"Como disciplina y como habilidad, la criptografía es extremadamente antigua, prácticamente surge con la escritura. De hecho, toda escritura es un código utilizado para comunicarse y para leer un texto escrito es necesario conocer ese código. Cuando el conocimiento de la escritura se empezó a extender, surgió, por motivos militares o políticos, el interés en poder codificar —o encriptar— aún más el mensaje, desarrollándose de este modo la criptografía y el criptoanálisis para intentar romper la seguridad de los códigos criptográficos. Si nos damos cuenta, la criptografía, como práctica, no es algo ajeno a nuestra cotidianidad, lo que sucede es que su uso más particular está relacionado profundamente con el poder, y el poder no es para todos: de ahí procede su opacidad."

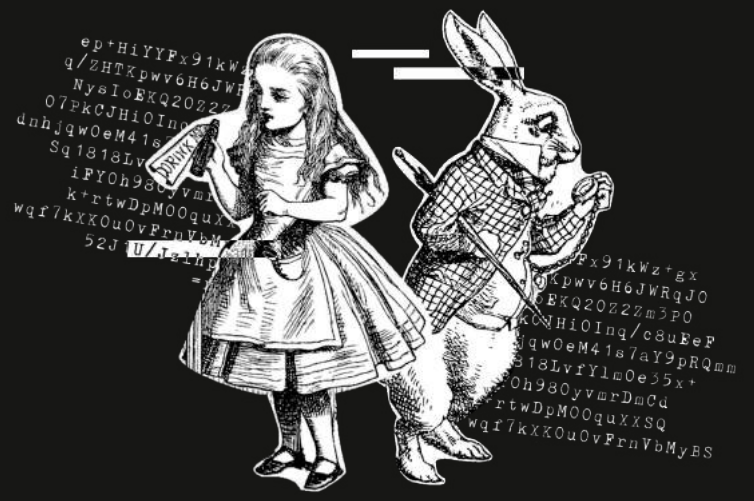
La copia comparte cultura.

colectivo disonancia

>_

Introducción a la criptografía digital

Colectivo Disonancia



¿Por qué Alicia en el País de las Maravillas?

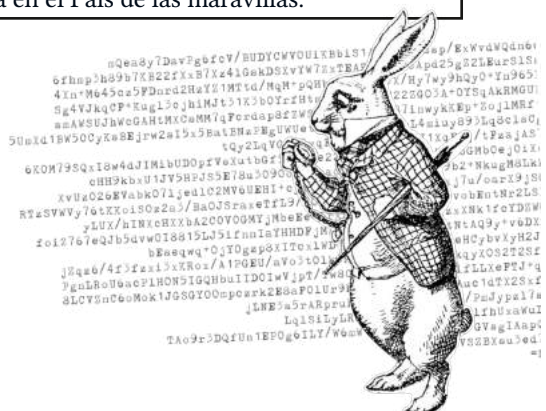
En 1978, Ron Rivest, uno de los creadores del algoritmo criptográfico RSA, publicó un artículo explicando el funcionamiento del cifrado de llaves. Consideró que usar las expresiones "A" y "B" como usuarios hipotéticos de la explicación dificultaba aún más enseñar este cifrado.
Por eso decidió darle nombres a esos usuarios para que fuera más simple entender el procedimiento e identificar estos usuarios:
así nacieron "Alice" y "Bob".

A method for obtaining digital signatures and public-key cryptosystems
https://dl.acm.org/doi/10.1145/359340.359342

Como en la cultura popular se relaciona a "Alicia" con la obra de Lewis Carroll, se hizo costumbre en los ambientes criptográficos usar el imaginario de "Alicia en el país de las maravillas" como representación gráfica de la criptografía.

"—Pero es que a mí no me gusta tratar a gente loca—protestó Alicia.
—Oh, eso no lo puedes evitar, aquí todos estamos locos. Yo estoy loco.
Tú estás loca.
—¿Cómo sabes que yo estoy loca?—preguntó Alicia.
—Tienes que estarlo, o no habrías venido aquí."

Lewis Carroll, Alicia en el País de las maravillas.



Introducción a la criptografía digital

Colectivo Disonancia

"Introducción a la Criptografía", Colectivo Disonancia.

Edición y diagramación por Colectivo Disonancia, 2022

colectivodisonancia.net
@cdisonancia

La copia comparte cultura.

Puedes descargar el Fanzine aquí:

https://colectivodisonancia.net/zines

https://cloud.disroot.org/s/ezoecDQFdBdwCzy

https://gitlab.com/cdisonancia/fanzine

Descarga este fanzine en:

- https://colectivodisonancia.net/zines
- https://cloud.disroot.org/s/ezoecDQFdBdwCzy
- https://gitlab.com/cdisonancia/zines

O accediendo al enlace en este QR

Implementación en GnuPG

GnuPG o GNU Privacy Guard es un programa perteneciente al proyecto GNU[6] y permite utilizar ambos tipos de cifrado. Es Software Libre[7] y además gratuito, disponible para varios sistemas operativos. Puedes revisar nuestros manuales para poder empezar a usarlos.

GnuPG desde terminal[8]
GnuPG desde Kleopatra[9] *(prográma gráfico)*

Referencias

Méndez Veiga, Iyán. Microcurso para físicos y matemáticos de criptografía práctica (2016).

Fernández, Santiago. "La Criptografía Clásica". Sigma 24. Fernández, Santiago. "La Criptografía Clásica". Sigma 24.

GNU. Guía de "Gnu Privacy Guard'' (1999) https://gnupg.org/gph/es/manual.html

Riseup. Managing OpenPGP Keys. https://riseup.net/es/security/message-security/openpgp/gpg-keys

Riseup. GPG buenas prácticas. https://riseup.net/es/security/message-security/openpgp/gpg-best- practices

[6] https://www.gnu.org/gnu/manifesto.es.html

[7] https://www.gnu.org/philosophy/free-sw.es.html

[8] https://colectivodisonancia.net/herramientas/cifrado-gpg-terminal/

[9] https://colectivodisonancia.net/herramientas/cifrado-gpg-kleopatra/

Índice

criptografía, podemos recuperar la autonomía de nuestra información y la de nuestra comunidad.

***

Firma Digital

Uno de los inconvenientes del cifrado asimétrico, además de su dependencia completa a nuestra habilidad para ocultar la llave privada y su contraseña, es la posibilidad de que alguien intercepte el mensaje cifrado original y lo reemplace por otro distinto, pero que también esté cifrado con la misma llave pública. De este modo, si uno espera un mensaje cifrado para abrir con nuestra llave, no tenemos garantía de que realmente corresponde al mensaje original si es que más de una persona posee la llave pública. Por este motivo, una de las ventajas del Algoritmo RSA es que permite, además, un procedimiento llamado firma digital, que sirve para verificar quién envía el mensaje.

El procedimiento es similar al cifrado asimétrico y, de hecho, se emplean las mismas llaves. Para esto, supongamos que queremos enviar un archivo, cifrado o no, a alguien que ya posee nuestra llave pública. En este caso, necesitamos que el destinatario corrobore que somos nosotros quiénes enviamos el archivo. Con este propósito, utilizamos nuestra llave privada para dejar una marca o firma digital, la cual no puede ser alterada porque emplea el mecanismo de cifrado contenido en nuestra llave privada. Una vez enviado el archivo firmado, el programa que usualmente se use para descifrar los mensajes identificará nuestra huella digital si es que posee la llave pública. Es decir, en términos sencillos, la firma digital es una marca irreemplazable dejada por nuestra llave privada y sólo podrá ser corroborada por quienes tengan nuestra correspondiente llave pública.

Extendiendo esta analogía, si las personas con las cuales nos comunicamos también tienen este par de llaves y nos compartimos mutuamente las llaves para cerrar, podremos establecer un intercambio de información y contenido muy seguro, sin importar que tan inseguro es el medio empleado.

Este tipo de cifrado es conocido como cifrado de llaves o cifrado asimétrico, en donde se genera un par de llaves, o archivos digitales llamados llaves, que cumplen la función descrita: uno para cifrar y otro para descifrar. En criptografía digital, la llave para cerrar, que es la que se comparte con quienes queremos comunicarnos, se llama «llave pública» porque no necesita resguardo y debe estar al alcance de quienes quieran establecer un contacto seguro con nosotros. En cambio, la llave para abrir o descifrar es llamada «llave privada» y a ella solo debemos tener acceso nosotros, además de asegurarnos de utilizarla en un dispositivo seguro junto a una contraseña fuerte.

Esta forma ingeniosa de cifrado tiene la ventaja de poder establecer un canal seguro y cifrado dentro de cualquier medio inseguro, como internet. Este procedimiento es posible gracias al uso de algoritmos que utilizan una factorización de números primos muy grandes que es, en la práctica, imposible de calcular para los computadores actuales, a menos que posean la llave privada y su contraseña. El algoritmo más utilizado en este sistema es RSA, que ya mencionamos por su consideración como arma para la jurisdicción norteamericana en la década de los 90. RSA, desarrollado a fines de la década del 70, permite cifrar información pero también firmar mensajes, posibilitando autentificar la validez de los mensajes en un intercambio de información cifrada. Si bien muchos de los programas, aplicaciones y sitios web que usamos a diarios se comunican entre sí por un sistema automático de cifrado de llaves, la ventaja de usar programas como GnuPG es poder tener control completo de las llaves empleadas, sin depender de servicios de terceros y centralizados. Usando de este modo la

¿Qué es la criptografía?

La criptografía evoca un lenguaje oculto, opaco para la mayoría, pero transparente y nítido para unos pocos. Del griego *«kriptos»*, que significa oculto o secreto, y grafa, escritura, es la disciplina que se dedica al estudio de los métodos con los cuales se pueden establecer códigos secretos de comunicación. Sin embargo, también se refiere a la habilidad o técnica de escribir en clave o de modo enigmático. Es decir, escribir o comunicarse en clave para que el mensaje no sea interpretado fácilmente por cualquiera.

Como disciplina y como habilidad, la criptografía es extremadamente antigua, prácticamente surge con la escritura. De hecho, toda escritura es un código utilizado para comunicarse y para leer un texto escrito es necesario conocer ese código. Cuando el conocimiento de la escritura se empezó a extender, surgió, por motivos militares o políticos, el interés en poder codificar —o encriptar— aún más el mensaje, desarrollándose de este modo la criptografía y el criptoanálisis para intentar romper la seguridad de los códigos criptográficos. Si nos damos cuenta, la criptografía, como práctica, no es algo ajeno a nuestra cotidianidad, lo que sucede es que su uso más particular está *relacionado profundamente con el poder*, y el poder no es para todos: de ahí

procede su opacidad.

Actualmente, en español, las expresiones «encriptar» o «**cifrar**» se usan indistintamente, ya que en la práctica significan lo mismo. Sin embargo, hay que señalar que en el ambiente técnico se tiende a preferir la expresión «cifrar» para su aplicación en tecnologías digitales. Aun así, toda técnica de cifrado o de encriptación forma parte de la criptografía. Un punto importante de mencionar es que la criptografía no significa ocultar el mensaje, sino que más bien se trata de que el contenido de un mensaje perfectamente visible solo sea legible para la persona a la cual nos dirigimos. O sea, su objetivo final no es ocultar la comunicación, sino que su foco está en la protección del contenido o mensaje de lo comunicado, evitando que otros agentes intermedios que puedan estar vigilando descubran el mensaje que estamos enviando a nuestro destinatario. Ahora bien, si nos interesa la técnica para ocultar la existencia misma del mensaje, es la esteganografía[1] lo que buscamos, que podemos revisar en otra ocasión.

***

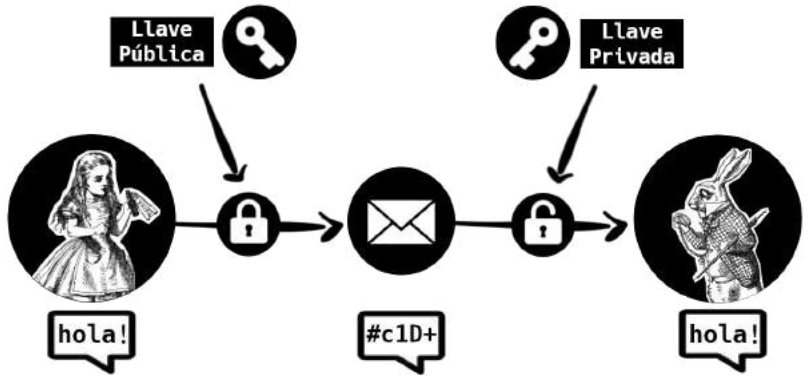
Una breve consideración histórica

Revisar la historia de la criptografía no solo es necesario porque nos da el contexto de su existencia, sino que también es sumamente interesante: su existencia va de la mano de importantes cambios sociales, en donde el avance técnico y la constitución del poder le dan forma. Históricamente, se suele distinguir dos momentos: la criptografía clásica y la criptografía moderna. La primera refiere a la criptografía anterior al uso informático del cifrado, mientras que la segunda a su desarrollo

[1] https://www.genbeta.com/truco/esteganografia-oculta-mensajes-dentro-de-un-archivo

de un canal inseguro ya existente. Ahora, antes de entender en qué radica su seguridad, es conveniente conocer cómo funciona.

Imaginemos que tenemos un cofre vacío, en el cual podemos guardar cualquier cosa de modo seguro una vez que es cerrado con su llave, ya que sólo quien posea esta llave podrá acceder a él, abriendo o cerrando el cofre. Ahora, imaginemos otra cosa, que esa llave se puede partir en dos, siendo una la mitad exacta de la otra, pero no sólo eso: ahora una mitad sólo servirá para cerrar el cofre y la otra mitad sólo para abrir el cofre. De esta manera, podemos hacer copias de la llave para cerrar y entregarla a quienes quieran enviarnos información o cualquier cosa dentro del cofre. Así, incluso si el cofre es interceptado una vez que está cerrado, sólo podremos abrirlo nosotros, que somos los únicos que poseemos la llave para abrir. Si lo consideramos, ni siquiera es necesario establecer un canal seguro o secreto para poder compartir nuestra llave para cerrar, ya que como solo sirve para eso, no permite acceder de ninguna manera al contenido una vez cerrado.



Esquema de Cifrado Asimétrico

bloque que consiste en cifrar el texto plano a partir de un bloque de bits de una longitud determinada (128 bits) en combinación con una clave de cifrado entregada por la estructura del algoritmo, que en el caso de AES puede ser de 128, 192 ó 256 bits, de modo que a mayor longitud de esta clave, mayor es la seguridad del procedimiento.

Si bien existen varios algoritmos seguros —considerando solo los que permite GPG— AES256, Twofish y Camellia256 son los más recomendables, por contar con llaves de 256 bits y catorce rondas o más en su procedimiento. En programas como Veracrypt[4], de necesitarse un algoritmo en extremo robusto, se suele sugerir combinar varios algoritmo incluyendo *Serpent*, que obtuvo el segundo lugar en el Advanced Encryption Standard, que le dio el primer lugar a Rijndael, hoy conocido como AES.

Cifrado Asimétrico

Con el cifrado simétrico podemos almacenar sin problemas información sensible en nuestros dispositivos cuando utilizamos contraseñas seguras, pero en el intercambio de información por medio de internet —un medio inseguro y lleno de amenazas—, el cifrado simétrico no es suficiente. Resulta extremadamente riesgoso compartir una contraseña en texto plano, sin cifrar previamente, ya que el mensaje puede ser interceptado y manipulado. De hecho esa es la realidad habitual de internet con programas de vigilancia como Tempora[5].

La criptografía asimétrica es la solución a este problema, ya que permite establecer un medio seguro de comunicación dentro

[4] https://www.veracrypt.fr/en/Home.html

5https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications- nsa/

posterior. Esta distinción de ninguna manera significa una superioridad del cifrado informático por sobre la criptografía clásica. Por ejemplo, existen cifrados clásicos en teoría inquebrantables como el OTP (*One-time Pad)*, así como también hay sistemas modernos como la función hash MD5 que ha sido quebrada y es completamente vulnerable.

Lo que sí podemos distinguir, además de la propia técnica informática, es el alcance social que tiene. Si bien la criptografía clásica podía ser usada por cualquiera, no tenía un uso cotidiano porque se empleaba para cifrar solo los mensajes que requerían mantener un contenido secreto. Es decir, la forma que tomó la criptografía clásica estaba directamente relacionada con las necesidades estratégicas de ese momento de una parte privilegiada de la sociedad. En la actualidad, en cambio, *con la criptografía moderna, el cifrado posee un uso diario y transversal*, aunque no nos demos cuenta o no sepamos nada de ella. Cuando navegamos por internet, cuando pagamos con una tarjeta bancaria o cuando enviamos un mensaje con nuestro teléfono, están en funcionamiento una serie de procedimientos de cifrado automático. Toda la tecnología que usamos interactúa entre sí intercambiando información, corroborando direcciones, cifrando y descifrando datos, sin que nosotros podamos decidir realmente cuánta de esa información controlamos. Evidentemente, estos mecanismos técnicos con los que se ejecutan el cifrado y el descifrado automático de nuestra información no son desinteresados.

La criptografía ha tomado nuevas formas, masivas y sofisticadas, y al igual que su período clásico, se adapta a la estrategia del poder, pero en contextos distintos. Tal vez para algunos esto sea en apariencia un salto lógico, un delirio conspirativo, no obstante, ningún uso técnico es inocente: sencillamente, si no somos nosotros quienes controlan el procedimiento del cifrado de nuestra información, son otros los

que tienen ese poder. En la actualidad, usar cifrado en nuestras comunidades y espacios de organización es la defensa más inmediata y efectiva que podemos emplear para combatir la vigilancia masiva[2], de Estados y corporaciones, de la cual todos somos objetivo.

De hecho, históricamente, la criptografía siempre ha tratado sobre el poder. Una de las técnicas más conocida de la criptografía clásica es el «cifrado Cesar», llamado así por ser el que empleaba el político y militar romano Julio Cesar para comunicarse con sus generales. A pesar de que se trata de un procedimiento simple, desplazar el orden del alfabeto para que una letra signifique otra (la A por la D, la B por E, etc), el interés era estratégico: dirigir un ejército que abarcaba un gran espacio territorial sin entregar los mensajes comunicados a los enemigos en caso de ser interceptado el mensajero. Conocida también fue la famosa máquina Enigma[3], utilizada por el régimen Nazi en la segunda guerra mundial para cifrar los mensajes que mantenía a su ejército comunicado. En este sentido, el lograr romper la técnica de cifrado de Enigma fue un avance significativo en la derrota del fascismo en Europa.

Ahora bien, esto se vuelve más relevante aún en el período contemporáneo. Como la utilidad del cifrado es estratégica, por motivos políticos o militares, ya durante la criptografía moderna la masificación del cifrado fue vista como una amenaza. El caso ejemplar es el protocolo «PGP» y el algoritmo «RSA», —cuya explicación se encuentra más adelante—. El cifrado PGP fue considerado un arma en EEUU en la década de los noventa luego de ser publicado por su creador, Phil Zimmermann, quien fue investigado formalmente por "exportar municiones sin licencia", lo que se extendía a toda forma de criptografía. Sí, la criptografía fue considerada un arma, por un Estado y su uso fue ilegal sin

[2] https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

[3] https://www.eldiario.es/turing/criptografia/alan-turing-enigma-codigo_1_5038272.html

Por ejemplo, si uso un programa de cifrado y utilizo la contraseña *Est0esUn4C0ntra5eñ4!* para cifrar el mensaje; la persona a la que le envíe el mensaje o archivo deberá conocer previamente la misma contraseña. Es similar a si quisiéramos compartir una cuenta de correo electrónico con otra persona; para que ambos accedan, deben conocer la misma clave. En este sentido, el cifrado simétrico se usa preferentemente para proteger archivos o dispositivos propios que no necesiten ser intercambiados con otra persona, haciendo del resguardo de la contraseña una precaución exclusivamente personal.

Debido a esto, la seguridad de la contraseña es fundamental. Mientras más larga y más combinación de caracteres tenga, mejor. Por muy seguro que sea el programa que se use para cifrar, si se emplea una contraseña de cuatro dígitos, un ataque de fuerza bruta —que busca probar todas las contraseñas posibles— podrá acceder a la información en un par de horas. Este consejo, por supuesto, es válido para cualquier cuenta digital que requiera contraseña. Es recomendable un mínimo de 20 caracteres con combinación de minúsculas, mayúsculas, números y signos:

Ej3mpl0de#Un4contr453ña*MUY-S3gur4%

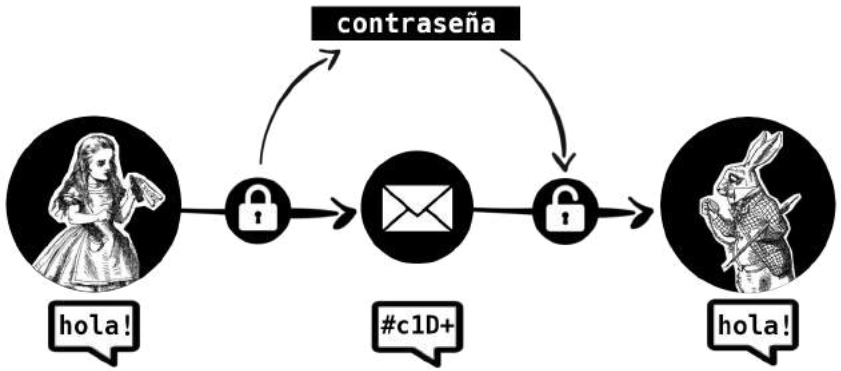
Sin embargo, como ya se mencionó, es habitual el uso del cifrado simétrico para almacenar información, de manera segura y a la que solo nosotros accederemos, como guardar algún documento en nuestro computador o respaldar con cifrado nuestra información en una memoria externa, evitando que alguien más pueda utilizarla.

El algoritmo de cifrado simétrico más usado hoy es AES (Advanced Encryption Standard), estandarizado en el año 2001, es el que utilizan la mayoría de los gobiernos, agencias de seguridad y entidades bancarias para almacenar la información sensible. Utiliza un procedimiento de criptográfico denominado cifrado de

funciona cada programa criptográfico. En este nivel, no existe un tipo mejor que otro, sino que la importancia de la diferencia consiste en saber elegir cuál necesitamos o en qué medida se pueden combinar. Por esto, debemos tener claro cuál es nuestra necesidad, nuestro objetivo y el lugar que tiene el cifrado en nuestro sistema de comunicación. Cada uno de estos tipos de cifrado poseen distintos algoritmos, los que sí determinan qué tan seguro es el programa a utilizar Los dos tipos generales de criptografía digital son el cifrado simétrico y el asimétrico.

Cifrado Simétrico

El cifrado simétrico es aquel en el cual se usa la misma clave para encriptar y para desencriptar la información. Así, quienes buscan mantener una comunicación segura en un medio inseguro, como es internet, deben conocer la clave previamente por algún otro medio más seguro.



Esquema de Cifrado Simétrico

autorización. En ese contexto, y ante esta persecución exagerada, el movimiento cypherpunk o movimiento de criptografía radical, a modo de protesta, empezó a intercambiar en sus correos electrónicos el algoritmo RSA de cifrado de llaves, haciendo alusión, paródicamente, a que traficaban armas.

Algoritmo RSA escrito en Perl:

```
#!/bin/perl -sp0777i<X+d*lMLa^*lN%0]dsXx++lMlN/dsM0<j]dsj $/
=unpack('H*',$_);$_=`echo 16dio\U$k"SK$/SM$n\EsN0p[lN*1
lK[d2%Sa2/d0$^Ixp"|dc`;s/\W//g;$_=pack('H*',/((..)*)$/)
```

Desde la década del 2000 las regulaciones sobre criptografía en EEUU se han relajado, aunque existen países en donde cifrar información, independiente de cuál sea el contenido, es un delito grave, como en China. Puede que la situación china nos parezca lejana, sin embargo hay otros ejemplos de restricciones o persecuciones más selectivas al cifrado. Existe, por ejemplo, en Reino Unido la ley RIPA, por sus iniciales en inglés, que faculta a los agentes policiales, bajo una orden particular, con la capacidad de obligar a las personas a descifrar sus dispositivos o a entregar las contraseñas. El solo hecho de negarse implica la presunción de culpabilidad.

Actualmente, con la presencia de la vigilancia masiva y el avance jurídico de las políticas de seguridad nacional, los estados y las empresas buscan alternativas para vulnerar las técnicas de cifrado y de navegación anónima, como Tor. Sin embargo, una gran red de organizaciones, colectivos y activistas se mantiene en una constante actividad para enfrentar la vigilancia y promover herramientas para proteger la autonomía y la cooperación en la Red.

***

Algunos conceptos centrales

Puede parecer complicado el uso del cifrado en nuestra cotidianidad, no obstante, tal como aprendimos alguna vez a utilizar un computador o a usar por primera vez un correo electrónico, es posible aprender a cifrar sin tener experiencia previamente. Manejar técnicas de cifrado no sólo implica conocer y usar las herramientas digitales, sino también conocer algunas nociones elementales que orientan el aprendizaje y el uso adecuado de la criptografía. Es a partir de aquí que este documento pretende ser una guía para todos aquellos que quieran aprender lo que hay tras una técnica transversal pero opaca. Algunas nociones elementales a considerar son:

Cifrar: Consiste en convertir un mensaje o información en un código solo descifrable para quien maneje el código o clave para descifrarlo. El uso de la expresión cifrar hoy se ha convertido en sinónimo de criptografía digital.

Descifrar: Reconstruir el mensaje o la información original dentro de un mensaje o archivo cifrado.

Texto plano: Mensaje escrito en lenguaje cotidiano, sin cifrar.

Texto cifrado: Mensaje al que se le aplicó una técnica de cifrado, por lo que es ilegible convencionalmente.

Contraseña: Grupo de caracteres, idealmente una frase, que determina el acceso a un texto o información cifrada. También autoriza el funcionamiento de una clave de cifrado.

Clave: Pieza de información que ejecuta la operación de un

algoritmo criptográfico. Es una secuencia de números o letras que especifica la transformación del texto plano a texto cifrado.

Llave: Archivo digital que permite el cifrado o descifrado de un mensaje o información. Básicamente, es una clave de cifrado, pero en criptografía asimétrica, se suele hablar de par de llaves en vez de claves.

Código: Líneas de programación que construyen el funcionamiento de un programa o algoritmo. La complejidad de los códigos de programación de los sistemas de cifrado es garantía de su seguridad. El Software libre o de código abierto permite conocer el código informático de los programas, permitiendo poner a prueba la seguridad y fiabilidad del software.

Algoritmo: En general, un algoritmo es un conjunto ordenado de tareas y operaciones que permite realizar alguna acción o solucionar un problema. Particularmente en informática, es la forma o lógica de trabajar de un programa informático, por lo que pueden existir muchos programas que realizan una misma tarea, pero su algoritmo puede ser diferente. En criptografía esto es esencial para poder saber qué tipo de seguridad ofrece un programa.

***

Algoritmos y tipos de cifrado

Para hacer uso de estos conceptos y para poder cifrar nuestras comunicaciones, necesitamos, además, distinguir los tipos de cifrado que existen según dos tipos de clasificaciones: el tipo y el algoritmo utilizado.

Los tipos de cifrado son las formas generales de cómo