

**SEGURIDAD EN LA RED:  
FIREWALLS Y ENCRIPCIÓN**

*ARISO*

*Alumnes:*

*JUAN ANTONIO FERNÁNDEZ*

*ALEJANDRO RÍOS BLANCO*

*Diciembre del 2001.*

## Introducción a la seguridad.

Con la introducción de los computadores, la seguridad de la información dentro de una organización, en las últimas décadas, ha sufrido, básicamente, dos cambios.

Antes de la aparición de los equipos procesadores de datos, esta seguridad, se conseguía fundamentalmente, mediante medios físicos, por ejemplo, el almacenamiento de documentos confidenciales en cajas fuertes con combinaciones de apertura, y mediante medios administrativos, como son los medios de investigación de personal en la fase de contratación.

Con la llegada de los computadores, eran necesarias herramientas “automáticas” para proteger ficheros e informaciones almacenadas en memoria, como en el caso de sistemas multiusuarios, pero podemos considerar como crítica la situación en la cual se puede acceder a la información mediante teléfonos públicos o redes de datos.

El segundo cambio, es la facilidad de comunicación existente, para el transporte de datos entre terminales de usuario y computadores, y de computador a computador. Estas medidas de seguridad, a nivel de red, son necesarias para proteger los datos durante la transmisión y garantizar la autenticidad de los datos transmitidos.

## Requisitos de la seguridad.

La seguridad en los computadores y en redes implica cumplir tres exigencias:

- *Secreto* : Implica que la información solo sea accesible por las personas autorizadas.
- *Integridad* : Los recursos de un computador únicamente sean modificados por entes autorizados.
- *Disponibilidad* : Los recursos de un computador estén disponibles a los entes autorizados.

## Amenazas de la seguridad.

La conexión de un sistema a Internet, se expone a numerosas amenazas de seguridad que aumentan día a día. Existen diversos tipos de amenazas, que podemos clasificar en cuatro tipos diferenciados:

- Vulnerabilidad de los datos.
- Vulnerabilidad del software.
- Vulnerabilidad física del sistema.
- Vulnerabilidad de la transmisión.

Los tipos y estilos de ataques son fácilmente definibles. Podemos encontrar nueve tipos básicos de ataques que se pueden llevar a cabo contra las redes conectadas a Internet:

- Basados en contraseñas.
- Interceptación de paquetes
- Ataques a accesos de confianza
- Uso de direcciones IP falsas
- Ataques de Ingeniería social.
- Predicción de números de secuencias
- Secuestro de sesiones.
- Ataques dirigidos a aprovechar los puntos vulnerables de la tecnología.
- Ataques dirigidos a aprovechar las bibliotecas compartidas.

A continuación explicaremos brevemente estos distintos estilos:

Los **ataques basados en las contraseñas** son los ataques a computadoras más clásicos. Inicialmente, el acceso se intentaba, mediante un identificador de acceso y una contraseña, probando una y otra vez hasta que encontraba la contraseña correcta. De aquí, pronto comenzó una nueva modalidad del ataque, *ataque basados en diccionario*, se trata de ataques automatizados a las contraseñas mediante el uso de un programa que recorre todo un diccionario.

La **Intercepción de paquetes (packet sniffer)**, es el más difícil de todos los ataques, y una amenaza seria para el comercio en Internet. Ya que pueden interceptar todo tipo de paquetes, desde los mensajes de inicio de sesión, transmisiones de los números de las tarjetas de crédito, correo electrónico... una vez capturado el paquete, se puede usar y leer toda la información contenida en él, como puede ser el nombre del host, nombre de usuario y la contraseña asociada al paquete. Normalmente, este tipo de ataque es el previo para el posterior ataque usando direcciones IP falsas.

El **ataque basado en acceso de confianza**, este tipo de ataque son especialmente usados, especialmente sobre sistemas UNIX, ya que sus mecanismos de confianza<sup>1</sup> son especialmente débiles. Con lo que los hackers pueden acceder al sistema simplemente con averiguar el nombre de una máquina de confianza.

Las **direcciones IP falsas** como hemos comentado anteriormente, entre los datos que envía un ordenador a otro, se incluye tanto la identidad del emisor como la del receptor. Con lo que el hacker utiliza este sistema para atacar su red proporcionando una información falsa acerca de la identidad de su ordenador. De esta forma tiene acceso a los paquetes entrantes (no a los salientes) en los sistemas y a los servicios de los mismos. Debemos tener en cuenta, que todas las respuestas a consultas y peticiones no llegarían al intruso, sino al host que se pretende emular.

Los **ataques de Ingeniería social** son cada vez más habituales y peligrosos, ya que cada vez se conectan más personas a Internet y a redes internas. Se trata de enviar un correo al usuario, fingiendo ser el administrador del sistema, para que este le comunique su password. Todo dependerá de la ignorancia del usuario acerca de ordenadores y de redes.

**Predicción de números de secuencia** es una técnica habitual para falsificar direcciones IP en redes UNIX.

El **secuestro de sesiones** es más popular que el de falsificación de direcciones IP. Se debe a que permite importar y exportar datos del sistema. Este tipo de ataque, más sencillo que el de predicción de números de secuencia, se establece siempre que el intruso encuentra una conexión entre servidor y cliente, y al penetrar a través de encaminadores desprotegidos o firewalls poco adecuados, y este detecta los números de secuencia entre usuarios. El intruso se apodera de las direcciones de un usuario legítimo, el usuario secuestra su sesión, para lo cual simula los números de la dirección del usuario. Después, el anfitrión desconecta al usuario legítimo y el intruso obtiene libre acceso a los archivos a los que podía acceder el usuario.

Los **ataques dirigidos a aprovechar los puntos vulnerables de la tecnología**, todos los sistemas operativos principales tienen sus puntos débiles. Algunos más accesibles que otros. Por otro lado, la probabilidad de que un hacker encuentre algún punto débil es extremadamente reducida.

Los **ataques dirigidos a aprovechar las bibliotecas compartidas**, utilizan bibliotecas<sup>2</sup> compartidas que suelen encontrarse en Unix. Los hackers reemplazan estos archivos por nuevos programas que les servirán a sus propósitos, como permitirles el acceso privilegiado.

A continuación comentaremos dos de los métodos de seguridad más empleados, aunque podemos destacar que son básicos.

## Firewalls

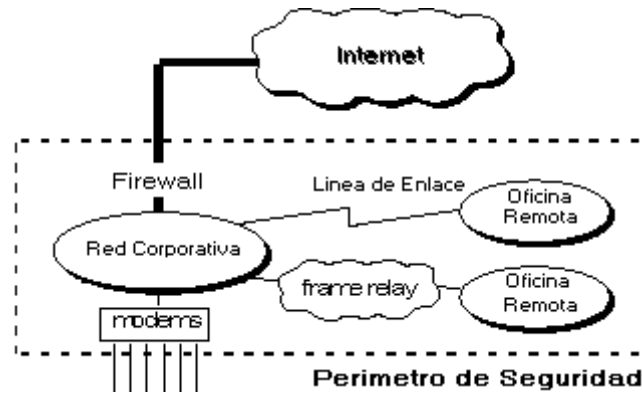
Debemos tener en cuenta que un firewall debería ser la base del sistema de seguridad de cualquier red que se conecte con Internet. Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cual de los servicios de red pueden ser accedidos desde dentro de esta por los que están fuera, es decir quien puede

---

<sup>1</sup> En un S.O. Unix los usuarios pueden crear archivos de host de confianza (los archivos .rhost de los directorios personales) en la cual se incluyen los nombres de los hosts o las direcciones desde las que un usuario puede acceder sin nombre de usuario ni contraseña. Se pueden conectar desde un dominio de confianza usando únicamente el comando rlogin y los argumentos adecuados.

<sup>2</sup> Conjunto de funciones comunes para los programas que el sistema operativo en RAM desde un archivo cada vez que lo solicita un programa.

entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración. desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.



### Beneficios de un firewall en Internet

Los firewalls en Internet administran los accesos posibles del Internet a la red privada. Sin un firewall, cada uno de los servidores propios del sistema se expone al ataque de otros servidores en el Internet. Esto significa que la seguridad en la red privada depende de la resistencia que puede tener cada servidor y es únicamente seguro tanto como la seguridad en la fragilidad posible del sistema.

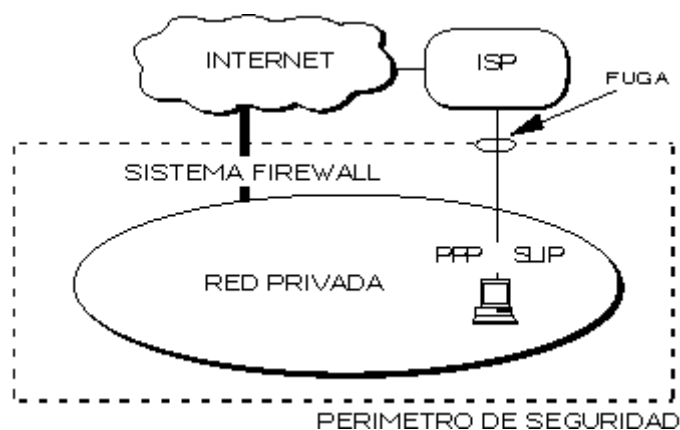
El firewall permite al administrador de la red definir un punto de choque, manteniendo al margen los usuarios no autorizados fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles. Uno de los beneficios clave de un firewall en Internet es que ayuda a simplificar los trabajos de administración, una vez que se consolida la seguridad en el sistema firewall, es mejor que distribuirla en cada uno de los servidores que integran nuestra red privada.



### Limitaciones de un firewall

Un firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación. Por ejemplo, si existe una conexión dial out sin restricciones que permita entrar a nuestra red protegida, el usuario puede hacer una conexión SLIP o PPP al Internet. Los usuarios con sentido común suelen "molestarse" cuando se requiere una autenticación adicional requerida por un Firewall Proxy server (FPS) lo cual se puede ser provocado por un sistema de seguridad circunvecino que esta incluido en una conexión directa SLIP o PPP del ISP.

Este tipo de conexiones derivan la seguridad provista por firewall construido cuidadosamente, creando una puerta de ataque.



Trataremos los tipos de Firewalls y sus características. Básicamente lo podemos definir con los siguientes conceptos básicos:

- ◆ Combina hardware y software para proteger de un acceso no autorizado.
- ◆ Debemos tener en cuenta que un firewall no impide la entrada de virus informáticos a la red.
- ◆ Existen tres principales tipos de firewalls:
  - A nivel de red.
  - A nivel de aplicación.
  - A nivel de Circuito.
- ◆ Las tres arquitecturas de firewalls más populares son:
  - Firewalls doble.
  - Firewalls de host protegido.
  - Firewalls de subred protegida.

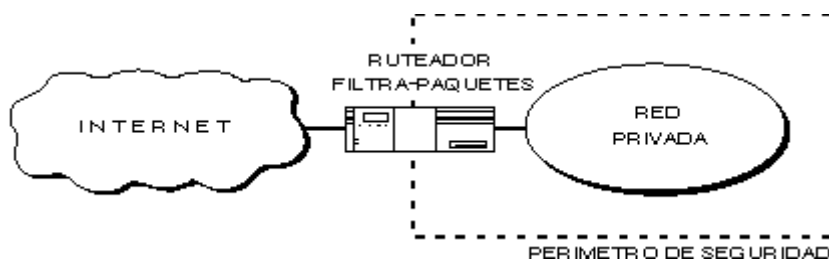
### Proteger la red frente a los intrusos del exterior.

Como ya sabemos, muchas empresas proporcionan acceso a Internet a sus empleados. Si los empleados, pueden acceder a Internet, la conexión de la empresa debería realizarse a través de un firewall. Un firewall combina hardware y software para asegurar la interconexión de dos o más redes. Y proporciona una localización central para controlar la seguridad.

### Principales tipos:

#### **Firewall a nivel de red.**

Suele ser un ordenador especial que examina las direcciones de los paquetes para determinar si el paquete debe pasar a la red local o debe impedirle el acceso. El firewall utiliza la información contenida en el header del paquete para controlar el acceso del mismo.



Como ejemplo, podríamos configurar un firewall para que bloquee todos los mensajes que provengan de un sitio determinado, así como todos los paquetes destinados a esa dirección. Para el funcionamiento del mismo, debemos indicar al encaminador que deseamos bloquear los paquetes con información que contenga la dirección de los sitios (de destino). Con este sistema podemos bloquear todo un sitio, es decir, toda una red entera, pero no un único usuario o un ordenador concreto de otra red.

Según hayamos construido el archivo del encaminador, podrá reconocer y realizara las acciones específicas para cada uno de los tipos incluidos en él. Podríamos programarlos para permitir que los usuarios puedan acceder a Internet pero no pueda acceder a sitios usando FTP y transferir archivos a su servidor. O incluso para que pueda descargar archivos, pero en cambio, no pueda transferir archivos al servidor. Normalmente se suele configurar para que tenga en cuenta:

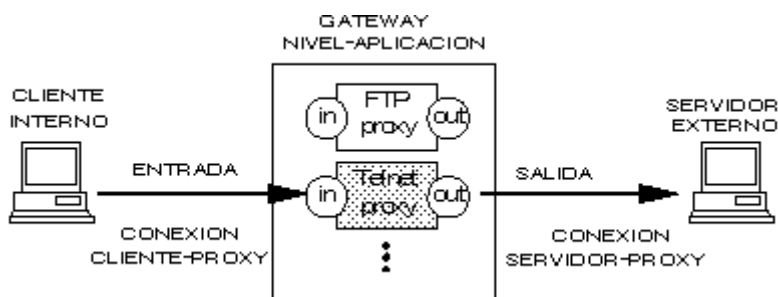
- Dirección de origen/destino de los datos.
- Protocolo de sesión de los datos. TCP, UDP o ICMP.
- Si el paquete es el inicio de una petición de conexión.
- El puerto de aplicación de origen/destino del servicio deseado.

Este tipo es muy rápido y casi totalmente transparente para los usuarios.

### Firewall a nivel de aplicación.

Normalmente llamado servidor proxy, estos servidores controlan el tráfico entre dos redes, es decir, se comunican con los servidores del exterior de la red en nombre de los usuarios. Por ejemplo, un usuario de una red que acceda a Internet a través del proxy, aparecerá a los otros ordenadores como si en realidad fuera el servidor proxy.

Como ejemplo, en la ilustración mostramos un **telnet-proxy**.



Cuando utilizamos este tipo de firewall, la red local no se conecta con Internet. En lugar de conectarse, el tráfico que fluye de una red a otra nunca interactúa con el tráfico de la otra red (ya que los cables de red no están en contacto). El servidor transmite de una red a otra una copia aislada de cada paquete autorizado. Estos firewalls enmascaran el origen de la conexión inicial y protegen la red frente a los usuarios de Internet que intentan recopilar información de su red privada.

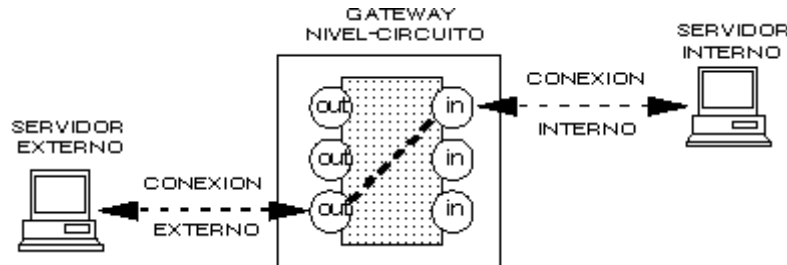
Ya que también reconoce los protocolos de red, podemos configurarlo para controlar los servicios que deseamos que proporcione la red, de igual modo que programaríamos un encaminador.

Debemos tener en cuenta que nuestros usuarios de red, utilicen programas clientes que puedan trabajar con proxy.

También debemos tener en cuenta que es un programa el que analiza la validez o no de los paquetes transmitidos, con lo que el rendimiento de la red, se ve notablemente reducido.

### Firewalls a nivel de circuito.

Similar al anterior tipo, ya que ambos son proxies. Debemos tener en cuenta que los firewalls a nivel de aplicación requieren la utilización de software de proxy especial para cada servicio que se desee incluir en la red, como FTP o HTTP.



Por el contrario este tipo de firewalls crea un circuito entre el cliente y el servidor sin necesidad de que la aplicación sepa nada del servicio. Protegen el inicio de la transacción sin interferir en la transacción que se está realizando. La principal ventaja reside en que proporciona servicios para una gran variedad de protocolos.

### Arquitecturas de firewalls.

Como ya hemos comentado anteriormente, existen tres tipos de arquitecturas que son las más populares, según las necesidades en tema de seguridad de red. Estas son *mediante host de doble conexión* (usa dos tarjetas de red separadas), *mediante filtrado de host* y *mediante filtrado de subred* (utilizan una combinación de encaminadores y servidores proxy).

#### Host de doble conexión.

Se trata de una configuración muy simple aunque muy efectiva. Se trata de la conexión de las dos redes mediante software, ya que esta compuesto por dos tarjetas de red separadas físicamente.

El principal inconveniente es que el usuario, podría habilitar fácilmente e incluso por error, el encaminamiento interno. Lo que deshabilitaría el firewall. Para funcionar utilizan un conjunto de proxies a nivel de aplicación o de circuito. El software ejecuta los proxies para controlar el tráfico entre ambas redes.

Debemos hacer una apreciación para los sistemas UNIX, ya que son especialmente susceptibles, ya que para que funcione este tipo de configuración es necesario que las funciones de encaminamiento estén desactivadas, sin embargo, en algunas versiones, en especial Berkeley Unix, estas funciones se habilitan de forma predeterminada. Por tanto es necesario comprobar que el sistema operativo haya desactivado todas las funciones de encaminamiento.

#### Filtrado de host.

Posiblemente este tipo de firewalls son los más seguros incluso más que los de doble conexión.

Al crearlo, le añadimos un encaminador de filtrado a la red, lo que nos permite separar el ordenador de Internet. Este tipo de configuración es muy efectivo y fácil de mantener.

Los usuarios que deseen conectarse con Internet deberán hacerlo a través de este ordenador. De este modo, los usuarios internos creen tener un acceso directo a Internet mientras que el host restringe el acceso a los usuarios externos.

#### Filtrado de subred.

Esta red permite aislar aún más la red privada de Internet. Esta compuesto por un servidor proxy y dos encaminadores de filtrado independientes. Los encaminadores controlan el tráfico de la red local, mientras que el proxy vigila y controla el tráfico de entrada y salida para Internet.

Esta configuración proporciona una defensa formidable frente a cualquier ataque. Al aislar el host de una red independiente, limita el daño que puede sufrir la red interna.

## Introducción a la encriptación

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).

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 protegerlo 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.

La criptología 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.

## Criptografía

Entendemos por Criptografía (Kriptos=ocultar, Graphos=escritura) la técnica de transformar un mensaje inteligible, denominado **texto en claro**, en otro que sólo puedan entender las personas autorizadas a ello, que llamaremos **criptograma** o texto cifrado. El **método** o sistema empleado para encriptar el texto en claro se denomina **algoritmo de encriptación**.

La Criptografía es una rama de las Matemáticas, que se complementa con el Criptoanálisis, que es la técnica de descifrar textos cifrados sin tener autorización para ellos, es decir, realizar una especie de Criptografía inversa. Ambas técnicas forman la ciencia llamada Criptología.

La base de las Criptografía suele ser la aplicación de problemas matemáticos de difícil solución a aplicaciones específicas, denominándose **criptosistema** o **sistema de cifrado** a los fundamentos y procedimientos de operación involucrados en dicha aplicación.

## Criptografía clásica.

El cifrado de textos es una actividad que ha sido ampliamente usada a lo largo de la historia, sobre todo en el campo militar y en aquellos otros en los que es necesario enviar mensajes con información confidencial y sensible a través de medios no seguros.

Aunque en cierta forma el sistema de jeroglíficos egipcio puede considerarse ya una forma de criptografía (sólo podían ser entendidos por personas con conocimientos suficientes), el primer sistema criptográfico como tal conocido de debe a Julio Cesar. Su sistema consistía en reemplazar en el mensaje a enviar cada letra por la situada tres posiciones por delante en el alfabeto latino. En nuestro alfabeto actual tendríamos la siguiente tabla de equivalencias:

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

Por lo que el mensaje "HOLA MUNDO" se transformaría en "KRQD OXPGR". Para volver al mensaje original desde el texto cifrado tan sólo hay que coger un alfabeto e ir sustituyendo cada letra por la que está tres posiciones antes en el mismo.

**La sustitución** consiste en cambiar los caracteres componentes del mensaje original en otros según una regla determinada *de posición natural en el alfabeto*. Por ejemplo, fijar una equivalencia entre las letras del alfabeto original y una variación de él, de forma análoga a lo que ocurre en el método de Julio Cesar. Si fijamos la equivalencia de alfabetos:

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

El mensaje "HOLA MUNDO" quedaría como "PXTJ UDVMX".

No es necesario que el alfabeto equivalente esté ordenado naturalmente, si no que puede estar en cualquier otro orden. Sólo se exige que tenga todos y cada uno de los elementos del alfabeto original.

Este tipo de sustituciones se denomina monoalfabético, pero existen métodos más eficaces, como los polialfabéticos, en los que existen varios alfabetos de cifrado, que se emplean en rotación.

**La trasposición** en cambio consiste en cambiar los caracteres componentes del mensaje original en otros según una regla determinada *de posición en el orden del mensaje*. Por ejemplo, si establecemos la siguiente regla de cambio en el orden de las letras en el texto:

la letra	1	2	3	4	5	6	7	8	9
pasa a ser la	5	1	4	7	8	2	9	3	6

la frase "HOLA MUNDO" nos quedaría "OUDL HOAMN".

Tanto la sustitución como la trasposición son técnicas básicas para ocultar la redundancia en un texto plano, redundancia que se transmite al texto cifrado, y que puede ser el punto de partida para un ataque por Criptoanálisis. La redundancia es el hecho de que casi todos los símbolos de un mensaje en lenguaje natural contienen información que se puede extraer de los símbolos que le rodean.

### Claves.

El problema inmediato que se plantea en cualquier sistema complejo, tanto de sustitución como de permutación, es recordar el nuevo orden que hemos establecido para obtener el mensaje camuflado, problema tanto más difícil de resolver cuanto más complicado haya sido el sistema elegido.

Una solución sería escribir en un soporte cualquiera (papel, disquete, etc.) éste nuevo orden, pero siempre queda entonces el nuevo problema de guardar el soporte, ya que si cae en manos extrañas dará al traste con el mecanismo de ocultación.

Mejor solución es implementar un mecanismo de sustitución o de permutación basado en una palabra o serie fácil de recordar. Por ejemplo, podemos establecer un mecanismo criptográfico que se base en una palabra corta. Consideremos que queremos cifrar la frase "HOLA MUNDO" basándonos en la palabra "HTML". Para ello escribimos una tabla o matriz con tantas columnas como letras tenga la palabra elegida, y colocamos en la fila superior dicha palabra. El mensaje a cifrar lo vamos situando en las filas siguientes consecutivamente y si sobran celdas las dejamos vacías:

H	T	M	L
H	O	L	A

M	U	N	D
O			

El paso siguiente será cambiar el orden de las filas, por ejemplo ordenando la palabra elegida en orden alfabético, con lo que nuestra tabla nos queda:

H	L	M	T
H	A	L	O
M	D	N	U
O			

Por último, podemos transformar las filas de la tabla en columnas:

H	H	M	O
L	A	D	
M	L	N	
O			

Y ya sólo nos queda obtener el nuevo mensaje, leyendo las filas obtenidas:

Transformación: "HOLA MUNDO"----->"HHMO LAD MLN O".

Para desencriptar el texto cifrado habrá que realizar las operaciones anteriores en sentido inverso.

El uso de una palabra o serie determinada como base de un sistema de cifrado posee la ventaja de que, si el sistema es complejo, tan sólo será fácil obtener el texto en claro a quién sepa dicha palabra, además de ser fácil de recordar. Esta palabra o serie base del mecanismo de cifrado se denomina **clave de cifrado**, y el número de letras que la forman se llama **longitud de la clave**.

Indudablemente, cuanto más complicado sea el mecanismo de cifrado y cuanto más larga sea la clave, más difícil será romper el sistema y obtener el mensaje original para un extraño. Pero más complicado será también para el destinatario del mensaje cifrado realizar las operaciones de descifrado y obtener el mensaje original, por lo que se crea el dilema seguridad / tiempo.

Las claves de encriptación van a ser la base fundamental de los modernos sistemas criptográficos, basados en operaciones matemáticas generalmente muy complejas.

### Criptografía moderna.

Como hemos visto en el apartado anterior, los sistemas criptográficos clásicos presentaban una dificultad en cuanto a la relación complejidad-longitud de la clave / tiempo necesario para encriptar y desencriptar el mensaje.

En la era moderna esta barrera clásica se rompió, debido principalmente a los siguientes factores:

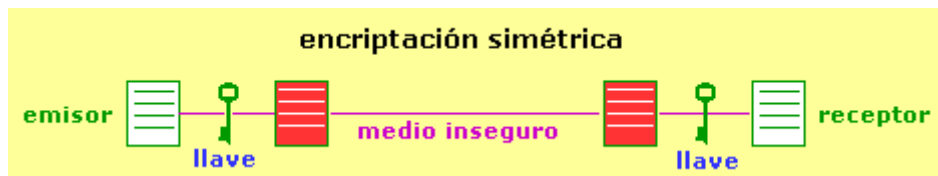
- velocidad de cálculo: con la aparición de los computadores se dispuso de una potencia de cálculo muy superior a la de los métodos clásicos.
- avance de las matemáticas : que permitieron encontrar y definir con claridad sistemas criptográficos estables y seguros.

- necesidades de seguridad: surgieron muchas actividades nuevas que precisaban la ocultación de datos, con lo que la Criptología experimentó un fuerte avance.

A partir de estas bases surgieron nuevos y complejos sistemas criptográficos, que se clasificaron en dos tipos o familias principales, los de clave simétrica y los de clave pública. Los modernos algoritmos de encriptación simétricos mezclan la trasposición y la permutación, mientras que los de clave pública se basan más en complejas operaciones matemáticas.

### Criptografía simétrica.

Incluye los sistemas clásicos, y se caracteriza por que en ellos *se usa la misma clave* para encriptar y para descryptar, motivo por el que se denomina simétrica.



Toda la seguridad de este sistema está basada en la llave simétrica, por lo que es misión fundamental tanto del emisor como del receptor conocer esta clave y mantenerla en secreto. Si la llave cae en manos de terceros, el sistema deja de ser seguro, por lo que habría que desechar dicha llave y generar una nueva.

Para que un algoritmo de este tipo sea considerado fiable debe cumplir varios requisitos básicos:

1. conocido el criptograma (texto cifrado) no se pueden obtener de él ni el texto en claro ni la clave.
2. conocidos el texto en claro y el texto cifrado debe resultar más caro en tiempo o dinero descifrar la clave que el valor posible de la información obtenida por terceros.

Generalmente el algoritmo de encriptación es conocido, se divulga públicamente, por lo que la fortaleza del mismo dependerá de su complejidad interna y sobre todo de la longitud de la clave empleada, ya que una de las formas de criptoanálisis primario de cualquier tipo de sistema es la de prueba-ensayo, mediante la que se van probando diferentes claves hasta encontrar la correcta.

Los algoritmos simétricos encriptan bloques de texto del documento original, y son más sencillos que los sistemas de clave pública, por lo que sus procesos de encriptación y descryptación son más rápidos.

Todos los sistemas criptográficos clásicos se pueden considerar simétricos, y los principales algoritmos simétricos actuales son **DES**, **IDEA** y **RC5**. Actualmente se está llevando a cabo un proceso de selección para establecer un sistema simétrico estándar, que se llamará **AES** (Advanced Encryption Standard), que se quiere que sea el nuevo sistema que se adopte a nivel mundial.

Las principales desventajas de los métodos simétricos son la distribución de las claves, el peligro de que muchas personas deban conocer una misma clave y la dificultad de almacenar y proteger muchas claves diferentes.

### Criptografía de clave pública.

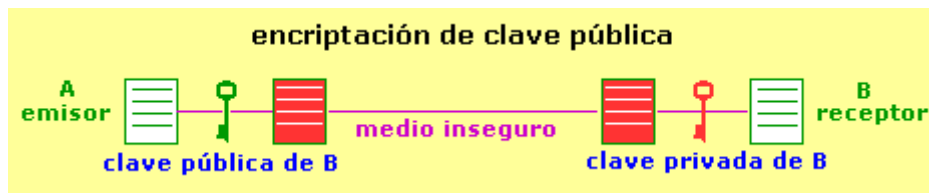
También llamada asimétrica, se basa en el uso de dos claves diferentes, claves que poseen una propiedad fundamental: una clave puede descryptar lo que la otra ha encriptado.

Generalmente una de las claves de la pareja, denominada **clave privada**, es usada por el propietario para encriptar los mensajes, mientras que la otra, llamada **clave pública**, es usada para descryptar el mensaje cifrado.

Las claves pública y privada tienen características matemáticas especiales, de tal forma que se generan siempre a la vez, por parejas, estando cada una de ellas ligada intrínsecamente a la otra, de tal forma que si dos claves públicas son diferentes, entonces sus llaves privadas asociadas también lo son, y viceversa.

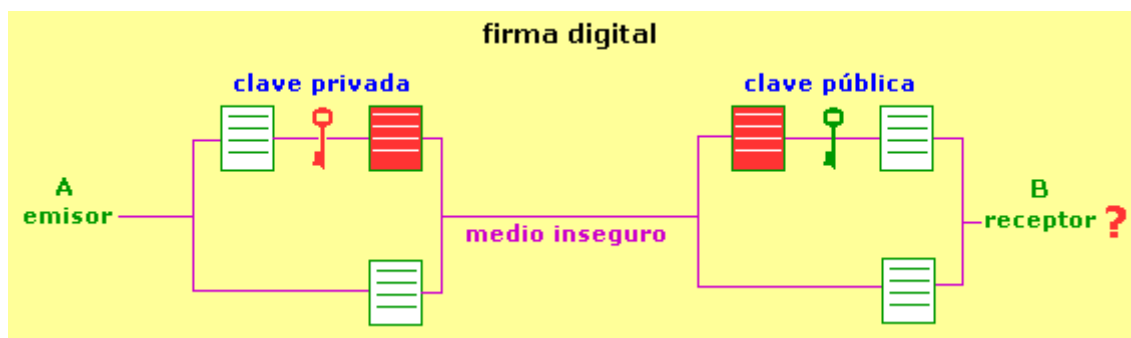
Los algoritmos asimétricos están basados en funciones matemáticas fáciles de resolver en un sentido, pero muy complicadas de realizar en sentido inverso, salvo que se conozca la clave privada, como la potencia y el logaritmo. Ambas claves, pública y privada, están relacionadas matemáticamente, pero esta relación debe ser lo suficientemente compleja como para que resulte muy difícil obtener una a partir de la otra. Este es el motivo por el que normalmente estas claves no las elige el usuario, si no que lo hace un algoritmo específico para ello, y suelen ser de gran longitud.

Mientras que la clave privada debe mantenerla en secreto su propietario, ya que es la base de la seguridad del sistema, la clave pública es difundida ampliamente por Internet, para que esté al alcance del mayor número posible de personas, existiendo servidores que guardan, administran y difunden dichas claves.



En este sistema, para enviar un documento con seguridad, el emisor (A) encripta el mismo con la clave pública del receptor (B) y lo envía por el medio inseguro. Este documento está totalmente protegido en su viaje, ya que sólo se puede desencriptar con la clave privada correspondiente, conocida sólo por B. Al llegar el mensaje cifrado a su destino, el receptor usa su clave privada para obtener el mensaje en claro.

Una variación de este sistema se produce cuando es el emisor A el que encripta un texto con su clave privada, enviando por el medio inseguro tanto el mensaje en claro como el cifrado. Así, cualquier receptor B del mismo puede comprobar que el emisor es A, y no otro que lo suplante, con tan sólo desencriptar el texto cifrado con la clave pública de A y comprobar que coincide con el texto sin cifrar. Como sólo A conoce su clave privada, B puede estar seguro de la autenticidad del emisor del mensaje. Este sistema de autenticación se denomina **firma digital**, y lo estudiaremos después con más detenimiento.



Para que un algoritmo de clave pública sea considerado seguro debe cumplir:

1. conocido el texto cifrado no debe ser posible encontrar el texto en claro ni la clave privada.
2. conocido el texto cifrado (criptograma) y el texto en claro debe resultar más caro en tiempo o dinero descifrar la clave que el valor posible de la información obtenida por terceros.
3. conocida la clave pública y el texto en claro no se puede generar un criptograma correcto encriptado con la clave privada.
4. dado un texto encriptado con una clave privada sólo existe una pública capaz de desencriptarlo, y viceversa.

La principal ventaja de los sistemas de clave pública frente a los simétricos es que la clave pública y el algoritmo de cifrado son o pueden ser de dominio público y que no es necesario poner en peligro la clave privada en tránsito por los medios inseguros, ya que ésta está siempre oculta y en poder únicamente de su propietario. Como desventaja, los sistemas de clave pública dificultan la implementación del sistema y son mucho más lentos que los simétricos.

### Sistemas mixtos

En muchas ocasiones se implementan sistemas criptográficos mixtos, en los que se usa la llave pública del receptor para encriptar una clave simétrica que se usará en el proceso de comunicación encriptada. De esta forma se aprovechan las ventajas de ambos sistemas, usando el sistema asimétrico para el envío de la clave sensible y el simétrico, con mayor velocidad de proceso, para el envío masivo de datos.

### Comunicación segura

Varios son los aspectos que hay que manejar en el proceso de transferencia de un documento electrónico y que definen una comunicación segura:

1. **Autenticidad:** consiste en la seguridad de que las personas que intervienen en el proceso de comunicación son las que dicen ser. Imaginemos que B recibe un documento procedente de A. ¿Cómo está seguro B de que en verdad es A el que se lo ha enviado y no otra persona?.

Como caso extremo, imagina que te conectas con el sitio web de tu banco para ver el estado de tus cuentas y te aparece la página de entrada de claves de acceso. Esta página tiene el logotipo del banco y un contenido textual en el que se afirma que pertenece a tu banco, pero...¿y si es una imitación de la página real del banco que te ha enviado un servidor pirata para hacerse con tus claves?.

El método más usado para proporcionar autenticidad es la firma digital.

2. **Confidencialidad:** se trata de la seguridad de que los datos que contiene el documento permanecen ocultos a los ojos de terceras personas durante su viaje por el medio desde A a B.
3. **Integridad:** consiste en la seguridad de que los datos del documento no sufren modificación a lo largo de su viaje por el medio inseguro desde A a B.

La Autenticidad es condición suficiente para la Integridad, por lo que si un documento es auténtico es íntegro, pero no al revés.

4. **No repudio:** se trata de que una vez enviado un documento por A, éste no pueda negar haber sido el autor de dicho envío.

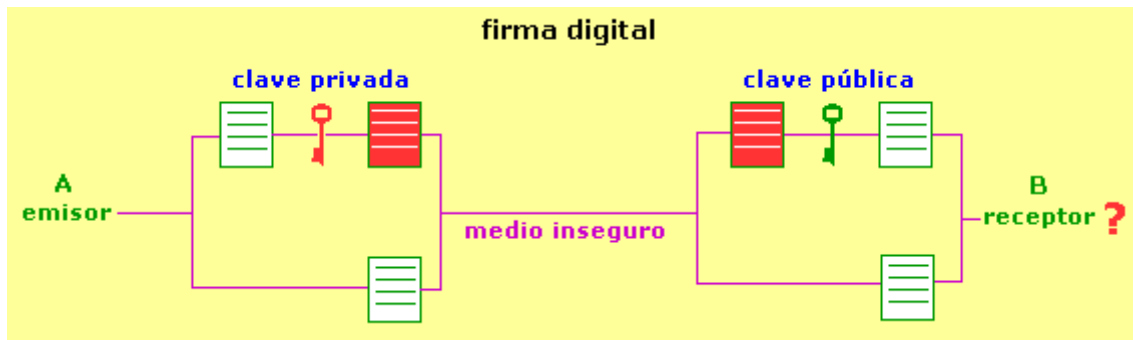
El No repudio es condición suficiente para la Autenticidad, por lo que si un documento es no repudiable es auténtico, pero no al revés.

Otro aspecto a tener en cuenta en lo que se refiere a seguridad en las comunicaciones, aunque se salga del campo de la criptografía, es el de los **Servicios de Autorización**, que proporciona al usuario acceso solamente a los recursos a los que está autorizado.

### Firma digital

Dada la importancia que está adquiriendo la firma digital en los actuales sistemas de pago electrónico y en los sistemas de autenticación, vamos a ampliar un poco su estudio.

Recordemos el esquema básico de una firma digital básica:



El proceso de firma digital consta de dos partes bien diferenciadas:

1. **Proceso de Firma:** en el que el emisor encripta el documento con su llave privada, enviando al destinatario tanto el documento en claro como el encriptado.
2. **Proceso de Verificación de la Firma:** el receptor desencripta el documento cifrado con la clave pública de A y comprueba que coincide con el documento original, lo que atestigua de forma total que el emisor del mismo ha sido efectivamente A.

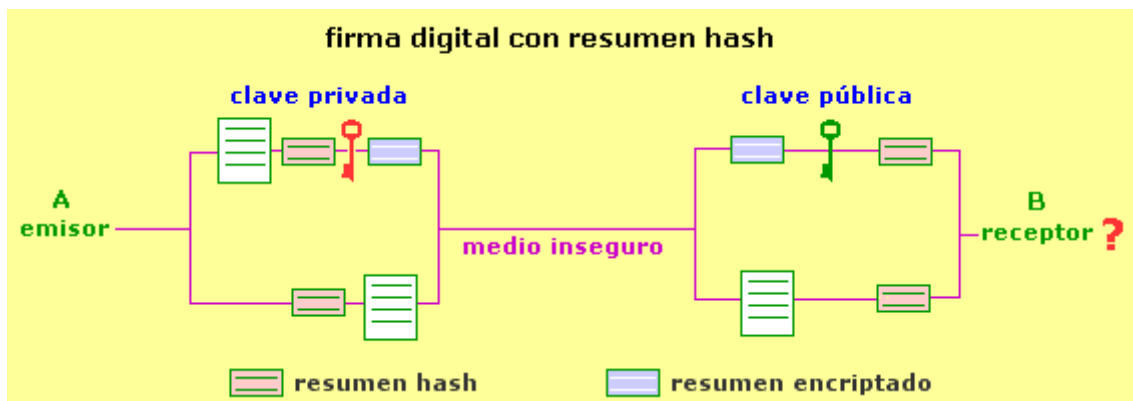
### Funciones hash

Si imaginamos el envío de un documento extenso que queremos firmar digitalmente, nos daremos cuenta de que cifrar el documento entero es una pérdida de tiempo, ya que los medios de encriptación de llave pública son lentos, pues precisan un gran proceso de cómputo.

Para solventar éste aspecto aparecen las funciones hash, que son unas funciones matemáticas que realizan un resumen del documento a firmar. Su forma de operar es comprimir el documento en un único bloque de longitud fija, bloque cuyo contenido es ilegible y no tiene ningún sentido real. Tanto es así que por definición las funciones hash son irreversibles, es decir, que a partir de un bloque comprimido no se puede obtener el bloque sin comprimir, y si no es así no es una función hash. Estas funciones son además de dominio público.

A un mensaje resumido mediante una función hash y encriptado con una llave privada es lo que en la vida real se denomina **firma digital**.

El esquema de firma digital mediante una función hash es el siguiente:



Y su mecanismo es el siguiente:

1. El emisor aplica una función hash conocida al documento, con lo que obtiene un resumen hash del mismo.
2. Encripta dicho resumen con su clave privada.
3. Envía al receptor el documento original plano y el resumen hash encriptado.
4. El receptor B aplica la función hash al resumen sin encriptar y desencripta el resumen encriptado con la llave pública de A.
5. Si ambos coinciden está seguro de que ha sido A el que le ha enviado el documento. Si no coinciden, está seguro de que no ha sido A o de que el envío ha sido interceptado durante el medio de envío y modificado.

El caso de que ambos resúmenes no coincidan contempla también la posibilidad de que el mensaje haya sido alterado en su viaje de A a B, lo que conlleva igualmente el rechazo del documento por no válido.

Las funciones hash y la firma digital son elementos indispensables para el establecimiento de canales seguros de comunicación, basados en los Certificados Digitales.

Para que una función pueda considerarse como función hash debe cumplir:

- Debe transformar un texto de longitud variable en un bloque de longitud fija, que generalmente es pequeña (algunas son de 16 bits).
- Debe ser cómoda de usar e implementar.
- Debe ser irreversible, es decir, no se puede obtener el texto original del resumen hash.
- Debe ser imposible encontrar dos mensajes diferentes cuya firma digital mediante la función hash sea la misma (no-colisión).
- Si se desea además mantener un intercambio de información con Confidencialidad, basta con cifrar el documento a enviar con la clave pública del receptor.

## 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.

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.

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

## RSA

El algoritmo de clave pública RSA fué creado en 1978 por Rivest, Shamir y Adlman, y es el sistema criptográfico asimétrico más conocido y usado. El sistema RSA se basa en el hecho matemático de la dificultad de factorizar números muy grandes. Para factorizar un número el sistema más lógico consiste en empezar a dividir sucesivamente éste entre 2, entre 3, entre 4,...., y así sucesivamente, buscando que el resultado de la división sea exacto, es decir, de resto 0, con lo que ya tendremos un divisor del número.

Ahora bien, si el número considerado es un número primo (el que sólo es divisible por 1 y por él mismo), tendremos que para factorizarlo habría que empezar por 1, 2, 3,..... hasta llegar a él mismo, ya que por ser primo ninguno de los números anteriores es divisor suyo. Y si el número primo es lo suficientemente grande, el proceso de factorización es complicado y lleva mucho tiempo.

Basado en la exponenciación modular de exponente y módulo fijos, el sistema RSA crea sus claves de la siguiente forma:

1. Se buscan dos números primos lo suficientemente grandes: **p** y **q** (de entre 100 y 300 dígitos).
2. Se obtienen los números  $n = p * q$  y  $X = (p-1) * (q-1)$ .
3. Se busca un número **e** tal que no tenga múltiplos comunes con **X**.
4. Se calcula  $d = e^{-1} \text{ mod } X$ , con mod = resto de la división de números enteros.

Y ya con estos números obtenidos, **n es la clave pública y d es la clave privada**. Los números p, q y X se destruyen. También se hace público el número e, necesario para alimentar el algoritmo.

El cálculo de estas claves se realiza en secreto en la máquina en la que se va a guardar la clave privada, y una vez generada ésta conviene protegerla mediante un algoritmo criptográfico simétrico.

En cuanto a las longitudes de claves, el sistema RSA permite longitudes variables, siendo aconsejable actualmente el uso de claves de no menos de 1024 bits (se han roto claves de hasta 512 bits, aunque se necesitaron más de 5 meses y casi 300 ordenadores trabajando juntos para hacerlo).

RSA basa su seguridad es ser una función computacionalmente segura, ya que si bien realizar la exponenciación modular es fácil, su operación inversa, la extracción de raíces de módulo X no es factible a menos que se conozca la factorización de e, clave privada del sistema.

RSA es el más conocido y usado de los sistemas de clave pública, y también el más rápido de ellos.

Presenta todas las ventajas de los sistemas asimétricos, incluyendo la firma digital, aunque resulta más útil a la hora de implementar la confidencialidad el uso de sistemas simétricos, por ser más rápidos. Se suele usar también en los sistemas mixtos para encriptar y enviar la clave simétrica que se usará posteriormente en la comunicación cifrada.

## *Bibliografía*

[www.freebsd.org/doc/en\\_US.ISO8859-1/books/handbook/firewalls.html](http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/firewalls.html)

[www.secinf.net/info/fw/steph](http://www.secinf.net/info/fw/steph)

[www.aebius.com/b\\_datos\\_doc/pages/firewalls1.htm](http://www.aebius.com/b_datos_doc/pages/firewalls1.htm) (UNIX)

[www.diarioti.com/noticias/oct98/not981006b](http://www.diarioti.com/noticias/oct98/not981006b).

[www.geocities.com/CapeCanaveral/2566/encrip/encrip.html](http://www.geocities.com/CapeCanaveral/2566/encrip/encrip.html)

[www.uoc.es/web/esp/launiversidad/inaugural01/encripcion.html](http://www.uoc.es/web/esp/launiversidad/inaugural01/encripcion.html)

[www.telecomsoft.net/encrypta.html](http://www.telecomsoft.net/encrypta.html)