UNIVERSIDAD DE COSTA RICA

SEDE DEL ATLÁNTICO

IF-6201 Informática Aplicada a los Negocios

Tema:

Criptografía

Integrantes:

Graciela Porras Rojas B75923

Jordan Castillo Arias B61599

Ronald Sancho Madrigal B66666

Profesor:

Rolando Herrera Sánchez

Año:

2020

Índice

Introducción

Para el ser humano la actividad de tener secretos y de mantenerlos lo más seguros posible ha estado siempre presente y a lo largo de la historia se han desarrollado diferentes técnicas de criptografía que se desarrollarán conforme se avance en el texto. Con la llegada del internet y toda la cantidad de datos que se manejan de forma virtual está claro que muchos tienen la necesidad de ocultar sus datos y solo compartirlos con personas de su selección personal.

La criptografía en términos generales es el estudio de cifrado y ocultamiento de la información contra los usuarios no autorizados, engloba diferentes técnicas de las cuales algunas muy importantes como la complejidad algorítmica, teoría de la información y la matemática discreta. Entonces con lo anterior claro es común preguntarse qué funciones puede ofrecer la criptografía a quien la necesite, hay cinco que son básicas como la confidencialidad que asegura que sólo usuarios autorizados pueden acceder a la información, la integridad de la información esto quiere decir que se da con seguridad que la información no será modificado ni eliminada de ninguna manera ni por el dueño ya sea de forma accidental o por algún tercero y por último la autenticación de usuario para asegurar que solo usuarios autorizados pueden acceder a la información.

Este es un tema extenso la criptografía pues es un tema de estudio muy importante para matemáticos porque si la criptografía utiliza la matemática pura y también para los informaticos con todo el tema de la seguridad de la información es por eso que se han descubierto dos tipos de criptografía los cuales son criptografía simétrica y la criptografía asimétrica que serán explicadas a profundidad cada una de ellas sus usos, ventajas y desventajas.

Historia de la criptografía

Según Ortega Triguero, J., López Guerrero, M., & García Crespo, E. (2006), los historiadores han dicho que la criptografía se puede considerar igual de antigua que la escritura y que esta se encontró presente en todas las civilizaciones antiguas. Aunque no fue hasta la Edad Media, con los árabes, y el Renacimiento, con los europeos, que se hizo uso regular de la misma.

El primer texto relacionado con la criptografía fue 1900 a.C aproximadamente en el antiguo Egipto, donde cambiaron simbología, pero esta no fue para ocultar información, sino que se dice que era para cierto tono de dignidad. La escritura de la antigua Mesopotamia también cambió cierta simbología de su escritura pero esta sí fue con la intención de ocultar el significado de la escritura. En el siglo IV a.C esta se ve presente en los antiguos textos hebreos, como los textos bíblicos.

Este método fue también implementado por gobiernos y sus ejércitos debido a que se tenía que transmitir información secreta. Antiguamente, en China y el ejército persa, llegaron a ocultar información donde hacían uso de cera para ocultar el mensaje y este se transportaba por un canal inseguro, por lo que se dio origen a esteganografía, ya que ocultaban información. Ya en el siglo V a.C. los espartanos diseñaron su primer criptosistema para uso militar, el cual denominaron "El escítalo". Se comenta que es similar a un baston redondo en el que se enrollaba una cinta de pergamino larga y estrecha, en ella se escribía un mensaje en forma longitudinal, si este se desarrollaban aparecían en otro orden formando secuencia sin sentido, el receptor del mensaje disponía de otro bastón exactamente igual y se descifraba el mensaje enrollando de nuevo la cinta.

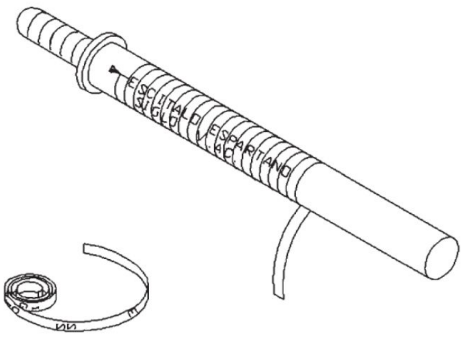


Figura 1.2
El escítalo espartano

Después del escitalo espartano y con el paso del tiempo se fueron dando otras formas para encriptar información. Chaves Jiménez H. (2008), menciona, que después de la segunda guerra mundial aparecen los computadores electrónicos, aquí la criptografía llega a su "edad adulta". Hoy en día se puede decir que el medio donde más se da esta práctica es en los sistemas de información, debido a que estos los encontramos en nuestra vida cotidiana y manejan gran cantidad información

¿Qué es criptografía ?

Ahora después de saber un poco más acerca de la historia de la criptografía es importante hablar sobre el concepto de criptología para poder llegar a tener un mayor y mejor conocimiento acerca de este tema.

La criptografía según Funes, Sette, Ramos & Langsam, 2020 en su sitio web nos dice que es el desarrollo de un conjunto de técnicas que permiten alterar y modificar mensajes o archivos con el objetivo de que no puedan ser leídos por todos aquellos usuarios que no estén autorizados a hacerlo. Hoy en día, en pleno auge de las comunicaciones digitales, funciona como la base para cualquier proceso de seguridad informática.

La criptografía podríamos mencionar que es la técnica que nos ayuda a proteger los documentos y datos que son importantes para un individuo o empresa, esta es utilizada por medio de cifras o códigos para poder así escribir datos o información importante, sensible y confidenciales que andan circulando en las redes locales o en internet.

Existen 2 métodos en la encriptación los cuales son muy importantes y principales de conocer estos serían el cifrado y el descifrado. El primer método es el proceso por el cual se toma un mensaje y es transformado en caracteres ilegibles y que no construyen ningún concepto o dato revelador de la información que se desea encriptar, el segundo método sería el proceso contrario por el cual podemos tener nuevamente el mensaje y poder descifrarlo mediante unas claves y otros tipos de criptografías los cuales serán mencionados y explicados más adelante.

Objetivo de la criptografía

Con respecto a la definición de la criptografía que se brindó en el apartado anterior, se puede deducir que su objetivo principal es el cifrado de la información para solucionar

problemas de seguridad en las comunicaciones y en los medios informáticos. Según Chaves Jiménez H. (2008), las propiedades que se deben tener en cuenta para cumplir este objetivo son las siguientes:

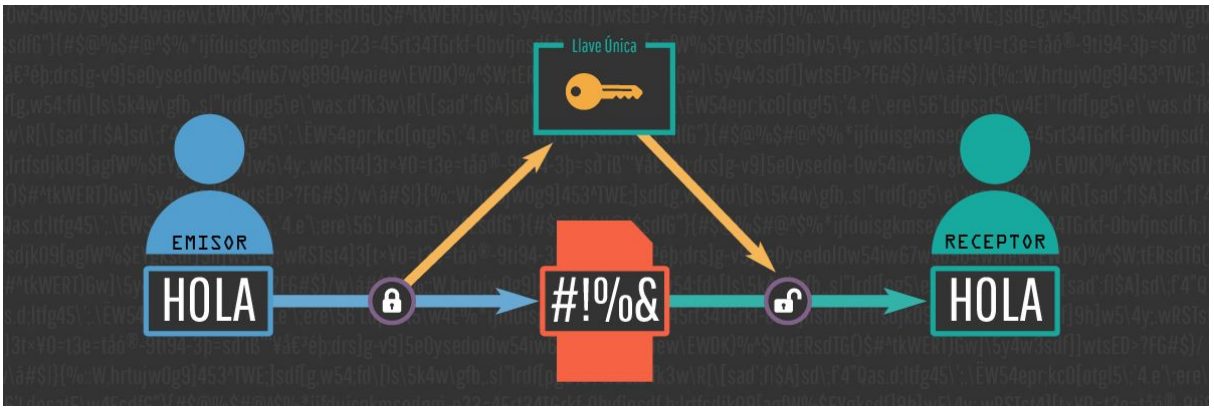
- La privacidad: Esto con el fin de que la información que se transmite solo pueda ser extraída por la persona autorizada.
- La integridad: Para que la información transmitida no pueda ser alterada por intrusos.
- La autenticidad: Esta permite al receptor verificar que el mensaje recibido es el correcto.
- El no rechazo. Evitar que el autor del mensaje niegue la autoría o envío del mismo.

Tipos de criptografía

Ya teniendo una mejor idea y conceptualización sobre la criptografía y sus principales objetivos; para poder aplicar este método en la actualidad existen diversos tipos de criptografía los cuales son los siguientes:

Criptografía simétrica

En este tipo solo se utiliza una clave para poder cifrar y descifrar. Esta clave debe ser previamente conocida por ambas partes o entes (emisor y receptor). Por ejemplo sería algo similar que la seguridad de nuestra casa " *Tenemos una llave para cerrar la puerta y estamos tranquilos que solo las personas con esa misma llave la van a poder abrir.*" (Funes, Sette, Ramos & Langsam, 2020) Para esta tenemos la gran ventaja que podemos compartir esta llave con cualquier persona de confianza, pero también se tiene una desventaja en la cual puede existir la posibilidad de que se extravíe, o de que alguien la robe.



- **Ventajas**

  Velocidad: esta sería la principal ventaja de este cifrado es muy rápido y ágil por lo que si se desea cifrar una gran cantidad de información y tener una mayor velocidad y eficiencia esta sería una de las mejores opciones ya que ahorrarás más tiempo.

- **Desventajas**

  Seguridad: según nos dice en su artículo este tipo no es tan seguro porque "*ya que el hecho de comunicar la clave supone una gran vulnerabilidad. Es muy importante buscar medios seguros para comunicar*"(OSI, 2019).

  Número de claves: por el gran aumento que esta pueda tener de usuarios presenta la desventaja de aumentar su número de claves.

- **Algunos de los más usados:**
  - AES: más conocido como Advanced Encryption Standard este "*es uno de los algoritmos de cifrado más utilizados y seguros actualmente disponibles, es de acceso público*" (Pfundmeier & Freudenreich, 2019). Este algoritmo se basa en varias sustituciones, permutaciones y transformaciones lineales, cada una de estas es ejecutada en bloques de 16 bytes.

- Blowfish: Esta es una técnica de cifrado diseñada por Brice Schneier en 1993 como alternativa a la técnica de cifrado DES, en su artículo nos dice lo siguiente "*más rápido que DES y proporciona una buena tasa de cifrado sin que se haya encontrado una técnica de criptoanálisis eficaz hasta la fecha. Es uno de los primeros cifrados de bloque seguros que no están sujetos a ninguna patente*" (Jain, S., Singh, D., Goel, S., & Baranwal, 2019), gracias a no tener ninguna patente este cifrado es gratuito.

Criptografía asimétrica

En este tipo también conocido como criptografía de clave pública se tiene como base la utilización de dos claves distintas es decir

> Son dos claves diferentes, pero vinculadas matemáticamente entre sí, utilizadas para cifrar y descifrar el mensaje. Una de ellas debe ser pública, propia de cada participante pero puesta a disposición de cualquier usuario, sea participante en el intercambio de información o no. La otra es una clave privada, también propia de cada uno de ellos, pero que debe permanecer en secreto y nunca ser revelada (Funes, Sette, Ramos & Langsam, 2020).

Gracias a este sistema en el cual cada usuario o ente requiere que posea un par de claves, una que no se comunique ni sea revelada a nadie llamada clave privada y la otra sería la pública la cual si es brindada o compartida con el resto de usuarios. Una de las característica más importante de este tipo es que permite garantizar la privacidad del mensaje o datos que estemos enviando ya que al emisor cifra el contenido con la clave pública del destinatario solo este receptor podrá recibir el mensaje y de esta forma descifrarlo.

- **Ventajas**

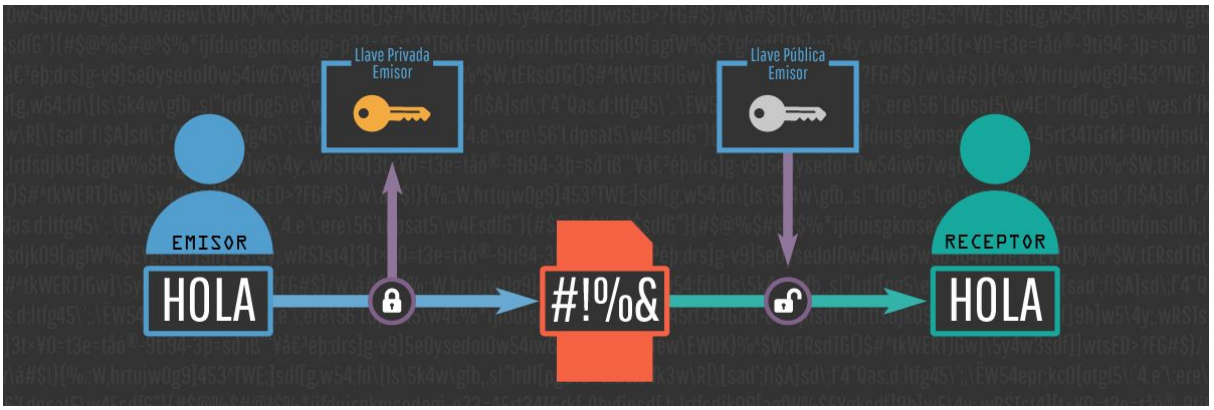
  Número de claves: esta ventaja como vemos en "*la administración de claves también es un beneficio al usar el cifrado asimétrico. Solo necesitas un par de claves, por usuario, para cada uno, para poder cifrar mensajes para todos los demás usuarios*" (OSI, 2019).

  Seguridad: Otra ventaja sería por la seguridad que esta nos podría brindar el hecho "d*e que puede comunicar, de forma segura, claves públicas a terceros*"(OSI, 2019). Aquí el usuario podrá entregar, compartir la llave pública, siempre y cuando él mantenga la clave privada.

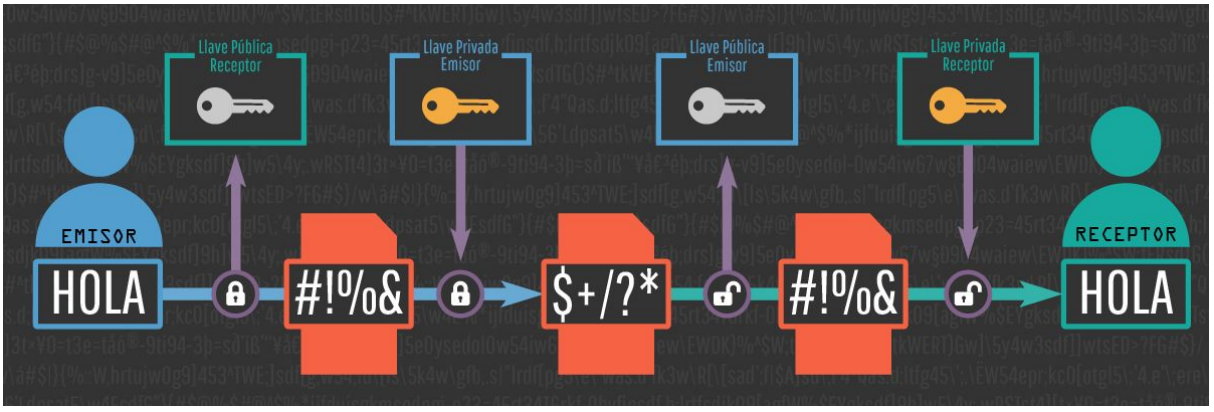
- **Desventajas**

  Velocidad: este tipo de cifrado es muy lento. Como se menciona en su artículo OSI, (2019) "Si el rendimiento es un factor clave a tener en cuenta no es la mejor opción, esto por su lentitud de cifrado es una de sus grandes desventajas.

- **Algunos de los más usados:**
  - RSA:según Boxcryptor 2018 en su artículo " *es uno de los sistemas de cifrado asimétricos más exitosos de la actualidad. Originalmente descubierto en 1973 por la agencia de inteligencia británica GCHQ, recibió la clasificación "top secret*"(Pfundmeier & Freudenreich, 2019). Debemos agradecer a los criptologos Rivest, Shamir y Adleman este cifrado a diferencia de los tradicionales trabaja complementarios entre sí, lo que significa que un mensaje cifrado con uno de ellos sólo puede ser descifrado por su contraparte.
  - GPG: este también conocido como GnuPG como su nombre lo dice privacidad bastante buena es "*una herramienta de línea de comandos con funciones para una fácil integración con otras aplicaciones, permite cifrar y firmar sus datos y comunicaciones, cuenta con un sistema de gestión de claves versátil*"(Project, 2020) , este es una versión de Windows de GnuPg un administrador de cifrado.



Sucedería lo contrario si el emisor codifica el contenido con su propia clave privada, cualquiera podría leerlo mediante la clave pública complementaria, pero se sabe con certeza que ese mensaje es enviado directamente del emisor, un ejemplo muy bueno es para las firmas digitales ya que se sabría con certeza de que el emisor sería la persona correcta.



Una de las desventajas o límites de esta criptografía es que al requerir cálculos muy complejos se convierte en un proceso mucho más lento. Por esta razón a nivel de trabajo se utilizan muchas veces una combinación entre ambos tipos de sistemas ya que con el método asimétrico realizan la comunicación con todos los involucrados y luego para poder mantener esta comunicación se utiliza el métodos simétricos que es más rápido.

Usos de la criptografía

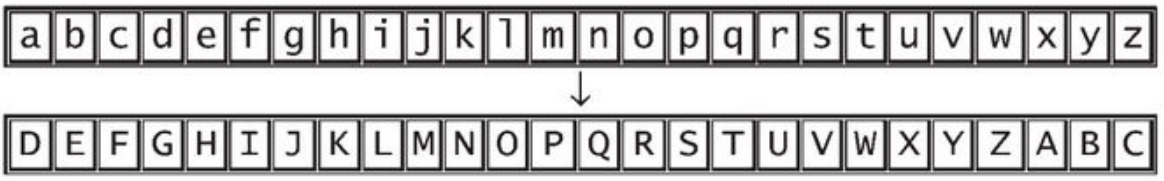
Con respecto a lo mencionado en apartados anteriores, a la criptografía prácticamente se le dio mayor uso para un carácter militar, pero en la actualidad, esta se encuentra presente en muchos entornos de la sociedad de la información de alguna u otra forma. Muchas veces esto no se tiene presente, pero cuando se hace uso de tarjetas de crédito, se ingresan a las cuentas de banco y se realizan compras a través de Internet, cuando se firma electrónicamente, se hace uso de correos electrónicos o por medio de la navegación por Internet.

Entre las principales aplicaciones de la criptografía, Delgado V. y Palacios R (2006) mencionan tres de ellas, las cuáles se pueden categorizar como las más usuales, estas son las siguientes:

- **Aplicaciones de cifrado:** La situación práctica en la que más se utiliza es la transferencia de información por canales de comunicación no seguros, como es Internet, ejemplo de ello es, el correo electrónico, y la transferencia de información mediante navegadores. También se utilizan las técnicas de cifrado para proteger documentos importantes dentro del disco duro o en cualquier medio de almacenamiento digital. Por lo tanto, el enfoque principal de esta aplicación es garantizar la confidencialidad, integridad, transferencia de los documentos. Se pueden encontrar varios tipos de cifrado como los siguientes

    - **Cifrados por Sustitución**

      Este tipo es uno de los más antiguos, consiste en sustituir letras del mensaje original con otras letras del alfabeto o con símbolos logrando así que el mensaje original pierda todo sentido y significado. Este método es bastante sencillo y fácil de entender por eso fue uno de los más usados en la antigüedad. Un ejemplo de cifrado por sustitución es el utilizado por Julio Cesar es bastante simple lo que se debe hacer es sustituir la letra del abecedario por una que esté tres posiciones adelante esto significa que la letra A equivaldrá a la letra D, la B la E, siguiendo esta regla las letras X,Y y Z serán A,B,C respectivamente.



Sustitución de Julio César

Entonces si deseamos cifrar el mensaje "Hola mundo" el resultado sería "KROD PXQGR" el mensaje pierde por completo su significado, entonces se ha logrado el objetivo. Para recuperar el mensaje original basta con hacer el proceso a la inversa teniendo claro que se debe poseer la clave porque es lo más importante de este tipo de cifrado todo radica en cómo emparejamos las letras del alfabeto original con otro ordenador con distintas reglas.

- **Cifrado por sustitución polialfabética**

  Este cifrado es un poco más complicado que el anterior pero promete ser más robusto y confiable. En el libro *Introducción a la criptografía historia y actualidad* se explica que el cifrado polialfabético es:

  > Los nuevos cifrados polialfabéticos lo hacen empleando una sustitución diferente en el cifrado de cada letra. Haciendo esto, una misma letra del alfabeto en claro se transforma en cada ocasión en un signo distinto del alfabeto de cifrado y se inutiliza así el citado análisis de frecuencias. Esta forma de encriptar recibe el nombre de cifrado polialfabético; ya que como cada sustitución trae consigo una reordenación del alfabeto de cifrado, al emplear varias da la impresión que se manejan múltiples alfabetos. (Ortega Triguero, Lopez Guerrero y Garcia del Castillo Crespo, 2006).

  En pocas palabras el texto anterior habla de que en esta técnica de cifrado se utiliza más de un alfabeto, para entender esto de mejor manera se puede imaginar un caso en el cual queremos cifrar la palabra "Hola mundo" ahora bien utilizamos el alfabeto español de veintisiete letras, luego desplazamos este mismo dos letras que quiere decir esto que por ejemplo la letra A ya no será la primera letra del abecedario pues su lugar lo tomó la letra C a causa del desplazamiento así que hacemos otro abecedario con un desplazamiento de siete letras y agregamos una

regla más se utilizara el abecedario 1 con las letras de la frase que esten en la posición impar y el abecedario 2 con las letras que están en la posición par dándonos como resultado de cifrado “jung ñaojq”.

Los alfabetos utilizados son:

Normal: A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z

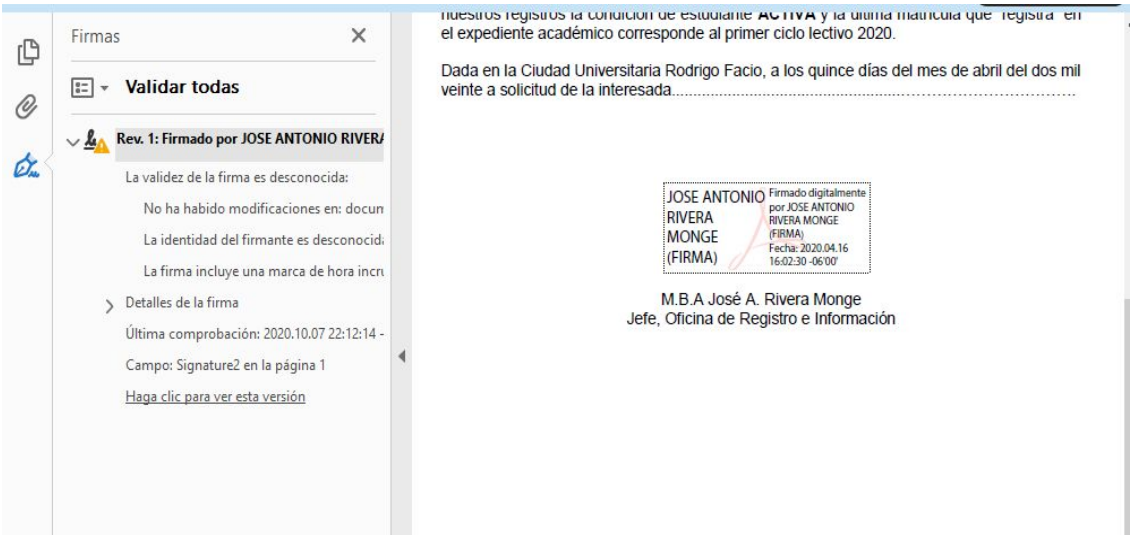
+2 letras: C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z A B

+7 letras: G H I J K L M N Ñ O P Q R S T U V W X Y Z A B C D E F

- **Cifrado por sustitución de transposición**

  Este cifrado consiste en que las letras del mensaje son cambiadas siguiendo unas reglas bien definidas. Por ejemplo el de transposición columnar se necesita una clave y un mensaje a cifrar, el primer paso es obtener la posición en el abecedario de cada una de las letras de la palabra clave, luego las letras del mensaje se van colocando debajo de las letras de la clave, lo siguiente es ordenar la clave de menor a mayor según su posición en el abecedario y luego colocar de nuevo las letras que ya habían sido colocadas debajo de las letras de la clave y el paso final es tomar las letras que que están debajo de cada letra de la clave y se escriben en horizontal dándonos como resultado el mensaje cifrado.

- **Aplicaciones de firma electrónica:** Esta se utiliza para conseguir integridad y autenticación. La firma electrónica es uno de los aspectos más importantes de la criptografía porque permite realizar muchas transacciones por Internet, evitando desplazamientos y pérdidas de tiempo. Un ejemplo de esto es la firma digital que hoy en día se ha estado implementando, en la siguiente imagen se puede observar que al hacer uso de esta firma en un documento digital, se puede corroborar que el documento no ha sido modificado, la fecha y hora de última vez de comprobación, el lugar donde fue ubicada la firma en el archivo y la identidad del firmante. Por estos aspectos es que se dice que la firma electrónica garantiza integridad y autenticación.

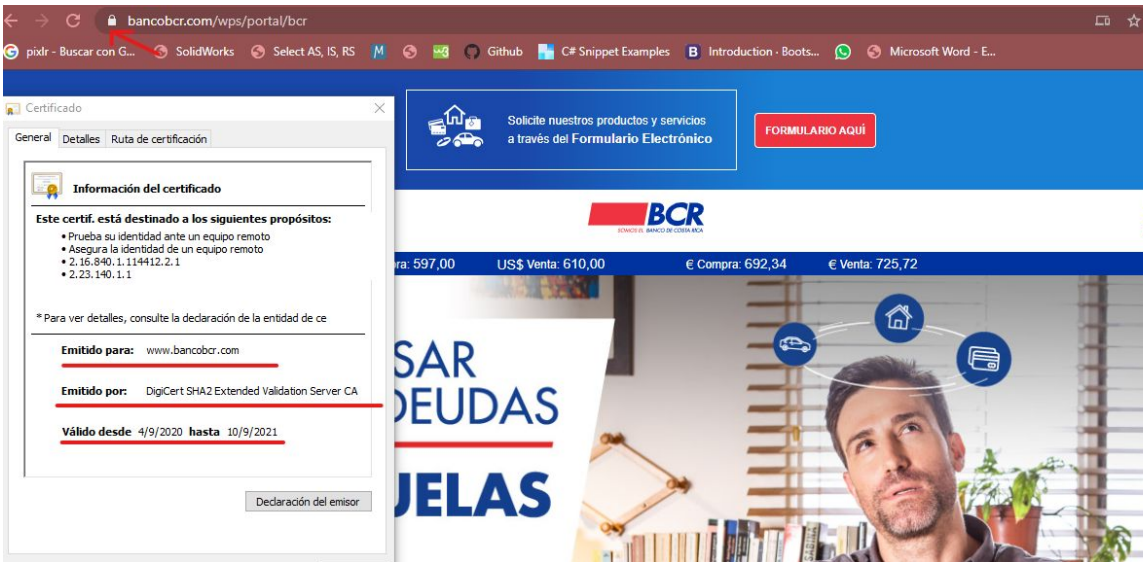


- **Certificados digitales:** Mecanismo para reforzar la seguridad de las claves públicas, independiente del emisor y del receptor, se encarga de firmar electrónicamente las claves. Su función principal es certificar que una clave es válida y pertenece a una determinada persona. La implementación práctica de este mecanismo se realiza guardando la clave pública junto con cierta información adicional dentro de un certificado digital y solicitar la firma electrónica de dicho certificado por parte de la entidad de certificación. Este mecanismo permite cifrar comunicaciones, firmar mensajes y documentos, identificación ante un sistema o autenticación de usuarios.

  Entre las entidades que brindan certificaciones digitales, se encuentran:

  - ➔ DigiCert
  - ➔ Let's Encrypt
  - ➔ Cloudflare

  Otro dato sobre las certificaciones digitales es que esta hace uso del protocolo https, por ejemplo, la página del Banco de Costa Rica hace uso de este, ya que es obvio que este tipo de plataformas manejan información sensible, una manera de verificar que la plataforma es segura es que su url tenga el protocolo https y también en la información de la certificación que posee la página.



Recomendaciones

La criptografía es un importante tema de estudio que está en constante evolución para mejorar la seguridad de la comunicación, las aplicaciones que utilizamos en nuestra vida cotidiana recopilan y manejan la información personal de los usuarios para funcionar correctamente o para mostrarte lo que quieres ver. Entonces ¿qué pasaría si estas aplicaciones o páginas web no contaran con algún tipo de cifrado? la respuesta es que un tercero tendrá el camino libre para hacerse con información que posiblemente los usuarios quieran esconder, como cuentas bancarias, contraseñas, mensajes ya sea de correo electrónico o del popular WhatsApp por dar algún ejemplo actual... . Es por eso que las empresas invierten en implementar algún algoritmo de cifrado que sea lo más robusto posible para mantener a salvo a los usuarios y así mismos porque si ocurre un robo de información toda la responsabilidad recae en la empresa. Debemos recordar que la información es una de las posesiones más preciadas que puede tener el ser humano, con el conocimiento correcto se pueden lograr cosas extraordinarias como detener una guerra, algún ataque terrorista o todo lo contrario provocar lo anterior. Entonces ya teniendo claro la importancia de la criptografía y la comunicación segura, se procederá hacer algunas recomendaciones sobre cómo una empresa podría empezar hacer uso de algoritmos de cifrado:

- Utilizar algoritmos estándar

  Se recomienda utilizar AES(AES (AES-128 y AES-256) en la actualidad (año 2020) es el algoritmo más utilizado por lo tanto se cree es el más seguro. Además al ser el más utilizado es revisado constantemente, es estudiado para mejorarlo y volverlo cada vez más impenetrable.

- Implementación algoritmos del sistema, enfocar más en la seguridad de las claves

  El cifrado depende de las claves así que entre más seguras sean estas más protección nos proveerán los algoritmos de cifrado.

- Tener en cuenta que esto no va a brindar una seguridad completa, sino que es una herramienta para reforzar

  Cifrar la información no solucionará todos los problemas de seguridad, es muy importante su implementación pero es necesario que la empresa tenga otros métodos.

- Cifrar sólo la información que se considere sensible

  No hay necesidad de cifrar toda la información en la mayoría de los casos no hará daño a nadie que terceros logren interceptar información de una empresa y esta sean cosas como nombres y apellidos, Sin embargo, es otra historia si logran obtener por ejemplo información bancaria.

- Mantener las claves lo más seguras posibles

  Las claves son el corazón del cifrado si se pierden o caen en manos equivocadas el cifrado será completamente inutil.

- Cifrar información que será enviada

  Toda información que será enviada debe ser encriptada antes de hacerlo para evitar fuga de información si es interceptada.

Referencias Bibliográficas

Chaves Jiménez, H., (2008). DISEÑO E IMPLEMENTACIÓN DE UN SOFTWARE MULTIMEDIA PARA EL APRENDIZAJE DE LA CRIPTOGRAFÍA. Universidad san Buenaventura. Bogotá D.C.. Recuperado de: http://biblioteca.usbbog.edu.co:8080/Biblioteca/BDigital/43336.pdf

Delgado, V. and Palacios, R. (2006). Aplicaciones prácticas de la criptografía. Recuperado de: https://www.icai.es/contenidos/publicaciones/anales_get.php?id=1235

Funes, M., Sette, A., Ramos, A., & Langsam, D. (2020). ¿Qué es criptografía?. https://nic.ar/es/enterate/novedades/que-es-criptografia

Jain, S., Singh, D., Goel, S., & Baranwal, S. (2019). Blowfish Algorithm with Examples - GeeksforGeeks. Recuperado de: https://www.geeksforgeeks.org/blowfish-algorithm-with-examples/

Oficina de Seguridad del Internauta. (2019). Recuperado de: https://www.osi.es/es/actualidad/blog/2019/07/10/sabias-que-existen-distintos-tipos-de-cifrado-para-proteger-la-privacidad

Ortega Triguero, J., López Guerrero, M., & García Crespo, E. (2006). Introducción a la criptografía : historia y actualidad. España. https://elibro-net.ezproxy.sibdi.ucr.ac.cr/es/ereader/sibdi/54964

Pfundmeier, A., & Freudenreich, R. (2019). Cifrado AES y RSA. Recuperado de https://www.boxcryptor.com/es/encryption/

Project, G. (2020). The GNU Privacy Guard. Recuperado de https://gnupg.org/index.html