DERECHO DE LA RED

CRIPTOGRAFÍA

Contenido

¿QUÉ ES LA CRIPTOGRAFÍA?

Cuando hablamos de criptografía o encriptaciones tenemos la sensación de que nos referimos a cuestiones matemáticas de alto nivel, a documentos fuera de la comprensión habitual de un lector, incluso a operaciones militares de alto nivel. En definitiva, parece que accedemos a un mundo donde solo unos pocos entienden cómo funciona.

Quizás no nos alejemos mucho de la realidad, realmente los métodos de encriptación, es decir la criptografía, es un arte que consiste en ocultar y proteger información y que tiene como finalidad preservar una información ante terceros.

Por lo tanto cuando hablamos de encriptación estamos hablando de una conversión de datos de un formato a otro no legible. Esta transformación permite proteger la privacidad de la información sea del tipo que sea.

¿Dónde se ha utilizado?

Existen múltiples evidencias de utilización de criptografía a lo largo de los siglos, estos métodos nos permiten entrever la necesidad de ocultar información y de transmitirla de modo que el receptor de esta, fuese el único con capacidad suficiente como para poder descifrarla.

CIFRADOS PROTAGONISTAS EN LA HISTORIA.

Los cifrados son algoritmos, o sea, un conjunto de instrucciones paulatinas que se utilizan para cifrar o descifrar información. A lo largo de la historia hemos podido ver varios de ellos:

Cifrados de sustitución:

Consisten en equiparar una letra a un número. De este modo cualquiera que tenga acceso a la secuencia de números (el pin) podrá descifrar cualquier cifrado generado con tal pin. Esto quiere decir que el vector de ataque en este cifrado (la vulnerabilidad del cifrado) está en el pin. El pin del descodificador es lo que conocemos con la clave.

Dentro de este estilo podemos encontrar diversas modalidades de las que vamos a destacar:

Cifrado cesar o cifrado por desplazamiento.

Es una de las técnicas más simples y utilizadas a lo largo de la historia, la creó Julio César para comunicarse con sus generales durante las batallas.

Este método consiste en utilizar las posiciones ordinales de las letras para una clave. Por ejemplo segundo = 2.

De otro modo también se puede rotar el punto de partida mediante sumatorios, por ejemplo si sumados 2 unidades al anterior ejemplo segundo = 4.

Del mismo modo este cifrado también consistía en escribir el mensaje con un alfabeto que estaba formado por el desplazamiento de las letras tres posiciones a la derecha, por ejemplo la letra A correspondería a la D la K a la N y así sucesivamente.

Por lo que tendríamos únicamente 26 formas de rotar el cifrado para poder conservar el orden de las letras. Esto implica que existen una cantidad muy pequeña de claves que se pueden utilizar para descifrar.

Cifrado Vigenère.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
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
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	A
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
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	C
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	C	D
F	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
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
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	G
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	G	H
J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W
Y	Z	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
Z	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

Originalmente proviene de Giovan Battista Belasso que escribió en 1553 la cifra del sig. En este libro, el autor, construyó el cifrado basándose en la tabula recta de Trithemius modificándola y añadiendo una clave repetida para cambiar cada carácter entre los diferentes alfabetos. Siglo más tarde, este cifrado, fue atribuido, erróneamente, a Blaise de Vigenère.

Este tipo de cifrado se considera una mejora del cifrado cesar, ya que permite aumentar las claves convirtiéndolas en múltiples opciones.

En el cifrado de Vigenère, para cada letra nueva de un mensaje, se cifra utilizando una letra diferente de la palabra clave.

Para encriptar el mensaje HELLO usando la palabra clave LAW, observando la siguiente tabla.

Texto sin formato	H	mi	L	L	O
Posición ordinal	8	5	12	12	15
Palabra clave	L	UN	W	L	UN
Posición ordinal de palabra clave	12	1	23	12	1
Suma	20	6	35	24	dieciséis
Suma, envolviendo	20	6	9	24	dieciséis
Texto cifrado	T	F	yo	X	PAGS

Para la primera letra, o H, la posición ordinal es 8. La primera letra de nuestra palabra clave es L, que tiene la posición 12. Las agregamos a las posiciones para obtener 20, y la letra en la posición 20 es T. Por lo tanto, la primera letra de nuestro texto cifrado es T.

Cuando nos quedemos sin letras para la palabra clave, podemos reutilizarla. Si nos fijamos en las dos L de HELLO se asignan a letras diferentes: I y X.

Por tanto en lugar de solo 26 palabras clave posibles, ahora tenemos 26 n palabras clave posibles, donde n es el número de letras de la palabra clave.

Cifrado de transposición o permutación.

Estos cifrados organizan algorítmicamente las letras de un mensaje. El problema con estos cifrados es que se descifran fácilmente.

GUERRAS MUNDIALES Y CRIPTOGRAFÍA.

PRIMERA GUERRA MUNDIAL.

EL TELEGRAMA DE ZIMMERMAN.

Durante la primera guerra mundial se comenzó a trabajar con armamento nuevo y ciertas tácticas militares. Una de ella fue el envío de un telegrama cifrado, por parte del gobierno Alemán hacia el embajador de Alemania en EEUU, el cuál debía mandarle el mismo telegrama al embajador alemán en México.

En este telegrama se confesaba la pretensión alemana de realizar una guerra submarina y la necesidad de una alianza con México, entre otras cosas.

El telegrama fue interceptado por los servicios de descifrado Room 40 y posteriormente descifrado por dos criptoanalistas.

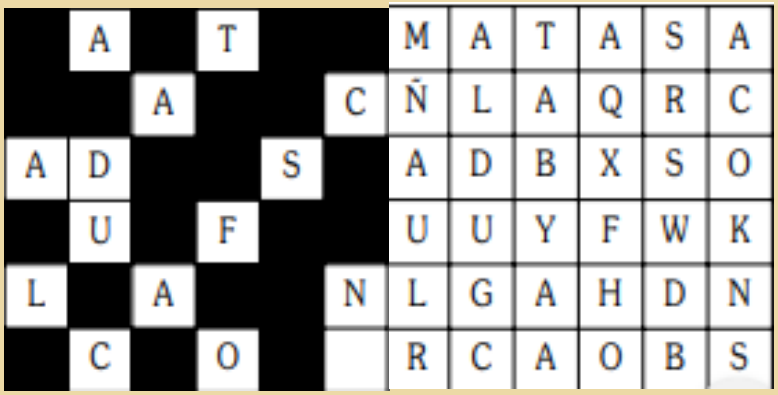
De este modo EEUU le declaró la guerra a Alemania, siendo así como la criptografía cambió el curso de la primera guerra mundial, tal y como ha sucedido en momentos previos de la historia.

LA REJILLA DE CARDANO.

También durante la Primera Guerra mundial se utilizaron otros métodos de cifrado y descifrado, aunque la mayoría eran versiones de otros sistema previamente establecido. Por ejemplo la rejilla de Cardano un sistema inventado en el siglo XVI que consistía en un método matemático para ocultar mensajes secretos. Estos se ocultaban mediante la colocación de un trozo de cartón con huecos sobre un papel y las letras del mensaje se iban escribiendo en esos huecos de izquierda a derecha y de arriba abajo.

En el caso en el que hubiera más letras en el mensaje que huecos e la rejilla, habría que colocar la rejilla debajo y seguir escribiendo. Una vez completado el mensaje se retiraba el cartón y se completaban los espacios restantes con otras letras al azar.

De este modo para revelar el mensaje oculto, el receptor debería colocar la rejilla encima de él mensaje. Al hacerlo, las letras que se querrían descifrar serían descubiertas en los huecos. PJ: “Atacad su flanco”.



Cifrado ADFGz.

Otro de los sistemas utilizados durante la primera Guerra Mundial fue el Cifrado ADFGX. Este sistema era más seguro que el propuesto por las rejillas de Cardano y sus mejoras sucesivas.

Consistía en una modificación del coronel Fritz Nebel del cifrado Polibio. Consistía en que se debía convertir las letras del mensaje en un par de otras letras según una tabla encabezada a izquierda y encima, por ADFGX y que contenía en su interior una mezcla aleatoria de otros caracteres.

Por ejemplo si queremos escribir la frase “nos atacan” deberíamos escribir las letras XA FA XF FX FG FX XX FX XA y según esta tabla descifrar las opciones.

	A	D	F	G	X
A	v	g	z	p	l
D	b	k	r	f	u
F	o	h	e	t	a
G	d	w	m	x	q
X	n	y	s	i/j	c

Para poder complicar el cifrado, este, se mezclaba con una palabra clave cualquiera que debían conocer tanto el emisor como el receptor del mensaje pj “Reich”. De este modo la tabla queda encabezada por la clave y seguida de las letras del mensaje cifrado.

R	E	I	C	H
X	A	F	A	X
F	F	X	F	G
F	X	X	X	F
X	X	A		

Como último paso se reordenaban las columnas de la table de manera que quedase en orden alfabético

C	E	H	I	R
A	A	X	F	X
F	F	G	X	F
X	X	F	X	F
	X		A	X

De este modo se obtuvo un método mucho más seguro que los que se habían utilizado en otros momentos. A pesar de ello fue descifrado durante la guerra.

SEGUNDA GUERRA MUNDIAL.

En la Segunda Guerra Mundial también hubo diversos intentos de encriptar mensajes, de este modo se pretendía transferir información de forma que el enemigo no pudiera entenderla. Algunos de ellos son los siguientes.

La máquina enigma

Uno de los ejemplos más claros de utilización de métodos criptográficos, fue la máquina enigma, incluso ha sido llevada a la gran pantalla.

Esta máquina consta de tres elementos básicos:

El teclado para introducir el mensaje original.

El sistema electromecánico de cifrado.

Panel en el que se iluminan las letras cifradas correspondientes a cada letra introducida.

De este modo el teclado se conectaba mediante cables eléctricos al rotor, que reenviaba la señal eléctrica hasta el panel luminoso mediante los cables. De este modo al pulsar una letra en el teclado se transmitía una corriente que llegaba al rotor, seguía el circuito de cables dentro de él y se dirigía hace el panel donde se iluminaba la letra correspondiente.

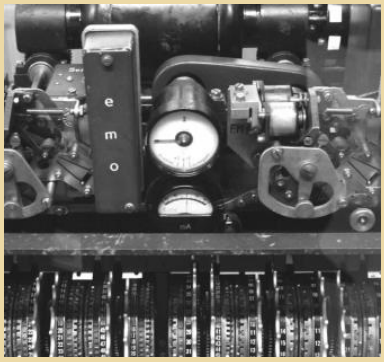
Además cada vez que se pulsaba una nueva letra en el teclado, el rotor giraba, y se modificada el circuito eléctrico, de este modo el cifrado de una misma letra iba variando.

El rotor volvía a su punto inicial cuando terminaba el alfabeto es decir cuando se completaba las 27 veces.

A lo largo del tiempo modificaron la máquina incluyéndole más rotores y permitiendo así multiplicar exponencialmente las posibilidades de cifrado, es decir ya no eran 27 veces ya era 27 elevado a n.

La máquina Lorenz.

Otra de las máquinas que se utilizaron para cifrar conversaciones fue la máquina Lorenz, su sistema de cifrado consistía en la combinación de dos métodos escritos por Vernam y Mauborgne.



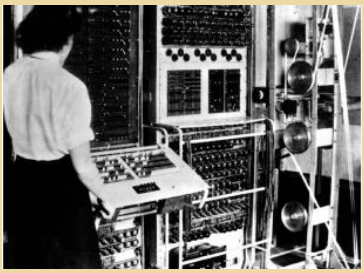
Las aportaciones de ambos dieron lugar a un sistema criptográfico que matemáticamente es muy complejo de vulnerar.

Consiste en transformar los caracteres del mensaje a un sistema binario, combinarlos con otros caracteres viarios aleatorios y obtener de dicha mezcla el mensaje cifrado mediante los caracteres binarios resultantes.

Estos eran transmitidos mediante un teletipo en cuya tinta se marcaban los 0 y 1, correspondiente a no perforado y perforado.

La libreta que utilizaba era pseudoaleatoria, además dicha máquina tenía un estructura similar a una máquina enigma. Estaba conformada por un teclado y un sistema electromecánico de cifrado compuesto por doce rotores.

Para descifrar estas opciones se construyó el colossus, el considerado el primer ordenador de la historia. De este modo se mecanizaba la labor de descifrado procesando dos cintas de teletipo, una con el mensaje cifrado y otra de patrones pseudoaleatorios.



Posteriormente se mejoró la máquina llegando por tanto a descifrar el desembarco de Normandía manteniendo a los ingleses al tanto y siendo un factor importante para la victoria de los aliados en 1945.

CIFRADO EN BLOCKCHAIN

Si tuviéramos que señalar un elemento diferenciador y novedoso de las criptomonedas no podríamos elegir otro que no fuese la criptografía.

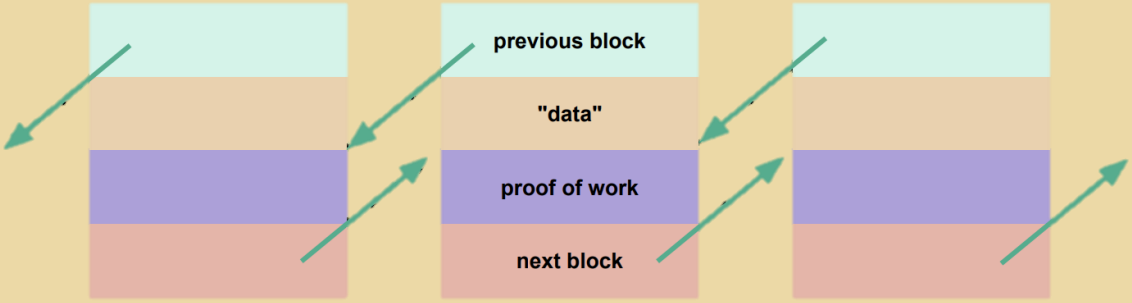
Los usuarios de las criptomonedas utilizan un sistema denominado “full node”, es decir, un registro donde se guardan las transacciones que se han realizado con la moneda utilizada, de este modo se pretende evitar cualquier tipo de fraude.

Por ello la moneda virtual está desarrollada en un marco de sistemas criptográficos que se establecen como base para autentificar la propiedad de la moneda.

Los diferentes métodos criptográficos, que utilizan las criptomonedas, generalmente están basados en una “arquitectura distribuida” (peer to peer). Esta arquitectura permite una comunicación y un tráfico de información entre dos individuos.

El uso más familiar de blockchain es para criptomonedas, como por ejemplo Bitcoin.

La cadena de bloques (blockchain) es esencialmente una lista enlazada. Es decir, en lugar de almacenar 3 valores (puntero anterior, puntero siguiente y datos), estos bloques almacenarán 4 valores.



Los "datos" en este caso es una lista de transacciones, cada transacción tiene una firma digital.

Para Bitcoin, las transacciones representan el intercambio de dinero. Sin embargo, los datos no tienen por qué ser una lista de transacciones. Podría ser una firma digital de un contrato entre dos personas, entre muchas otras posibilidades.

Por ello encontramos en esta modalidad uno de los mayores usos de la criptografía.

¿CÓMO CIFRAR Y DESCIFRAR ARCHIVOS?

La criptografía es un proceso de contrarios, es decir, hablamos de encriptación y desencriptación casi paralelamente ya que la una no tiene sentido sin la otra. Esto se debe a que cuando ciframos una información, para poder leerla posteriormente, necesitamos deshacer el proceso, es decir devolverlos a su formato de origen en el que la información es legible.

Este proceso de contrarios necesita una información adicional, es decir una información que permita leer y ocultar y que sea conocida a nivel mundial. Es decir, necesitamos una clave.

A) Criptografía simétrica o de clave privada/secreta.

Este método es uno de los más utilizados en el intercambio de información. En dicho procedimiento contamos con una clave que es conocida por emisor y receptor del mensaje. Por lo tanto, A envía un mensaje a B cifrado con una clave (conocida por B) y al llegarle a este el mensaje los desbloquea introduciendo la clave.

Desventajas

Uno de los principales inconvenientes de este tipo de criptografía es la circulación de las claves, ya que se tienen que utilizar mediante canales secundarios "seguros" de comunicación. De este modo ambas partes tendrían la clave.

Por su parte, otro de los inconvenientes que podemos determinar es la gestión de las claves, ya que cada usuario debe conocer las claves del resto

B) Criptografía asimétrica o de clave pública.

Este sistema utiliza dos tipos de claves una privada y la otra pública. La clave privada es personal y únicamente conocida por la persona que la adquiere mientras que la pública puede ser conocida por cualquier usuario.

De modo que para descifrar un mensaje de esta tipología primero se debe conocer la clave pública del usuario que va a recibir el mensaje y con la clave privada se desbloquearía el cifrado.

Desventajas

Este tipo de criptografía es poco eficiente, ya que se toman bastante tiempo en aplicar las claves a los documentos cifrados, esto se debe a la longitud de las claves ya que de este modo se aseguraría la independencia con respecto a otras claves.

Las claves que conforman esta criptografía deben estar continuamente actualizadas ya que si se usan de forma repetida puede provocar un riesgo ya que algunos ataques criptográficos se basan en analizar los paquetes cifrados.

Por otro lado tenemos que proteger la clave privada. Las claves privadas se guardan todas juntas en un fichero llamado keyring (llavero) el cual está protegido mediante cifrado simétrico.

Por último, como desventaja, tenemos que señalar que hay que transportar la clave privada. Esto provoca un grave riesgo si se pierden.

C) Hash.

Funciones unidireccionales, basadas en algoritmos que permiten convertir la entrada en una salida alfanumérica resumen de toda la información.

Estos algoritmos son operaciones matemáticas que se realizan sobre datos de cualquier longitud o tamaño, y cuya salida es siempre del mismo tamaño (con independencia de la dimensión del documento original). Se generan códigos hash muy diferentes para datos similares.

Ejemplos de funciones hash más comunes:

- MD5: función de 128 bits.
- SHA-1: función de 160 bits. La función de comprensión es más compleja que MD5, y más robusta y segura.
- SHA-2: función de 224, 256, 384 o 512 bits. Se diferencia con SHA-1 en el diseño y estos rangos de salida. Es más segura, pero a su vez el procesamiento es más lento.

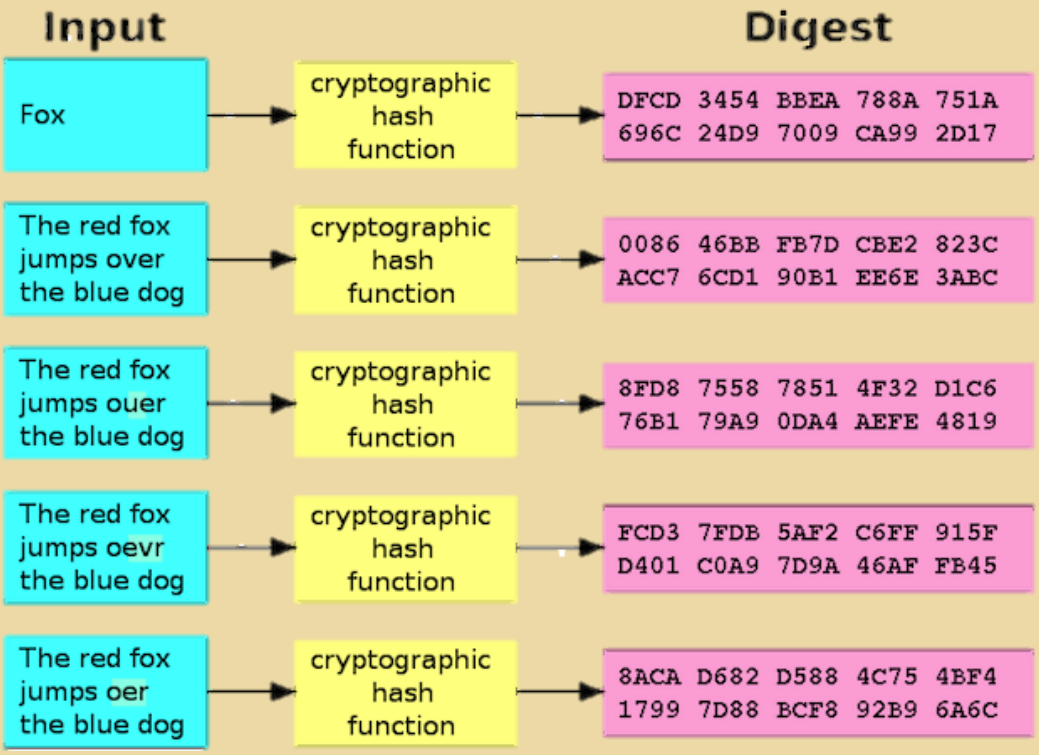


Imagen tomada de: kaspersky.com/blog

De este modo estamos ante un método criptográfico de un archivo o documento que certifica su originalidad. Estas claves nos la dan las diferentes técnicas criptográficas

LIMITACIONES DE LA CRIPTOGRAFÍA

Los algoritmos criptográficos tienden a degradarse con el tiempo. A medida que transcurre el tiempo, los algoritmos de encriptación se hacen más fáciles de descifrar debido al avance de los equipos de desencriptación.

Todos los algoritmos criptográficos son vulnerables a los ataques de fuerza bruta ya que es más fácil de aplicar con el paso del tiempo. La fuerza bruta consiste en probar, sistemáticamente, con cada posible clave de encriptación, así se pretende crear colisiones para funciones hash, factorizando grandes números, etc.

La fuerza bruta es más fácil de aplicar en la medida que pasa el tiempo. Además de esta avanzan las matemáticas fundamentales que proveen nuevos métodos y técnicas de criptoanálisis.

FIRMAS DIGITALES.

Las firmas digitales se pueden considerar como lo contrario del cifrado. Al usar una firma digital, se puede verificar la autenticidad del remitente de un documento.

Suelen estar conformadas por 256 bits, lo que significa que son posibles 2^{256} firmas digitales distintas.

El flujo general de verificación de una firma digital actúa de la siguiente manera:

La parte de firma del proceso incluye lo siguiente:

- Desde la parte superior izquierda, en los datos, tenemos un archivo con una firma.
- Pasar este archivo a través de una función hash (generalmente conocida) y obtenemos un hash.
- Encriptar el hash con una clave privada.
- Enviar la firma encriptada junto con el archivo original.

La parte de verificación del proceso incluye lo siguiente:

- Los datos firmados digitalmente incluyen el archivo original y la firma cifrada.
- Nos fijamos en la firma cifrada y utilizamos la clave pública del firmante. Tras realizar el descifrado, obtenemos un hash.
- A continuación ejecutamos el archivo a través de la misma función hash que el firmante usó para obtener otro hash.
- Si estos dos hashes son iguales, es muy probable que la firma sea válida.

ESTENOGRAFÍA.

La estenografía consiste en abordar la inaccesibilidad de la información a personas no autorizadas, es decir oculta información no la recodifica como hace el cifrado. Por ejemplo oculta un texto en una imagen o un video.

Para saber más sobre este tema Íñigo Ladrón escribió un artículo sobre ello. https://derechodelared.com/que-es-la-esteganografia/

Uno de los programas que se pueden utilizar para realizar ocultamiento de información es Openstego.

CONCLUSIONES.

Por tanto, no podemos ver la criptografía como algo lejano o perteneciente a la ciencia ficción sino como un recurso que ha pertenecido a la historia y que lo seguirá haciendo en el futuro.

Una de las primeras conclusiones a las que podemos llegar es la necesidad de transmitir y ocultar información, como hemos visto en diversos momentos de la historia se han dado avances sistemáticos para mejorar estas técnicas y por tanto poder ponerse en cabeza en una batalla, un proyecto o un liderato.

El desarrollo de diversos tipos de elementos criptográficos nos ha permitido vislumbrar grandes hechos históricos, pero también reforzar nuestro intelecto intentando mejorar y superar aquellas opciones que ya existían. De este modo se pudo llegar, únicamente mediante la idea de ocultar información, al diseño del primer prototipo de ordenador.

Otra de las preocupaciones de la sociedad ha sido poder ocultar información de forma rápida y sencilla, es decir, maximizando la eficacia. Por ello se han desarrollado técnicas como el cifrado simétrico o asimétrico y el hash.

A pesar de que estos tengas sus ventajas e inconvenientes particulares, los solemos utilizar a diario de forma consciente o inconsciente. Permitiendo así la posibilidad de sentirnos seguros ante el tráfico de información y el flujo de datos.

Sin embargo, no podemos dejar de lado las limitaciones de la criptografía. Este sistema cuenta con una rápida obsolescencia, así como una escasa capacidad de protección a diversos sistemas de ataque para averiguar la información.

Uno de estos ataques es la fuerza bruta, que a pesar de ser un ataque burdo si es constante y eficaz puede comprometer la integridad de los datos cifrados.

Por lo que no solo no podemos dejar de utilizar la criptografía y los elementos que te permiten llevarla a cabo, sino que también debemos actualizarla y mejorarla sistemáticamente. A pesar de que esto convierta a la criptografía en una tarea en la que invertir mucho trabajo y capacidad de renovación.

BIBLIOGRAFÍA.

- Universidad de Granada, material de seguridad en Redes. Profesor: Juan Antonio Gómez Hernández.
- Trabajo fin de Grado, Marta Violat Ávila.
- Estenografía Íñigo Ladrón. https://derechodelared.com/que-es-la-esteganografia/
- Análisis del anonimato aplicado a las criptomonedas.
- Curso CS50, Harvard.
- Ángel Gutiérrez Criptografía y criptoaálisis en las dos guerras mundiales https://www.acta.es/medios/articulos/comunicacion_e_informacion/052063.pdf
- Criptografía como elemento de seguridad informática http://scielo.sld.cu/scielo.php?pid=S102494352003000600012&script=sci_arttext&tlng=pt#cargo