Protección de la informática a través del cifrado

José Antonio Labodía Bonastre
Director de Seguridad
joseantonio.labodia@securitas.es

Desde estas páginas me permito realizar una serie de preguntas, que creo interesan a cualquier usuario de la informática, sea más o menos apasionado de los equipos informáticos y todo aquello que los rodea:

1. ¿Quieres proteger la información de tu PC?
2. ¿Quieres firmar digitalmente tus mensajes?
3. ¿Quieres mantener unas comunicaciones seguras?
4. ¿Quieres poder comprar en Internet de forma protegida?

¿Adivinas cual es la respuesta a todas estas interrogantes? La respuesta esta clara. El cifrado.

Por motivos de espacio vamos a centrarnos únicamente en la primera pregunta. En cómo proteger la información presente en nuestro PC, en el ordenador situado en nuestra casa, frente al que pasamos horas y horas y cuyos datos queremos proteger de miradas indiscretas. O el del trabajo, en el que no queremos que nadie fisgonee en algunos de los datos presentes en él.

Imaginemos que alguien quiera acceder a nuestro PC. ¿Nuestro hermano? ¿Nuestra esposa?... El "*maleante*" comprueba nuestro equipo antes de llevar a cabo su sibilino ataque. La primera barrera con la que puede encontrarse es la cerradura de bloqueo. Pero como andábamos escasos de fondos hemos comprado un ordenador que no dispone de ella, algo bastante común, por otra parte. El "*malhechor*" suspira aliviado. Conecta el equipo. Si hubiésemos comprado un PC con cerradura tampoco le hubiera supuesto un problema demasiado importante.

El ruido del ventilador se extiende por la habitación. Conecta el monitor y en la negra pantalla aparecen los primeros signos de vida, los primeros mensajes. Se inicia el conteo de memoria, los caracteres le informan acerca de las características de la BIOS, su fecha y de repente... Primer problema. Un mensaje de la BIOS del sistema le informa de que para entrar, necesita teclear una *password* (en adelante, palabra de paso). Una medida de seguridad que hemos tomado porque somos un poco neuróticos y evitamos que al menos nos trasteen en el "*setup*" de la BIOS, y digo esto porque nuestro hermano nos montó una buena trifulca el día que no pudo jugar en nuestro PC.

¿Qué hace el individuo ahora? Lo más lógico es que eche mano a un destornillador, abra el PC y busque en la placa madre la serigrafía que le informe de cual es el "*swicht*" para quitar la palabra de paso. En el supuesto de que no encuentre la notación, siempre tiene la opción de quitar la pila que alimenta la BIOS. Con las BIOS actuales que detectan automáticamente las características del sistema, discos duros, memoria, etc., no existe mayor problema.

Ya ha entrado. Interesado, quizás incluso nervioso, ve los mensajes que informan sobre qué es lo que está haciendo el ordenador. Iniciando Windows xx... Y finalmente aparece el logotipo de Windows, en cualquiera de sus versiones, dado que es el sistema operativo de nuestro ordenador al igual que en el 99% de los casos de los sistemas informáticos caseros que pululan a lo largo y ancho de este orbe.

Bien. El intruso ya está dentro. Tiene acceso a todas las aplicaciones del disco duro, a nuestros datos... Han caído todas las barreras que protegen nuestros datos. Llegados a este punto, si queremos proteger la información, nuestra preciada información, que duerme en nuestro ordenador, no nos queda otra alternativa que la de recurrir al cifrado, como la última muralla que protege nuestra intimidad.

¿No te parece interesante lo relatado? ¿No has notado un glaciar escalofrío en tu espalda mientras lo leías? Quizás esté ocurriendo ahora mismo...

Los sistemas operativos más usuales, dejando a un lado UNIX y sus variantes, como Linux, son monousuario, y la seguridad de los mismos deja bastante que desear. Este panorama cambiara con la aparición de Windows 2000. Lógicamente, estamos hablando de PCs domésticos, no de ordenadores empresariales que en su mayor parte están gobernados por Windows NT y que ofrecen un nivel de seguridad mayor, aunque de este sistema operativo, también se podría hablar desde el punto de la seguridad.

Bien. Parece que la única forma de protegernos de visitas indeseadas en la utilización del cifrado. ¿Pero en qué consiste el cifrado? Básicamente se trata de convertir un texto - o dato - claro (comprensible) en un texto o, dato, irreconocible utilizando para ello un algoritmo de cifrado. Para convertir el texto irreconocible en un texto claro (comprensible) de nuevo, hará falta disponer de una clave.

Flujo de cifrado

Flujo de descifrado

Cuando se cifra un texto se siguen los siguientes pasos

- **Cifrado:** proceso de transformación de un texto original – o datos - en un texto o datos cifrados.
- **Descifrado:** proceso de transformación de un texto o datos cifrado en el texto o los datos originales, previos al proceso de cifrado.
- **Clave:** parámetros que controlan los procesos de cifrado y descifrado.

UNA PEQUEÑA INTRODUCCIÓN HISTÓRICA AL CIFRADO

Las técnicas de cifra han existido desde que el hombre ha considerado que tenía una información que no le interesaba que conociese nadie excepto él y quizá algunas personas que contasen con su confianza, esto es, el cifrado ha tenido un desarrollo paralelo a la historia de la Humanidad, y parejo a la complejidad tecnológica disponible.

Así, en el devenir histórico, se han utilizado diversos métodos con el fin último de ocultar la información ayudándose en la "*prehistoria del cifrado*" de elementos tales como el escítalo lacedemonio, que consistía en dos bastones de idéntica longitud y diámetro sobre los que se enrollaba una tira de papiro o cuero. El emisor de mensaje escribía sobre la citada tira, la desenrollaba y la enviaba al receptor, que no tenía más enrollarla en su bastón para que el mensaje apareciese de forma comprensible. Tal sistema fue usado por los espartanos y los atenienses.

Pasaron los siglos y en la época de la República Romana se utilizó el cifrado que César empleaba para realizar sus comunicaciones diplomáticas y militares y que consistía en sustituir cada letra del mensaje por otra seleccionada de forma fija.

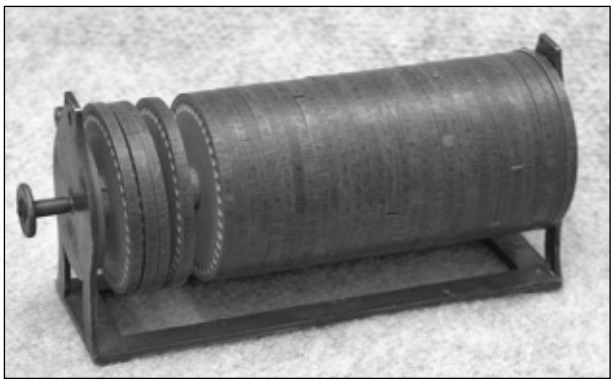
Posteriormente Augusto César creó un sistema de cifra basado en el de su tío. Este método consistía en un alfabeto escrito sobre dos ruedas concéntricas. Girando las ruedas un determinado número de veces, la letra sustitutoria se escribía como texto cifrado. El sistema no era muy seguro, puesto que el número máximo de claves era de 26.

Estos sistemas de cifra, y es de imaginar que paralelamente y junto a otros de menor entidad, predomina-

ron hasta el Renacimiento época en la cual Cicco Simonetta, secretario de los Sforza en Milán entre los años 1375 y 1383 publicó la obra monográfica más antigua conocida sobre cifrado y que se conoce, el *Liber Zifrorum*. En el siglo XV León Battista Alberti nacido en Génova en el año 1404 y muerto en 1472, dio el empuje definitivo al análisis de textos cifrados, apareciendo en siglos sucesivos distintos sistemas con el único afán de proteger, y claro desproteger la información cifrada.

Otro intento serio tuvo lugar en el año 1790 en el que Thomas Jefferson ideó el denominado Cilindro Jefferson que constaba de 36 discos con las letras del alfabeto impresas en sus bordes exteriores. La disposición inicial de los discos solamente era conocida por las personas que mandaban o recibían los mensajes. Para descifrar uno de ellos, únicamente se tenía que aplicar las filas de caracteres sin sentido que componían el mensaje cifrado sobre el cilindro. La clave era bastante segura, de hecho la Marina de Guerra USA lo utilizó hasta el año 1920, ya que los 36 discos, con 26 letras, suponían 1.041 variaciones.

En el año 1871 Decius Wadsworth utilizó un método basado en el utilizado por César Augusto, empleando también dos discos concéntricos, pero dejando, y ahí radicaba la innovación, un espacio adicional que mejoraba ostensiblemente la aleatoriedad. Este mismo sistema fue mejorado en el año 1860 por Sir Charles Wheatstone que incluyó un índice que señalaba los caracteres en claro y los cifrados.



Este estado de cosas, continuó hasta principios de siglo XX. En el año 1917 Vernam ideó sin duda alguna el sistema de cifra más seguro y que posteriormente se utilizó para proteger el denominando y famoso "*teléfono rojo*", en realidad un telex, que unía Moscú y París. En este método, conocido como "*Cifra de Vernam*" la clave se generaba de forma totalmente aleatoria y se utilizaba solamente una vez (*one-time pad)* siendo tan larga como el mensaje. Es evidente que esta clave no era muy práctica cuando los mensajes a cifrar eran muy largos y sólo se puede utilizar para determinadas aplicaciones, en las que la seguridad debe predominar sobre cualquier otra razón.

En la década de los años 30 Boris Hagelin, construyó un teclado que imprimía texto cifrado, retomando la idea del marqués De Viaris (año 1870), denominado M-209. Un modelo similar fue construido por la firma Siemens y Haskel - el T-52 - y que fue utilizado en los circuitos telegráficos durante la II Guerra Mundial, hasta mediados de los años 40.

Sin duda alguna el cifrado y el criptoanálisis sufrieron sus cambios más importantes de su historia a raíz de las dos Guerras Mundiales, principalmente la II, en las que ambos contendientes hicieron esfuerzos gigantescos tanto para ocultar su información, como para acceder a la de los otros.

Los alemanes idearon una máquina a la que llamaron Enigma, y que comenzó a desarrollarse en los años 30. Esta máquina constaba de 26 rotores de caracteres que giraban sobre un eje solidario de forma que cada rotor disparaba el siguiente nivel de cifrado. Los alemanes modificaron la máquina con un tablero de conmutación de 26 clavijas identificadas de la A a la Z y 10 cables de extremos iguales. Ambos extremos se conectaban a las clavijas, dejando abiertas seis de ellas, lo que suponía la posibilidad de permitir un reordenamiento de la secuencia de conexiones en caso de que se capturara una máquina cualquiera. Estas máquinas eran capaces de efectuar cifrados muy complejos para la época.

Pero después de la invasión de Polonia por parte del Ejército del III Reich, un grupo de científicos polacos huyó al Reino Unido, y desarrollaron una serie de trabajos para los servicios de inteligencia, que permitieron a los aliados descifrar los mensajes generados por Enigma, aunque los alemanes continuasen pensando en que la seguridad de sus comunicaciones no había sido comprometida.

El cifrado moderno se inicia en la segunda mitad de la década de los años 70, con la invención del sistema conocido como DES, del cual volveremos a hablar más adelante.

MÁS SOBRE EL CIFRADO

Con la aparición y posterior desarrollo de la informática el cifrado ha desarrollado increíblemente tanto sus posibilidades de protección de información, como las de vulnerar dicha protección, apoyándose tanto en las modernas máquinas de cifra utilizadas para salvaguardar información militar o de estado, como en los superordenadores y sus ingentes capacidades de tratamiento automatizado de la información.

Todos están interesados en proteger las telecomunicaciones y la ingente cantidad de información que se maneja en las últimas décadas, tanto si la misma se encuentra almacenada, como durante su transmisión. La seguridad de las técnicas de cifrado, aplicadas a la T.I. radica en que se tarde tanto en acceder a la información protegida, que ésta no tenga ninguna validez cuando se consiga romper el algoritmo de cifrado.

A grandes rasgos, el cifrado permite:

La confidencialidad: Los datos solamente deben ser accesibles a aquellas personas que estén autorizadas a conocer la información.

Integridad: Los datos deben ser genuinos y estar asegurada su integridad. De nada sirve una base de datos cuyos registros han podido ser cambiados o no estén completos.

Disponibilidad: Cualquiera que sea su formato, deben estar disponibles para su consulta o tratamiento, por parte de las personas autorizadas.

Autenticación: La información es generada por las personas y en los equipos autorizados a generarla, quedando constancia de quien la ha generado.

Como se ve, las posibilidades del cifrado, desde el punto de vista de la seguridad, son importantes. En definitiva se trata de asegurar que únicamente una persona, el propietario de la información, o las personas autorizadas por ella, puedan acceder a la misma.

¿Qué técnicas de cifrado se utilizan para proteger los datos?

- **Cifradores de Sustitución:** Cada letra o grupo de letras se sustituye por otra letra o grupo de letras que ocultan el texto original que queremos cifrar. Un ejemplo de ello es el cifrado de César, mencionado en la pequeña reseña histórica anterior.

- **Cifradores monoalfabéticos:** En este tipo de cifradores se produce la sustitución de cada símbolo único del texto (cada letra) por otro, sin tener que mantener las letras sustituidas y las sustitutas una relación de orden en el alfabeto.

- **Cifradores polialfabéticos**: En ellos se utilizan varios alfabetos de cifrado usándolos en rotación. (Vg.: cifrado Vigenère)

- **Códigos:** Utilizando unidades más grandes a la hora de cifrar, el cifrado generado comenzará a parecerse a un código. Antes de que aparecieran los ordenadores, los códigos se podían clasificar en dos tipos diferentes y claramente diferenciados: *Códigos de una parte*, en los que la palabra original y la codificada se encontraban en el mismo orden y *códigos de dos partes*; en los que la palabra original y la codificada no se encontraban en este orden.

- **Supercifrado:** En él se combinan códigos y cifradores complicando el trabajo de rotura de la clave utilizada para cifrar la información.
- **Cifradores de transposición:** Estos cifradores no enmascaran los símbolos, pero sí alteran su orden, a diferencia de los códigos y cifradores de sustitución en los que los que se preservan tanto el orden de los símbolos como el texto original, aunque los enmascaran.
- **Cifradores *hardware*:** Para aumentar las velocidades, tanto de cifrado como de descifrado de datos (a través de la realización de transposiciones y sustituciones de bits fundamentalmente), se implementaron circuitos de *hardware* específicos que descargaban la CPU y permitían aumentar la velocidad, frente a las aplicaciones *software* de cifrado.

En la actualidad, todos los algoritmos de cifrado utilizados, pertenecen a uno de estos dos grandes grupos:

1. **Sistemas simétricos:** En los que se utiliza la misma clave para cifrar y descifrar. Aunque no existe un tipo de diseño modelo, quizá el más utilizado es el de *Fiestel*, en el que básicamente se aplica un número finito de interacciones de cierta forma y que finalmente da como resultado el mensaje cifrado. Dentro de los sistemas de cifrado simétrico existe una clasificación en tres grandes familias:

   - El cifrado simétrico de bloques (*block cipher*)
   - El cifrado simétrico de lluvia (*stream cipher*)
   - Cifrado simétrico de resumen (*hash functions*).

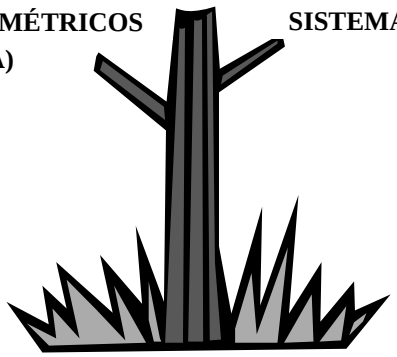
   Aunque con ligeras modificaciones, un sistema de cifrado simétrico de bloques puede modificarse para convertirse en alguno de las otras dos formas, e inversamente.

   Dentro de este grupo quizás el algoritmo más famoso sea el DES (*Data Encryption Standar*), ideado en el año 1976 y que ha sido el algoritmo de cifrado estándar de la NSA americana y de gran parte de las empresas bancarias del mundo. DES es un sistema de cifrado que toma como entrada un bloque de 64 bits del mensaje y lo somete a 16 interacciones, con una clave de 56 bits La seguridad del DES, parte de cuyas operaciones son secretas - no se conoce de forma pública como realiza las operaciones de permutación, las famosas cajas S - estaba en tela de juicio, hasta que finalmente se ha conocido que ha sido roto, al menos en dos ocasiones; la primera vez una de sus variantes, el Triple-DES en su variante CBC, que fue violentado mediante el procesamiento - de un texto cifrado con él - por varios miles de ordenadores a través de Internet. Finalmente el 14 de julio del año 1999, la EFF (*Electronic Frontier Foundation*) ha creado un ordenador especial, llamado *DES Cracker* (RevientaDES), capaz de descifrar textos cifrados con DES en unos tres días.

   En la actualidad el cifrado simétrico se utiliza, básicamente, para proteger aquellos datos que se encuentran en nuestro disco duro y que queremos mantener a salvo de curiosos o de otros usuarios ocasionales del equipo, de forma que no puedan acceder a los mismos en claro.

2. **Sistemas asimétricos:** En los que la clave de cifrado y la de descifrado son distintas. Su nacimiento surgió al estar buscando el modo más práctico de intercambiar las claves simétricas. Diffie y Hellman propusieron una forma para hacerlo, pero no fue hasta que aparece el RSA cuando se concreta el cifrado asimétrico. Su funcionamiento está basado en la imposibilidad de factorizar números enteros grandes.

   Los algoritmos de cifrado asimétricos son aquellos que disponen de dos claves; una pública y otra privada y que son distintas entre sí. En estos algoritmos la denominada clave pública está disponible para toda la comunidad de usuarios de Internet y habitualmente se deposita en servidores de claves públicas (en España existe uno gestionado por RedIris). Enviar la clave a un servidor cualquiera implica comunicárselo a todos los demás servidores de claves, puesto que se las van comunicando entre ellos. Si alguien quiere mandar un mensaje cifrado, lo cifra con esta clave pública y lo envía al receptor del mensaje. El mensaje únicamente podrá ser descifrado con la clave privada de la persona a quien va dirigido el mensaje, dado que se ha cifrado con su clave pública. Lógicamente, en este caso no es necesario disponer de un "*canal seguro*" para enviar la clave de cifrado. Un ejemplo de estos algoritmos es el RSA que recibe su nombre de las iniciales de sus inventores (**R**ivest, **S**hamir, **A**dleman) y que fue creado en el año 1978. Los algoritmos asimétricos se utilizan – fundamentalmente - para enviar o recibir información a través de redes de comunicación inseguras (Vg: correo electrónico).



¿Qué sistema utilizar? La elección de utilizar un sistema u otro está en función de cuales son nuestras necesidades. En cualquier caso es necesario que el algoritmo utilizado cumpla el principio de Kerchhoff, esto es, el código del algoritmo debe ser público, lo cual permite asegurarse de que no existe ninguna "*puerta secreta*", ninguna debilidad que permita a un atacante descifrar la información protegida.