel Morales-Sandoval, Luis Armando Rodriguez-Flores, Rene Cumplido, Jose Juan Garcia-Hernandez, Claudia Feregrino, and Ignacio Algredo-Badillo. A compact FPGA-based accelerator for curve-based cryptography in Wireless Sensor Networks. *Journal of Sensors, special issue: Recent Advances in Security and Privacy for Wireless Sensor Networks*, 2021:1–13, 2021. ISSN 1687-725X. doi: 10.1155/2021/8860413. URL https://doi.org/10.1155/2021/8860413.
[15] Carlos Andres Lara-Nino, Miguel Morales-Sandoval, and Arturo Diaz-Perez. Lightweight key establishment for WSNs. In *2019 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*, pages 1–8, University of Victoria, Canada, August 2019. doi: 10.1109/PACRIM47961.2019.8985101. URL https://ieeexplore.ieee.org/document/8985101.
[16] Carlos Andres Lara-Nino, Arturo Diaz-Perez, and Miguel Morales-Sandoval. Post-quantum cryptography on wireless sensor networks: Challenges and opportunities. In *Integration of WSNs into Internet of Things: A Security Perspective*, pages 81–99. CRC Press, 1 edition, 2021. ISBN 9780367620196. URL https://doi.org/10.1201/9781003107521.
[17] Daniel J Bernstein, Andreas Hülsing, Stefan Kölbl, Ruben Niederhagen, Joost Rijneveld, and Peter Schwabe. The sphincs+ signature framework. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 2129–2146, 2019.
[18] Miguel Angel Perez Sanchez. Arquitectura de un sistema de firma digital poscuántica para entornos de cómputo móvil y distribuido. Master's thesis, Cinvestav Tamaulipas, Ciudad Victoria, Tamps, 2021.
[19] Dustin Moody. Round 2 of nist pqc competition. *Invited talk at PQCrypto*, 2019.
[20] Reza Azarderakhsh, Matthew Campagna, Craig Costello, LD Feo, Basil Hess, Amir Jalali, David Jao, Brian Koziel, Brian LaMacchia, Patrick Longa, et al. Supersingular isogeny key encapsulation. *Submission to the NIST Post-Quantum Standardization project*, 2017.
[21] T.R. Reshmi. Information security breaches due to ransomware attacks - a systematic literature review. *International Journal of Information Management Data Insights*, 1(2):100013, 2021. ISSN 2667-0968. doi: https://doi.org/10.1016/j.jjimei.2021.100013. URL https://www.sciencedirect.com/science/article/pii/S2667096821000069.