Nombre del alumno: Johanne Joaquín Arriaga Díaz

Nombre del profesor: Icel Bernardo Lepe Arriaga.

Nombre del trabajo: Ensayo de unidad I.

Materia: Redes de computadoras III.

Grado: Séptimo cuatrimestre

Grupo: ISC13SDC0119-F

Frontera Comalapa, Chiapas a 19 de Septiembre de 2021

CRIPTOGRAFÍA

Introducción a la criptografía

La criptografía, es la ciencia que se basa en la escritura de códigos y cifrados para proteger las comunicaciones, es uno de los elementos más importantes que hacen posible la existencia de criptomonedas modernas y blockchains.

Es el arte de escribir mensajes en clave secreta o forma enigmática: encargada de transformar la información parra que ésta quede descubierta y no se peda acceder sin autorización Sus objetivos son: confidencialidad de información y la autenticidad del par remitente/emisor; a las personas que decidan a estudiar y desarrollar métodos para resguardar así la información se les llama criptógrafos.

A continuación, los momentos importantes en la criptografía.

En el siglo V a.C. durante la guerra entre Atenas y Esparta, se encuentra el primer registro de escritura secreta, en el 400 a.C. los espartanos utilizaron la Scítala o Escítalo, que puede considerarse el primer sistema de criptografía por transposición, en el siglo II a.C. Polybio, historiador griego, le permiten escribir historia: Invento un cuadro de 5×5 que permitía intercambiar los distintos signos entre si y fue tan importante en su época que se utilizó en muchos sistemas criptográficos posteriores, en el siglo I a.C surge el cifrado César, el cual se considera que fue utilizado por Julio César El cifrado consiste en mover el carácter a representar 3 posiciones adelante dentro del alfabeto a utilizar, en el siglo I d.C Carlomagno luchó contra diversos pueblos obteniendo la victoria, un factor determinante fue la comunicación con sus ejércitos y aliados sustituía las letras por símbolos extraños, en el siglo XV se escribe la “Liber Zifrorum”, escrita por Cicco Simoneta consejero y secretario de la cancillería de los duques Sforza en Milán, en la que se estudian diversos sistemas basados en la sustitución de letras y diversas representaciones en las que incluyen símbolos convencionales. Hacia 1466, Alberti escribe otra obra “De Compendis Cifris” y concibe el sistema poli alfabético, esto es, un cifrador que emplea varios alfabetos, saltando de uno a otro cada tres o cuatro palabras, en el siglo XVI, eso es, Giovan Battista Belasco de Brescia instituyó una nueva técnica. La clave formada por una palabra o frase, debía transcribirse letra a letra sobre el texto original y cada letra del texto se debía cambiar por la correspondiente en el alfabeto que comienza en la letra clave, dentro del período renacentista italiano, Jérome Cardan un célebre matemático físico y astrólogo aportó en 1550 un sistema basado en una carta o tarjeta con agujeros perforados, de tal manera que el mensaje en claro se obtenía al colocarlo sobre determinado texto preconcebido, lo que sería llamado después “Mascaras Rotativas”.

En el siglo XVIII, se usó de la criptografía para información relacionada con todo aquello que representa el poder, esto es: secretos de estado, asuntos militares, de espionaje y diplomáticos, y siempre rodeada de todo lo que representa misterio.

En 1883, el Dr. Auguste Kerckhoffs lingüista y criptógrafo francés quien rompe el sistema llamado “gran cifrador” creado por Rossignols y descifra mensajes cifrados con el sistema de transposición militar francés, lo que hace que el ministro de guerra decida cambiar el esquema de cifrado por uno nuevo el método de Vigenére fue llevado hasta su última extensión lógica muchos años más tarde por un criptógrafo americano, el ingeniero Gilbert Sandford Vernam, quien lo demostró que para que el cifrado de Vigenére fuera seguro no solamente era necesario que la clave de cifrado fuera más larga que el mensaje, sino que además ésta debía ser utilizada una sola vez.

En 1919 se patento una máquina criptográfica, llamada Enigma, obra de Alexander Koch y el Arthur Scherbius, este último realizó varias versiones de Enigma junto con Richard Ritter, para llevar a cabo la producción comercial de la máquina. Fue puesta en venta en 1923 y se llamó Enigma-A a esta le siguieron tres modelos comerciales Enigma B, C y D, siendo la última la más importante, ya que tuvo un éxito rotundo después de haber sido adquirida en 1926 por la marina alemana.

Con las computadoras, la criptografía alcanzó niveles mayores que en la era analógica. La encriptación matemática de 128-bits, mucho más fuerte que cualquier cifrado antiguo es ahora el estándar para muchos dispositivos sensibles y sistemas informáticos. En 1990, se pondría en marcha toda una nueva forma de criptografía, apodada criptografía cuántica. Más recientemente, técnicas criptográficas han sido también utilizadas para hacer posibles las criptomonedas: sirve de puntal a Bitcoin y a otros sistemas de criptomonedas, al proporcionar una seguridad complementaria y garantizar que los fondos sólo pueden ser utilizados por sus legítimos dueños.

CIFRADOS POR SUSTITUCIÓN.

El cifrado César es uno de los primeros métodos de cifrado conocidos históricamente. Julio César lo usó para enviar órdenes a sus generales en los campos de batalla. Consistía en escribir el mensaje con un alfabeto que estaba formado por las letras del alfabeto latino normal desplazadas tres posiciones a la derecha.

El receptor del mensaje conocía la clave secreta de éste y podía descifrarlo, más de 1500 años después, un cifrado similar fue utilizado por la reina María Estuardo de Escocia, para conspirar junto con los españoles contra su prima Isabel I

Cifrados por sustitución mono alfabeto

Una sustitución mono alfabeto como la del cifrado César puede expresarse mediante una transformación congruente lineal (también conocida criptográficamente como transformación afín). En el cifrado César esta se escribiría como $E(M)= (M+3) \bmod N$, siendo N la longitud o cardinal del alfabeto original.

Criptoanálisis de los Métodos de Cifrado Monoalfabéticos

El cifrado monoalfabético es la familia de métodos criptográficos más simple de criptoanalizar, puesto que las propiedades estadísticas del texto claro se conservan en el criptograma, su principal debilidad es que el texto cifrado mantiene la misma distribución de frecuencia de caracteres que tiene el texto claro original, lo que hace que los cifrados mono alfabeto sean criptoanalizables por métodos estadísticos sencillos.

Cifrado de Vigenère

Es cifrado poli alfabético la clave está constituida por una secuencia de símbolos del alfabeto $K = \{k0, k1, ..., kd-1\}$, de longitud d.

RELLENOS DE UNA SOLA VEZ.

La construcción de un cifrado inviolable consiste en escoger una cadena de bits al azar como clave. Luego se convierte el texto normal en una cadena de bits, por ejemplo, usando su representación ASCII. Por último, se calcula el or exclusivo (XOR) y cuya tabla de valores lógicos puede verse en la siguiente figura, de estas dos cadenas, bit por bit.

El texto cifrado no puede descifrarse porque cada texto normal posible es un candidato igualmente probable. El texto cifrado no proporciona al criptoanalista ninguna información en absoluto. En una muestra suficientemente grande de texto cifrado, cada letra ocurrirá con la misma frecuencia, al igual que cada diagrama (combinación de dos letras) y cada trigrama (combinación de tres letras) pero tiene varias desventajas: la clave no puede memorizarse, la cantidad total de datos que pueden transmitirse está limitada a la cantidad de clave disponible. Otro problema es la sensibilidad del método a la pérdida o inserción de caracteres. Si el transmisor y el receptor pierden la sincronía, todos los datos a partir de ahí aparecerán alterados.

Criptografía clásica

La criptografía clásica se basa en algoritmos sencillos y claves muy largas para la seguridad. Las técnicas criptográficas clásicas son básicamente dos, el cifrado por sustitución y el cifrado por trasposición.

Dos principios criptográficos fundamentales.

Existen dos principios fundamentales que sostienen la criptografía y que es importante entender. El primer principio es que todos los mensajes cifrados deben contener redundancia, es decir, información no necesaria para entender el mensaje.

Redundancia: definiremos redundancia como cierta repetición de la información contenida en un mensaje, que permite, a pesar de la pérdida de una parte de este, reconstruir su contenido.

Todos los mensajes deben contener redundancias para evitar que pueda modificarse aleatoriamente un mensaje con cierta probabilidad de obtener un mensaje válido desde el punto de vista del descifrado, pero con datos alterados. Por ello, una cadena aleatoria de palabras sería mejor para incluir en la redundancia.

Actualización.

El segundo principio criptográfico es el de actualización el cual implica que se deben tomar medidas para asegurar que cada mensaje recibido se verifique a fin de saber siesta actualizado. Esto permite evitar que posibles intrusos activos reproduzcan mensajes antiguos. Una de las medidas es incluir en cada mensaje una marca de tiempo válida por ejemplo durante 10 segundos, para compararlo con los mensajes nuevos que lleguen y filtrar los duplicados. Los mensajes con una antigüedad mayor a10 segundos pueden descartarse.

Criptografía simétrica

La criptografía simétrica solo utiliza una clave para cifrar y descifrar el mensaje, que tiene que conocer el emisor y el receptor previamente y este es el punto débil del sistema, la comunicación de las claves entre ambos sujetos, ya que resulta más fácil interceptar una clave que se ha transmitido sin seguridad, otro inconveniente que tiene este sistema es que si quieres tener un contenido totalmente confidencial con 10 personas tienes que aprenderte o apuntarte las 10 claves para cada persona.

Criptografía asimétrica

La criptografía asimétrica se basa en el uso de dos claves: la pública (que se podrá difundir sin ningún problema a todas las personas que necesiten mandarte algo cifrado) y la privada (que no debe de ser revelada nunca).

Sabiendo lo anterior, si queremos que tres compañeros de trabajo nos manden un archivo cifrado debemos de mandarle nuestra clave pública (que está vinculada a la privada) y nos podrán mandar de forma confidencial ese archivo que solo nosotros podremos descifrar con la clave privada.

Puede parecer a simple vista un sistema un poco cojo ya que podríamos pensar que sabiendo la clave pública podríamos deducir la privada, pero este tipo de sistemas criptográficos usa algoritmos bastante complejos que generan a partir de la frase de paso (la contraseña) la clave privada y pública que pueden tener perfectamente un tamaño de 2048bits (probablemente imposible de reventar).

Diferencias entre criptografía simétrica y asimétrica

Las principales diferencias son por ejemplo que la criptografía simétrica es más insegura pero se puede cifrar y descifrar en menor tiempo del que tarda la criptografía asimétrica, que es el principal inconveniente y es la razón por la que existe la criptografía híbrida.

Criptografía híbrida

- Este sistema es la unión de las ventajas de los dos anteriores, debemos de partir que el problema de ambos sistemas criptográficos es que el simétrico es inseguro y el asimétrico es lento.
- El proceso para usar un sistema criptográfico híbrido es el siguiente (para enviar un archivo):
- Generar una clave pública y otra privada (en el receptor).
- Cifrar un archivo de forma síncrona.
- El receptor nos envía su clave pública.
- Ciframos la clave que hemos usado para encriptar el archivo con la clave pública del receptor.
- Enviamos el archivo cifrado (síncronamente) y la clave del archivo cifrada (asíncronamente y solo puede ver el receptor).