Capítulo 6

Criptografía

...Ya sabes lo que te dijo el Juez! no toques más los ordenadores!-Al otro extremo de la línea silencio.- Me estás escuchando? Joder, ya ha vuelto a colgarme! exclamó la señora Doran, y colgó a su vez... Recordarle que no tocara ningún ordenador era como hablar con la pared .A Billy siempre lo habían atraído esas maquinitas, y hacía apenas un par de años había escrito su propio virus polimórfico y lo había soltado en la red. El virus recorrió millones de kilómetros de cables, invadió millones de cuentas de correo electrónico y colapsó la red durante tres días. Billy tenía sólo trece años y en su rostro la inocencia perdida de un chico revoltoso...

Desde tiempos inmemoriales se ha buscado la forma de cifrar u "ocultar" mensajes mediante técnicas reversibles, pero a su vez hacían los textos ininteligibles. Cifrar un texto o mensaje supone que de ser interceptado no pueda descifrarse sin la clave correcta.
Los sistemas criptográficos se han extendido como la pólvora por la red; buenos y malos emplean la criptografía para "esconder" sus mensajes. Por su lado los Crackers más hábiles tratan de demostrar que también los sistemas criptográficos más modernos caen ante ellos.
Una buena muestra es el crack del código DES en 56 horas, de modo que la polémica está servida. Por otro lado tenemos que en su día, se trataron sistemas de criptografía o cifrado en señales de televisión, refiérase a "Hackers, piratas tecnológicos", donde se exponían los diferentes sistemas de cifrado reversibles.

Igual que sucede con la televisión de pago, las comunicaciones, los programas y la propia red de internet deben contar con una seguridad que proteja la intimidad de los datos.

Los canales de televisión se pueden proteger mediante modificaciones en la señal compuesta. Estos procesos de encriptación de componentes son reversibles con el fin de obtener la información clara en el punto autorizado para tal fin.
Igual proceso debe seguir el campo de la informática, pero se detiene uno a pensar que aunque la palabra seguridad se maneja en todas partes, poco se parecen ambos métodos, lógicamente por ser de distinta naturaleza. Un canal de televisión está compuesto por ciertas funciones analógicas y unos componentes indicativos de la señal. Todos esos componentes pueden sustituirse por otros elementos o transformarse. A eso se llama proceso de enmascaramiento o encriptación.
En informática, aunque no existen los mismos elementos de una señal de vídeo, también es posible encriptar la información. A ese proceso se le denomina Criptología.
Criptología es el arte de transformar un mensaje claro en otro sin sentido alguno. Este mensaje debe ser reversible en el otro extremo, y mostrarse igual que si no hubiera sucedido nada. Es más fácil encriptar un texto que una señal de vídeo, pero siempre resultará más complicado desencriptar el texto que la señal de vídeo. En una señal de vídeo siempre puedes ver qué sucede, pero lógicamente en un texto no puedes adivinar nada. Además los ficheros aparecerán encriptados y no podrán ser leídos por los comandos estándares.
Pero la Criptología o programas criptográficos no constituyen toda la seguridad que se pretende obtener. A su vez existen diversos complementos que aumentan la seguridad de un terminal informático. Un ordenador es un equipo sofisticado que procesa datos, y como los descodificadores, puede tener palabras de acceso que pueden bloquear el sistema si no se conocen. En los descodificadores eso se llama bloqueo paterno, mientras que en los ordenadores es una clave de acceso para empezar a trabajar con él.
En ambos equipos se debe introducir una clave o contraseña antes de iniciar la sesión.
En los descodificadores suelen ser claves de cuatro dígitos por la reducida seguridad que necesitan. Normalmente las claves son para evitar que alguien ajeno a la familia manipule el descodificador o receptor, pero como en los ordenadores se guardan datos valiosos, la seguridad debe ser mayor.

En estas circunstancias debemos saber que un terminal de ordenador posee dos puertas de acceso al corazón del sistema. Una es a través del teclado, que es la puerta de introducción de datos más usual, y la otra puerta es el MODEM que comunica el ordenador con el mundo exterior gracias a internet.

En el primer caso se debe introducir una contraseña de más de cuatro dígitos si se desea, para poder acceder al sistema operativo. Esta protección vale para que nadie pueda entrar en nuestro ordenador desde el teclado sin nuestra autorización. Este método es ciertamente seguro para nuestra intención.
Pero en la red existen peligrosos Hackers capaces de hacer cosas impensables, por ello la segunda puerta requiere un mayor grado de seguridad. Comúnmente, en base al buen entendimiento entre dos ordenadores, los dos terminales deben poseer un inicio a modo de saludo para que los dos se identifiquen y puedan trabajar conjuntamente. Es algo así como en el teléfono, si no se marca un número definido por el usuario, jamás se podrá conectar con la persona deseada. Con los ordenadores ocurre exactamente lo mismo. Cada ordenador debe tener asignado un nombre de identificación y además debe ser capaz de dialogar con el otro terminal, en los extremos más simples como envío de un saludo, acuse de recepción y otros detalles.
Sin esos detalles un terminal no podría identificar nunca al del otro extremo, ni dejar constancia de ello. De esa manera se controla el tráfico y se evitan nudos indeseables en las comunicaciones. Pero hasta ahora esa puerta no tenía más seguridad que los números de identificación del terminal a la dirección que le corresponde.
Y esos números son fácilmente reconocibles como se reconoce el número de teléfono de cada persona gracias a la guía telefónica. Los firewalls o muros de fuego, son la solución para tapar el agujero en esta segunda puerta. Este programa puede identificar al que solicita el servicio de nuestro ordenador e impedir además que entren datos a nuestro ordenador. Por otra parte estos firewalls pueden reconocer comandos dañinos o peligrosos para nuestro terminal.
Sin embargo, con eso no se termina de cuestionar la seguridad total.
Podemos impedir que un intruso entre en nuestro sistema, pero ¿qué sucede cuando tenemos que enviar algo a otro punto de la red? Inevitablemente nuestro trabajo corre peligro de ser capturado por algún indeseado. El programa PGP de Zinmerman es una muy buena solución a este problema. Nuestro terminal además de velar por la seguridad de las dos puertas al exterior, debe ser capaz de generar archivos ininteligibles para cualquier ordenador remoto que no tenga la autorización correspondiente.

Estos programas criptográficos son capaces de encriptar textos u otra información, gracias al empleo de algoritmos de encriptación altamente seguros. Podemos encontrar varios de los sistemas que se emplean y los vamos a tratar a continuación.

Un poco de historia

Ya en el antiguo Egipto se empleaban sistemas criptográficos, y lo prueban los jeroglíficos no estándar hallados en las paredes de las pirámides y en algunas tumbas.
Datan de 4.000 años atrás y el sistema se basaba en figuras geométricas y dibujos que conformaban un mensaje no descifrable. Ese sistema podía ser realmente complejo ya que una forma geométrica determinada podría decir muchas cosas o no decir nada.
Por otro lado, los griegos también empleaban sistemas criptográficos, aproximadamente por el año 500 A.C. Utilizaban un curioso artilugio llamado "*cítale" que* consistía en un cilindro alrededor del cual se enrollaba una tira de cuero. Se escribía un mensaje sobre la tira, y al desenrollarla se podía ver una sarta de letras, aparentemente sin sentido alguno. Nótese que ya desde esa temprana edad, los sistemas de cifrado se basaban en intercambiar las palabras de los textos, y por tanto se trataba
de sistemas de cifrado clásicos, ya que únicamente se necesitaba encriptar mensajes escritos.
Julio César también empleó un sistema de cifrado durante su reinado. Dicho sistema ha sido convenientemente detallado en párrafos anteriores, como uno de los métodos clásicos. Pero vamos a recordarlo aquí y ahora. Su sistema se basaba en sustituir la letra a encriptar por otra letra distanciada tres posiciones más adelante. De esa forma se obtenían mensajes ininteligibles, y ni durante su reinado ni posteriormente se desencriptó nunca el sistema.
En el siglo XII, el sabio inglés Roger Bacon describió diversos métodos criptográficos al igual que Gabriel di Lavinde "*quien inventó el sistema Nomemclator"* que publicó en 1379 una compilación de sistemas a petición del

Papa Clemente VII. Es bien curioso que hasta la propia Iglesia tenía que echar mano a sistemas criptográficos.

Los sistemas empleados por esas fechas indudablemente se basaban en los métodos clásicos por sustitución.
En 1467 León Battista Alberti inventó el primer sistema criptográfico polialfabético y no fue sino en el siglo XVIII que se descifró. En 1790 Thomas Jefferson inventó su cilindro de transposiciones, que fue ampliamente utilizado durante la segunda guerra mundial por la armada de los Estados Unidos. Pero el sistema no duraría mucho, ya que se basaba en un sistema polialfabético y en 1861 se publicó la primera solución generalizada para resolver cifrados polialfabéticos, poniendo fin a 400 años de silencio.
Sin embargo los sistemas criptográficos no experimentaron parada alguna, ni mucho menos demora en sus sistemas de cifrado. Las grandes guerras impulsaron la creación de nuevos sistemas criptográficos más potentes y difíciles de entender. La máquina "Enigma", desarrollada por los alemanes a mediados de los 70 fue un duro golpe para el criptoanálisis y sobre todo para los expertos en sistemas criptográficos.
Poco después de los 70 aparecieron los sistemas criptográficos denominados modernos. Así, en 1976 hizo su aparición el código DES gracias al desarrollo de computadores digitales. A partir de ahí los algoritmos y sistemas de criptografía experimentarían un interés innegable. El sistema DES fue el primero de los sistemas complejos, pero introdujo la clave secreta que debía guardarse muy bien si se quería mantener la fuerza del sistema; pero ese mismo año hacían su estelar aparición Diffie y Hellman, creadores del primer sistema de cifrado basado en claves públicas. Sistemas altamente seguros.
Un año después Rivert, Shamir y Adelman sacaban de la manga el sistema criptográfico de actualidad, el RSA. Un sistema basado en buscar números primos, nada fácil de solucionar. Hasta la fecha el sistema está siendo empleado por computadores y sistemas de codificación de canales de televisión.
Finalmente, el sistema criptográfico más conocido en la red de internet para todos los cibernautas, es el sistema PGP de Phil Zimmerman, creado en 1991. Sin embargo hay que decir que este sistema criptográfico, más que eso, es un programa que reúne los sistemas criptográficos más fuertes del mercado como el DSS y el de Diffie-Hellman.

Pero lo que se hace es jugar con ellos, y así se obtienen brillantes encriptaciones realmente seguras.

Hoy por hoy el sistema objetivo de gran número de Hackers es el mencionado PGP, ya que es el más ampliamente utilizado por los navegantes. De momento no se ha conocido ninguna apertura de ese sistema. Sin embargo los ordenadores del futuro ponen en manos de los Hackers herramientas verdaderamente potentes que acabarán con todos esos sistemas criptográficos de gran seguridad.
Si no, tiempo al tiempo.

Criptografía, sistemas de cifrado

Criptografía significa literalmente "*escritura secreta",* es la ciencia que consiste en transformar un mensaje inteligible "*en otro que no lo sea en absoluto"* para después devolverlo a su forma original, sin que nadie que vea el mensaje cifrado sea capaz de entenderlo.
Esta es la definición más correcta de la criptografía. Ya hemos comentado por qué debemos echar mano de ella, y ahora vamos a explicar qué sistemas existen y de qué forma se efectúan los mensajes criptográficos. Los Hackers son muy habilidosos para descifrar esos textos, pero lo cierto es que hace falta poseer un buen programa para poder descifrar incluso mensajes cifrados de forma sencilla.
Existen dos tipos de criptosistemas, simétricos y asimétricos. Los sistemas simétricos,
son sistemas de cifrado basados en "*claves secretas" y* emplean la misma clave para encriptar y desencriptar el mensaje y los datos de control del descodificador.
Los sistemas asimétricos, sin embargo, operan con dos claves distintas. Emplean una "*clave pública" para* encriptar y otra "*clave secreta"“para* desencriptar. Este cifrado es más complejo y por tanto con un mayor nivel de seguridad.
Como se puede intuir, los sistemas de cifrado simétricos son más débiles que los asimétricos, y es así porque ambos, emisor y receptor, deben emplear la misma clave, tanto para el proceso de encriptación como para el proceso de desencriptación. De esa forma esta clave debe enviarse a través de un medio de transmisión. Un Hacker podría leer esta clave y emplearla para desencriptar el mensaje.
Si ciframos esa clave con otra clave, siempre estaríamos igual, ya que la última clave revelaría siempre la clave oculta. Sin embargo, los sistemas de cifrado

asimétricos, al emplear distintas claves, permiten el uso de medios de transmisión poco seguros.
Además de los sistemas de cifrado enunciados, podemos encontrar otros no menos importantes, que se han empleado siempre para cifrar textos y mensajes. Estos sistemas de cifrado son útiles para ordenadores y equipos de impresión de textos. Los sistemas de cifrado simétricos y asimétricos son sistemas útiles para encriptar datos e información digital que se enviarán después por medios de transmisión libres.
Pero de alguna manera siempre se cifraron los textos, y aquí también surgen grupos de interés. Podríamos dividirlos en dos grandes familias. En primer lugar tenemos los "*métodos clásicos" y* en segundo lugar "*los métodos modernos"*.Obviamente, sabemos a qué nos referimos. Los métodos clásicos son aquellos que existieron desde siempre y son métodos desarrollados para cifrar mensajes escritos a mano o en máquinas de impresión. Los métodos modernos son los ya mencionados sistemas simétricos y asimétricos.
Los métodos clásicos se basan en la sustitución de unas letras por otras, y en la transposición, y juegan con la alteración del orden lógico de los caracteres del mensaje. A los métodos clásicos les han salido dos formas de cifrado, denominados grupos, que son "*métodos por sustitución "y* "*métodos por transposición".*

Los métodos por sustitución son aquellos que cambian unas palabras por otras; esta simple forma de cifrar ha dado siempre buenos resultados.

Los métodos por transposición son aquellos que alteran el orden de las palabras del mensaje.

Los métodos modernos se basan en combinar secuencias de dígitos creados de forma aleatoria con los dígitos del mensaje, mediante puertas lógicas, en el caso de los módulos PRG sencillos. Otros emplean algoritmos matemáticos de gran complejidad para permutar mensajes de cierta longitud de bits.

Dentro de los métodos clásicos podemos encontrarnos con varios sistemas como los que siguen:

Cifrado César o monoalfabético simple.
Cifrado monoalfabético general.

Cifrado por sustitución polialfabética.
Cifrado inverso.
Cifrado en figura geométrica.
Cifrado por filas.

De los seis sistemas de cifrado mencionados los tres primeros se basan en los métodos por sustitución y obviamente los restantes se basan en los métodos de transposición. Explicaremos cada uno de ellos y veremos qué efecto de cifrado se obtiene en los mensajes.
Sistema de cifrado César o monoalfabético simple: es un método extremadamente simple y lo emplearon los romanos para encriptar sus mensajes, de ahí el nombre de César, dado que fue durante su reinado que nació este sistema de cifrado. Este sistema de cifrado consiste en reemplazar cada letra de un texto por otra que se encuentra a determinada distancia. Se sabe que César empleaba una distancia de tres, así;

sustituir 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

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

Así el mensaje "El Hacker acecha de nuevo", quedaría de la siguiente manera;

HÑ KDFNHU DFHFKD GH PXHYR

Sistema de cifrado monoalfabético general: es un sistema que se basa en sustituir cada letra por otra, de forma aleatoria. Esto supone un grado más de complejidad que en el método de cifrado anterior. Un ejemplo sería el siguiente;

Sustituir 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

Por Z C Q V A J G Ñ W N FB U M R H Y O D Y X T P E S L K

Y empleando el mismo mensaje anterior quedaría de la siguiente forma;

AF ÑZQNAO ZQAQÑZ VA UXATR

Sistema por sustitución polialfabética: es un método que emplea más de un alfabeto de sustitución. Esto es, se emplean varias cadenas de palabras aleatorias y diferentes entre sí, para después elegir una palabra distinta según una secuencia establecida. Aquí nacen las claves secretas basadas en números. Este sistema es algo más complejo que los anteriores y a veces resulta difícil descifrar mensajes cuando se emplean más de diez columnas de palabras aleatorias. Un ejemplo es el que sigue;

Sustituir 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

Por 1/ F Q R A L K Z S J Ñ M Y T Y V D B E W V N O C X H P G

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

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

Con una clave 2-3-1, el mensaje sería así;

HY SGOMHM FWDRVAF HD YPDCJ

Sistema de cifrado inverso: es quizás una de las formas más simples de cifrar una imagen y probablemente la conocemos todos nosotros. Es corriente escribir al revés cuando estamos aburridos, y lo cierto es que ese es un sistema de cifrado. La forma de hacerlo es simplemente escribiendo el mensaje al revés.

"El Hacker acecha de nuevo":
(oveun de ahceca rekcah le)

Sistema en figura geométrica: ya es más complejo que la versión anterior. En esta ocasión se empieza por escribir el mensaje siguiendo un patrón preestablecido y se encripta siguiendo una estructura geométrica basada en otro patrón. Este último patrón puede ser verdaderamente complejo según la extensión del mensaje escrito y la forma de seguimiento de las líneas. Un ejemplo simple sería el que sigue;

El HAC

KER ESTA
AL ACE
CHO

Patrón de cifrado;

Mensaje cifrado; ECALHKAHOACRECEATSE

Método por transposición de fila: consiste en escribir el mensaje en columnas y luego determinar una regla para reordenarlas. Esa regla elegida al azar será la clave para cifrar el mensaje. También aquí es importante saber la clave secreta para poder descifrarlo En esta ocasión el mensaje puede estar fuertemente encriptado si se emplean textos relativamente largos. Un buen ejemplo y sencillo es el que sigue:

ELHACK Si la clave es 6 3 1 5 4 2 KHECAL
ERESTA AEETSR
ALACEC CAAECL
CHO OCH

Como hemos podido ver, todos los métodos criptográficos clásicos emplean la misma clave para cifrar y descifrar un mismo mensaje. Con la llegada de los ordenadores, la solución de estos sistemas se tornó prácticamente trivial y por eso han surgido nuevos métodos de encriptación más trabajados y seguros. Algunos de ellos también basados en claves secretas, cuya computación es bastante compleja y prácticamente inalcanzable.
Tal como se ha dicho, los métodos modernos son más complejos de elaborar y un ejemplo de ello se puede ver en el capítulo 11 de este libro. Además de los ordenadores, las tarjetas de acceso electrónicas son capaces de trabajar con estas encriptaciones por la alta velocidad de computación que presentan. Al estar basadas en complejas transformaciones matemáticas de una secuencia, es indispensable disponer de una ágil memoria y capacidad de procesamiento. Estos sistemas de cifrado modernos, son capaces de cifrar palabras de más de 128 bits y normalmente se cifran en bloques.
Aunque aquí no vamos a detallar de nuevo estos sistemas criptográficos, sí vamos a enumerarlos, por supuesto los más importantes que se emplean en la red de internet. Para ello vamos a dividirlos en tres grupos: uno, que abarcará los sistemas de cifrado basados en claves públicas; otro grupo de cifrados basados

en claves secretas; y un último grupo más reciente y que se emplea en la televisión digital, los métodos empleados en algoritmos.

Sistemas de cifrado de clave pública:

** RSA.....E*s quizás el sistema de cifrado que más se emplea en la actualidad. Este sistema es el elegido para trabajar con los códigos del sistema de codificación Videocrypt, algoritmo que el Capitán Zap consiguió romper, aunque se dice que a pesar de eso sigue siendo el sistema de cifrado más fuerte del mundo. Hay una anécdota que hace pensar lo contrario; en 1997 un chaval de 16 años, un cerebro de la informática, fue capaz de romper el código RSA con una longitud de 200 bits en menos de cuatro horas.
El sistema RSA se basa en la multiplicación de números primos, por lo que implica grandes operaciones matemáticas. Fue inventado en 1977 por Rivest, Shamir y Adelman, de ahí el nombre RSA. También es cierto que el sistema de cifrado comentado ha sido modificado por sus inventores aumentando el grado de seguridad. El sistema permite utilizar documentos de diferentes tamaños; 512 bits, 768 bits, 1029 bits, 2048 bits...

** Diffie - Hellman....d*ata de 1976 y se emplea fundamentalmente para el intercambio de claves. Como se ha comentado y se comentará en otras páginas, es bastante delicado enviar la clave que permite el descifrado de un mensaje. Por ello se creó este sistema de cifrado que se emplea únicamente para proteger claves.

Otros métodos no menos importantes son los siguientes:

** Sistema de curvas elípticas: e*stá diseñado exclusivamente para cifrar textos escritos en ordenador y no se emplea para sistemas de encriptación de señales de televisión analógicas o digitales. El sistema se basa en los movimientos del ratón que el usuario hace habitualmente antes de instalar el programa. Este sistema puede resultar realmente complejo.

** DDS:* el sistema no se ha publicado hasta ahora, pero se sabe que se basa en

transmutar la secuencia de los dígitos o bits. También emplea métodos de permutación y rotación de dígitos en un módulo pseudo aleatorio. Ya hay Hackers que han trajinado con él...

** El garral: por el nombre* parece un sistema español pero no es así.
También se basa en palabras más o menos largas para el cifrado de mensajes. Está desarrollado para sistemas informáticos y transacciones.

** LUC:....*sólo se sabe de él que fue creado en 1993.
Los sistemas de cifrado basados en claves secretas también han conocido una muy buena aceptación, gracias a la tecnología de los ordenadores que permiten hacer computaciones elevadas sea cual sea la longitud de bits elegida. Mencionaremos sólo tres de ellos. El más importante quizás sea el código DES. Este sistema de encriptación es de habitual empleo en sistemas de encriptación de señales de televisión, para proteger los datos ECM de control de descodificación de la señal. Sin embargo según los Hackers todos los sistemas de seguridad tienen sus fallos, y por lo tanto pueden dejar de ser seguros si el pirata es lo suficientemente hábil.

** DES:...é*ste sí que es un sistema de cifrado. Altamente seguro, el rey de los sistemas basados en claves secretas, ha demostrado su fuerza en los últimos veinte años desde su creación. Hasta ahora no se ha podido abrir. Básicamente se emplea para las transiciones de datos interbancarios y transferencias de alto riesgo. Las tarjetas de acceso inteligente de los telebancos también operan según esta clave, con una palabra de unos 200 bits. El sistema de encriptación de señales de vídeo Nagravisión lo emplea para proteger los datos ECM y EMM del sistema. El sistema de cifrado DES se basa en la permutación de la longitud de bits, unos 200 por lo general, en al menos 16 permutaciones en la primera versión de este sistema de cifrado; después los datos son rotados a situaciones irrelevantes. El sistema se describe en el capítulo Carding, pero es más que probable que a estas alturas hayan modificado la estructura del algoritmo de cifrado. De cualquier manera es prácticamente imposible de abrir, aún cuando se sabe la ruta que siguen los bits en toda la secuencia.

** IDEA:...*este sistema fue desarrollado en Zurich en 1990, emplea claves de encriptación de 128 bits de longitud y se considera muy seguro. Es uno de los algoritmos más conocidos actualmente. El método de cifrado, se puede esperar, se basa en modificar la orientación de cada bit y combinarla con una puerta lógica

variable.

** RC4:....*este algoritmo fue desarrollado por el grupo RSA y un buen día se publicó, por lo que su seguridad descendió vertiginosamente. El sistema se basa en combinar cada bit con un bit de otra secuencia. Acepta claves de cualquier longitud y emplea un generador de números aleatorios. Es muy difícil de romper y su fuerte está en la velocidad de computación admisible. Además, es el método empleado por el SSL de Nestcape en su versión con clave de 40 bits.
Además de estos sistemas de cifrado basados en claves publicas o secretas, existen
otros sistemas de cifrado basados en algoritmos. Estos nuevos sistemas no emplean
claves de ningún tipo, sino se basan en extraer una determinada cantidad de bits a partir de un texto de longitud arbitraria. Esto es, cada cierta cantidad de texto, elegida de forma arbitraria, se procede a realizar una transformación de bits; y de esa transformación se obtiene una palabra longitud clave, Esta palabra longitud tiene una extensión de x bits preestablecidos. De esta forma el texto es irreconocible ya que sólo se pueden leer números secuenciales y no guardan relación alguna entre sí. Quizás éste es el método más complejo que existe hasta el momento. Trabajar con estos algoritmos requiere sistemas informáticos, esto es, ordenadores o tarjetas de acceso inteligentes que sólo comuniquen el tipo de algoritmo empleado. Estos algoritmos se basan normalmente en complejas operaciones matemáticas de difícil solución. Y el secreto precisamente está ahí, en qué operaciones matemáticas sigue el algoritmo.
Entre los sistemas desarrollados a partir de la creación de algoritmos, cabe destacar al menos dos, por su complejidad e importancia social.

** MD5:....*es un algoritmo desarrollado por el grupo RSA y es un intento de probar con otros sistemas criptográficos que no empleen claves. El algoritmo desarrollado es capaz de obtener 128 bits a partir de un determinado texto. Como es lógico, hasta el momento no se sabe cuáles son las operaciones matemáticas a seguir, pero hay quien dice que es más que probable que se basen en factores de números primos.

** SHA:.....*es un algoritmo desarrollado por el gobierno de los EE.UU. y se pretende implantar en los sistemas informáticos de alta seguridad del Estado como estándar para la protección de documentos. El algoritmo obtiene 160 bits de

un texto determinado. Se sabe que existen Hackers que han probado suerte, pero hasta el momento nadie ha dicho nada más al respecto.

Criptoanálisis

Este sí que es un tema complejo. Esta ciencia o parte de ella, también denominada hacking por los *underground y chiberpunks*, es el arte de estudiar mensajes ilegibles, esto es, encriptados, para transformarlos en legibles sin conocer la clave ni el método empleado. Esto es, romper el cifrado y hacer crack. Como se ha comentado en otros capítulos de este libro, un buen principio es tener mucha paciencia y gran intuición. Esta última es quizás el factor más importante de todos, sin ella probablemente estés perdido. También es lógico que debas ser un experto en sistemas criptográficos. Lo primero que puedes hacer es estudiar los sistemas ya existentes, que posiblemente te servirán de algo.

Estudiar los sistemas de cifrado basados en métodos clásicos potenciará tu creatividad y es probable que puedas abrir algún mensaje encriptado con alguno de ellos. Sin embargo, los textos encriptados con cualquier sistema basado en métodos modernos son algo más complejos. En tal caso debes emplear un ordenador como mínimo y crear un programa que resuelva con elegancia algunas combinaciones lógicas y otras tantas operaciones matemáticas.
La operación para abrir un sistema criptográfico te puede llevar días, cuando no semanas. Además estos métodos modernos, sobre todo los basados en algoritmos, son muy difíciles de descubrir. Como ya se ha dicho, los métodos basados en claves públicas son los sistemas más fuertes.
Los principales hacks realizados en la red se basan en falsear los IP, protocolos de entrada en ordenadores remotos. Muy pocos Hackers son capaces de descubrir y reventar los algoritmos o mensajes cifrados. Se trata de un reducido número de
componentes y normalmente no lo hacen por hacer daño, sino para demostrar que todos los programas tienen bugs. El Hacker más peligroso es el que crea virus informáticos, abre puertas lógicas y modifica los ficheros de tu ordenador.
Los virus informáticos también pueden ser algoritmos complejos de desencriptar.

Se crean así, para que los sysops o policías cibernéticos no puedan descubrir la forma de reconocer ni anular el virus. En este caso también se procede al criptoanálisis del virus.
Por otro lado los Hackers más deseados siempre estarán bien protegidos, ya que son los idóneos para proporcionar ayuda en operaciones delicadas como el espionaje del enemigo. Sin ir más lejos, en la guerra del Golfo Pérsico fue necesario
desencriptar muchos mensajes para frenar las fuerzas de Sadam Hussein, cosa que muchos han ignorado siempre.
En cualquier guerra actual más o menos importante y en las míticas y nunca olvidadas primera y segunda guerras mundiales, se ha empleado
y se emplea siempre la encriptación de los mensajes. Y desde siempre existió el criptoanálisis para desencriptar los mensajes del enemigo. Una famosa alusión al respecto, es "*Enigma"* una máquina de escribir que imprimía la Z en lugar de la A, por ejemplo.

Este hecho ha pasado a la historia de la criptografía y del criptoanálisis, por la dureza del sistema enigma, ya que el caso no es de menospreciar. En los años 20 los alemanes desarrollaron "la segunda guerra mundial" con una máquina altamente sofisticada a la que llamaron "E*nigma".* Su misión era crear textos cifrados de alta seguridad totalmente incomprensibles. Su aspecto exterior era el de una máquina de escribir convencional, con la particularidad de que al teclear la letra Z imprimía la A y así con las demás letras del alfabeto. En un principio podía tratarse de un método clásico siguiendo un patrón fijo, sin embargo el truco no estaba ahí. La relación pulsación/resultado cambiaba de forma aleatoria y de eso se trataba, con lo cual era prácticamente imposible descubrir ningún ordenamiento.
De esta forma "Enigma" fue el instrumento para cifrar las órdenes y mensajes durante la segunda guerra mundial. Fue entonces cuando entró de lleno la ciencia del criptoanálisis y de los Hackers "*oficiales".*
Sin embargo, fue en 1933 cuando un experto en criptografía, Marian Rajewsky, perteneciente al servicio de inteligencia polaco, consiguió descifrar los mensajes de "Enigma". Tardaron varios años de criptoanálisis continuados en clonar
o fabricar una máquina exacta a la "Enigma" de los alemanes.
Pero la máquina experimentó cierta evolución y Marian Rajewsky, conjuntamente con la ciencia polaca, nunca pudo enterarse de la inminente invasión nazi. Sin embargo los ingleses, muy activos a la hora de hacer hacking y que han sido siempre pioneros en sistemas de desencriptación de canales de pago, continuaron

con la investigación del sistema enigma mejorándolo, y por fin en 1940 apareció el primer mensaje descifrado de las nuevas "Enigma". El artífice fue un genio llamado Alan Turing y un grupo de personas sacadas "*debajo de las piedras",¿* qué otras podían ser sino verdaderos Hackers?
También la Biblia pudo ser cifrada mientras se escribió, o eso es lo que afirma un tal Michael Drosnin, que asegura también, que mediante el criptoanálisis y la ayuda de una potente computadora, ha conseguido descifrar mensajes muy importantes para la humanidad, entre ellos cuándo será el fin del mundo.