Redes de Computadores
I. Informática
Universidad Complutense de Madrid

TEMA 7
Conceptos avanzados: DHCP. Firewalls. NAT. DNS.
Introducción a al seguridad

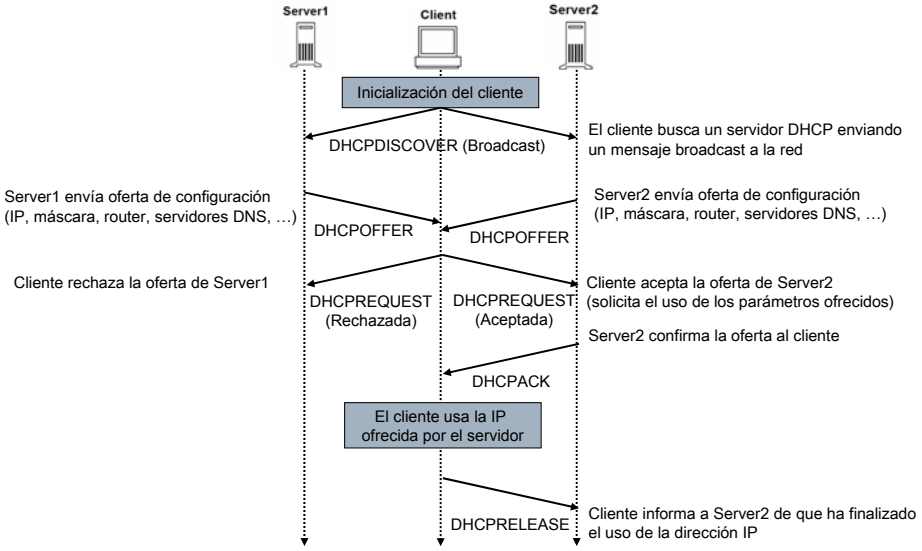
PROFESOR: *Rubén Santiago Montero*

DHCP: Configuración Dinámica de Hosts

- **DHCP (Dynamic Host Configuration Protocol)**
  - ¿Qué es DHCP?
    - Configuración automática de los parámetros de la red
      - Dirección, máscara, router predeterminado, servidores DNS, etc.
    - Clientes DHCP
      - No disponen de una configuración de red fija
      - Cuando arranca el sistema busca un servidor DHCP que le proporcione la información de configuración de red necesaria
    - Servidor DHCP
      - Proporciona los parámetros de configuración de la red a los clientes que lo solicitan
    - Ámbitos de aplicación
      - Entornos móviles (redes inalámbricas, hoteles, congresos, etc.)
      - Acceso telefónico o ADSL a través de ISP

DHCP: Configuración Dinámica de Hosts

Funcionamiento del protocolo DHCP



DHCP: Configuración Dinámica de Hosts

Mensajes del protocolo DHCP

- DHCPDISCOVER:
  - Mensaje broadcast del cliente para localizar a los servidores DHCP activos
- DHCPOFFER:
  - Respuesta del servidor, con una oferta de parámetros de configuración conforme a la situación del cliente
- DHCPREQUEST:
  - Mensaje del cliente con dos posibles respuestas
    - Oferta aceptada y solicitud del uso los parámetros ofertados
    - Oferta rechazada
- DHCPACK
  - Mensaje de confirmación y cierre desde el servidor hacia el cliente indicando los parámetros definitivos
- DHCPRELEASE
  - Mensaje del cliente para informar al servidor de que ha finalizado el uso de la dirección IP

DHCP: Configuración Dinámica de Hosts

- **Configuración del servidor DHCP en Linux (i)**
  - Proceso servidor: **dhcpd**
  - Archivo de configuración: **/etc/dhcp.conf**
    - **/etc/dhcp.conf** (archivo ejemplo)

```
subnet 192.168.1.0 netmask 255.255.255.0 {
   range 192.168.1.201 192.168.1.220;
   default-lease-time 86400;
   max-lease-time 86400;
   option routers 192.168.1.1;
   option broadcast-address 192.168.1.255;
   option subnet-mask 255.255.255.0;
   option domain-name-servers 192.168.1.100;
}
```


DHCP: Configuración Dinámica de Hosts

- **Elementos del archivo de configuración** /etc/dhcp.conf
  - subnet 192.168.1.0 netmask 255.255.255.0
    - Subred a la que se da servicio DHCP
  - range 192.168.1.201 192.168.1.220
    - Rango de direcciones IP ofrecidas dinámicamente a los clientes DHCP
  - default-lease-time 86400
    - Tiempo por defecto de alquiler de la dirección IP (en segundos)
  - max-lease-time 86400
    - Tiempo máximo de alquiler de la dirección IP (en segundos)
  - option routers 192.168.1.1
    - Router predeterminado anunciado a los clientes DHCP
  - option broadcast-address 192.168.1.255
    - Dirección de broadcast anunciada a los clientes DHCP
  - option subnet-mask 255.255.255.0
    - Mácara de subred anunciada a los clientes DHCP
  - option domain-name-servers 192.168.1.100
    - Lista de servidores DNS anunciada a los clientes DHCP

DHCP: Configuración Dinámica de Hosts

Configuración del cliente DHCP en Linux

- Necesario modificar el archivo de configuración de la red
  - **Red-Hat o Fedora:** `/etc/sysconfig/networking/devices/ifcfg-eth0`

Cliente con IP fija

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.1.40
NETMASK=255.255.255.0
GATEWAY=192.168.1.1
```

Cliente con IP dinámica (DHCP)

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=dhcp
IPADDR=
NETMASK=
GATEWAY=
```

  - **Debian o Suse:** `/etc/network/interfaces`

Cliente con IP fija

```
auto eth0
iface eth0 inet static
        address 192.168.1.40
        netmask 255.255.255.0
        network 192.168.1.0
        broadcast 192.168.0.255
        gateway 192.168.1.1
```

Cliente con IP dinámica (DHCP)

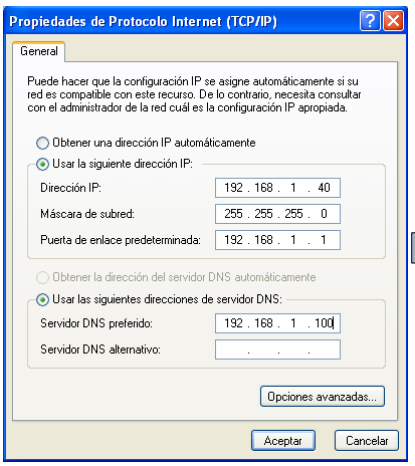
```
auto eth0
iface eth0 inet dhcp
```


DHCP: Configuración Dinámica de Hosts

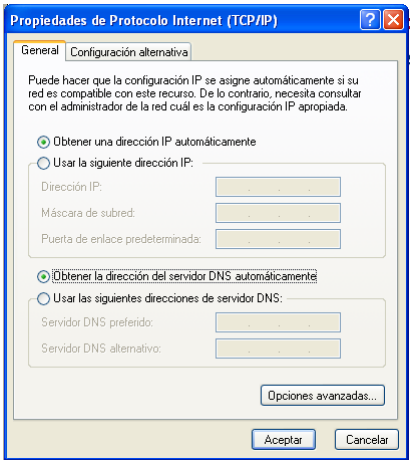
Configuración del cliente DHCP en Windows

- Necesario modificar las propiedades de TCP/IP

Cliente con IP fija



Cliente con IP dinámica (DHCP)



Firewalls: conceptos básicos

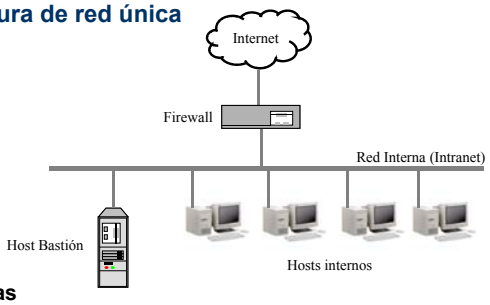
- Funciones principales de un firewall
  - Filtrado de paquetes
    - El firewall protege un equipo o una red controlando y limitando los paquetes de entrada y de salida
  - Registro de actividad (LOG)
    - El firewall puede registrar las acciones realizadas con los paquetes que entran o salen del equipo o de la red
  - Traducción de direcciones de red (NAT)
    - La mayoría de firewalls permiten realizar operaciones de NAT
- Tipos de firewalls
  - Firewalls personales
    - Aplicación software para proteger un único equipo de forma individual
  - Firewalls de red
    - Permiten filtrar el tráfico de entrada o salida de una red completa
    - Pueden ser de dos tipos:
      - Router dedicado con posibilidad de filtrado (Cisco, 3Com, etc.)
      - Computador con varias tarjetas y un software adecuado (Linux+IPTables, Solaris+SunScreen, NT+Firewall-1, etc.)

Firewalls: Nomenclatura típica

- **Host bastión**
  - Es un sistema que representa un punto crítico de la seguridad de la intranet
    - Es un sistema muy vulnerable a ataques al ser un sistema visible desde Internet y tener numerosos puertos abiertos
    - Suele se objetivo habitual de atacantes
    - Muchas de las medidas de seguridad de la red deben centrase en el host bastión
  - El host bastión suele ser una máquina que ofrece uno o varios servicios tanto a usuarios internos como externos:
    - Servidor de Web y FTP anónimo para usuarios externos
    - Servidor de DNS para usuarios internos
    - Servidor de correo electrónico
- **Host interno**
  - Es un sistema conectado a la intranet que puede contener información privada y confidencial de la empresa/organismo/institución
    - El acceso a los hosts internos desde el exterior debe ser restringido
      - Totalmente prohibido o únicamente permitido para usuarios autorizados y debidamente autentificados
    - Los host internos deben tener un grado de seguridad elevado
      - Los puertos no usados deben estar cerrados
      - Sólo debe permitir conexiones seguras (ssh, etc)

Arquitecturas de firewall (1)

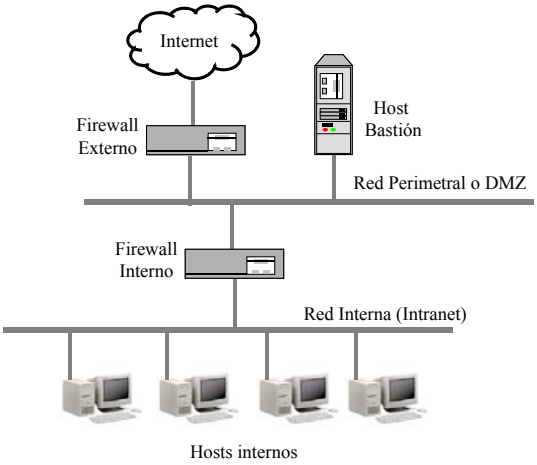
Arquitectura de red única



- **Ventajas**
  - Arquitectura sencilla. Solución económica
  - Mantenimiento de un único firewall
- **Desventajas**
  - El host bastión está ubicado en la misma red que los hosts internos
    - La posible vulneración del bastión pone en peligro la integridad de toda la red
  - Si un atacante consigue entrar en el host bastión:
    - Puede acceder a todos los datos privados que circulan por la red mediante un simple sniffer
    - Puede acceder con mayor facilidad a otros hosts internos de la red

Arquitecturas de firewall (2)

Arquitectura de red perimetral o DMZ



Arquitecturas de firewall (3)

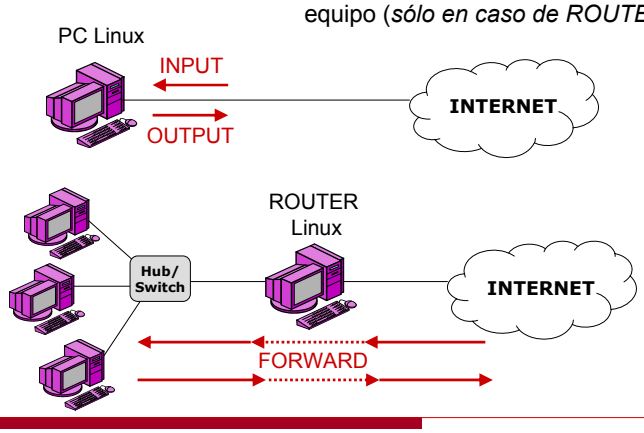
Elementos de la arquitectura de red perimetral o DMZ

- Red perimetral o DMZ (Demilitarized Zone)
  - Esta red alberga al host bastión
  - También se denomina red de servicios, ya que las máquinas que ofrecen servicios a Internet están ubicadas en esta red
  - La información que circula por la DMZ es considerada insegura (no confidencial)
  - Si un atacante consigue entrar en el host bastión puede ver toda la información que circula por esta red
  - Sin embargo, este atacante no puede ver la información que circula por la red interna
- Host bastión
  - Está ubicado en la DMZ, protegido únicamente por el firewall externo
  - Ofrece uno o varios servicios tanto a usuarios internos como externos
- Hosts internos
  - Están protegidos por el firewall externo e interno
  - Un atacante que consigue vulnerar el FW externo y entrar en el bastión, tiene un obstáculo adicional para poder alcanzar a los hosts internos
- Firewall interno
  - También se denomina firewall de contención o de choque (*choke firewall*)
  - Realiza el filtrado del tráfico entre la DMZ y la red interna
- Firewall externo
  - También se denomina firewall de acceso
  - Realiza el filtrado del tráfico entre Internet y la DMZ

Reglas de filtrado: IPtables de Linux (1)

Cadenas de reglas de filtrado

- Cadena INPUT → Para paquetes que entran al equipo
- Cadena OUTPUT → Para paquetes que salen del equipo
- Cadena FORWARD → Para paquetes que pasan a través del equipo (*sólo en caso de ROUTERS*)



Reglas de filtrado: IPtables de Linux (2)

Principales criterios de filtrado de IPTables

Opción/Ejemplo	Significado
-A INPUT -A OUTPUT -A FORWARD	Añade regla a cadena de entrada Añade regla a cadena de salida Añade regla a la cadena forward (sólo en caso de routers)
-s 192.168.1.1 -d 140.10.15.1	Filtrado por dirección IP origen Filtrado por dirección IP destino
-p tcp -p udp -p icmp	Filtrado de paquetes TCP Filtrado de paquetes UDP Filtrado de paquetes ICMP
--sport 3000 --dport 80 --icmp_type 8	Filtrado por nº de puerto origen (sólo para TCP o UDP) Filtrado por nº de puerto destino (sólo para TCP o UDP) Filtrado por código del paquete ICMP (sólo para ICMP)
-i eth0 -o eth1	Filtrado por interfaz de red de entrada Filtrado por interfaz de red de salida

Reglas de filtrado: IPtables de Linux (3)

Filtrado por estado de la conexión

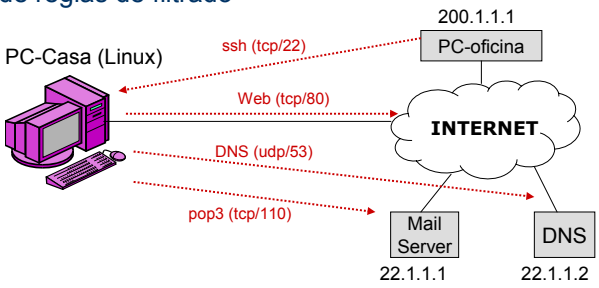
Opción	Significado
-m state --state NEW	Filtrado de paquetes correspondientes a conexiones nuevas (el primer paquete visto en una conexión)
-m state --state ESTABLISHED	Filtrado de paquetes correspondientes a conexiones ya establecidas
-m state --state RELATED	Filtrado de paquetes relacionados con otras conexiones existentes (Ej. conexión de datos FTP, o paquetes ICMP)
-m state --state INVALID	Filtrado de paquetes que no pertenecen a ninguno de los estados anteriores

Acciones

Opción	Significado
-j ACCEPT	El paquete es aceptado
-j DROP	El paquete es rechazado

Reglas de filtrado: IPtables de Linux (4)

Ejemplo de reglas de filtrado



- Conexiones entrantes permitidas
  - Servicio SSH desde PC-oficina (200.1.1.1)
- Conexiones salientes permitidas
  - Servicio web a cualquier destino
  - Servicio pop3 a servidor de correo (22.1.1.1)
  - Servicio DNS a servidor DNS (22.1.1.2)
- Resto conexiones: RECHAZADAS

Reglas de filtrado: IPtables de Linux (5)

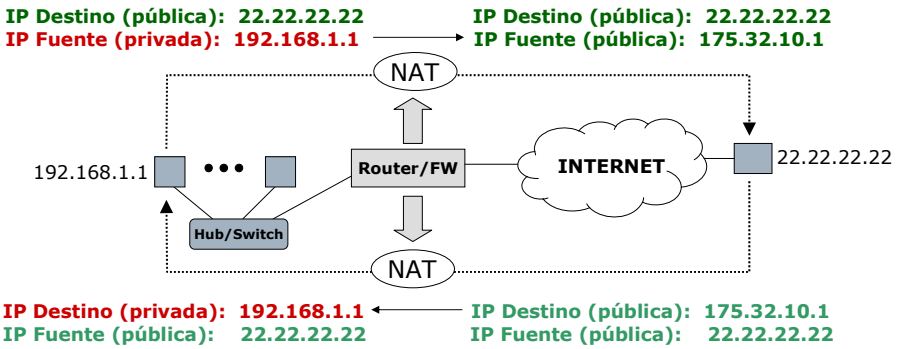
Ejemplo de reglas de filtrado (cont.)

```
# Establecemos política por defecto para cadenas INPUT, OUPUT y FORWARD
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
# Dejamos entrar o salir cualquier paquete correspondiente a
# conexiones establecidas o relacionadas
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
# Permitimos conexiones entrantes SSH (tcp/22) desde pc-oficina
iptables -A INPUT -s 200.1.1.1 -p tcp --dport 22 -m state   \
        --state NEW -j ACCEPT
# Permitimos conexiones web salientes (tcp/80) a cualquier destino
iptables -A OUTPUT -p tcp --dport 80 -m state --state NEW -j ACCEPT
# Permitimos conexiones pop3 salientes (tcp/110) con servidor de correo
iptables -A OUTPUT -d 22.1.1.1 -p tcp --dport 110 -m state   \
         --state NEW -j ACCEPT
# Permitimos conexiones DNS salientes (udp/53) con servidor DNS
iptables -A OUTPUT -d 22.1.1.2 -p udp --dport 53 -m state   \
         --state NEW -j ACCEPT
```

NAT: Traducción de Direcciones de Red

NAT (Network Address Translation)

- Redes privadas
  - Necesidad de traducir IP privadas a IP públicas



NAT: Traducción de Direcciones de Red

Tipos de NAT (1)

- NAT estático
  - N direcciones privadas ⟷ N direcciones públicas
  - Asignación fija
  - Ejemplo (N=7)

Tabla de traducción NAT (estática)

IP Privada	IP Pública
192.168.1.1	175.20.12.1
192.168.1.2	175.20.12.2
192.168.1.3	175.20.12.3
192.168.1.4	175.20.12.4
192.168.1.5	175.20.12.5
192.168.1.6	175.20.12.6
192.168.1.7	175.20.12.7

NAT: Traducción de Direcciones de Red

Tipos de NAT (2)

- NAT dinámico
  - N direcciones privadas ⟷ M direcciones públicas (M<N)
  - Asignación dinámica
    - Sólo puede darse salida a Internet a M máquinas simultáneamente
  - Ejemplo (N=7; M=3)

Tabla de traducción NAT (dinámica)

IP Privada	IP Pública
192.168.1.3	175.20.12.1
192.168.1.7	175.20.12.2
192.168.1.5	175.20.12.3

192.168.1.1
192.168.1.2
192.168.1.4
192.168.1.6
} Sin posibilidad de acceso a Internet hasta que se libere una IP pública

NAT: Traducción de Direcciones de Red

Tipos de NAT (3)

- NAPT (Network Address/Port Translation) o Masquerading
  - N direcciones privadas ⟷ 1 dirección pública
  - Funcionamiento
    - La única IP pública disponible es la IP pública del Router/FW
    - El nº puerto cliente de la máquina origen se traduce a un puerto libre del Router/FW
  - Ejemplo:

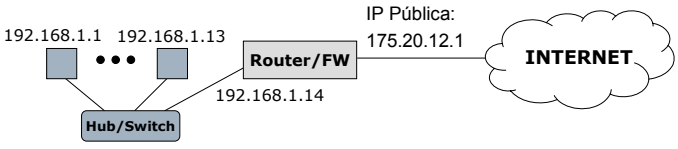


Tabla de traducción NAPT

IP_Privada:Port_Cliente	IP_Pública:Port_Cliente_FW
192.168.1.1:3289 →	175.20.12.1:10001
192.168.1.7:4256 →	175.20.12.1:10002
192.168.1.5:3882 →	175.20.12.1:10003

NAT: Traducción de Direcciones de Red

Tipos de NAT (4)

- Port Forwarding o Virtual Servers
  - N direcciones privadas ⟷ 1 dirección pública
  - Permite tener servidores en la red privada "visibles" desde Internet
    - Desde Internet, todos los servidores se ven con una misma IP pública (la IP del Router/FW)
    - El Router/FW debe redireccionar los paquetes al servidor real de la red interna
- Ejemplo:

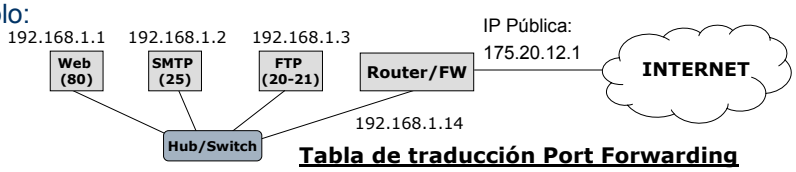


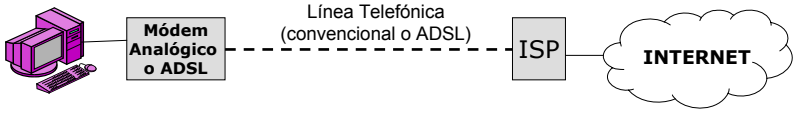
Tabla de traducción Port Forwarding

IP_Privada:Port_Servidor	IP_Pública:Port_Servidor
192.168.1.1:80 ←	175.20.12.1:80
192.168.1.2:25 ←	175.20.12.1:25
192.168.1.3:20 ←	175.20.12.1:20
192.168.1.3:21 ←	175.20.12.1:21

NAT: Traducción de Direcciones de Red

Configuraciones de redes de acceso telefónico y ADSL (1)

- Configuración 1: módem convencional o módem ADSL
  - Un solo PC conectado a Internet (monopuesto)
    - No necesario NAT



- Configuración 2: Router ADSL
  - Varios PCs conectados a Internet a través del router (multipuesto)
    - El propio router ADSL puede hacer NAPT y Port Forwarding (según configuración)

NAT: Traducción de Direcciones de Red

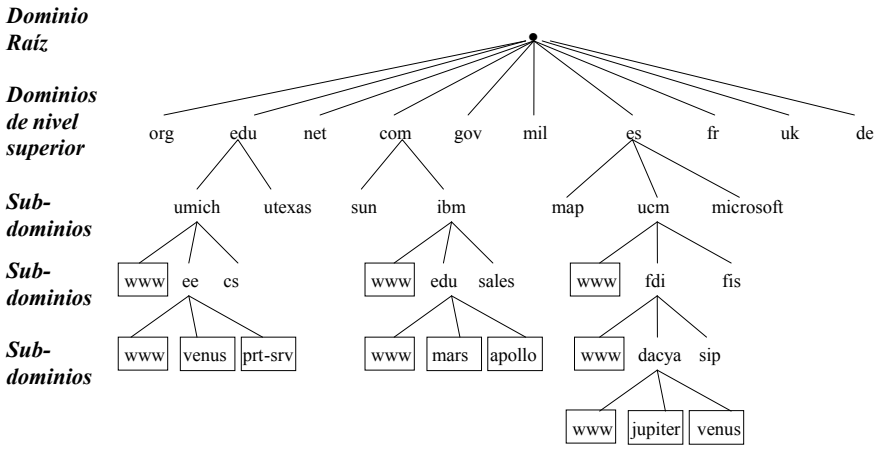
- **Configuraciones de redes de acceso telefónico y ADSL (2)**
  - Configuración 3: módem convencional o ADSL + Router Linux
    - El PC conectado a Internet a través de módem se configura como un Router
      - Preferible S.O. Linux en el router
      - Implementación de NAPT y Port Forwarding mediante IPTables

DNS: Sistema de nombres de dominio

- **Introducción a DNS (1)**
  - Para qué sirve DNS
    - Servicio para traducir nombres simbólicos a direcciones IP
      - Ejemplo: www.ucm.es → 147.96.1.15
    - Los nombres son mucho más fáciles de recordar que las direcciones IP
  - La resolución de nombres local (archivo /etc/hosts)
    - En los primeros años de Internet el único mecanismo de traducción que existía, consistía en una base de datos local en el archivo **/etc/hosts**
      - Actualmente este fichero se sigue usando y suele contener las máquinas de nuestra red que más utilizamos
    - Problema que plantea la resolución local
      - Los nombres deben ser únicos (no pueden existir dos nombres iguales)
      - En la actualidad existen millones de máquinas conectadas a Internet
        - El mantenimiento de un fichero de resolución local con todas las máquinas de Internet es inviable

DNS: Sistema de nombres de dominio

Organización jerárquica de DNS (1)



DNS: Sistema de nombres de dominio

Organización jerárquica de DNS (2)

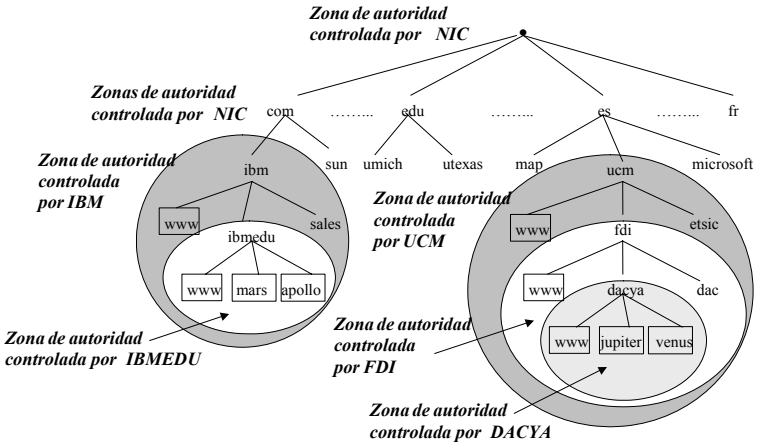
- Dominios de nivel superior
  - Dominios genéricos
    - **com:** organizaciones comerciales
    - **edu:** organizaciones educativas (principalmente norteamericanas)
    - **org:** organizaciones sin ánimo de lucro
    - **net:** organizaciones relacionadas con Internet y servidores de acceso
    - **gov:** instituciones gubernamentales norteamericanas
    - **mil:** instituciones militares norteamericanas
    - **arpa:** Dominio para la resolución inversa de direcciones
  - Dominios de países
    - **es:** España
    - **fr:** Francia
    - **uk:** Reino Unido
    - **it:** Italia
    - **de:** Alemania
    - **jp:** Japón
    - **mx:** Méjico
    - **ar:** Argentina
    - **….**

DNS: Sistema de nombres de dominio

- **Nombres DNS**
  - Nombres de dominio completamente cualificados (FQDN, Fully Qualified Name of a Domain)
    - Un nombre completamente cualificado se especifica añadiendo al nombre del nodo, todos los nombres de dominios, usando el punto como separador, hasta llegar al **dominio raíz**, que también se representa mediante un punto final
    - Ejemplos
      - jupiter.dacya.fdi.ucm.es.
      - mars.edu.ibm.com.
  - Restricciones en los nombres de dominios
    - No hay límite en el número de subdominios de la jerarquía
    - No obstante es necesario observar algunas restricciones
      - El FQDN puede ocupar un máximo de 255 caracteres (incluyendo los puntos)
      - Cada nombre de dominio o subdominio, puede tener un máximo de 63 caracteres
      - Los nombres únicamente pueden llevar caracteres alfanuméricos y guiones. (el resto de signos de puntuación y otros caracteres están prohibidos)

DNS: Sistema de nombres de dominio

- **Servidores DNS y zonas de autoridad (1)**
  - Cada servidor DNS de la red tiene asignada una ZONA DE AUTORIDAD
    - Una zona de autoridad es el espacio de nombres para el cual el servidor tiene autoridad



DNS: Sistema de nombres de dominio

Servidores DNS y zonas de autoridad (2)

Zona de autoridad raíz y servidores de nombres raíz

- La zona de autoridad raíz (.), está gestionada por el NIC (Network Information Center)
  - Consta de 13 servidores de nombres raíz repartidos por distintos países (por motivos de seguridad)
    - a.root-servers.net
    - b.root-servers.net
    - c.root-servers.net
    - …..
  - El fichero con las direcciones de todos los servidores raíz se puede obtener de
    - ftp://ftp.rs.internic.net/domain/named.root
- Información almacenada en los servidores raíz
  - Los servidores raíz conocen las direcciones IP de todos los servidores de nombres de los dominios de nivel superior (com., org., net., es., fr., …)
  - Los servidores raíz no conocen las direcciones del resto de máquinas de cada uno de estos dominios

Zonas de autoridad de dominios de nivel superior

- Cada dominio de nivel superior (com., org., net., es., fr., …) es una zona de autoridad distinta
  - Estas zonas están gestionadas por el NIC (ARIN, RIPE, APNIC, etc.)
  - Cada zona cuenta con un número variable de servidores de nombres
- Información almacenada en los servidores de nivel superior
  - Estos servidores conocen las direcciones IP de todos los servidores DNS de los subdominios que dependen directamente de ellas
  - Estos servidores no conocen en detalle las direcciones del resto de máquinas de cada uno de los subdominios

DNS: Sistema de nombres de dominio

Servidores DNS y zonas de autoridad (3)

Zonas de autoridad de subdominios

- Cada subdominio puede estar dividido en una o varias zonas de autoridad
- Si un subdminio forma una única zona de autoridad
  - El servidor DNS del dominio deberá conocer en detalle los nombres y direcciones IP de todas las máquinas del dominio
- Si un subdminio está dividido a su vez en varias zonas de autoridad
  - El servidor DNS de mayor nivel conocerá
    - Los nombres y direcciones IP de todas las máquinas que dependen de él
    - Los servidores DNS de las zonas de autoridad independientes por debajo de él (no conocerá en detalle las organización de estas zonas de autoridad independientes)
    - La lista de servidores DNS raíz
  - El servidor DNS de zonas de autoridad por debajo conocerá
    - Los nombres y direcciones IP de las máquinas que dependen de él
    - La lista de servidores DNS raíz

DNS: Sistema de nombres de dominio

Servidores DNS y zonas de autoridad (4)

- Ejemplo
  - Los servidores DNS raíz (**.**) conocerán
    - Los servidores DNS de los dominios .com, .org, .net, .es, .fr. …..
    - No conocerán en detalle los nombres y direcciones de las máquinas dentro de estos dominios
  - Los servidores DNS del dominio **es.** conocerán
    - La lista de servidores DNS raíz
    - Los servidores DNS de los subdominios map.es., ucm.es., microsoft.es., …
    - No conocerán en detalle los nombres y direcciones de las máquinas dentro de estos subdominios
  - Los servidores DNS del dominio **ucm.es.** conocerán
    - La lista de servidores DNS raíz
    - Los nombres y direcciones de todas las máquinas que dependen directamente de él (www.ucm.es., ftp.ucm.es., etc.)
    - Los servidores DNS de los subdominios que formen una zona de autoridad (fdi.ucm.es., fis.ucm.es., …)
      - No conocerán en detalle los nombres y direcciones de las máquinas dentro de los subdominios que formen una zona de autoridad independiente

DNS: Sistema de nombres de dominio

Servidores DNS y zonas de autoridad (5)

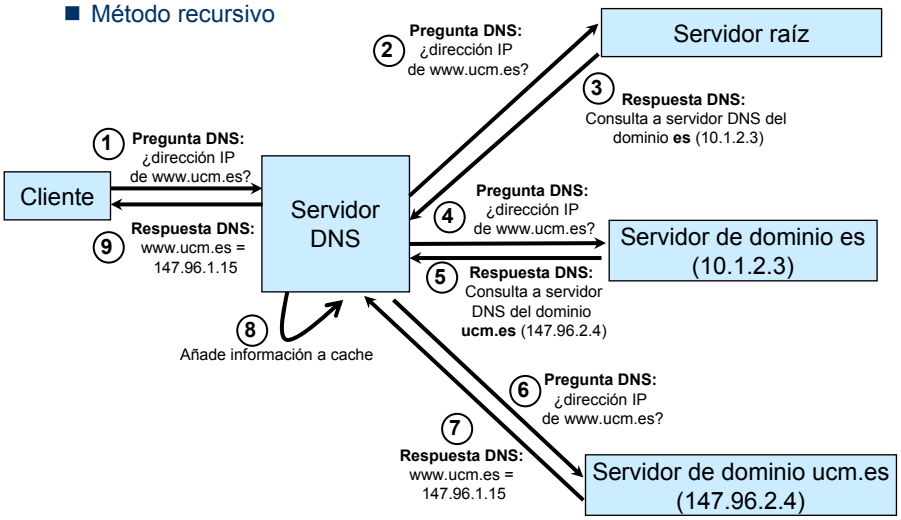
- Ejemplo (cont.)
  - Los servidores DNS del dominio **fdi.ucm.es.** conocerán
    - La lista de servidores DNS raíz
    - Los nombres y direcciones de todas las máquinas que dependen directamente de él (www.fdi.ucm.es., ftp.fdi.ucm.es., etc.).
      - Esto incluye los nombres y direcciones de todas las máquinas que pertenecen a subdominios que NO forman una zona de autoridad independiente (por ejemplo pc-1.sip.fdi.ucm.es.)
    - Los servidores DNS de los subdominios que formen una zona de autoridad (dacya.fdi.ucm.es.)
      - No conocerán en detalle los nombres y direcciones de las máquinas dentro de los subdominios que formen una zona de autoridad independiente
  - Los servidores DNS del dominio **dacya.fdi.ucm.es.** conocerán
    - La lista de servidores DNS raíz
    - Los nombres y direcciones de todas las máquinas que dependen directamente de él (www.dacya.fdi.ucm.es., venus.dacya.fdi.ucm.es., jupiterdacya.fdi.ucm.es., etc.)

DNS: Sistema de nombres de dominio

- **Tipos de servidores DNS**
  - Servidores primarios o maestros
    - Mantiene la base de datos con la información sobre la zona
      - Los cambios sobre la información del dominio se llevan a cabo en el servidor primario
  - Servidores secundarios o esclavos
    - Poseen una copia de la base de datos del servidor primario.
      - Proporciona redundancia frente a fallos
      - Permiten equilibrar la carga de la red, ya que pueden resolver nombres igual que los servidores primarios
      - Periódicamente se sincronizan con el servidor primario para tener siempre la información actualizada
  - Servidores de sólo cacheo
    - No mantiene ninguna zona
    - Sólo almacena en su memoria temporal las consultas que recibe de los clientes, para utilizarlas en caso de una nueva consulta.

DNS: Sistema de nombres de dominio

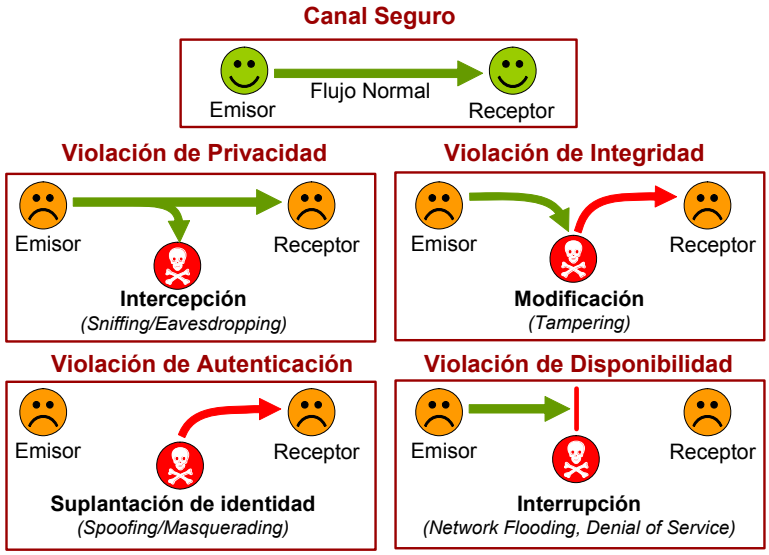
- **El proceso de resolución de nombres**
  - Método recursivo



Aspectos clave de la seguridad

- Confidencialidad
  - Debe garantizarse que la información enviada sólo puede ser leída por personas debidamente autorizadas.
- Integridad
  - Debe garantizarse que la información no puede ser alterada en el transcurso hacia su destino.
- Autenticación
  - Debe garantizarse que los participantes en el intercambio de información son realmente quienes dicen ser
- Disponibilidad
  - Debe garantizarse la información está disponible en el momento adecuado para las personas autorizadas

Clasificación de las amenazas



Técnicas de criptografía o cifrado de los datos (1)

- Utilidad
  - Permiten garantizar la **confidencialidad** de los datos
- Principales técnicas de criptografía o cifrado de la información
  - Encriptación por clave simétrica
  - Encriptación por clave pública
  - Encriptación por clave secreta compartida
  - Encriptación por clave de sesión

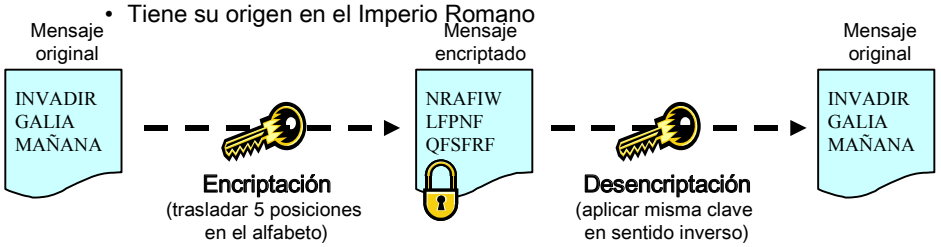
Técnicas de criptografía o cifrado de los datos (2)

¿Qué es la criptografía?

- Técnica que permite
  convertir un texto legible o plano ("*plain text*")
  en un texto encriptado o cifrado ("*cipher text*")
  a través de la aplicación del un algoritmo de cifrado
  basado en una clave criptográfica (LLAVE)

El origen de la criptografía

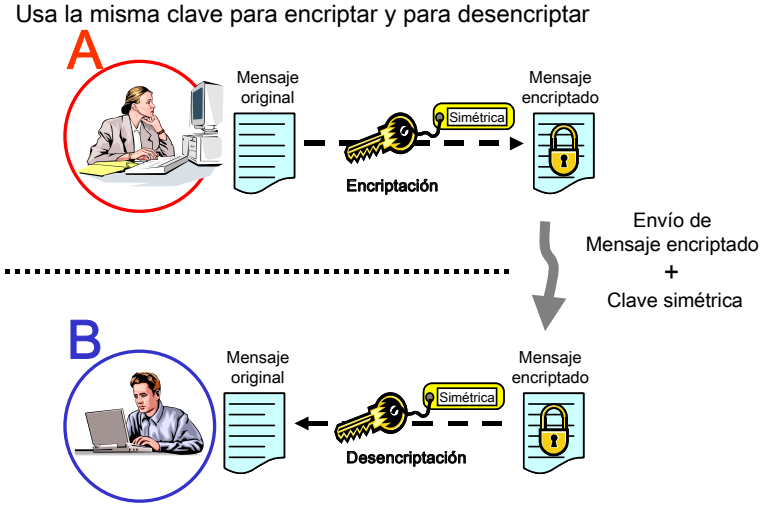
- Tiene su origen en el Imperio Romano



Técnicas de criptografía o cifrado de los datos (3)

Criptografía de clave simétrica (i)

- Usa la misma clave para encriptar y para desencriptar



Técnicas de criptografía o cifrado de los datos (4)

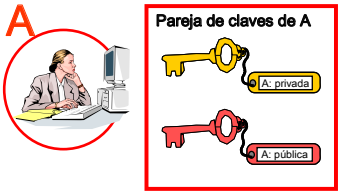
Criptografía de clave simétrica (ii)

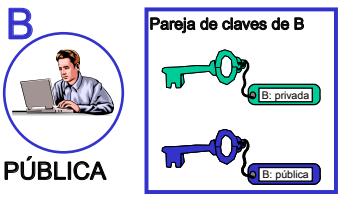
- **Ventajas**
  - Mecanismo muy rápido
- **Problemas**
  - Necesidad de distribuir la clave
  - Si alguien consigue leer el mensaje y la clave podrá descifrar el mensaje
- **Ejemplos de algoritmos de clave simétrica**
  - DES (Data Encryption Standard)
  - 3DES (Triple DES)
  - RC2, RC4, RC5 (Ron´s Code, version 2, 4, 5)
  - AES (Advanced Encription Standard)

Técnicas de criptografía o cifrado de los datos (5)

Criptografía de clave asimétrica o pública (i)

- Cada usuario del sistema ha de poseer una pareja de claves:
  - **Clave privada:** será custodiada por su propietario y no se dará a conocer a nadie
  - **Clave pública**: será conocida por todos los usuarios



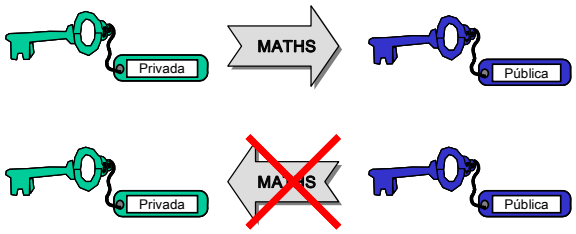


- La pareja de claves es **complementaria**:
  - Mensaje cifrado con **CLAVE PRIVADA**
    → Sólo puede ser descifrado con **CLAVE PÚBLICA**
  - Mensaje cifrado con **CLAVE PÚBLICA**
    → Sólo puede ser descifrado con **CLAVE PRIVADA**

Técnicas de criptografía o cifrado de los datos (6)

Criptografía de clave asimétrica o pública (ii)

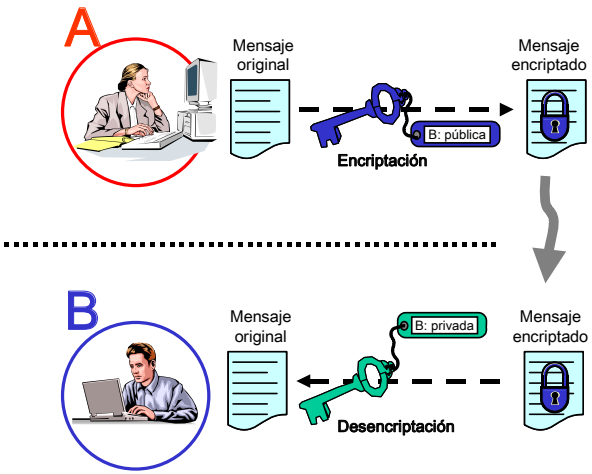
- **Relación matemática entre las claves**
  - La clave pública se genera matemáticamente a partir de la privada
  - Sin embargo, obtener la clave privada a partir de la pública es matemáticamente y computacionalmente imposible



Técnicas de criptografía o cifrado de los datos (7)

Criptografía de clave asimétrica o pública (iii)

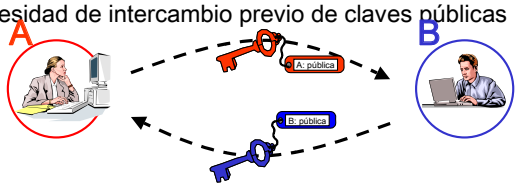
- **Funcionamiento**



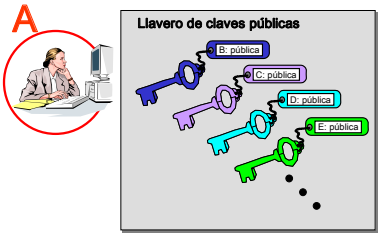
Técnicas de criptografía o cifrado de los datos (8)

Criptografía de clave asimétrica o pública (iv)

- **Funcionamiento**
  - Necesidad de intercambio previo de claves públicas



  - Colección de claves públicas de otros usuarios:
    Llavero de claves públicas



Técnicas de criptografía o cifrado de los datos (9)

Criptografía de clave asimétrica o pública (v)

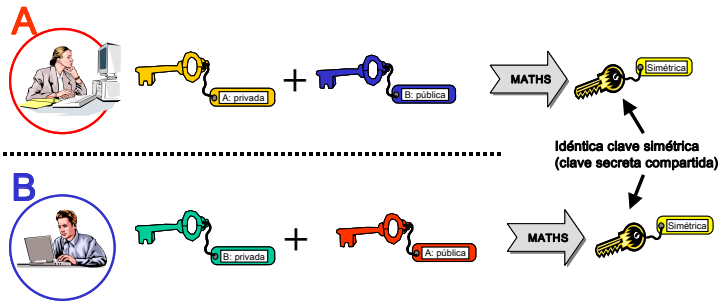
- **Ventajas**
  - Muy seguro
- **Desventaja**
  - Proceso de cifrado lento
  - Poco recomendable para mensajes muy largos
- **Solución:**
  - Combinar mecanismo de clave simétrica con mecanismo de clave asimétrica

- **Ejemplos de algoritmos de clave asimétrica o pública**
  - RSA (Rivest, Shamir y Adleman)

Técnicas de criptografía o cifrado de los datos (10)

Encriptación por clave secreta compartida (i)

- Basado en clave simétrica
  - La clave simétrica no se intercambia
  - La genera cada uno de los extremos de la siguiente manera



Técnicas de criptografía o cifrado de los datos (11)

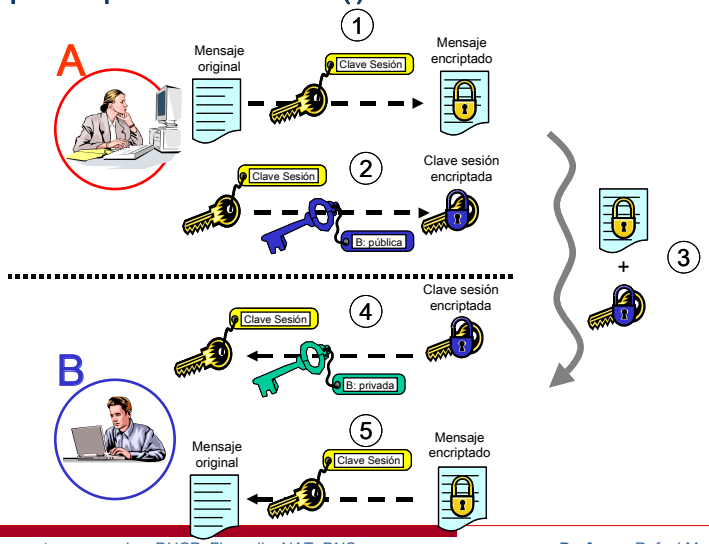
Encriptación por clave secreta compartida (ii)

- **Ventajas**
  - Rápido al ser simétrico
  - Seguro, al no tener que intercambiar la clave
- **Inconvenientes**
  - Capa pareja de usuarios utiliza siempre la misma clave
  - Cuanto más veces se utiliza una clave, más fácil es averiguar dicha clave

- **Ejemplos**
  - Diffie-Hellman

Técnicas de criptografía o cifrado de los datos (12)

Encriptación por clave de sesión (i)



Técnicas de criptografía o cifrado de los datos (13)

Encriptación por clave de sesión (ii)

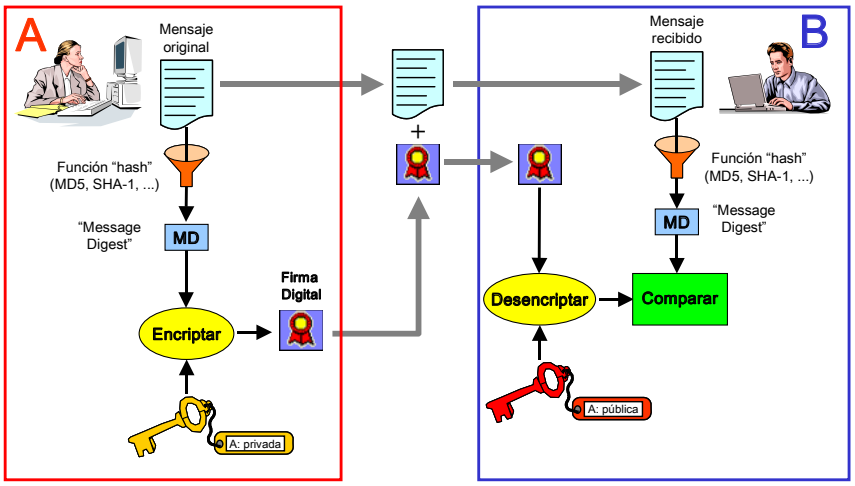
- **Ventajas**
  - Rápido al ser simétrico
  - Seguro
    - La clave de sesión se envía encriptada
    - Para cada transmisión se utiliza una clave de sesión distinta

- **Ejemplos**
  - SSL (Secure Socket Layer)
    - Utilizado en servidores Web seguros (https)

Autenticación e Integridad: firmas y certificados digitales (1)

- ¿Para qué sirve una firma digital?
  - Permite al receptor verificar la identidad del remitente
    - ➔ Autenticación
  - Permite al receptor verificar que la información no ha sido modificada
    - ➔ Integridad
- La firma se genera a partir de:
  - La clave privada del remitente
    - El remitente debe disponer de una pareja de claves pública y privada
    - La clave privada se emplea para generar la firma digital
    - Esto garantiza la autenticación
  - El mensaje original
    - A partir del mensaje original, se aplica una función de resumen (hash)
    - Este resumen se encripta con la clave privada, formando la firma digital del remitente
    - Esto garantiza la integridad

- **Autenticación e Integridad: firmas y certificados digitales (2)**
  - Generación de la firma digital



- **Autenticación e Integridad: firmas y certificados digitales (3)**
  - Generación de la firma digital: la función HASH
    - Características
      - Transformar un texto de longitud variable en un bloque de longitud fija
      - Longitud pequeña (algunas son de 16 bits).
      - Irreversible
      - Propiedad de no colisión
      - Sencilla de implementar
    - Ejemplos
      - MD4 (Message Digest 4).
      - MD5 (Message Digest 5).
      - SHA-1 (Secure Hash Algorithm 1).

Autenticación e Integridad: firmas y certificados digitales (4)

Combinación de firma digital y encriptación

	No encriptado No firmado	Encriptado No firmado	No encriptado Firmado	Encriptado Firmado
Confidencialidad	NO	SÍ	NO	SÍ
Integridad	NO	NO	SÍ	SÍ
Autenticación	NO	NO	SÍ	SÍ

Problemas de la firma digital

- ¿Cómo tener certeza de que la clave pública de un usuario corresponde realmente a ese individuo y no ha sido falsificada por otro?
- ¿Quién verifica la identidad del poseedor de la clave pública?

Solución

- Certificados digitales

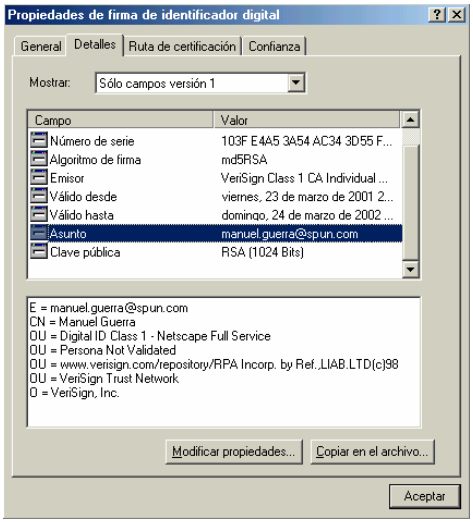
Autenticación e Integridad: firmas y certificados digitales (5)

Certificados digitales

- ¿Qué es un certificado digital?
  - Fichero digital intransferible y no modificable,
  - Emitido por una tercera parte de confianza (**Autoridad de Certificación**)
  - Que asocia a una persona o identidad una clave pública.
- Autoridad de Certificación (CA)
  - Organización emisora de certificados digitales

- **Autenticación e Integridad: firmas y certificados digitales (6)**
  - Información contenida en un certificado digital

- **Autenticación e Integridad: firmas y certificados digitales (7)**
  - Ejemplo de certificado digital



Seguridad en la Web: protocolo SSL (1)

Utilidad del protocolo SSL en servidores Web

- Se utiliza para transacciones seguras a través de WEB (**servicio https**)
  - Compras por Internet
  - Banca Electrónica
  - Etc.
- Basado en el mecanismo de **encriptación por clave de sesión**
  - El servidor debe disponer de un certificado digital válido
    - Este certificado contiene la clave pública del servidor
  - El cliente no necesita disponer de un certificado digital
    - La clave simétrica se encripta con la clave pública del servidor

Seguridad en la Web: protocolo SSL (2)

Funcionamiento del protocolo SSL

- El cliente se conecta a una página Web de tipo https
- El servidor envía su Certificado Digital al cliente, que incluye la clave pública del servidor
- El cliente comprueba que el certificado ha sido emitido por una CA de confianza y que dicho certificado es válido
- El cliente y el servidor acuerdan un algoritmo de encriptación soportado por ambas partes
- El cliente genera una clave simétrica de sesión
- El cliente encripta la clave de sesión con la clave pública del servidor y envía dicha clave encriptada
- El servidor recibe la clave de sesión y la desencripta con su clave privada
- El cliente y el servidor, a partir de este momento, se comunican de forma cifrada usando la clave de sesión compartida