UNIDAD 7 FUNDAMENTOS DE CRIPTOGRAFIA

7.1 INTRODUCCIÓN A LA CRIPTOGRAFÍA

Se entiende por ***criptología*** el estudio y práctica de los sistemas de cifrado destinados a ocultar el contenido de mensajes enviados entre dos partes: emisor y receptor.
La criptografía es la parte de la ***criptología*** que estudia como cifrar efectivamente los mensajes.
Para establecer una comunicación de datos entre dos entidades (personas, equipos informáticos, etc) hacen falta al menos tres elementos básicos: el emisor del mensaje (la fuente), el receptor del mismo (el destino) y un soporte físico por el cual se transfieran los datos (el medio).

En una comunicación normal los datos se envían a través del medio tal como son, sin sufrir modificaciones de ningún tipo, de tal forma que el mensaje que representan puede ser interceptado y leído por cualquier otra entidad que acceda a él durante su viaje por el medio.

Pero hay ocasiones en las que nos interesa que dicho mensaje solamente pueda ser interpretado correctamente por el emisor del mismo y por el receptor al que va dirigido. En estas ocasiones es necesario implementar algún mecanismo de protección de la información sensible tal que el mensaje viaje seguro desde la fuente al destino, siendo imposible la interceptación por terceros del mensaje, o que si se produce ésta, el mensaje capturado sea incomprensible para quien tenga acceso al mismo.

Una de las formas de conseguir esto es enviar el mensaje en claro, tal como lo ha redactado el emisor, y pretejerlo en el camino mediante sistemas de fuerza que lo defiendan durante el camino, como es el caso de la protección de mensajes mediante personal de seguridad.

Otro método posible es el enviar el mensaje por un camino con tanto tráfico de información que resulte muy difícil a las terceras personas detectar que se trata de información confidencial (la mejor forma de ocultar un árbol es dentro de un bosque), como es el caso de enviar el mensaje mediante una carta por el sistema estándar de correo.

Desafortunadamente estos métodos de protección de mensajes, al igual que otros análogos, han demostrado su in efectividad a lo largo de los tiempos, por lo que hubo que buscar otro tipo de mecanismos para proteger la información sensible en su camino entre emisor y receptor.

La criptografía ha demostrado con el tiempo ser una de las mejores técnicas para resolver esta cuestión. Tanto es así que actualmente, en la época de los ordenadores y la

información, es el mecanismo más usado en los procesos de protección de datos, como las transacciones bancarias por Internet, el correo electrónico cifrado, etc.

Esto es así porque es tal vez el único medio asequible y fácil de implementar para lograr un acceso controlado a la información en un medio, Internet, que por su propia naturaleza es abierto y de acceso libre a la información.
Tanta ha sido la importancia de los sistemas criptográficos que, por ejemplo, en la Segunda Guerra Mundial la famosa máquina alemana ENIGMA trajo en jaque durante mucho tiempo al ejercito aliado, al permitir a los nazis el envío de información cifrada a sus tropas.
Y en la actualidad los sistemas de cifrado están financiados en su mayoría por los gobiernos y sus militares, constituyendo el resultado de las investigaciones materia reservada.

7.2 OBJETIVOS DE LA CRIPTOGRAFÍA

La criptografía puede aplicarse en dos ámbitos de la seguridad informática: en el almacenamiento de información y en la transmisión de la misma.

La criptografía es fundamental para la seguridad incluso en sistemas inseguros. Aunque se superen las barreras de seguridad física establecidas, e incluso las barreras de seguridad lógica para el control de accesos en el S.O, la criptografía permite mantener algunas de las características de la seguridad informática.
Aunque no salvaguarda la integridad de los datos ante un posible borrado total o parcial de los mismos, si asegura su integridad en el sentido en que facilita la detección de cualquier tipo de modificación, incluido el añadido o borrado de información.
Obviamente y en primera instancia protege el secreto/confidencialidad de la información.
Veamos ahora como se relaciona la criptografía con cada una de las características de la seguridad informática y como puede utilizarse para añadir algunas nuevas.
De entrada hemos de decir que la criptografía no puede utilizarse para garantizar la disponibilidad de la información. Esta característica debe ser preservada mediante el uso de otro tipo de mecanismo.

Secreto o confidencialidad
Obviamente el cifrado de la información es un excelente método para proteger la confidencialidad de la misma. Aunque se acceda a la información, o se intercepte mientras se transfiere, si está cifrada sigue siendo inútil a menos que pueda descifrarse.

Integridad y precisión
Algunos sistemas criptográficos incorporan medios para prevenir que se dañe la integridad de la información, esto es, que ésta sea modificada voluntaria o involuntariamente. El sistema permite detectar cualquier pequeño cambio que se haya producido en el mensaje original.
Tal y como ya dijimos, en el ámbito militar o diplomático la principal preocupación se

centra en mantener la confidencialidad de la información. Sin embargo, en la mayoría de los entornos comerciales y financieros, la principal preocupación es la integridad. Imaginemos por ejemplo un sistema de transferencia de datos interbancario. Un buen sistema criptográfico debe garantizar que no se ha modificado inadvertida o maliciosamente la información enviada. Debe garantizar que no se ha deslizado ningún punto decimal o se ha producido algún tipo de redondeo no deseado en ciertas transacciones.
Además debe garantizarse que no se ha añadido ningún mensaje nuevo y que no ha sido borrado ninguno.

Autentificación
La criptografía también puede usarse para asegurar la autenticidad de los mensajes. Esto es, asegurar que el mensaje ha sido enviado por quién se identifica como su emisor. Se trata pues de identificar sin posible error el origen de los mensajes.
En relación con la autentificación suelen utilizarse las denominadas firmas digitales. Se trata de añadir algún tipo de información en el mensaje o de utilizar de algún modo las claves para validar en destino el origen del mensaje. En el apartado 8 trataremos con mayor profundidad este tema.
En el ámbito de la transferencia de mensajes cifrados la autentificación está muy relacionado con la integridad, y en muchas ocasiones se usa este término incluyendo al segundo. Así, la autentificación de mensajes influiría tres aspectos:

1. Asegurar que el mensaje no ha sido alterado, ni maliciosa ni inintencionadamente, durante su transmisión. El mensaje llegó tal y como se envío. (integridad).
2. Asegurar que el mensaje no es el reenvió de uno previamente emitido e interceptado. (no reenvío).
3. Asegurar que el emisor es quién dice que es. (autenticidad).

De hecho la autentificación puede usarse en conjunción con el cifrado o en solitario:

o En solitario se trata de autentificar el texto en claro.
o En combinación se autentifica el texto cifrado.

No repudio
Es una característica más inusual que se relaciona con la transmisión de mensajes cifrados. Se trata de prevenir que la persona que envió el mensaje (el emisor) pueda alegar con posterioridad que él no envió ese mensaje (repudiarlo). El receptor debe disponer de mecanismos que demuestren ante terceros que sólo el emisor pudo enviar el mensaje.

7.3 HISTORIA DE LA CRIPTOGRAFÍA

La criptografía es una técnica muy anterior a la utilización de los ordenadores, aunque con éstos ha alcanzado su plena madurez.

De hecho la criptografía ya era utilizada por los egipcios en el año 2000 A.C. Hasta muy recientemente, y fundamentalmente hasta la aparición de los ordenadores y las redes informáticas, la criptografía se usaba fundamentalmente en el ámbito militar y diplomático. En la actualidad, sin embargo, aparte de en estas áreas se está utilizando muy ampliamente en el ámbito comercial y financiero para la transferencia de todo tipo de información a través de las redes informáticas, o para salvaguardar información confidencial.

El desarrollo de la criptografía moderna se inició fundamentalmente en la segunda guerra mundial, y particularmente con la rotura de la máquina Enigma utilizada por los alemanes.

La máquina Enigma fue desarrollada originalmente en Alemania por el ingeniero eléctrico Arthur Scherbius durante la primera guerra mundial. Existe una primera versión del año 1918, pero la armada alemana comenzó a utilizarla a partir del año 1926.

El primer intento de romper su sistema de cifrado proviene de Polonia a finales de los años 20. Macian Rejewski y otros dos matemáticos consiguieron descifrar algunos de los primeros mensajes de la máquina.

En 1930 el alemán Hans-Thilo Schmidt ofreció a la inteligencia francesa alguna información sobre el funcionamiento de la máquina, pero tanto franceses como ingleses rechazaron esta información por ser insuficiente para romper el sistema. Los franceses ofrecieron la información a los polacos, y Rejewski la uso para avanzar en la averiguación de los códigos usados por la máquina.

Después de la caída de Polonia en 1939 los polacos pasaron la información de que disponían a los franceses y británicos. Bajo la dirección del matemático Alan Turing, los británicos pusieron en marcha el proyecto secreto "Ultra" que se dedicó a descifrar los mensajes de la armada alemana y que propicio la construcción de alguno de los primeros ordenadores modernos, el Colossus.

A partir de este momento se puede considerar que se comienzan a utilizar sistemáticamente los ordenadores para el cifrado de información y rotura de sistemas criptográficos.

La criptología descansa sobre tres importantes campos teóricos:
- La teoría de la información
- La teoría de los números
- La teoría de la complejidad algorítmica.

Una introducción algo más detallada de la relación entre los tres campos anteriores y la criptología puede encontrarse por ejemplo en [MRS97] o [Pfl97]

La fundamentación matemática de la teoría de la comunicación y su posterior aplicación a los sistemas criptográficos puede encontrarse en los trabajos de C.E. Shannon. A partir de

las investigaciones de este autor, la criptografía deja de ser un arte y pasa a convertirse en una ciencia.
En este ámbito, destacaremos tan solo que la seguridad de los sistemas criptográficos descansa sobre dos conceptos fundamentales, como son la difusión y la confusión.

El propósito de la difusión de la información es distribuir las propiedades estadísticas de los mensajes en claro, sobre todo el texto cifrado. Esto se puede conseguir de varias formas, por ejemplo:
o Haciendo que se altere la posición de los caracteres mediante cifrados por transposición.
o Haciendo que cada carácter del texto cifrado dependa de tantos caracteres del mensaje como sea posible.

El propósito de la confusión es establecer una relación lo más compleja posible entre la clave y el texto cifrado. De este modo, un criptoanalista no podrá deducir información acerca de la clave mediante un estudio del texto cifrado. Esta propiedad puede conseguirse por ejemplo mediante la aplicación de sustituciones.

Ambas técnicas, la difusión y la confusión, por separado, proporcionan fortaleza a los criptosistemas, sin embargo utilizadas conjuntamente pueden dar lugar a sistemas muy difíciles de atacar. El ejemplo más característico de combinación de estas técnicas es el DES (Data Encryption Standard). En este, las permutaciones (P-boxes) proporcionan difusión, mientras las sustituciones (S-boxes) proveen la necesaria confusión.

7.4 TIPOS DE ATAQUES

Existen tres técnicas fundamentales utilizadas por los criptoanalistas para atacar un criptosistema, aunque casi siempre se utilizan combinaciones de ellas. En general las modernas técnicas de criptoanálisis suponen unos conocimientos matemáticos avanzados y utilizan mecanismos estadísticos, software y hardware muy sofisticados y en ocasiones muy caros.

1. Ataque a partir sólo del texto cifrado. El criptoanalista tan solo dispone de textos cifrados para obtener la clave. Todo sistema debe poder resistir este tipo de ataque, aún cuando el criptoanalista conozca la función de cifrado y el lenguaje del mensaje.
   En este método se utilizan estudios estadísticos de las características del texto cifrado, tales como distribución de caracteres, digramas, trigramas, etc.
2. Ataque a partir de algún mensaje conocido. El criptoanalista puede interceptar un texto cifrado y conocer la posición de determinadas palabras o grupos de palabras en el mismo. Se ataca el sistema mediante parejas mensaje-cifrado, dado m y c, se trata de deducir tal que .

3. Ataque por elección de mensaje. Este tipo de ataque se produce cuando el criptoanalista puede introducir mensajes en el criptosistema y ver el resultado del cifrado.

Un ejemplo de este tipo de ataque es el ataque mediante diccionario a las contraseñas cifradas de un sistema UNIX. El criptoanalista dispone de los textos cifrados y cifra toda una serie de textos en claro hasta encontrar uno que coincida con alguno de los cifrados.

7.5 TIPOS DE FUNCIONES CRIPTOGRAFICAS

SISTEMAS DE CIFRADO CLÁSICOS
Criptosistemas clásicos

Podemos considerar como criptosistemas clásicos aquellos que son anteriores al uso sistemático de los ordenadores en el campo de la criptografía.
Sus características fundamentales son su simplicidad y la facilidad para recordar los algoritmos y la clave. Dado que se aplicaban en el ámbito militar los mensajes tenían que poder cifrarse y descifrarse de modo rápido y sencillo. y el método utilizado debía ser fácil de recordar.

Estas características convertían a los sistemas en muy débiles y fáciles de atacar mediante métodos muy sencillos. Un ejemplo de criptoanálisis de un sistema por sustitución puede encontrarse en el relato "El escarabajo de oro" de Edgar Allan Poe.

Fundamentalmente podemos distinguir dos tipos de cifrado clásicos: por transposición y por sustitución.

Cifrados por transposición (o permutación)
Se reordenan los bits, caracteres o bloques de caracteres del texto en claro para obtener el texto cifrado.

El ejemplo más sencillo de este tipo de sistema es el método de transposición simple, en el que se cambian las posiciones de las letras en bloques sucesivos de texto.

Cuando este sistema se aplica en ordenadores, el dispositivo encargado de permutar cada bloque de texto suele denominarse P-box (Permutation box).
Otro ejemplo de este sistema es el denominado de transposición por columnas. En este se dispone el texto por filas de una determinada longitud, rellenándose el final de la última fila con un carácter cualquiera. El texto cifrado se obtiene leyendo la matriz resultante por

columnas. La clave de descifrado es simplemente el número de columnas utilizado.
EN UN LUGAR DE LA MANCHA

E	**N**	**U**
N	**L**	**U**
G	**A**	**R**
D	**E**	**L**
A	**M**	**A**
N	**C**	**H**
A	**X**	**X**

ENGDANANLAEMCXUURLAHX

Cifrados por sustitución.
Se reemplazan bits, caracteres o bloques de caracteres del texto en claro por otros en el texto cifrado.

La versión más sencilla de este tipo de método es el denominado cifrado por sustitución simple o monoalfabeto. En este sistema cada carácter del texto en claro es siempre sustituido por un mismo carácter en el texto cifrado
Un caso especial de sustitución simple es el cifrado Cesar, en el que como ya vimos cada carácter es sustituido por el situado 3 posiciones por delante en el alfabeto.
EN UN LUGAR DE LA MANCHA
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
\- -
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
HP XP ÑXJDU GH ÑD ODPFKD

Otra modalidad de sistema por sustitución es el cifrado por sustitución polialfabeto. En este, cada carácter del texto en claro es sustituido por un carácter distinto en el texto cifrado cada vez que aparece. En la práctica se utiliza un número limitado de alfabetos de modo que cada vez que aparece el carácter en el texto en claro se usa cíclicamente uno de los alfabetos.

La máquina Enigma utilizaba un sistema de sustitución polialfabeto para cifrar los textos.

Un ejemplo de sistema de cifrado polialfabeto es el Método de Vigenére. En este sistema se utiliza como clave una palabra cuyas letras definen el desplazamiento de los distintos alfabetos a usar. Veámoslo con un ejemplo.

Supongamos que utilizamos como palabra clave SOL
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
alf. 1 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
alf. 2 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

alf. 3 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
Cifrado
Mensaje P L A N T A A T O M I C A
Clave S O L S O L S O L S O L S
Cifrado I Z L F I L S I Z E W N S

En general se representa la función de cifrado como siendo : desplazamiento del alfabeto i-ésimo, i:1, ..., m (m: longitud de la clave)
equivale al valor numérico de la i-ésima letra de la clave. : valor numérico de la j-ésima letra del alfabeto, j:1,.., n (n longitud del alfabeto)

Sistemas de cifrado modernos
Los sistemas criptográficos modernos se desarrollan con la aparición de los ordenadores, y basan su funcionamiento en la utilización de potentes y complejas herramientas hardware y software. Su funcionamiento no se basa en simples sustituciones o transposiciones. En lugar de ello, se utilizan claves secretas de gran longitud para controlar una compleja secuencia de operaciones con la información que pueden incluir tanto transposiciones como sustituciones. Su posibilidad de uso se basa en la potencia de los ordenadores, que permiten aplicar algoritmos de gran complejidad y coste en tiempos admisibles.
Los criptosistemas modernos pueden dividirse en dos grandes categorías en función del tipo y número de claves que utilizan:

- criptosistemas simétricos, también llamados de clave única o de clave privada.
- criptosistemas asimétricos, también llamados de clave pública o de dos claves.

Ambos sistemas tienen características bien diferenciadas, lo que define su uso para diferentes fines. De hecho ambos tipos de sistemas suelen combinarse para llevar a cabo distintas acciones y lograr ciertos objetivos de seguridad.
Además existe algún sistema adicional que no encaja bien en ninguna de las dos categorías anteriores, como es el denominado criptosistema one-time pad.

Criptosistemas de clave privada
En estos sistemas se utiliza la misma clave para el cifrado y para el descifrado. Esta clave se denomina clave privada (secreta o única) debido a que tan solo es conocida por el emisor y por el receptor del mensaje. Para que este tipo de sistema sea efectivo la clave debe ser mantenida en secreto por ambas componentes de la comunicación.

La seguridad de este tipo de sistemas depende totalmente del nivel de protección de la clave.
Un ejemplo clásico de criptosistema de clave privada es el DES (Data Encryption Standard) que describiremos con mayor detalle en un apartado posterior.
En este tipo de sistemas, el secreto (confidencialidad) y la autenticidad se obtienen al mismo tiempo.

Cuando se descifra un mensaje usando la clave privada, el hecho de que ésta sea tan solo conocida por el emisor y el receptor garantiza dos propiedades:
1. Que el mensaje no es inteligible por nadie más, es decir, que es confidencial.

2. Que si el texto descifrado es inteligible, sólo hay un emisor posible, aquel que conoce la clave privada. Esto garantiza la autenticidad del mensaje.

El problema fundamental de este tipo de criptosistema es la generación, almacenamiento y sobretodo el intercambio de claves. Todos estos procesos constituyen la denominada gestión de claves.

Las claves privadas deben intercambiarse de modo totalmente seguro, pues sobre ellas descansan todas las características de seguridad del sistema. Además, si cada pareja de usuarios necesita compartir una clave distinta, el número de éstas aumenta cuadráticamente con el número de usuarios. Si existen n usuarios, cada usuario necesita n-1 claves distintas para comunicarse con el resto. Así pues el total de claves involucradas, si todos los usuarios deben estar completamenteconectados, es de n*(n-1), esto es, de n2.

Criptosistemas de clave pública.
En este tipo de sistemas se utilizan dos claves: una clave pública y una clave privada. En un grupo de usuarios, cada uno de ellos posee dos claves distintas:
o La clave pública, K', como su propio nombre indica, puede ser conocida por todos los usuarios del sistema.
o La clave privada, K, tan solo es conocida por su propietario.

Aunque estas claves están relacionadas matemáticamente, la fortaleza del sistema depende de la imposibilidad computacional de obtener una a partir de la otra.
Este tipo de sistemas se denominan asimétricos porque no podemos usar una misma clave para cifrar y descifrar un mensaje. Ambas claves deben usarse en el proceso. Si ciframos un mensaje con una de ellas, debemos descifrarlo con la otra.
¿ Cómo usar ambas claves para obtener un sistema seguro?
Si un usuario (emisor) quiere enviar un mensaje secreto a otro (receptor), debe cifrarlo utilizando la clave pública del receptor.

El mensaje tan solo puede descifrarse utilizando la clave privada del receptor, con lo que se garantiza la confidencialidad del mismo. La clave pública del receptor no sirve para descifrar el mensaje, y por tanto tan solo el receptor (que es el único que conoce su propia clave privada), puede descifrarlo.
Por otra parte el mensaje NO es autentico. Dado que cualquier usuario puede conocer la clave pública del receptor, cualquier usuario puede ser el emisor del mensaje. La recepción de un mensaje cifrado con la clave pública del receptor no identifica unívocamente al emisor, y por tanto no lo autentifica.
Si el emisor quiere garantizar la autenticidad de un mensaje, debe cifrarlo con su clave pública.

El receptor podrá descifrarlo usando la clave pública del emisor. Dado que todo el mundo puede conocer la clave pública del emisor, no se garantiza la confidencialidad del mensaje. Cualquiera puede descifrarlo. Sin embargo, dado que tan solo el emisor conoce su propia clave privada, tan solo él puede ser el origen del mensaje, con lo que se garantiza la autenticidad del mismo.

Como hemos podido ver, en este tipo de sistemas el secreto y la autenticidad del mensaje se logran por separado. Tal y como veremos en el apartado dedicado a la firma digital, para lograr ambas características de seguridad es necesario combinar ambas claves y realizar un doble proceso de cifrado y descifrado.

Criptosistemas híbridos

Tanto la criptografía de clave pública como la de clave privada tienen sus ventajas y sus inconvenientes. Debido a ello se suelen utilizar para distintos fines, y por tanto los criptosistemas de clave pública no son un sustituto de los de clave privada.

Existen dos razones que hacen que la criptografía de clave pública sea poco adecuada para la transferencia de información cifrada:

1. Los algoritmos de clave pública son lentos. Normalmente son unas 1000 veces más lentos que los de clave privada.
2. Los algoritmos de clave pública son vulnerables a ataques mediante elección de mensaje. Dado que la clave pública es de dominio público, cualquiera puede tratar de cifrar todos los mensajes posibles y comparar los resultados con los textos cifrados. Esto es especialmente posible cuando la cantidad de mensajes posibles es limitada o se tiene alguna información adicional sobre su estructura o contenido.

Debido a las dos razones anteriores, la transferencia de información cifrada se suele realizar mediante criptosistemas de clave privada, mientras los de clave pública se reservan para funciones tales como la transferencia de claves.

Veamos un ejemplo práctico de como combinar ambos tipos de criptosistemas para lograr una transmisión segura.

La información a transferir se cifrara mediante un criptosistema de clave privada, y utilizará una clave de sesión. La clave de sesión será aleatoria y se utilizará tan solo en una transmisión. El criptosistema de clave pública se utilizará para la distribución segura de la clave. Dado un emisor S y un receptor R, los pasos a seguir son los siguientes.

1. El emisor S, envía al receptor su clave pública K's
2. El receptor R, genera aleatoriamente una clave de sesión X
3. El receptor R, cifra la clave de sesión mediante la clave pública de S
E(X, K's)
y se la envía a S
4. S descifra el mensaje mediante su clave privada y obtiene la clave de sesión
X=D(E(X, K's), Ks)
5. S y R utilizan la clave de sesión como clave privada para cifrar y transferir toda la información.

Claves de un solo uso

Los criptosistemas de clave de un solo uso (one-time pad) pueden considerarse los únicos irrompibles. Su enorme fortaleza recae en la enorme longitud de la clave y en que ésta tan solo se utiliza una vez.

La idea de estos sistemas es la siguiente. Para cifrar un mensaje dado, se genera aleatoriamente una clave de igual o mayor longitud que el mismo. La seguridad del sistema recae en la aleatoriedad de la clave, por lo que suelen utilizarse procesos de generación de números aleatorios basados en alguna fuente aleatoria natural, tal como el proceso de radiación de ciertos materiales.

El emisor y receptor del mensaje comparten una única copia de la clave, y en este punto recae el problema del sistema, en la distribución segura de la misma.
El proceso de cifrado y descifrado queda representado en la siguiente figura.

La propiedad en la que se basa este criptosistema es bastante simple: la doble aplicación de la función XOR nos lleva al dato original:
(A XOR B) XOR B = A

Si se intenta atacar este sistema mediante fuerza bruta, esto es, probando todas las claves posibles, llegaremos a una situación bastante curiosa. Aunque la enorme longitud de la clave impide la implementación material de este sistema, ocurre además que dada una clave adecuada, a partir del mismo texto cifrado podemos llegar a cualquier mensaje descifrado que queramos. De este modo cualquier mensaje descifrado es igualmente posible, con lo que un ataque por fuerza bruta es complemente inútil.

7.6 DES Y TRIPLE DES

DES (Data Encryption Standard) es un esquema de encriptación simétrico desarrollado en 1977 por el Departamento de Comercio y la Oficina Nacional de Estándares de EEUU en colaboración con la empresa IBM, que se creó con objeto de proporcionar al público en general un algoritmo de cifrado normalizado para redes de ordenadores. Estaba basado en la aplicación de todas las teorías criptográficas existentes hasta el momento, y fué sometido a las leyes de USA.
Posteriormente se sacó una versión de DES implementada por hardware, que entró a formar parte de los estándares de la ISO con el nombre de DEA.

Se basa en un sistema monoalfabético, con un algoritmo de cifrado consistente en la aplicación sucesiva de varias permutaciones y sustituciones. Inicialmente el texto en claro a cifrar se somete a una permutación, con bloque de entrada de 64 bits (o múltiplo de 64), para posteriormente ser sometido a la acción de dos funciones principales, una función de permutación con entrada de 8 bits y otra de sustitución con entrada de 5 bits, en un proceso que consta de 16 etapas de cifrado.

En general, DES utiliza una clave simétrica de 64 bits, de los cuales 56 son usados para la encriptación, mientras que los 8 restantes son de paridad, y se usan para la detección de errores en el proceso.

Como la clave efectiva es de 56 bits, son posible un total de 2 elevado a 56 = 72.057.594.037.927.936 claves posibles, es decir, unos 72.000 billones de claves, por lo que la ruptura del sistema por fuerza bruta o diccionario es súmamente improbable, aunque no imposible si se dispone de suerte y una grán potencia de cálculo.

Los principales inconvenientes que presenta DEs son:

- Se considera un secreto nacional de EEUU, por lo que está protegido por leyes específicas, y no se puede comercializar ni en hardware ni en sofware fuera de ese país sin permiso específico del Departamento de Estado.
- La clave es corta, tanto que no asegura una fortaleza adecuada. Hasta ahora había resultado suficiente, y nunca había sido roto el sistema. Pero con la potencia de cálculo actual y venidera de los computadores y con el trabajo en equipo por Internet se crée que se puede violar el algoritmo, como ya ha ocurrido una vez, aunque eso sí, en un plazo de tiempo que no resultó peligroso para la información cifrada.
- No permite longitud de clave variable, con lo que sus posibilidades de configuración son muy limitadas, además de permitirse con ello la creación de limitaciones legales.
- La seguridad del sistema se ve reducida considerablemente si se conoce un número suficiente textos elegidos, ya que existe un sistema matemático, llamado Criptoanálisis Diferencial, que puede en ese caso romper el sistema en 2 elevado a 47 iteraciones.

Entre sus ventajas cabe citar:

- Es el sistema más extendido del mundo, el que más máquinas usan, el más barato y el más probado.
- Es muy rápido y fácil de implementar.
- Desde su aparición nunca ha sido roto con un sistema práctico.

Actualmente DES ya no es estándar y fué roto en Enero de 1999 con un poder de cómputo que efectuaba aproximadamente 250 mil millones de ensayos en un segundo.

Triple DES

Como hemos visto, el sistema DES se considera en la actualidad poco práctico, debido a la corta longitud de su clave. Para solventar este problema y continuar utilizando DES se creó el sistema Triple DES (TDES), basado en tres iteraciones sucesivas del algoritmo DES, con lo que se consigue una longitud de clave de 128 bits, y que es compatible con DES simple.

Este hecho se basa en que DES tiene la característica matemática de no ser un grupo, lo que implica que si se encripta el mismo bloque dos veces con dos llaves diferentes se aumenta el tamaño efectivo de la llave.

Para implementarlo, se toma una clave de 128 bits y se divide en 2 diferentes de 64 bits, aplicándose el siguiente proceso al documento en claro:

1. Se le aplica al documento a cifrar un primer cifrado mediante la primera clave, C1.
2. Al resultado (denominado ANTIDES) se le aplica un segundo cifrado con la segunda clave, C2.
3. Y al resultado se le vuelve a aplicar un tercer cifrado con la primera clave, C1.

Si la clave de 128 bits está formada por dos claves iguales de 64 bits (C1=C2), entonces el sistema se comporta como un DES simple.
Trás un proceso inicial de búsqueda de compatibilidad con DES, que ha durado 3 años, actualmente TDES usa 3 claves diferentes, lo que hace el sistema mucho más robusto, al conseguirse longitudes de clave de 192 bits (de los cuales son efectivos 168), mientras que el uso de DES simple no está aconsejado.

7.7 IDEA

Sistema criptográfico simétrico, creado en 1990 por Lai y Massey, que trabaja con bloques de texto de 64 bits, operando siempre con números de 16 bits usando operaciones como OR-Exclusiva y suma y multiplicación de enteros.

El algoritmo de desencriptación es muy parecido al de encriptación, por lo que resulta muy fácil y rápido de programar, y hasta ahora no ha sido roto nunca, aportando su longitud de clave una seguridad fuerte ante los ataques por fuerza bruta (prueba y ensayo o diccionarios).

Este algoritmo es de libre difusión y no está sometido a ningún tipo de restricciones o permisos nacionales, por lo que se ha difundido ámpliamente, utilizándose en sistemas como UNIX y en programas de cifrado de correo como PGP.

El futuro estándar.
El NIST de EEUU, en busca de un nuevo sistema de encriptación simétrico que reuna las características funcionales y de seguridad necesarias, decidió convocar en 1977 un concurso a nivel mundial, invitando a los principales desarrolladores de este tipo de sistemas a crear un algoritmo que pueda ser tomado como estándar para los próximos años.

Este nuevo sistema de llamará AES (Advanced Encryption Standard), y el algoritmo que utilice se denominará AEA (Advanced Encryption Algorithm).
A este concurso se presentaron numerosos autores, y trás un largo proceso de selección el

ha seleccionado como futuro estándar el denominado Rijndael, creado por los belgas Vincent Rijmen y Joan Daemen.

Rijndael es un cifrador de bloque que opera con bloques y claves de longitudes variables, que pueden ser especificadas independientemente a 128, 192 ó 256 bits.

El resultado intermedio del cifrado se denomina Estado, que puede representarse como una matriz de bytes de cuatro filas.

A partir de ésta base se realilza una serie de bucles de cifrado, cada uno de ellos consistente en las siguientes operaciones:
1. Sustitución de bytes no lineal, operando independientemente sobre cada uno de los bytes del Estado.
2. Desplazamiento de las filas del Estado cíclicamente con offsets diferentes.
3. Mezcla de columnas, que se realiza multiplicando las columnas del Estado módulo x4+1, consideradas como polinomios en GF(28), por un polinomio fijo c(x).
4. Adición de la clave de vuelta, en la que se aplica al Estado por medio de un simple XOR. La clave de cada vuelta se deriva de la clave de cifrado mediante el esquema de clave.

El esquema de clave consiste en dos operaciones, expansión de clave y selección de clave de vuelta de cifrado, y el proceso de cifrado consta de tres pasos: una adición inicial de la clave de vuelta, n-1 vueltas de cifrado y una vuelta final.

Otra buena demostración del proceso de cifrado que efectúa Rijndael lo tenéis en este enlace, en el que de nuevo Don José de Jesús Ángel Ángel, de la empresa Seguridata, lo explica estupendamente.

7.8 SKIP JACK/BLOWFISH

Skipjack fue desarrollado por la NSA inicialmente para los chips Clipper y Capstone. Su diseño comenzó en 1985 y se completó su evaluación en 1990. Digamos algo más sobre los chips antes de comenzar con la descripción del algoritmo.

El chip Clipper
Este chip, también conocido como MYK-78T , de diseño anti - manipulaciones (tamper-proof) del tipo VLSI, fue pensado para encriptar mensajes de voz. Lo manufactura VLSI Technologies y Mykotronx, Inc lo programa.

El aspecto más controvertido del chip es, por supuesto, el protocolo de depósito de claves. Cada chip tiene una clave especial que no se usa para los mensajes, sino para encriptar una copia de la clave que el usuario utiliza para sus mensajes. Como parte del proceso de sincronización, el Clipper emisor genera y envía un "Law Enforcement Access Field

(LEAF)" al Clipper receptor. El LEAF contiene una copia de la clave de sesión actual encriptada con una clave especial llamada unit key. Esto permite a un 'cotilla' del gobierno de EE.UU. recuperar la clave de la sesión y en consecuencia toda la conversación.

Supuestamente el chip resistiría un intento de ingeniería inversa por un adversario sofisticado y con bastante dinero; pero se rumorea que en los Laboratorios Nacionales Sandia ya se ha hecho. Incluso aunque no fuera así, es de suponer que los mayores fabricantes de chips podrían realizar la ingeniería inversa de Clipper. Es sólo cuestion de tiempo que aparezca alguien con la combinación adecuada de recursos y (falta de) ética.

El chip Capstone. Capstone, también conocido como MYK-80, es también un chip VLSI que implementa el EES (Escrowed Encryption System) e incorpora las siguientes funciones:
o Uso del algoritmo Skipjack
o Un algoritmo de intercambio de claves públicas (KEA)
o Un algoritmo de firma digital (DSA)
o El algoritmo de hash seguro (SHA)
o Un algoritmo de uso común de tipo exponencial
o Un algoritmo de generación de números aleatorios que utiliza una fuente pura de ruido.

Capstone proporciona las funcionalidades criptográficas necesarias para el comercio electrónico y otras aplicaciones basadas en el ordenador. La primera aplicación del chip Capstone fue la tarjeta Fortezza.

El algoritmo
Siguiendo con Skipjack, decir que es un cifrado simétrico que usa bloques de 64 bits y una clave de 80 bits. Como queda dicho se usaba en el programa Clipper, pero no tenía el depósito de claves (key escrow) incorporado (el depósito de claves era parte del mecanismo de intercambio de claves y no del cifrado de datos).

Es un algoritmo de alto riesgo, lo que quiere decir que había un elevado riesgo de que fuera comprometido. Por tanto, es improbable que la NSA ponga en él sus diseños mas secretos (o inteligentes).

Es más lento que Blowfish y alguna de las propuestas AES, pero aún así es el doble de rápido que DES en micros de 32 bits. Es rápido cuando se usa en tarjetas inteligentes y eficiente en hardware. Tampoco lleva tiempo la preparación de la clave. Si no fuera por que el tamaño de la clave es pequeño (80 bits), podríamos tenerlo en cuenta para nuestras aplicaciones.

Skipjack es interesante sobre todo por su diseño. Es el primer algoritmo desarrollado por la NSA que podemos ver. La criptografía es una ciencia de adversarios. Alguien diseña un algoritmo, yo lo rompo. Yo diseño otro; alguien más lo rompe. Así es como aprendemos. Skipjack es un buen blanco, es un algoritmo diseñado usando metodologías secretas por una organización respetada.
Skipjack es una red no equilibrada de Feistel (específicamente una construcción incompleta), pero es obviamente un producto de la criptografía militar. La criptografía

académica esta basada fundamentalmente en el trabajo de Feistel a mediados de los 70 en IBM: redes SP y redes de Feistel. La criptografía militar comenzó con maquinas de rotor, y luego se generalizó a los registros de desplazamiento (shift registers). El diagrama de bloques y la descripción de Skipjack muestran claramente sus raíces en los registros de desplazamiento. Resulta fascinante que las dos formas de diseño estén convergiendo.

Lo primero que se observa en Skipjack es su simplicidad. Hay pocos elementos de diseño, y pensándolo un poco puedes señalar cada uno de ellos y explicar porqué está allí. No hay constantes misteriosas. Hay 32 rondas y 32 rondas pueden esconder un montón de fallos, pero el diseño parece sólido.
Y a la vez muy frágil. Algunos algoritmos son fuertes porque son de un tipo fuerte de algoritmo. Los algoritmos similares también serán fuertes, pero Skipjack no es así, es un único algoritmo fuerte en un mar de mediocridad. Haz casi cualquier modificación a Skipjack, incluso una pequeña y el resultado puede romperse.

Podemos prever que los trabajos de criptoanálisis más interesantes vendrán del criptoanálisis de variantes de Skipjack.
Algunas personas ya intentan criptoanalizar Skipjack. Sobre todo hemos visto rupturas de versiones modificadas del algoritmo, junto con explicaciones de por qué el ataque no funcionaría contra Skipjack propiamente dicho. Y Skipjack con menos rondas puede romperse, pero eso era de esperar.
Finalmente, Skipjack no es una propuesta para AES (Advanced Encription System), no cumple las condiciones. AES será un cifrado de bloques de 128 bits; Skipjack usa 64 bits. AES podrá utilizar claves de 128, 192 y 256 bits frente a los 80 bits de Skipjack. Creo que podría incrementarse el tamaño de bloque que utiliza Skipjack sin afectar a la seguridad; pero no hay una forma obvia de incrementar la longitud de la clave del algoritmo.

La desclasificación de Skipjack.
La NSA ha desclasificado Fortezza. Específicamente, han desclasificado Skipjack y KEA (un algoritmo para intercambio de claves públicas). SHA-1 (una función hash) y DSA (digital signature algorithm) son también parte de Fortezza pero ya eran públicos.
No lo hicieron para ayudar a la industria ni a los criptógrafos ni a nadie. Lo hicieron para ayudarse a sí mismos porque tenían que protegerse de una equivocación.
DMS (Defense Messaging System) es un sistema clasificado de mensajes por ordenador; más o menos como el e-mail, que utiliza tarjetas Fortezza PCMIA como medida de seguridad. Como algunos de los algoritmos de Fortezza estaban clasificados, las tarjetas con Fortezza tenían todos los controles físicos y características de resistencia a la manipulación que se necesitaban para proteger dichos algoritmos.

Dentro de los protocolos DMS no hay manera de tener varios cifrados diferentes. S/MIME por ejemplo, define múltiples algoritmos, hay una variable en el mensaje S/MIME que dice al receptor qué algoritmos fueron utilizados para encriptar ese mensaje en particular.
El problema surgió porque la NSA no podía instalar tarjetas Fortezza y lectores lo suficientemente deprisa. No sé si eran demasiado caras (*son* caras), si no podían aumentar la producción a suficiente velocidad o si instalar la infraestructura (lectores de tarjetas PCMCIA etc.) era demasiado problema para ellos. Estoy seguro de que contaban con tener lectores de PCMCIA en todos los ordenadores.

Cualquiera que fuera la causa, la mayoría de la gente que necesitaba participar en DMS no tenía el hardware necesario. Si pudieran establecer un conjunto de algoritmos alternativos en DMS, entonces podrían distribuir una versión sólo de software con algoritmos no clasificados: triple-DES, Diffie-Hellman, etc. Cada terminal sabría si estaba comunicándose con un DMS con Fortezza habilitada o con un DMS sólo software y el problema desaparecería. Pero el DMS no podía permitir esto, o usas Skipjack/KEA o nada. Así que o eliminaban el cifrado o pasaban los algoritmos clasificados a software.

Una vez que haces eso, también podrías desclasificarlo. El comportamiento del gobierno de EE.UU. ha sido simplemente hacer de la necesidad virtud.

Algoritmo de Encriptación Blowfish

Blowfish es un codificador simétrico de bloques. Toma una clave de longitud variable, entre 32 y 448 bits.

7.9 FORTALEZA DE LOS ALGORITMOS

Hemos visto cómo la criptografía nos proporciona medios para poder comunicarnos de forma segura con otras personas a través de redes de todo tipo. Vamos a ver ahora hasta dónde llega esa seguridad y qué podemos hacer para aumentarla.

Puesto que los sistemas criptográficos se basan en algoritmos matemáticos y en el uso de claves, los primeros aspectos a considerar serán la seguridad del algoritmo y la fortaleza de la clave.

En general los sistemas simétricos son, a igualdad de longitud de clave, más seguros que los asimétricos, ya que se suelen basar en procedimientos como la trasposición y la permutación, que son más dificiles de romper, si están bien construidos, que los sistemas basados en funciones matemáticas.

Ahora bien, no todos los sistemas criptográficos simétricos tienen algoritmos de igual nivel de seguridad, por lo que conviene que antes de decidirnos por implementar en nuestro sistema de comunicaciones alguno de ellos comprobemos antes que es un sistema conocido y de probada seguridad, rechazando criptosistemas débiles o poco ensayados.

Y lo mismo cabe decir de los algoritmos de clave pública.

En cuanto a la longitud de las claves, para los sistemas de clave pública como RSA la longitud de clave recomendada es de 1024 bits. Para los sistemas simétricos las longitudes

recomendadas son:
· DES: al menos 56 bits, siendo el tamaño óptimo de 128 bits.
· TDES: 168 bits.
· RC4: 128 bits.

Elección de claves.
Las aplicaciones de encriptación pueden estar basadas bien en sistemas que permiten al usuario elegir sus claves, bien en otros que se encargan de hacerlo ellos.
Los sitemas que permiten al usuario elegir sus claves suelen ser poco confiables, ya que para que una clave sea fuerte ante el criptoanálisis precisa no sólo ser de un tamaño adecuado, si no también haber sido elegida con mucho cuidado.

Es normal que las personas elijan claves basadas en su nombre, apellidos, fecha de nacimiento, matrícula del automovil, etc. Estas, por su propia constitución, son inapropiadas, ya que lo primero que suele hacer el que busca nuestras claves es someter el sistema a un ataque basado en fuerza bruta (prueba con generadores de palabras, números o mezcla de ambos), basado en la prueba de miles y miles de palabras comunes en un idioma (ataques de diccionario) o en palabras comunes en el entorno de la persona propietaria de las mismas (basado en asociación de ideas).

En el caso de que tengamos que elegir nosotros las claves debemos procurar mezclar en ellas letras y números, creando una palabra o frase que no tenga ningún sentido en el mundo real, y con la máxima extensión permitida por el algoritmo. Y debemos también procurar escoger una clave diferente para cada algoritmo, para evitar depositar toda nuestra seguridad en una única clave.

Por otra parte, en los sistemas en los que es la propia aplicación de seguridad la que fija las claves hay que tener en cuenta que estas se obtienen mediante sistemas de generación de números aleatorios, por lo que es muy importante que dichos números sean en realidad aleatorios, para que las claves que genere para dos usuarios distintos no coincidan.

Puede parecer extraño que se produzca esta coincidencia, pero es que en realidad la mayoría de los programas de generación lo que sacan en realidad son números pseudoaleatorios, ya que se basan para empezar en unas series especiales llamadas semillas.

Es por tanto responsabilidad fundamental del usuario elegir software de seguridad que contemple este aspecto a fondo.

Conservación de las claves.
Si las claves criptográficas son tan importantes, sería normal que las mantuvieramos protegidas de miradas indiscretas, pero muchas veces no es así.
Como norma general, deberemos tener todas nuestras claves en un fichero especial, que debe estar encriptado a su vez con una clave simétrica que conozcamos sólo nosotros. Para elegir esta clave hay que tener en cuanta las recomendaciones vistas en el punto anterior.

Esta consideración debe ser especialmente aplicada en el caso de las claves privadas de sistemas asimétricos, ya que de ellas dependerán elementos tan importantes como nuetra

firma digital. Una suplantación de nuestra personalidad mediante la firma de un documento comprometido puede resultar una verdadera catástrofe para nosotros.

La cosa no acaba ahí, ya que el fichero de claves es suceptible de multiud de ataque diferentes estando en un ordenador conectado a una red, y sobre todo, a Internet. Ataques de este tipo pueden ser la introducción en nuestro sistema de un troyano, como BackOrifice o NetBus, que puden capturar tanto el fichero de claves como éstas en sí en el momento de ser utilizadas. Eso sin contar con ataques mucho más sencillos, como el acceso directo a nuestro equipo por parte de alguna de las personas conectadas a nuestra propia red local o de nuestra propia empresa.

La llave privada sólo debe encontrarse desencriptada cuando está en la RAM de nuestro ordenador, y sólo mientras está funcionando el programa de seguridad, y la forma más segura de protegerla es firmar y abrir ficheros encriptados en una computadora aislada física y virtualmente del mundo exterior.