Tema-4FR.pdf

mhm01

Fundamentos de Redes

3º Grado en Ingeniería Informática

Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación
Universidad de Granada

TEMA 4: SEGURIDAD EN REDES

1. Introducción a la Seguridad en Redes

---------- Introducción

Una red de comunicaciones es segura cuando se garantizan todos los aspectos de la misma. Por ello no hay protocolos ni redes 100% seguros.

¿Qué es la seguridad? Esta pregunta tiene múltiples aspectos:

- Confidencialidad/privacidad: el contenido de la información es comprensible sólo para entidades autorizadas.
- Autenticación: las entidades son quienes dicen ser.
- Control de accesos: los servicios son accesibles sólo para entidades autorizadas.
- No repudio o irrenunciabilidad: el sistema impide la renuncia de la autoría de una determinada acción.
- Integridad: el sistema detecta todas las alteraciones (intencionadas o no) de la información.
- Disponibilidad: el sistema mantiene las prestaciones de los servicios con independencia de la demanda.

La seguridad se debe situar en TODOS los niveles/capas. El grado de seguridad lo determina el punto más débil.

Se dice que hay un ataque de seguridad cuando hay una acción intencionada o no que menoscaba cualquiera de los aspectos de la seguridad.

----- Ejemplos de Tipos de Ataques

- **Intercepción**:
  - **Sniffing**: es una vulneración a la confidencialidad como puede ser escuchar.

- **Fabricación**:
  - **Poofing**: suplantación de la identidad de entidades.

- **Intercepción/Modificación:**
  - **Distributed Denial of Service (DdoS):** denegación de servicio distribuido

- **Interrupción**:
    - **Malware**: troyano (software oculto con la apariencia de otro programa), gusano (virus que se replica), spyware (programa que captura datos privados), backdoor(punto desconocido de acceso a nuestra máquina), rootkit(software que proporciona acceso remoto), ransomware (captura o modificación de datos), keylogger(captura las pulsaciones de teclas que hacemos y las envían).

----- Mecanismos de Seguridad

- **De Prevención:**
    - mecanismos de autenticación e identificación.
    - mecanismos de control de acceso.
    - mecanismos de separación (física, temporal, lógica, criptográfica y fragmentación).
    - mecanismos de seguridad en las comunicaciones (cifrado de la información).

- **De Detección:** IDS (Intrusion Detection System).

- **De Recuperación:**
    - copias de seguridad (backup).
    - mecanismos de análisis forense: averiguar alcance, las actividades del intruso en el sistema y cómo entró.

2. Mecanismos de Seguridad

Los mecanismos de seguridad más utilizados son: el cifrado (que puede ser simétrico o asimétrico), la autentificación con clave secreta, el intercambio de Diffe-Hellman (que es el establecimiento de la clave secreta), las funciones Compendio o Hash, la firma digital y los certificados digitales.

---------- Cifrado

Se basa en la criptografía y en la definición de un criptosistema: con el alfabeto de partida, los espacios de claves, el conjunto de transformaciones de cifrado y el conjunto de transformaciones de descifrado.

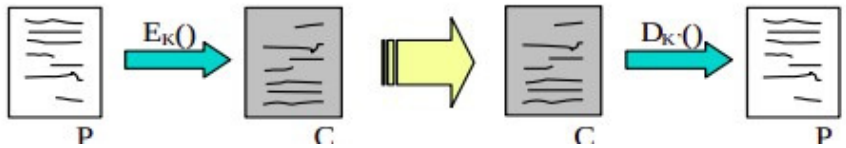
Los tipos de criptosistemas pueden ser:
- **Simétricos** o de **clave privada** (DES, Data Encryption Standard)
- **Asimétricos** o de **clave pública** a (RSA, Rivest-Shamir-Adleman)

KEEP CALM AND ESTUDIA UN POQUITO

WUOLAH + #QuédateEnCasa

El cifrado es un proceso para garantizar la confidencialidad:

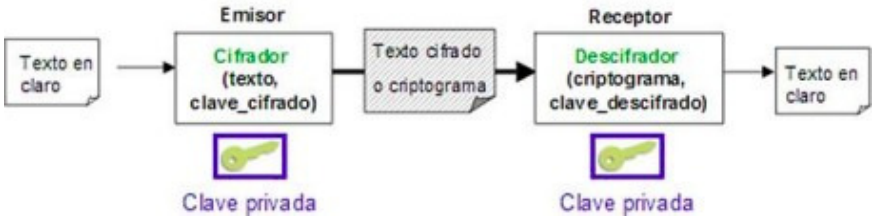
- Se parte de un Texto llano/claro (plain text)
- Se aplica un algoritmo de cifrado conocido como $E_k()$
- Y un algoritmo de descifrado llamado $D_k()$
- Ambos dependen respectivamente de una clave de cifrado K y de una clave de descifrado K'
- El texto plano P se cifra y se convierte en C, se transmite y posteriormente se descifra C para obtener P de nuevo.



----- Cifrado Simétrico: Algoritmos de Clave Secreta

- *K = K'*

El emisor y el receptor comparten la misma clave. LA clave sólo es conocida por ellos (privada/secreta). El emisor encripta con ella y el receptor desencripta con ella. La clave deben compartirla por un canal seguro.

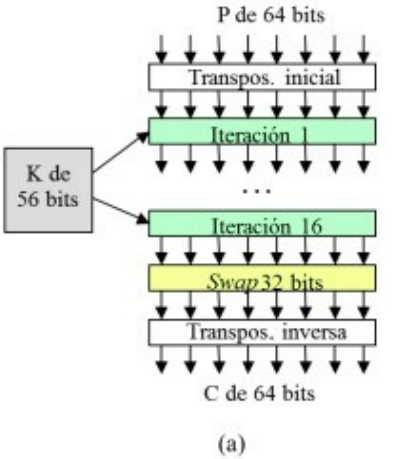


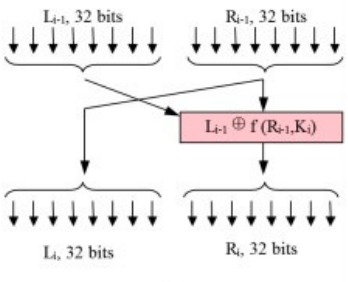
- Algoritmo DES (Data Encryption Standard):

1. Se hace una transposición al bloque inicial de bits P

2. Se realizan 16 interaciones aplicando la clave K de 56 bits
   a)32 bits de la derecha pasan a ser los de la izquierda para la iteración siguiente
   b) 32 bits de la derecha se obtienen haciendo XOR con los de la izquierda, junto con la aplicación de una función de transposición y duplicación de bits sobre R y K de la iteración actual, i. En dicha función también se utilizan módulos de sustitución para cada grupo de 6 bits (8 grupos) y se obtienen 4 bits por cada bloque. Por último se hace una nueva transposición del resultado.

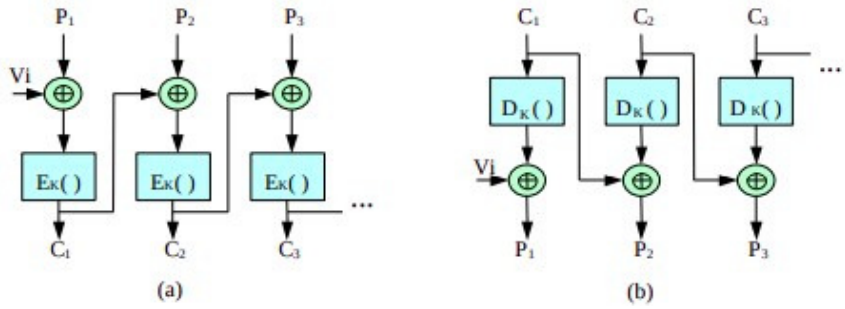
3. Hay un intercambio de 32 bits de orden más alto por los más bajos.





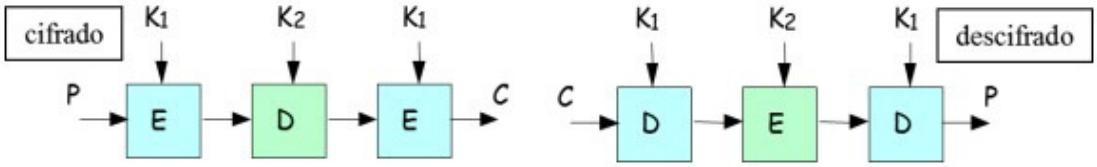
4. Transposición inversa de 1.

Se realizan varios encriptamientos consecutivos y se combinan los resultados. Con cada encriptamiento se aumenta en 2^{56} la dificultad para describir la clave.



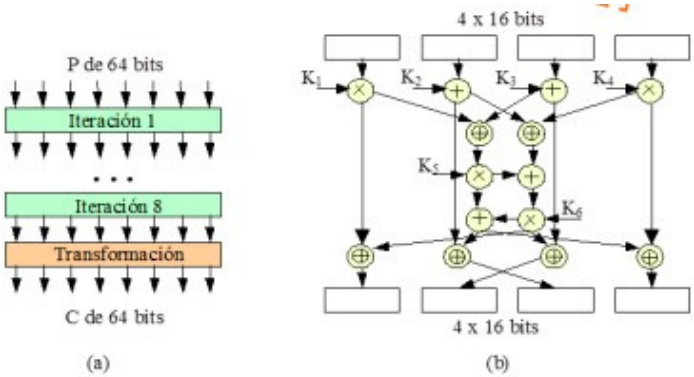
- Algoritmo 3DES (Data Encryption Standard):

Se hacen dos fases de encriptado y una de desencriptado entre ellas, usando cada vez una clave diferente.



- Algoritmo IDEA (International Data Encryption Algorithm):

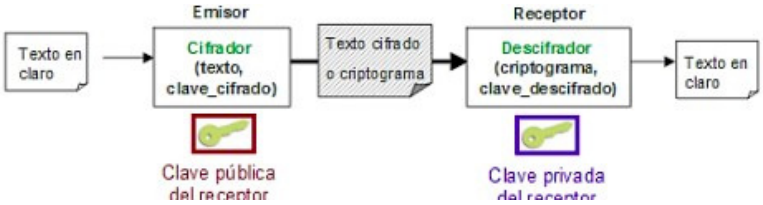
Este algoritmo utiliza claves de 128 bits. Puede operar en tiempo real y es fácil de implementar. Hace 8 iteraciones aplicando las operaciones: XOR, suma de módulo 2^{16} y multiplicaciones de módulo $2^{16} + 1$.



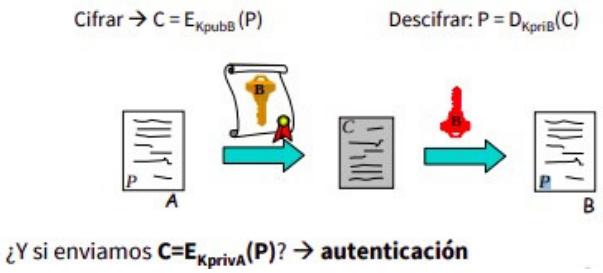
----- Cifrado Asimétrico: Algoritmos de Clave Pública

El receptor tiene una clave pública y una clave privada (de la que deriva la pública). Envía la clave pública a los emisores potenciales (por cualquier medio). El emisor encripta con la clave pública del receptor. El receptor desencripta con su clave pública.

- K != K'



Hay dos claves por usuario (B): una pública K_{PUBB} y otra privada K_{PRIB} distintas. Una vez conocida K_{PUBB} es imposible conocer K_{PRI}. Hay diferentes claves para cifrar y descifrar:



- Algoritmo RSA (Rivest, Shamir, Adleman):

1. Elegimos p y q primos grandes (>10^{100})
2. n = (p * q) y z = (p-1) * (q-1) (Función de Euler)
3. Elegimos d coprimo con z, es decir, que no tienen factores primos en común.
4. Calculamos e tal que e*d mod z = 1 (Algoritmo de Euclides)
5. K_{pub} = (e, n) y K_{pri} = (d, n), de modo que:
   - C = P^e mod n
   - P = C^d mod n

Ejemplo:

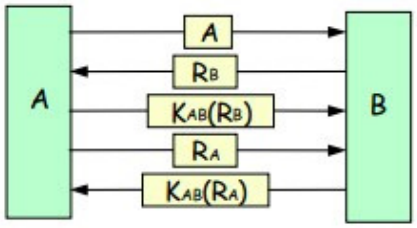
p = 3, q = 11
n = p·q = 33, z = (p-1)·(q-1) = 20 (= 5 · 2 · 2 en factores primos)
d = 7, coprimo respecto a z
e = 3, e·d mod z = 1
Kpub=(3,33) y ***Kpri=(7,33)***

Simbólico	Numérico	P^3	P^3 mod 33	C^7	C^7 mod 33	Simbólico
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	01	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	05	E
	P		C		P	

---------- Autenticación y Cifrado de Clave Secreta

----- Esquema Reto-Respuesta (criptográfica):

- A desea autenticarse en B
- B le plantea un "reto" a A
- A responde al reto encriptándolo con la clave privada/secreta compartida entre A y B
- B comprueba si la respuesta es correcta y si lo es A se autentica
- El proceso se puede repetir para autenticar a B.



----- Variante no Criptográfica:

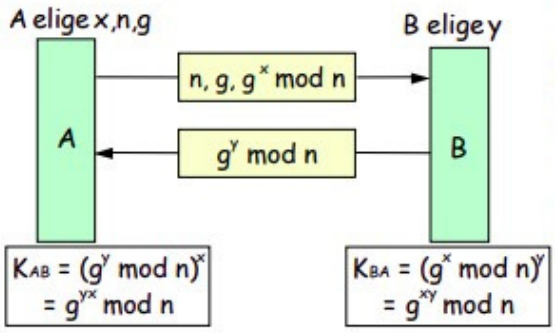
- Si la respuesta es la contraseña, hay un ataque replay.
- Si la respuesta es la contraseña con identificador, hay un ataque replay con id.
- Contraseña de un solo uso.

---------- Clave Secreta

----- Establecimiento de la Clave Secreta

- **El Intercambio de Diffie-Hellman:** permite establecer una clave secreta entre dos entidades a través de un canal no seguro.

Ejemplo:



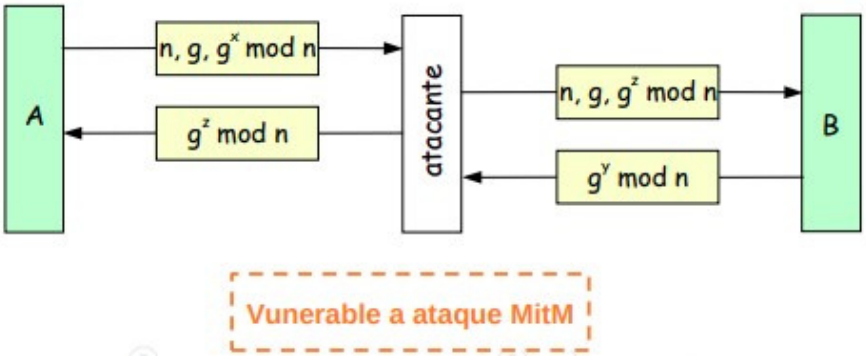
g=7 , n=23

1. *A elige **x = 3** y calcula R1 = 7^3 mod 23 = 21.*
2. *A envía el número 21 a B.*
3. *B elige **y = 6** y calcula R2 = 7^6 mod 23 = 4.*
4. *B envía el número 4 a A.*
5. *A calcula la clave privada/simétrica K = 4^3 mod 23 = 18.*
6. *B calcula la clave privada/simétrica K = 21^6 mod 23 = 18.*

El valor de K es el mismo para A y B:

g^{xy} mod n = 7^{18} mod 23 = 18.

Usando números grandes no es vulnerable a la escucha del canal.



---------- Funciones Hash

----- Funciones Compedio

Son funciones unidireccionales (irreversibles) de cálculo sencillo. Tiene un texto de entrada (M) de longitud variable.

M → H(M), siendo H(M) de longitud fija de 256 o 512 bits.

Es imposible obtener M de su resumen H(M). Estas funciones son invulnerables a ataques de colisión, dado M es imposible encontrar un M' tal que: M != M' y H(M) = H(M').

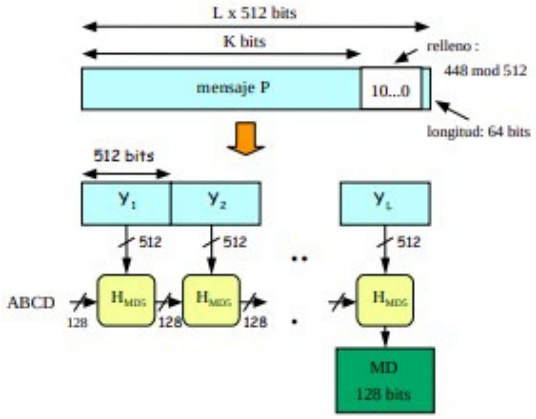
Las funciones Hash se pueden usar para garantizar la integridad y la autenticación (claveK):

- Hash Message Authentication Code (HMAC): M + H(K|M) pero para evitar ataques de extensión se usa M + H(K | H(K | M)).

Algunos ejemplos de funciones Compendio/Digest/Hash son: MD5, SHA-1, SHA-512

----- MD5 (Message Digest 5, RFC 1321)

Hay un relleno de bits "100..0" por la derecha de longitud máxima 448 bits y una adición de campo de longitud de 64 bits. A continuación hay que dividir el mensaje en bloques de 512 bits y procesarlos de manera secuencial por bloques. De cada bloque se obtiene un digest de 128 bits.



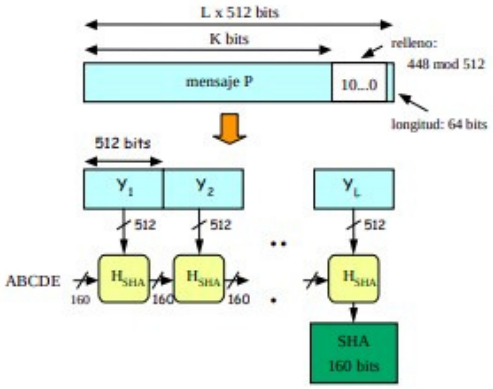
ABCD son 4 registros de 32 bits con valores constantes hexadecimales.

En MD5, en cada bloque que se procesa:

- se usan varias funciones (F, G, H, I) de operadores binarios (XOR, AND, OR, NOT) combinadas.
- se aplican los valores de los registros A, B, C, D.
- se hacen desplazamientos de bits.
- se hacen varias pasadas.
- se hace una suma final módulo 2^{32}.
- la salida de un bloque será la entrada del siguiente.

----- SHA-1 (Secure Hash Algorithm 1)

Relleno bits “100..0” por la derecha de longitud máxima 448 bits. Hay una adición de campo de longitud de 64 bits. A continuación, se divide el mensaje en bloques de 512 bits y se hace un procesamiento secuencial por bloques. De cada bloque, se obtiene un digest de 160 bits.



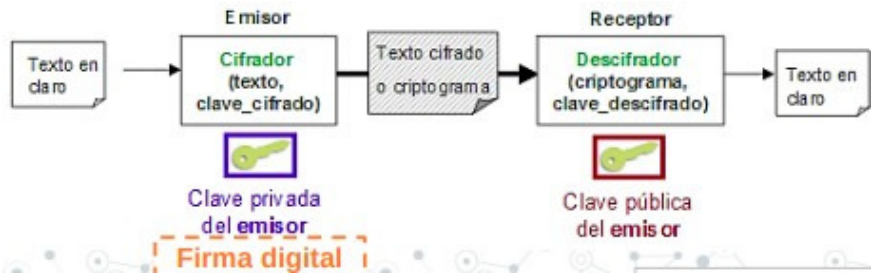
ABCDE son 5 registros de 32 bits con constantes hexadecimales diferentes a los de MD5.

En SHA-1, en cada bloque que se procesa:

- Se divide el bloque en palabras de 32 bits.
- Se extienden las palabras combinándolas hasta tener 80.
- Se agrupan de 20 en 20 y se combinan usando funciones.
- Se usan varias funciones de operadores binarios (XOR, AND, OR, NOT) combinadas entre sí.
- Se aplican los valores de los registros A, B, C, D, E.
- Se hacen 4 pasadas de este proceso.
- Se hace una suma final módulo 2^{32} .
- La salida de un bloque será la entrada del siguiente.

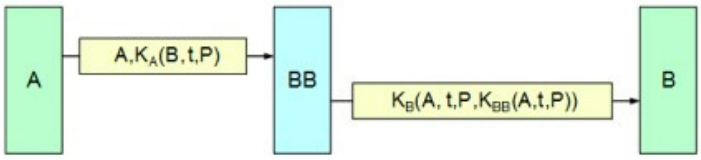
---------- Firma Digital

Una firma digital es un conjunto de datos que, consignados junto a otros o asociados con ellos, pueden ser utilizados como medio de identificación del firmante. Los objetivos de la firma digital son: que el receptor pueda autentificar al emisor, que no haya repudio (que el emisor no pueda alegar que él no envió el mensaje) y que el emisor tenga garantías de no falsificación de su mensaje (integridad).



----- Firma Digital: Big Brother

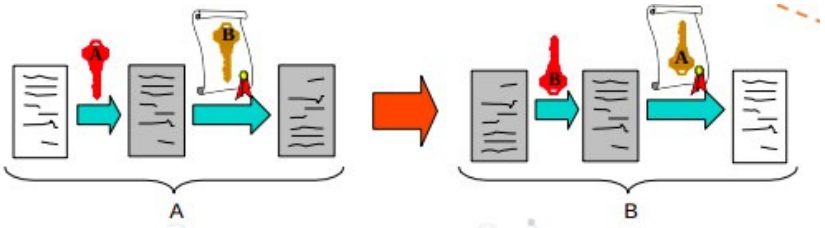
Hay una entidad central (BB) que interviene en el proceso de firma digital para la transmisión de un mensaje P entre A y B. A envía el mensaje cifrado con una clave que comparte con BB, K_A, incluyendo además el propio destino del mensaje, B, y una marca de tiempo t. BB envía el mensaje cifrado con la clave que comparte con él, K_B, la identidad de A, el mensaje P, su propia marca de tiempo t y su firma digital. La firma serán estos mismo valores encriptados con su propia clave K_{BB}.



----- Firma digital con Clave Asimétrica. Doble Cifrado

Tenemos un cifrado por autentificación, con K_{priA} y otro para proporcionar privacidad, con K_{pubB}. Para firmar, hay que enviar $K_{pubB}(K_{priA}(P))$. En el receptor se desencripta: $K_{pubA}(K_{priB}(K_{pubB}(K_{priA}(P)))) = P$.

Hay un problema que es garantizar el no repudio: Asociación fehaciente e indisoluble de A con su clave pública $K_{pubA.}$



---------- Firma Digital

Un certificado digital sirve para garantizar la asociación identidad-clave, es decir, para que un usuario no pueda corromper una clave pública (de otro) y decir que es suya.

----- Autoridades de Certificación (AC)

Es una entidad para garantizar la asociación entre entidad y claves. Su funcionamiento consiste en:

- El usuario obtiene sus claves pública y privada
- Éste envía una solicitud, firmada digitalmente, a la AC indicando su identidad y su clave pública
- AC comprueba la firma y emite el certificado solicitado:
  * Identidad de AC, identidad del usuario, clave pública del usuario y otros datos como, por ejemplo, el período de validez del certificado.
  * Todo ello se firma digitalmente con la clave privada de AC con objeto de que el certificado no pueda falsificarse

El formato de los certificados suele ser X.509.

Las AC son responsables de emitir los certificados, asignarles una fecha de validez y revocarlos antes de esta fecha (en casos determinados).

Las AC más reconocidas son: ACE, VeriSign, CAMERFIRMA y CERES.

----- Tipos de Certificados

- Certificados Firmados Localmente: son aquellos firmados por un servidor local y que son de uso interno en un a red privada (intranet). Se usan para garantizar los intercambios confidenciales y para autenticar usuarios.

- Certificados Firmados por una Autoridad de Certificación: son válidos en todo internet. Nos sirve para garantizar los intercambios seguros con usuarios anónimos y para acreditar la identidad de un nuevo usuario.

---------- Resumen

La relación que tiene que haber entre los mecanismos de seguridad y los servicios de seguridad deben de cumplir:

- **Confidencialidad**: se consigue mediante Cifrado que puede ser simétrico o asimétrico.

- **Autenticación**: se consigue con los mecanismos de autenticación (reto-respuesta), y la firma digital (big brother, doble cifrado: cifrado en el emisor con clave privada y descifrado en receptor con clave pública).

- **No repudio o Irrenunciabilidad:** se consigue mediante la firma digital (big brother, doble cifrado) y el certificado digital.

- **Integridad**: se consigue añadiendo resúmenes generados con funciones hash/digest.

- **Disponibilidad**: los mecanismos no proporcionan disponibilidad por sí mismos. Serán necesario sistemas antiataque, redundancia en las líneas de acceso, en los servidores, etc.

3. Implementación de Mecanismos de Seguridad

La seguridad perimetral la podemos controlar con: Firewalls, IDS (sistemas de detección de intrusiones) y IRS (sistemas de respuesta frente a las intrusiones).

---------- Protocolos de Seguridad

- Capa de Aplicación: destacan Pretty Good Privacy (PGP) y Secure Shell (SSH).

- Capa de Transporte: destacan Secure Socket Layer (SSL) donde encontramos HTTPS, IMAPS, SSL-POP y Transport Layer Security (TLS).

- Capa de Red: destaca IPSec (VPN)

- Capas Inferiores: PAP, CHAP, MS_CHAP, EAP…

---------- Cortafuegos (Firewall)

Es una combinación de técnicas, políticas de seguridad y tecnologías hardware y software. Proporciona seguridad en la res, controlando el tráfico que entra y sale normalmente entre una red privada e internet.

----- Funciones

- Controlar (permitiendo o denegando) los accesos desde la red local hacia el exterior y los accesos desde el exterior hacia la red local.
- Filtrar los paquetes que circulan, de modo que sólo los servicios permitidos puedan pasar.
- Monitorizar el tráfico, supervisando destino, origen y cantidad de información recibida y/o enviada.
- Almacenar total o parcialmente los paquetes que circulan a través de él para analizarlos en caso de problemas.
- Establecer un punto de cifrado de la información si se pretende comunicar dos redes locales a través de Internet

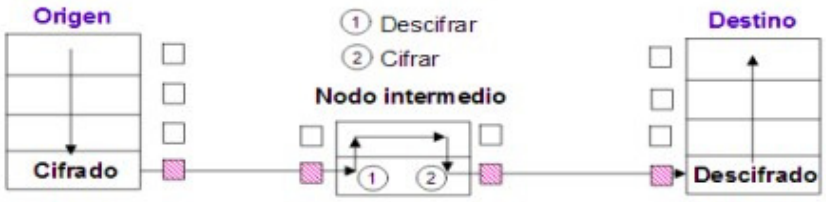
----- Técnicas Aplicadas

- Filtrado de Paquetes: reglas que especifican qué tipos de paquetes pueden circular en cada sentido y cuáles se bloquearán. Las reglas se basan en las cabeceras de los paquetes.

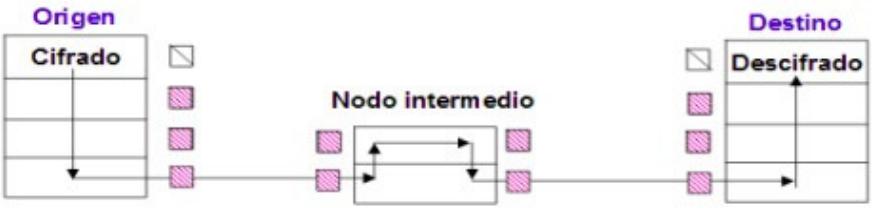
- Servicios de Proxy: Son aplicaciones especializadas que funcionan en un cortafuegos. Hacen de intermediarios entre los servidores y los clientes reales. Reciben las peticiones de servicios de los usuarios, las analizan y en su caso modifican, y las transmiten a los servidores reales. Son transparentes al usuario.

---------- Cifrado en Redes

- Cifrado de Enlace: es en la capa 2 de OSI. Cifra todo el mensaje, incluidas las cabeceras de niveles superiores. Requiere de nodos intermedios con capacidades de cifrado/descifrado. La información está protegida entre cada par de nodos consecutivos usando distintas claves para cada par. Es necesario descifrarla, aunque sea parcialmente, para procesos de encaminamiento, control de errores, etc.

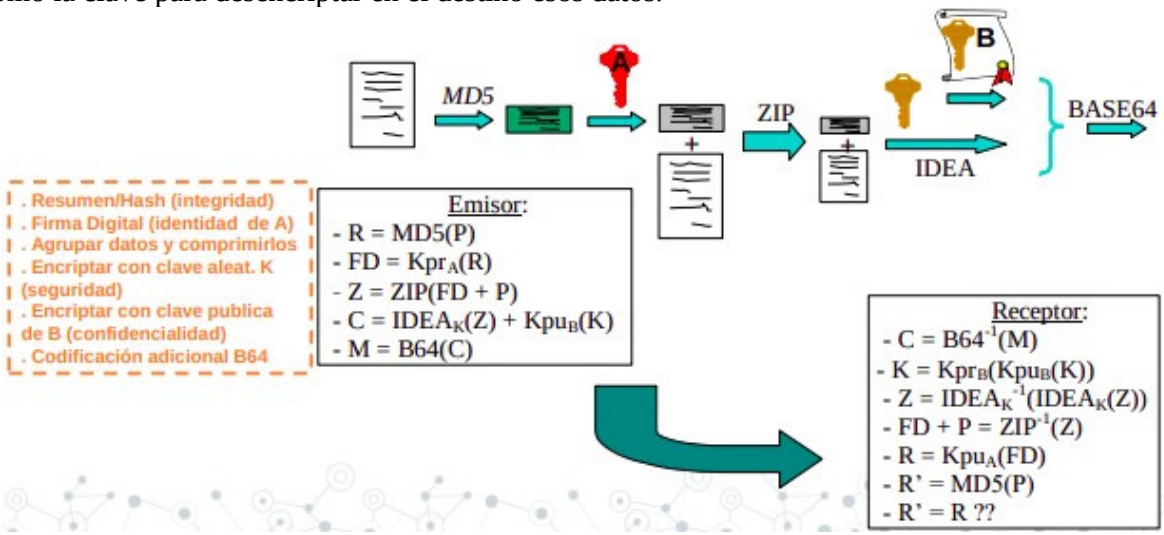


- Cifrado Extremo a Extremo: ocurre en la capa 7 de OSI. Sólo se cifran los datos, las cabeceras se añaden y se transmiten sin cifrar.



---------- Preatty Good Privacy (PGP)

Se usa para el correo electrónico seguro y otros documentos en Internet). Se encripta tanto los datos como la clave para desencriptar en el destino esos datos.



---------- SSH (Secure Shell)

SSH es un protocolo de nivel de aplicación para crear conexiones seguras entre dos sistemas sobre redes no seguras. Es una alternativa a programas de acceso remoto no seguros, como telnet, ftp, rlogin, rsh y rcp. Proporciona un terminal de sesión cifrada con autentificación fuerte sel servidor y el cliente, usando criptografía de clave pública. Incluye características como :

- Variedad de mecanismos de autenticación de usuarios (incluyendo autenticación externa Kerberos).
- Conexiones TCP arbitrarias de tunneling a través de la sesión SSH, protegiendo protocolos inseguros como IMAP y permitiendo el paso seguro a través de cortafuegos.
- Transferencias seguras de ficheros.
- Soporte para entorno gráfico.

----- Secuencia de Eventos de una Conexión SSH

1. Se crea una capa de transporte segura para que el cliente sepa que está efectivamente comunicándose con el servidor correcto. Luego se cifra la comunicación entre el cliente y el servidor por medio de una clave simétrica/privada.

2. Una vez conectado de forma segura, el cliente se autentica ante el servidor sin preocuparse de que la información de autenticación pudiese exponerse.

3. Con el cliente autentificado ante el servidor, se pueden usar varios servicios diferentes con seguridad a través de la conexión, como una sesión de terminal interactivo, aplicaciones y túneles TCP/IP.

---------- **Transport Layer Security (SSL/TLS)**

- SSL: fue desarrollado en Netscape en 1994 y puesto en dominio público para la definición de canales seguros sobre TCP.

- TLS: es un sucesor y una mejora de SSL. Corrige las vulnerabilidades de SSL y permite la autentificación de emisor y receptor. Se basa en el uso de certificados digitales para establecer la conexión. Posteriormente, emisor y receptor comparten una clave privada.

Ambos son protocolos criptográficos que permiten realizar comunicaciones seguras sobre una red no segura.

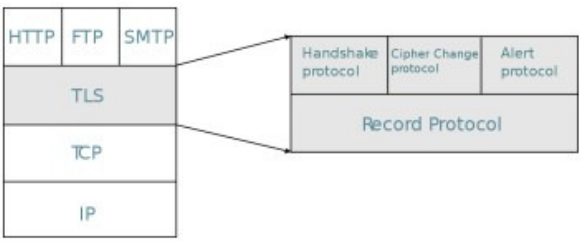
----- **Capas**

- **SSL Record Protocol:** encapsula los protocolos y ofrece un canal seguro con privacidad, autenticación e integridad.

- **SSL Handshake Protocol:** negocia el algoritmo de cifrado y la función Hash. Autentica al servidor con X.509. El cliente genera claves de sesión aleatorias cifradas con K_{pub_server} o con Diffie-Hellman.

- **SSL Alert Protocol:** informa sobre errores en la sesión.

- **Cipher Change Espec Protocol:** para notificar cambios en el cifrado.

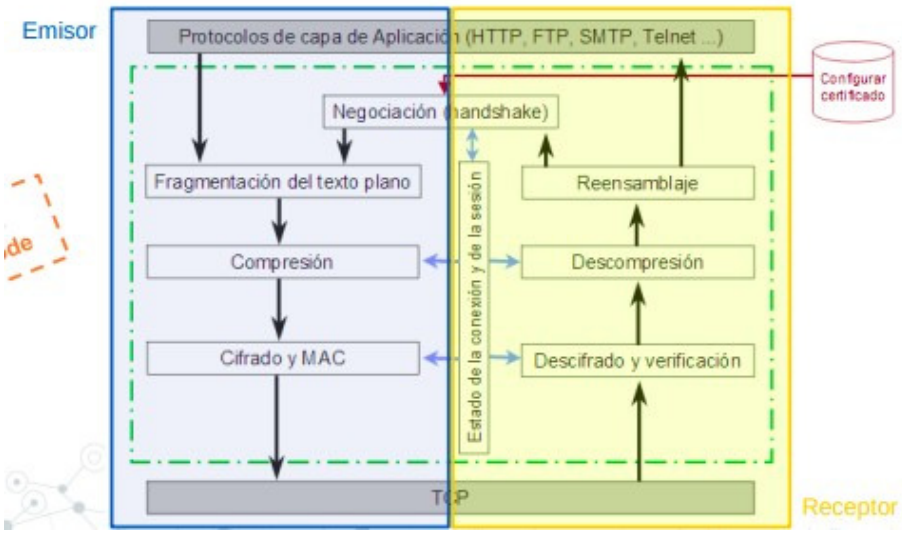


----- Funcionamiento

El cliente al hacer la conexión informa sobre los sistemas criptográficos que tiene disponibles, y el servidor responde con un identificador de la conexión, su clave certificada e información sobre los sistemas criptográficos que soporta. El cliente elegirá un sistema criptográfico y verificará la clave pública del servidor. Entonces se generará una clave privada (de uso único) cifrada con la clave pública del servidor. Si alguien pudiese descifrar la información, sólo conseguiría romper esa conexión/sesión, ya que una sesión posterior requeriría una clave privada diferente. Una vez finalizado este proceso, los protocolos toman el control de nivel de aplicación, de modo que SSL/TLS nos asegura que:

- Los mensajes que enviamos o recibimos no han sido modificados (integridad).
- Ninguna persona sin autorización puede leer la información transmitida (confidencialidad).
- Efectivamente envía/recibe la información quien debe enviarla/recibirla (autenticación).

----- Arquitectura



La versión actual de SSL es la 3.0. SSL es capaz de trabajar de forma transparente con todos los protocolos que trabajan dobre TCP. Para ello el IANA tiene asignado un número de puerto por defecto a cada uno de ellos:

Identificador de protocolo	Puerto TCP	Descripción
https	443	HTTP sobre SSL
smtps	465	SMTP sobre SSL
nntps	563	NTTP sobre SSL
ladps	646	LDAP sobre SSL
telnets	992	TELNET sobre SSL
imaps	993	IMAP sobre SSL
ircs	994	IRC sobre SSL
pop3s	995	POP3 sobre SSL
ftps-data	989	FTP-Datos sobre SSL
ftps-control	990	FTP-Control sobre SSL

---------- IPSec (IP Security)

Proporciona seguridad en la capa de res y a las superiores que se apoyen en IP. Su objetivo es garantizar la autenticación, la integridad y (opcionalmente) la privacidad a nivel IP.

IPSec consiste en 3 procedimientos:

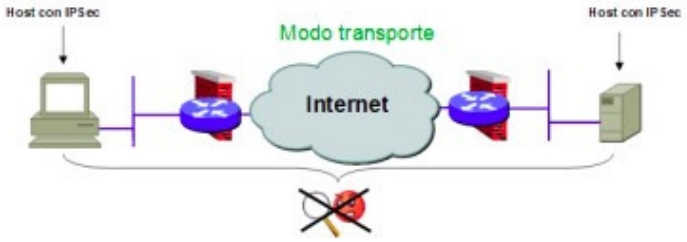
1) Establecimiento de una "Asociación de seguridad": IKE (Internet Key Exchange, RFC 2409)
- Objetivo: establecimiento de clave secreta (Diffie-Hellman).
- Incluye previamente autenticación (con certificados) para evitar el ataque de MitM.
- Es simplex: la asociación de seguridad tiene un único sentido.
- Se identifica con la IP origen + Security Parameter Index (32 bits).
- Vulnera el carácter NO orientado a conexión de IP.

2) Garantizar la autenticación e integridad de los datos: protocolo de "Cabeceras de autenticación"

3) (Opcional) Garantizar la autenticación e integridad y privacidad de los datos: protocolo de "Encapsulado de seguridad de la carga"

IPSec tiene 2 modos de operación:

- **Modo Transporte:** la asociación se hace extremo a extremo entre el host origen y el host destino. Se protege la carga útil IP (payload) (Capa de Transporte). La comunicación es segura extremo a extremo. Requiere de la implementación de IPSec en ambos hosts.



- **Modo Túnel:** la asociación se hace entre dos routers intermediarios. Se protegen paquetes IP (Capa de Red). Para la comunicación segura entre routers/gateways de seguridad sólo se puede usar este modo. Permite incorporar IPSEc sin afectar a los hosts. Se integra fácilmente con VPNs.