UNCUYO
UNIVERSIDAD NACIONAL DE CUYO
FACULTAD DE INGENIERÍA
Licenciatura en Ciencias de la Computación

Redes de Computadoras

Unidad 6

Seguridad en Redes

Dr. Ing. Pablo Daniel Godoy (pablo.godoy@ingenieria.uncuyo.edu.ar)

Temario

- **Problemas de seguridad en redes de computadoras**
- Criptografía de clave simétrica y de clave pública
- Generación de claves secretas compartidas
- Firmas digitales y certificados
- Implementaciones de seguridad

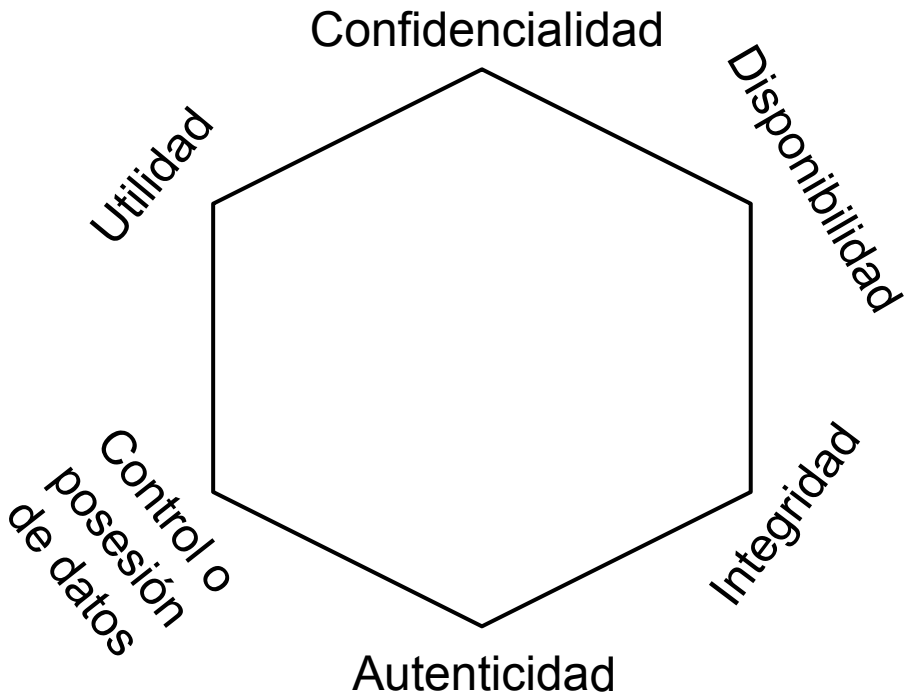
El tema seguridad Informática es muy amplio, siendo la seguridad en redes de computadoras una parte del mismo.

Seguridad en redes de computadoras

- Tipos problemas de seguridad en redes de computadoras: Los problemas de seguridad pueden atacar:
  - **Confidencialidad** o **privacidad**: Que alguien pueda ver datos a los que no tiene permiso (contraseñas, datos privados personales o de empresas, etc.).
  - **Control de los datos**: Que solo el propietario pueda hacer uso de los datos.
  - **Autenticación**: El atacante se hace pasar por una empresa o persona.
  - **No repudio**: Negar que se envió un mensaje que efectivamente se envió.
  - **Integridad**: Que un mensaje sea alterado.
  - **Disponibilidad**: Impedir el acceso a servicios disponibles a través de redes de computadoras.
  - **Utilidad**: Hacer que la información o recursos pierdan utilidad (ejemplo: ransomware).
- Los algoritmos de seguridad pueden implementarse tanto en hardware (velocidad) o software (flexibilidad).

Triángulo de seguridad

Hexágono Parkerian



Pasos usuales de un ataque

- 1° paso: **Conocer al objetivo**
  - IPs visibles desde el exterior.
  - Servicios ofrecidos (escaneo de puertos).
  - Sistemas operativos, versiones de los mismos, servidores que se ejecutan, versiones, etc.
- 2° paso: muy variable.
  - Utilizar un “**exploit**” (herramienta creada para aprovechar vulnerabilidades).
  - Idear un **mecanismo de ataque**.

Algunos tipos de ataques

Tipos: Según la RFC 2828 pueden ser **Pasivos** (intenta ver información si afectar el sistema) y **activos** (influye en el funcionamiento de la red o altera recursos).

Ataques pasivos

- **Sniffing** (escuchar tráfico pasivamente) .
  - Dos propósitos:
    - Ver el mensaje.
    - Análisis de tráfico: Determinar la ubicación de las computadoras, frecuencia y longitud de los mensajes, etc, y obtener alguna información útil para el atacante.
  - Junto con el escaneo de puertos suele ser el primer paso antes de un ataque.
  - Crítico si quien escucha captura información importante (claves de cuentas bancarias, etc.).
  - A través de software o hardware (Interfaz en modo promiscuo[1]).

[1] Interfaz que camptura todo el tráfico que recibe.

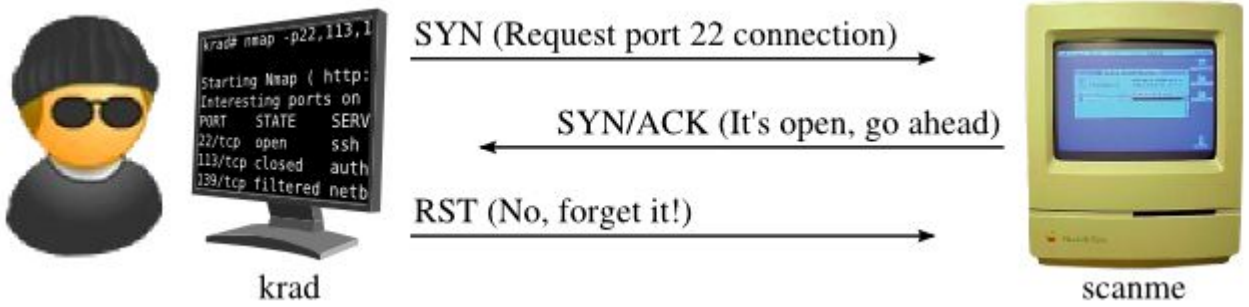
Algunos tipos de ataques

- **Escaneo de puertos**
  - Propósito: Obtener información de objetivos a atacar para detectar vulnerabilidades.
    - Escaneo Ping: conocer computadoras visibles desde el exterior.
    - Escaneo TCP o UDP a diferentes puertos: conocer servicios brindados por una computadora.
    - Escaneo con diferentes combinaciones de sondas:
      - Conocer sistemas operativos, software que implementa diferentes servicios, versiones, etc.
        - Diferentes SO y software responden de diferentes maneras.
      - Saltar firewalls o sistemas de detección de intrusos: Un firewall podría bloquear algunos tipos de mensajes (por ejemplo: SYN), pero otros no (por ejemplo: FIN).

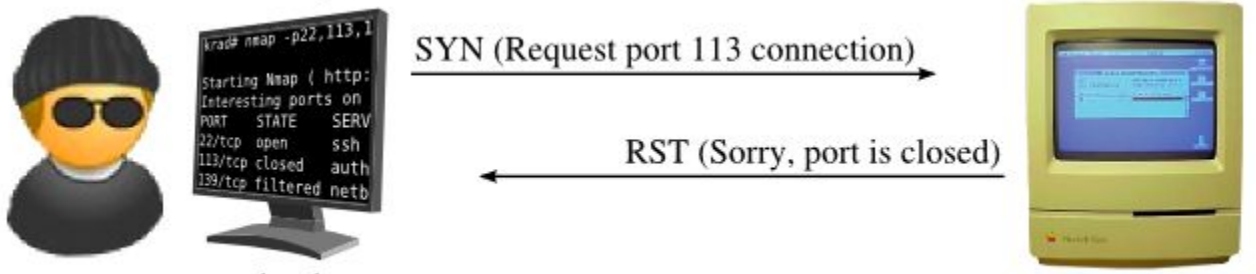
UNCU
UNIVERSIDAD NACIONAL

as de la

Puerto abierto



Puerto cerrado



Puerto filtrado

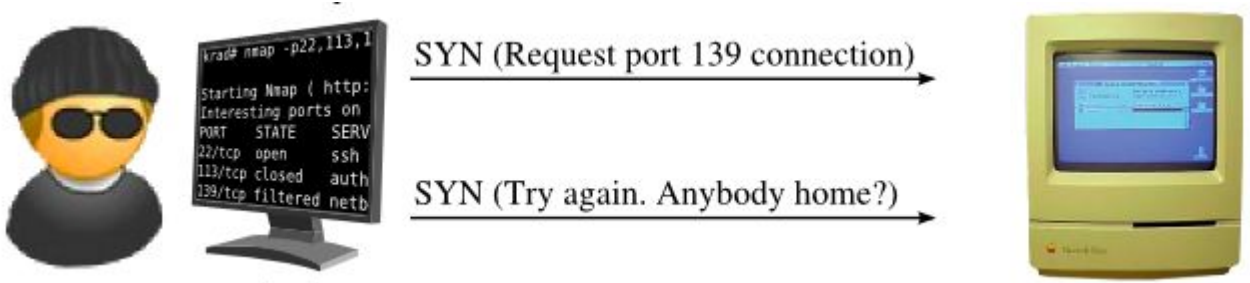


Figura obtenida de https://nmap.org/

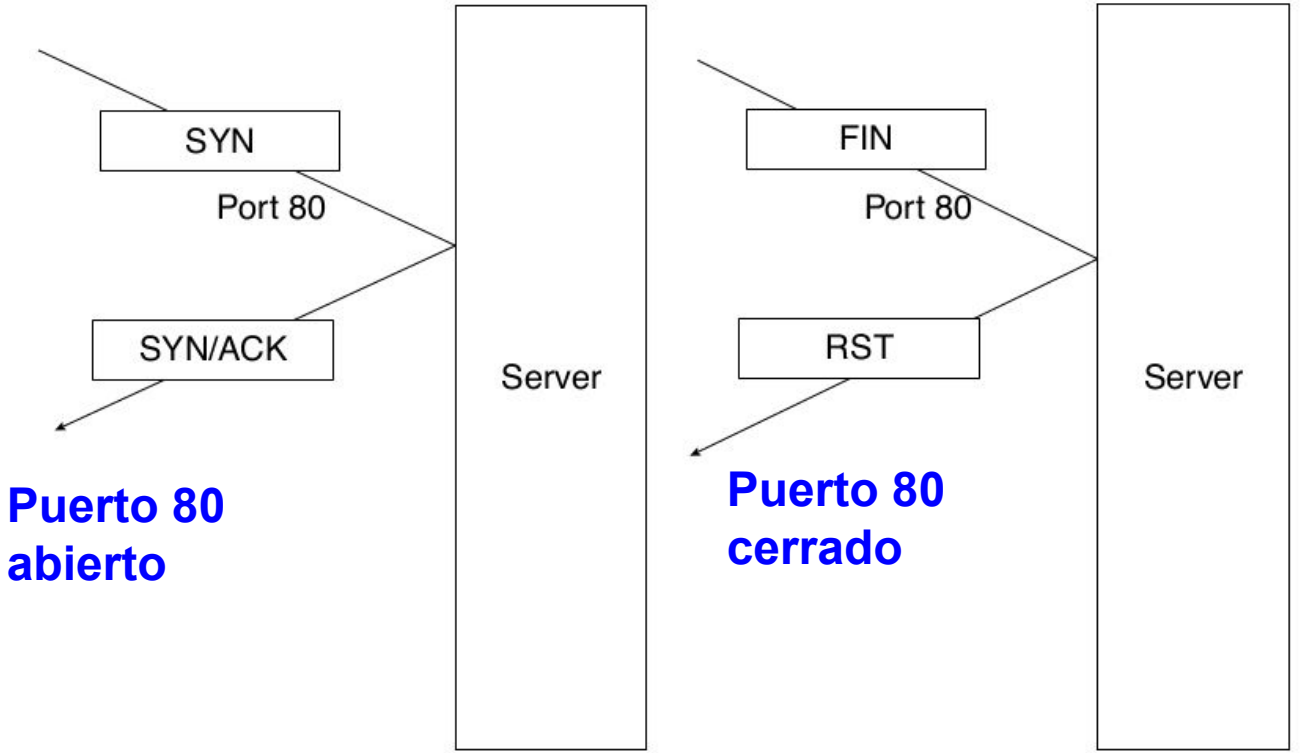


Figura obtenida de Tanenbaum et. al. "Computer Networks". 6º edición. 2021. Página 741.

Ejemplos de escaneo de puerto: escaneo Zombie

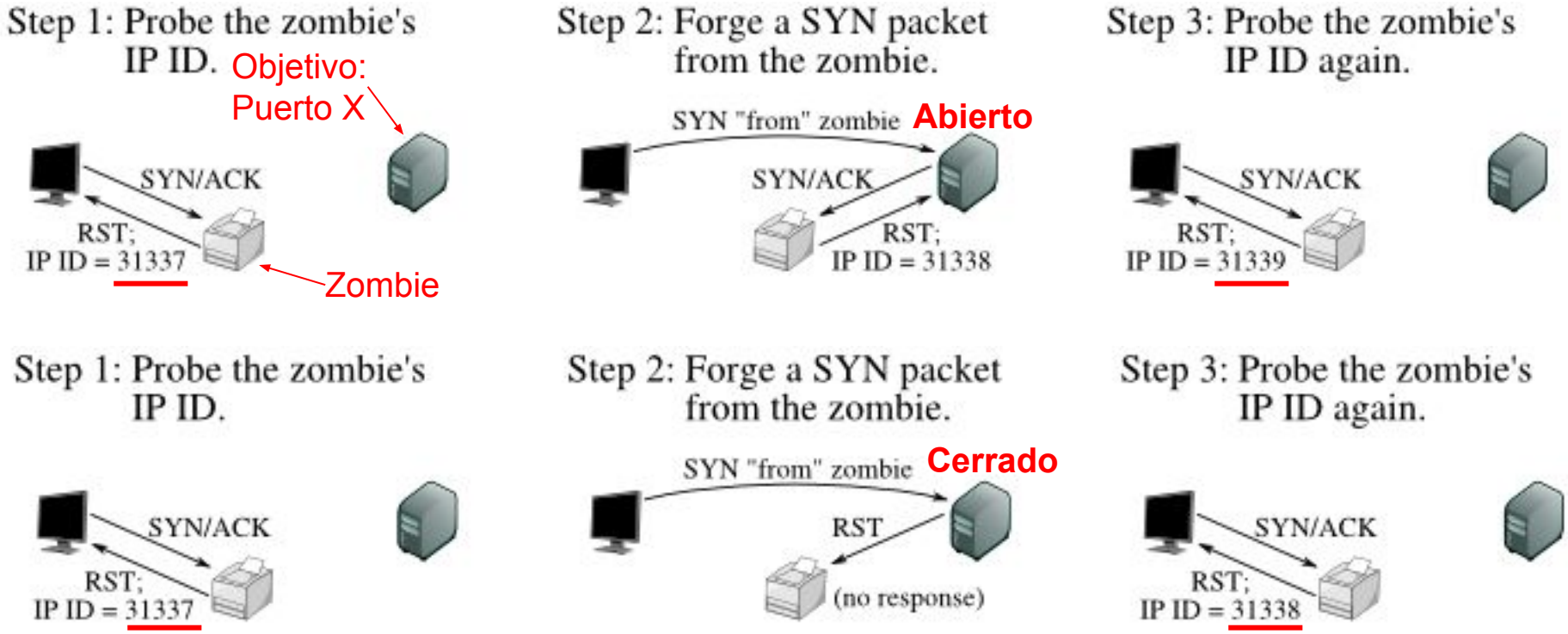
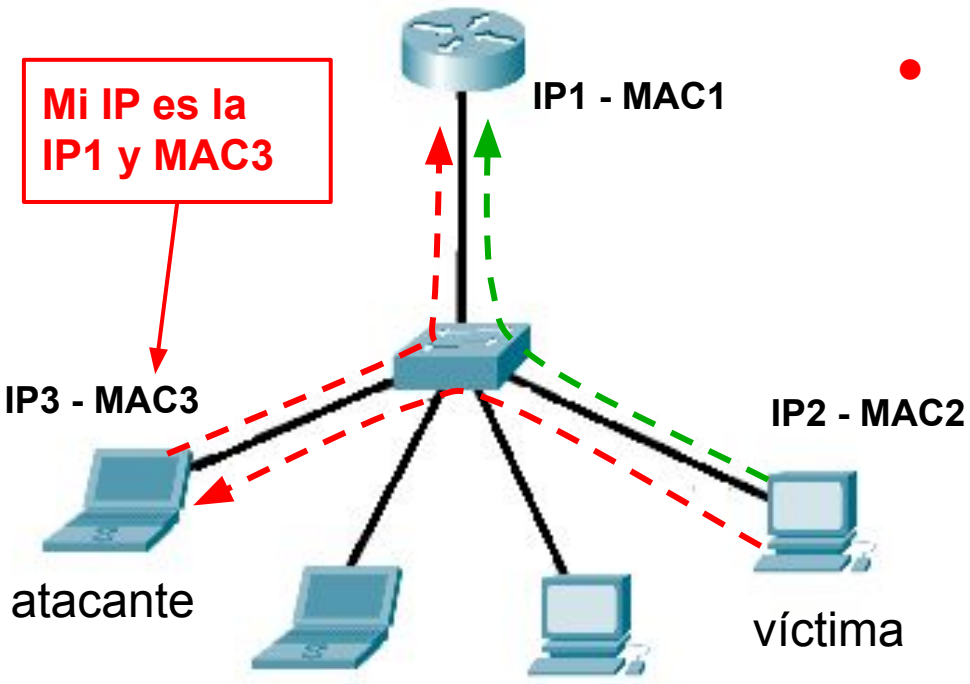


Figura obtenida de https://nmap.org/

Ataques activos

- **Spoofing** (Suplantación de identidad). Varios tipos.

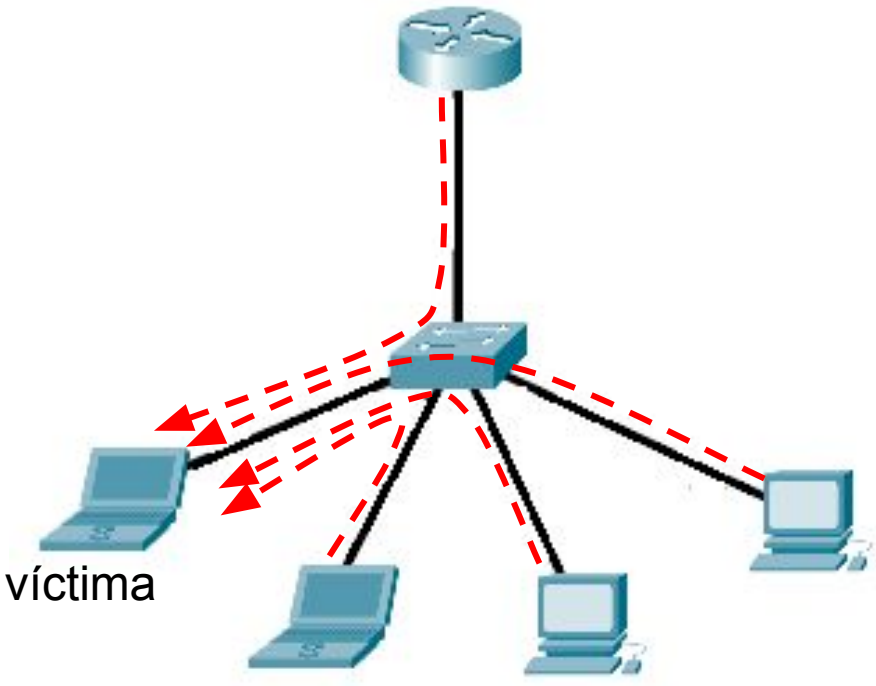
Spoofing ARP



- En una Ethernet conmutada no puedo realizar sniffing de forma directa.
- **Spoofing IP** y **envenenamiento de tablas ARP**
  - Envío de información ARP incorrecta a los equipos a atacar.
  - El tráfico puede desviarse hacia el atacante.
  - El atacante puede reenviar la información al destino real, haciendo que la víctima no se percate del ataque.

- **Spoofing IP**
  - Suplanta la **IP origen** del atacante por la de la víctima. Las respuestas estarán dirigidas a la víctima.
  - Ataque Smurf: se envían paquetes ping a direcciones broadcast suplandanto la IP origen. La víctima recibirá todas las respuestas.

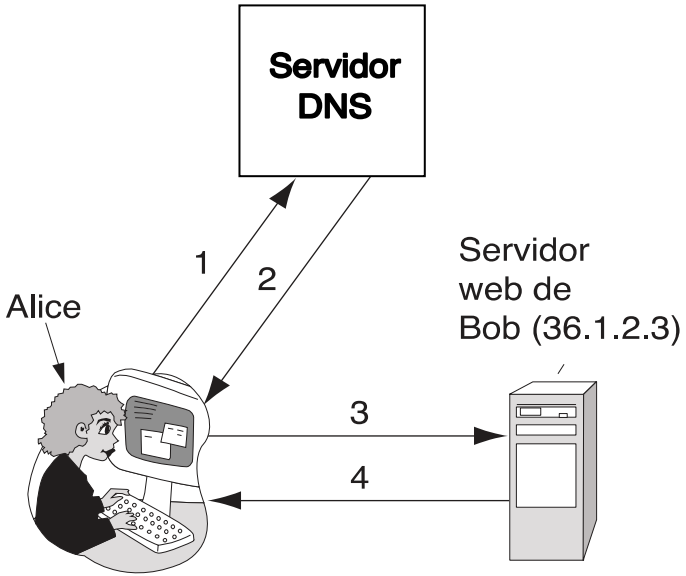
Ataque Smurf



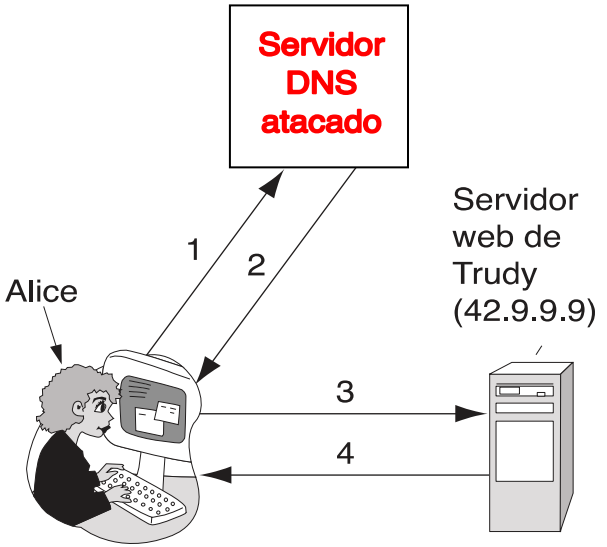
Algunos tipos de ataques

- **Spoofing DNS** (**Envenenamiento de tablas DNS**)
  - Alteran la asignación DNS - IP de un servidor DNS para dirigir el tráfico hacia un servidor malicioso.
  - Forma de realizarlo: enviar una consulta DNS a un servidor DNS (¿Cuál es la IP de www.redes.com.ar?) e inmediatamente una respuesta falsa con la alteración deseada (La IP es 200.0.2.1) suplantando la IP del servidor autorizado. Si el servidor DNS no tiene la IP, pregunta al servidor de jerarquía superior. Si la respuesta falsa llega antes, suplanta a la respuesta del servidor.
  - Muy complejo:
    - hay que alterar la IP origen del paquete de respuesta “falso” con la IP del servidor DNS de mayor jerarquía.
    - Las consultas DNS agregan un ID de 16 bits, y la respuesta debe tener ese “ID”. La respuesta “falsa” debe tener ese ID.

Spoofing DNS



1. Dame la dirección IP de Bob.
2. 36.1.2.3 (dirección IP de Bob)
3. GET index.html.
4. Página de inicio de Bob.



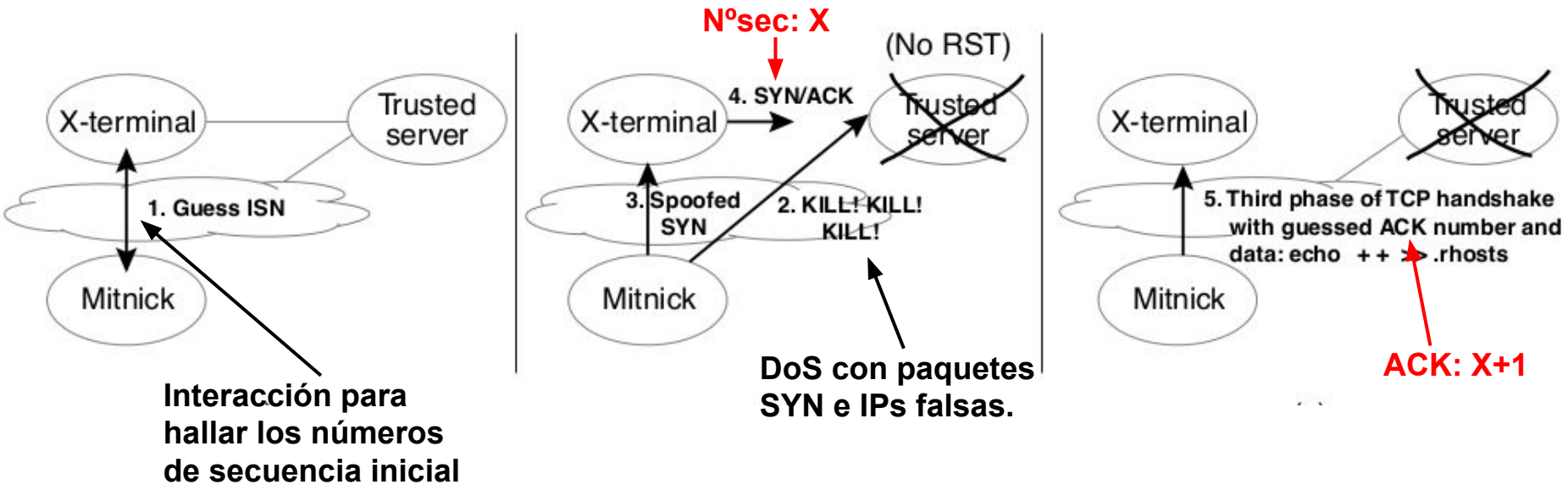
1. Dame la dirección IP de Bob.
2. 42.9.9.9 (dirección IP de Trudy).
3. GET index.html.
4. Falsificación que hace Trudy de la página de inicio de Bob.

Figura obtenida de: A. Tanenbaum, D. Wetherall, "Redes de computadoras", Quinta edición (2012), pag. 729

- **Spoofing web**.
  - Suplanta una página web.
  - La víctima ingresa a la página web falsa en lugar de la real.
  - Enlace (e-mail o página web) malicioso o Virus.
- **Spoofing SMTP**
  - Suplantar la dirección de correo de la fuente.
  - Usualmente para reenviar al usuario a una página web falsa o hacer que el usuario descargue un virus.
- **Spoofing conexión TCP.**
  - Spoofing de una conexión: el atacante intenta comenzar una conexión pretendiendo ser otra computadora.
  - Secuestro de conexión: el atacante inyecta datos en una conexión existente.
  - Muy complejo, se debe conocer el número de secuencia de los paquetes.
  - Ataque de **Kevin Mitnick**.

Ataque de Kevin Mitnick

- TCP spoofing contra el San Diego Supercomputing Center.



Consecuencia: Los números de secuencia inicial de TCP se generan aleatoriamente con un algoritmo muy potente.

Figura obtenida de: A. Tanenbaum, D. Wetherall, "Redes de computadoras", Sexta edición (2021), pag. 751

- **Denegación de servicio (DoS) por Ping de la muerte** (paquete Ping con tamaño mayor a 64KB, cuyo tamaño prohíbe IP, pero si el paquete se fragmenta, puede viajar por la red, ya que no hay un campo de “cantidad de segmentos”. Satura los buffers del receptor).
- **DoS de servicio servidor web**
  - Inundación ICMP (Ping) o UDP.
  - Inundación SYN
  - Ataque Smurf.
- **DoS de servidor DHCP**
  - Realiza múltiples peticiones DHCP hasta agotar las IP disponibles.
- **DoS distribuida**
  - El atacante primero ataca otras máquinas, para luego ordenarles que ataquen todas al mismo tiempo (Botnet).
    - Las botnets pueden alquilarse a través de la deep web.

- **DoS mediante ataque por reflexión**
  - Enviar peticiones a servidores con IP spoofing (utilizando como IP origen la IP de la víctima).
    - Los servidores enviarán respuestas a la víctima.
  - Ventajas:
    - La víctima confiará en las respuestas ya que son servidores legítimos.
    - Amplificación: mensajes cortos pueden causar respuestas largas.

AD
ENIERÍA

Protocol	Bandwidth amplification factor
DNS	28 to 54
NTP	556.9
SNMPv2	6.3
NetBIOS	3.8
SSDP	30.8
CharGEN	358.8
QOTD	140.3
BitTorrent	3.8
Kad	16.3
Quake Network Protocol	63.9
Steam Protocol	5.5
Multicast DNS (mDNS)	2 to 10
RIPv1	131.24
Portmap (RPCbind)	7 to 28
LDAP	46 to 55
CLDAP	56 to 70
TFTP	60

Figura obtenida de
https://doi.org/10.1016/j.cose.2021.102380

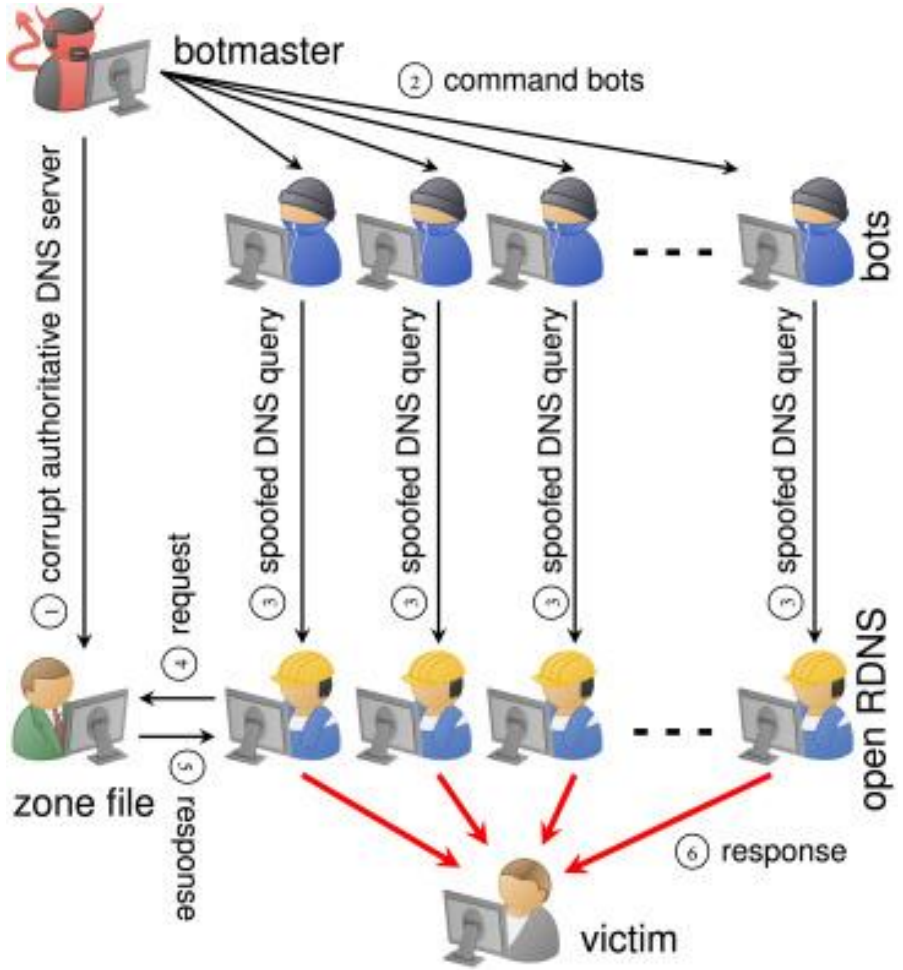
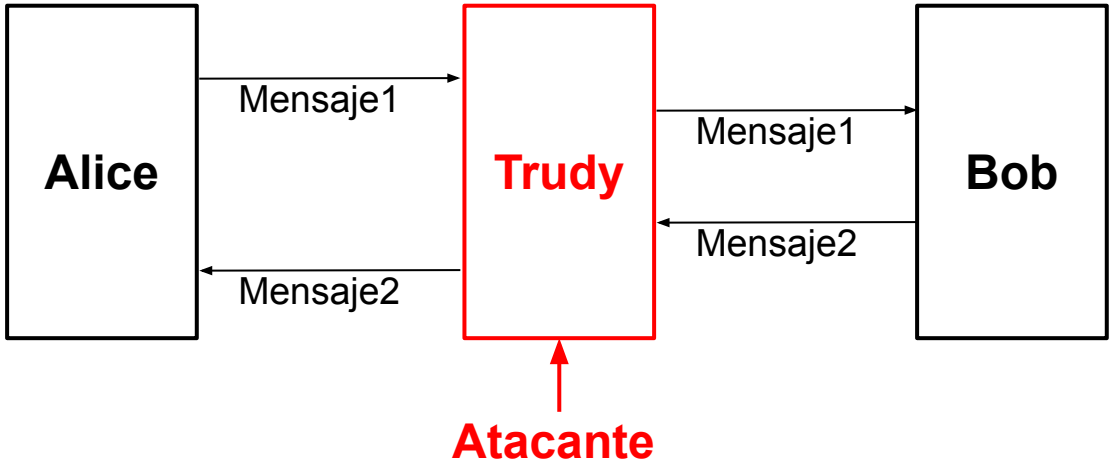


Figura obtenida de
https://doi.org/10.1016/B978-0-12-803306-7.00008-5

- **Ataque del intermediario (Man-in-the-middle attack)**.
  - Alice quiere comunicarse con Bob.
  - Trudy intercepta mensajes de Alice hacia Bob y luego los reenvía a Bob (puede solo leerlos o modificarlos).
  - Alice y Bob no saben lo que está ocurriendo mientras se comunican.



Adversary	Goal
Student	To have fun snooping on people's email
Cracker	To test someone's security system; steal data
Sales rep	To claim to represent all of Europe, not just Andorra
Corporation	To discover a competitor's strategic marketing plan
Ex-employee	To get revenge for being fired
Accountant	To embezzle money from a company
Stockbroker	To deny a promise made to a customer by email
Identity thief	To steal credit card numbers for sale
Government	To learn an enemy's military or industrial secrets
Terrorist	To steal biological warfare secrets

Figura obtenida de Tanenbaum et. al. "Computer Networks". 6º edición. 2021. Página 741.

Temario

- Problemas de seguridad en redes de computadoras
- **Criptografía**
- Generación de claves secretas compartidas
- Firmas digitales y certificados
- Implementaciones de seguridad

Criptografía

- Enviar **mensajes "secretos"** de manera que sólo el destinatario pueda leerlos.
- Empleada para:
  - Evitar que un mensaje sea leído por quien no debe hacerlo.
  - Evitar que un tercero pueda captar y modificar un mensaje.
  - Certificar la identidad de alguien.
- Dos métodos:
  - **Cifrado**: transformación caracter por caracter.
  - **Código**: Reemplazan una palabra por otra o por un símbolo.
    - No utilizados actualmente.
- Principio de **Kerckhoff**: Los algoritmos deben ser públicos, las claves secretas.
- Dos componentes:
  - Algoritmos de encriptación y desencriptación: Conocidos por todos.
  - Clave: Secreta.
- Criptografía: crea y estudia algoritmos para encriptar mensajes y su efectividad
- Criptoanálisis: Estudia los métodos para quebrar algoritmos de encriptación.

Modelo de cifrado

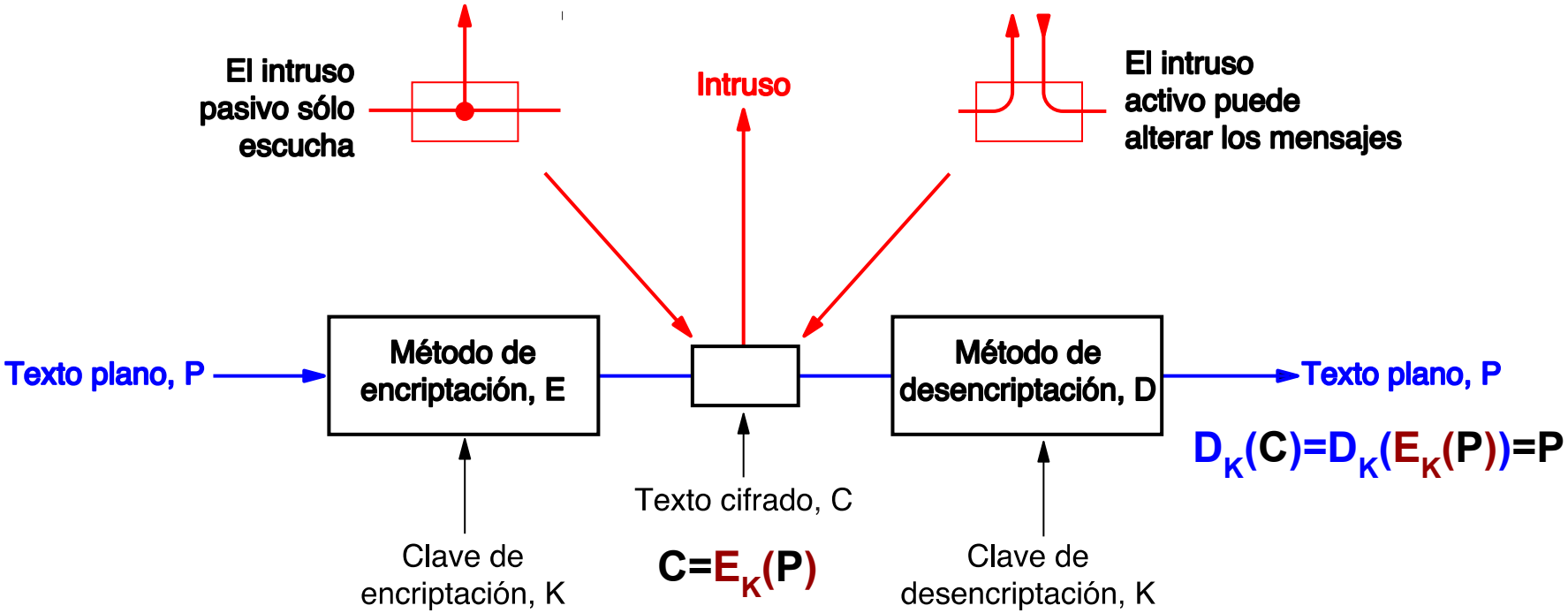


Figura obtenida de: A. Tanenbaum, D. Wetherall, "Redes de computadoras", Quinta edición (2012), pag. 661

Tipos de Cifrado por bloque

Cifrado por bloque: Toma bloques de igual tamaño del texto original, los cifra y genera bloques cifrados de igual tamaño que la entrada.

- **Cifrado por sustitución**: Cada letra o byte se reemplaza por otro.
  - Ejemplo:

texto plano: 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
texto cifrado: q w e r t y u i o p a s d f g h j k l z x c v b n m
ataque=qzqjxt

- **Cifrado por transposición**: Las letras o bytes se reordenan (sin cambiarse).
  - El texto se divide en bloques (ejemplo: 64 letras).
  - Luego se reordena: Ejemplo: 4, 12, 20, 28, 36, 44, 52, 60, 5, 13, . . . , 62

texto plano: pleasetransferonemilliondollarstomyswissbankaccountsixtwotwo
texto cifrado: afllsksoselawaiatoossctclnmomantesilyntwrnntsowdpaedobuoeriricxb

- Cifrado por transposición (continuación)
  - Forma práctica de implementar: filas y columnas + una clave.

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
↓	↓	↓	↓	↓	↓	↓	↓
p	l	e	a	s	e	t	r
a	n	s	f	e	r	o	n
e	m	i	l	l	i	o	n
d	o	l	l	a	r	s	t
o	m	y	s	w	i	s	s
b	a	n	k	a	c	c	o
u	n	t	s	i	x	t	w
o	t	w	o	a	b	c	d

Texto plano
pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Texto cifrado
AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

Figura obtenida de: A. Tanenbaum, D. Wetherall, "Redes de computadoras", Quinta edición (2012), pag. 664

Relleno de una sola vez

- Se transforma el mensaje plano en una secuencia de bits (ejemplo: ASCII)
- Se elige una cadena de bits como clave (llamada relleno).
- Se aplica XOR bit por bit. Para desencriptar, se vuelve a aplicar XOR.
  - Ejemplo (clave: RKrU]c*Wf+):

	I		L	O	V	E		Y	O	U	.
Mensaje 1:	1001001	0100000	1101100	1101111	1110110	1100101	0100000	1111001	1101111	1110101	0101110
Relleno 1:	1010010	1001011	1110010	1010101	1010010	1100011	0001011	0101010	1010111	1100110	0101011
Texto cifrado:	0011011	1101011	0011110	0111010	0100100	0000110	0101011	1010011	0111000	0010011	0000101

Figura obtenida de: A. Tanenbaum, D. Wetherall, "Redes de computadoras", Quinta edición (2012), pag. 665

Relleno de una sola vez

Ventajas:

- Muy robusto.
  - Al intentar desencriptar con otra clave, pueden obtenerse mensajes válidos.
  - El texto encriptado es muy similar a texto normal.

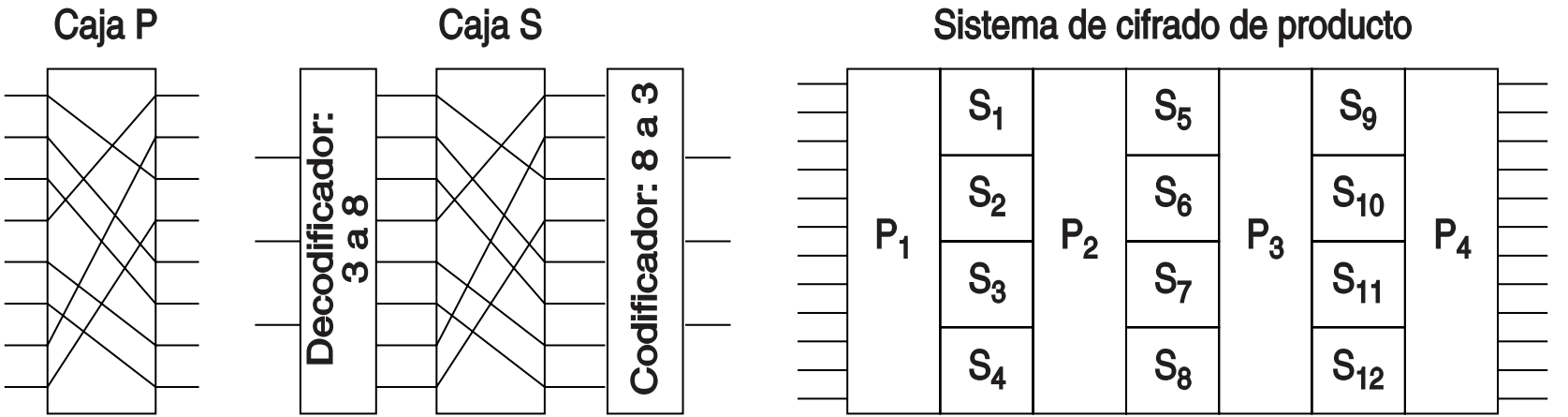
Texto cifrado:	0011011	1101011	0011110	0111010	0100100	0000110	0101011	1010011	0111000	0010011	0000101
Relleno 2:	1011110	0000111	1101000	1010011	1010111	0100110	1000111	0111010	1001110	1110110	1110110
Texto plano 2:	1000101	1101100	1110110	1101001	1110011	0100000	1101100	1101001	1110110	1100101	1110011
	E	L	V	I	S		L	I	V	E	S

Desventajas:

- Muy sensible a caracteres insertados o perdidos.

Figura obtenida de: A. Tanenbaum, D. Wetherall, "Redes de computadoras", Quinta edición (2012), pag. 665

Implementaciones por Hardware de Cifrado por Sustitución y Transposición



Transposición (por bits, bytes, palabras)

Sustitución (por bits)

Producto

Figura obtenida de: A. Tanenbaum, D. Wetherall, "Redes de computadoras", Quinta edición (2012), pag. 671

Métodos de criptoanálisis

- Fuerza bruta: Probar todas las claves posibles.
- Probar primero las claves más comunes.
- Buscar patrones + análisis estadístico.
  - Ejemplo: Buscar patrones de repetición de símbolos que se correspondan con patrones de repetición de letras en un idioma.
    - Letras más usadas en un idioma.
    - Digramas (dos letras) o trigramas más comunes.
  - Buscar palabras comunes o altamente posibles.
    - Ejemplo: buscar el patrón de símbolos de “dollars” o “cuenta”.
  - Contramedida: que para un mismo texto, la salida varíe (cifrado por bloques).

Algoritmos de clave simétrica

- Utilizan la misma clave para encriptar que para desencriptar.

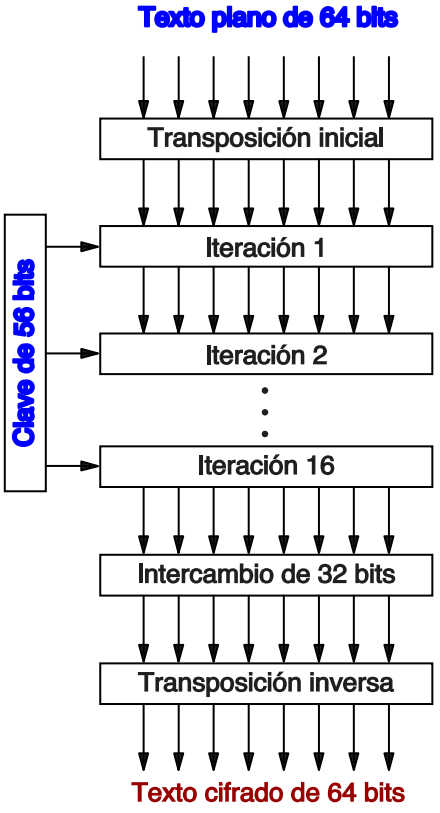
Algoritmo DES (Data Encryption Standard)

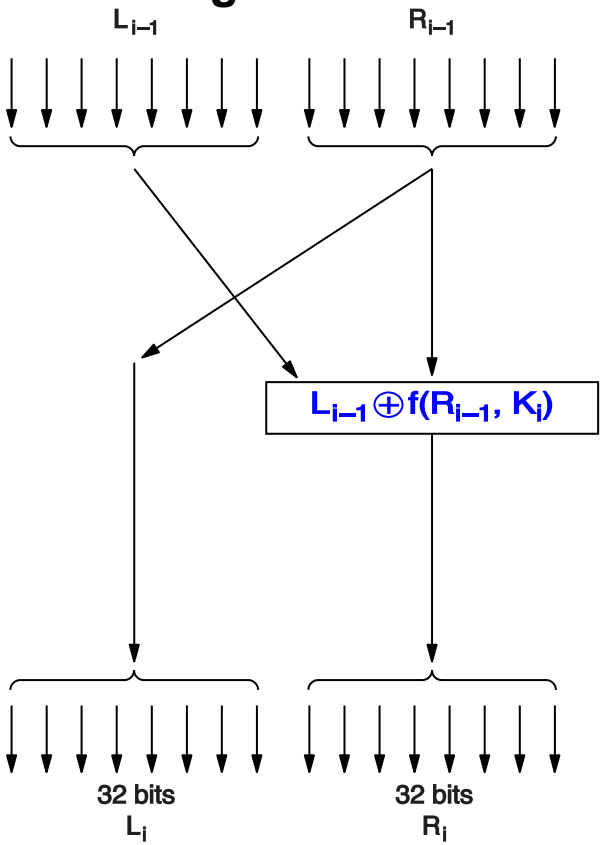
- Basada en el algoritmo llamado Lucifer de IBM. Adoptado por el gobierno de Estados Unidos como el algoritmo oficial.
- Actualmente no seguro en su forma original.
  - Diffie y Hellman construyeron una máquina para descifrar DES.
- Sistema de cifrado por bloques (de 64 bits).
- Clave de 56 bits (La propuesta original de IBM era usar una clave de 128 bits [1]).
- Crítica más importante: ¿Tiene “puerta de atrás” [2] para la NSA?

[1] Se redujo a 56 bits por acuerdo entre IBM y la NSA (National Security Agency)

[2] Sistema para permitir que alguien “entre” (descifre la clave)

Algoritmo DES





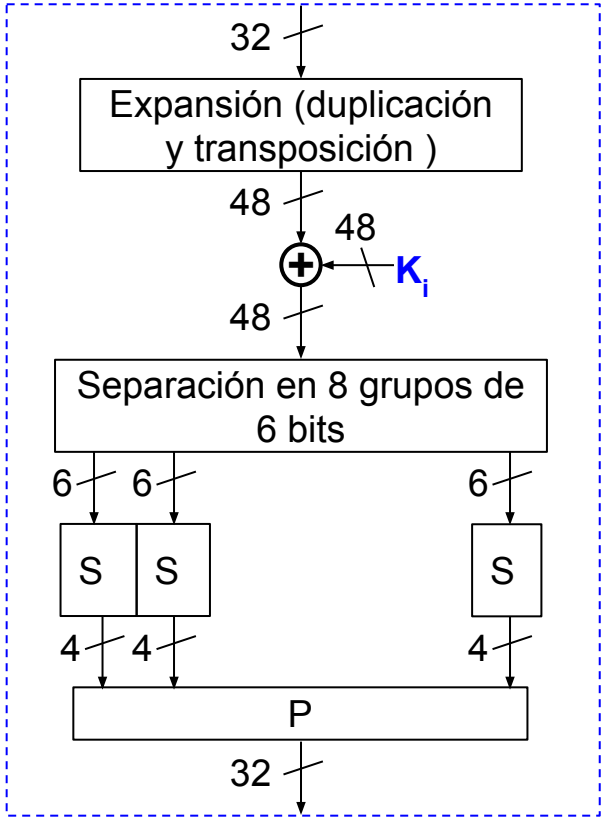
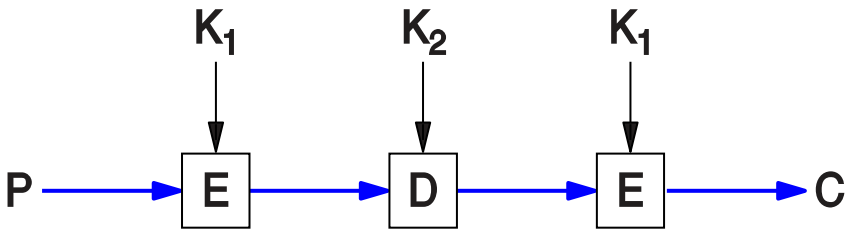


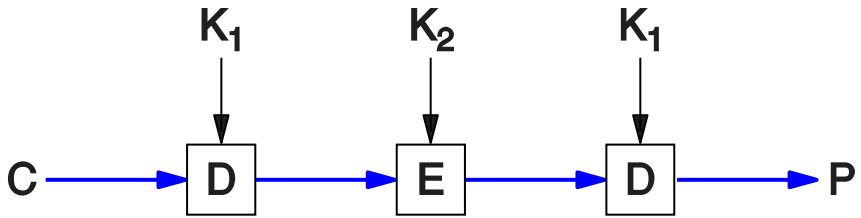
Figura obtenida de: A. Tanenbaum, D. Wetherall, "Redes de computadoras", Quinta edición (2012), pag. 672

Triple DES

- En 1979 IBM dedujo que la clave de 56 bits era demasiado corta.
- 3 etapas de encriptación (E) y desencriptación (D) DES con dos claves DES K_1 y K_2 (112 bits).
- Se usa un esquema que permita compatibilidad con DES original
  - Si K_1=K_2 la 2° y 3° etapa se anulan. Queda un DES original (simple).



Encriptación



Desencriptación

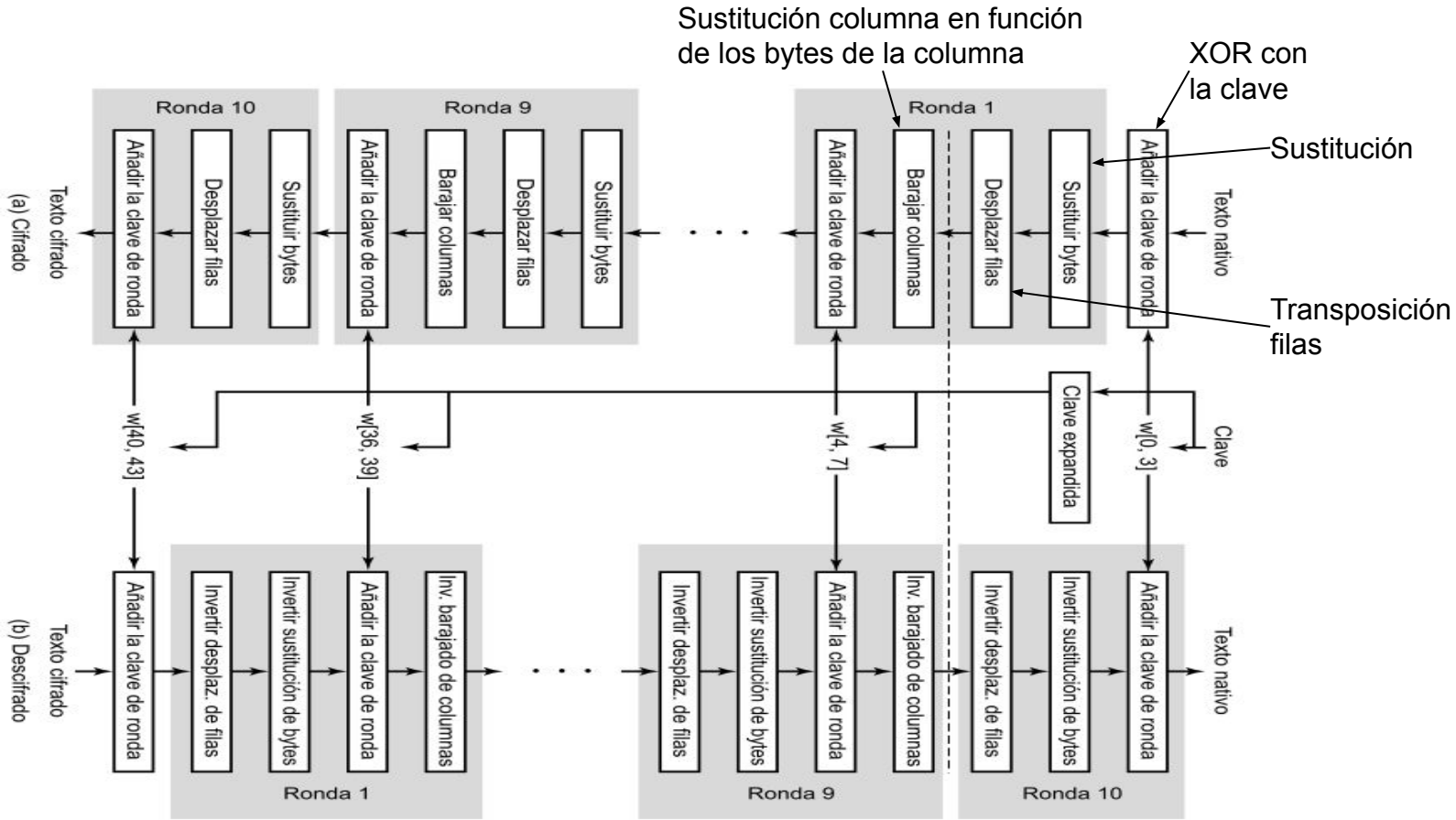
Figura obtenida de: A. Tanenbaum, D. Wetherall, "Redes de computadoras", Quinta edición (2012), pag. 674

Algoritmo AES
(Advanced Encryption Standard)

- Surgió a través de un concurso propuesto por el NIST (Nacional Institute of Standards and Technology) .
  - 15 propuestas. Varias conferencias invitando a los asistentes a encontrar errores.
- Algoritmo ganador: **Rijndael**, creado por Vincent Rijmen y Joan Daemen (investigadores Belgas).
- Hoy día es parte del hardware de muchos procesadores.
- Utiliza bloques de 128 bits. Claves de 128, 192 y 256 bits.
- Utiliza algoritmos matemáticos complejos (campos de Galois) mediante rondas de sustituciones y permutaciones.

AES

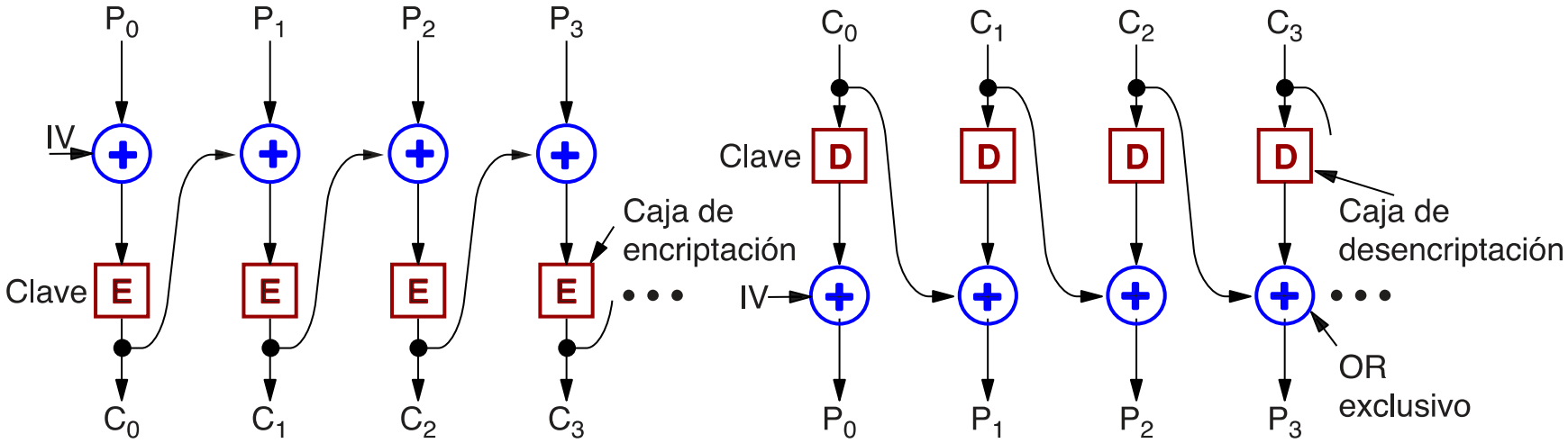
Funciona en base a columnas



Encadenamiento por bloques de sistema de cifrado

- Los algoritmos anteriores producen siempre la misma salida para una misma entrada.
  - Un atacante que conoce la estructura de la información puede cambiar un campo que sabe producirá algún efecto dañino o no deseado para el atacado (o deseado para el atacante).
  - Es simple el criptoanálisis estadístico.
- **Solución: Hacer que los mismos datos de entrada produzcan diferentes salidas en diferentes momentos.**
  - Modo de encadenamiento de bloques de sistema de cifrado.
  - Modo de retroalimentación de sistema de cifrado.
  - Modo de sistema de cifrado de flujo.
  - Modo de contador.

Modo de encadenamiento de bloques de sistema de cifrado



IV: Initialization Vector

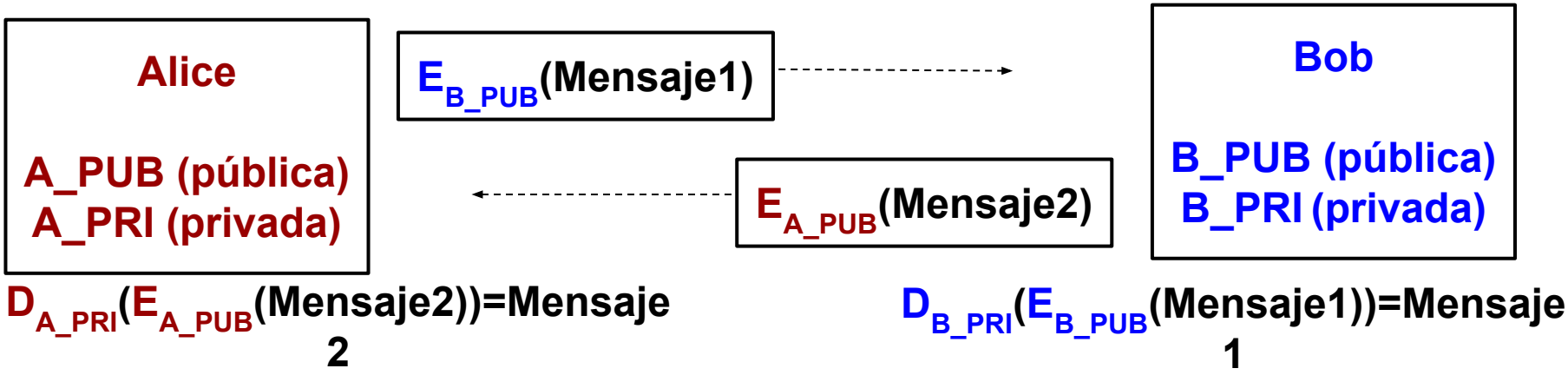
Figura obtenida de: A. Tanenbaum, D. Wetherall, "Redes de computadoras", Quinta edición (2012), pag. 678

Encriptación de clave pública

- **Problemas de los algoritmos de clave simétrica: Las personas deben comunicarse la clave.**
  - **Si la clave es interceptada, se pierde toda la seguridad.**
- **Algoritmos de Clave pública**:
  - Propuestos por Diffie y Hellman (1976).
  - Se requieren dos claves: clave de encriptación y clave de desencriptación que cumplan:
    - $D_{K\_1}(E_{K\_2}(P))=P$
    - Es demasiado difícil deducir K_2 a partir de K_1 y viceversa.

E: Algoritmo de encriptación
D: Algoritmo de desencriptación

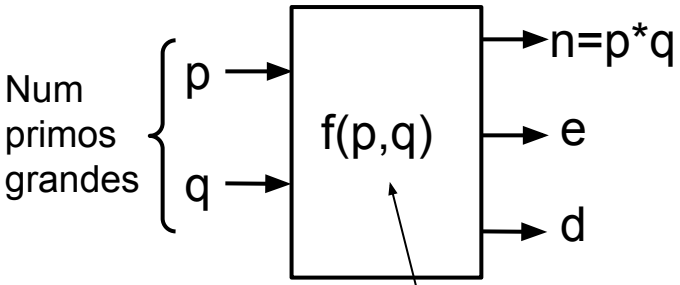
Algoritmos de clave pública



- Los algoritmos D y E pueden ser estándares (conocidos por todos) y parametrizables.

Algoritmos de clave pública: Algoritmo RSA

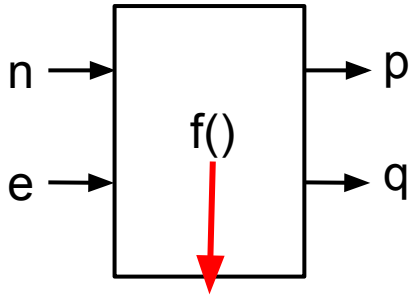
- Investigadores del MIT (Rivest, Shamir y Adleman). 1978.
- Las funciones **$C=P^e \pmod n$** y **$P=C^d \pmod n$** son inversas.
- Para claves de 4096 bits, un millón de procesadores de 1 GHz en paralelo demoraría 10^{16} años en resolver el problema con el mejor algoritmo conocido.
- **Desventaja: La clave requiere muchos bits (1024 o más), lo que lo hace lento.**



Detalles del algotitmo y ejemplo: William, Stallings: “Data and Computer Communications”, 8ed, 2007, pag. 746

Clave pública: (e,n)

Clave privada: (d,n)



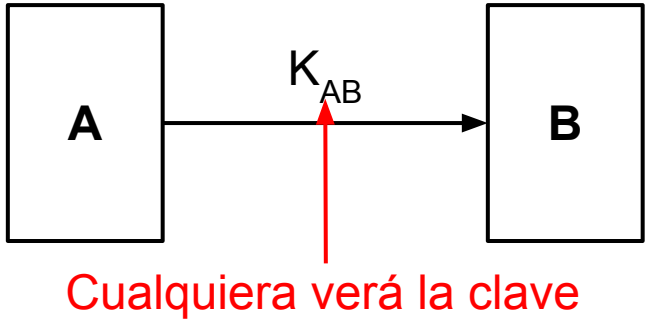
No existe algoritmo práctico para hallar p y q. Se pueden hallar por pruebas sucesivas.

Temario

- Problemas de seguridad en redes de computadoras
- Criptografía
- **Generación de claves secretas compartidas**
- Firmas digitales y certificados
- Implementaciones de seguridad

Generación de clave secreta compartida

- Clave secreta compartida de sesión: Siempre se utiliza una **diferente** para limitar la cantidad de información comprometida ante un robo de la clave.
- Métodos para el intercambio de una clave secreta compartida:
  - A y B conocen previamente la clave común (no práctica).
  - A y B intercambian la clave por un medio diferente a la red (no práctico).
  - Protocolo de intercambio de clave.



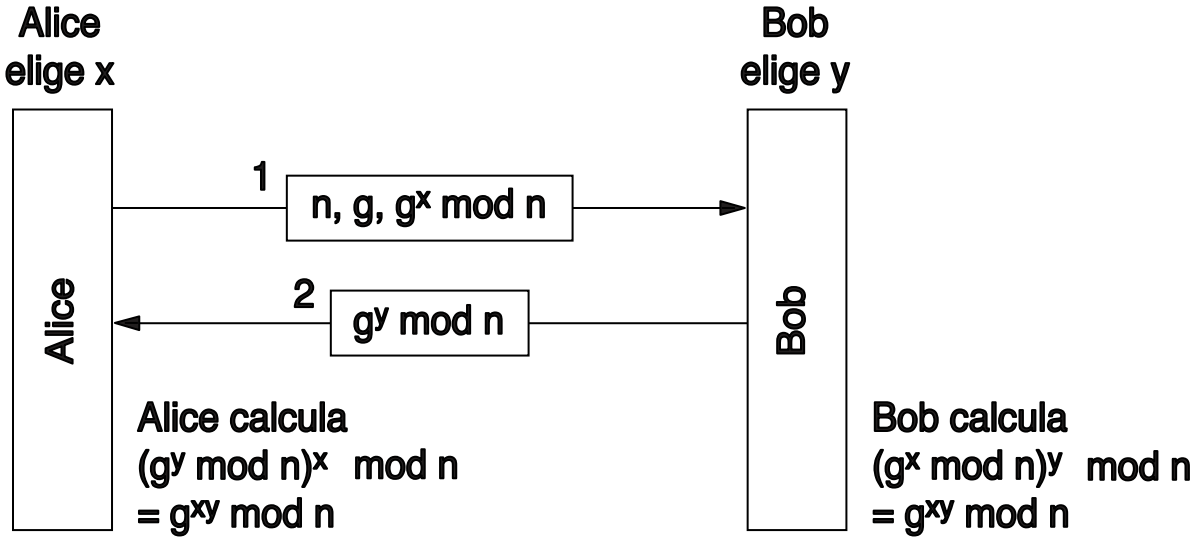
Generación de clave secreta compartida

Soluciones:

- **Protocolo de intercambio de claves:**
  - **Diffie-Hellman**
  - **WPA (Wifi).**
- **Centros de distribución de claves**
- **Encriptación de clave pública + Certificados**

Protocolo de intercambio de claves Diffie-Hellman

- Permite que dos procesos establezcan una clave secreta común.
- Se basan en un problema matemático muy difícil de resolver[1].



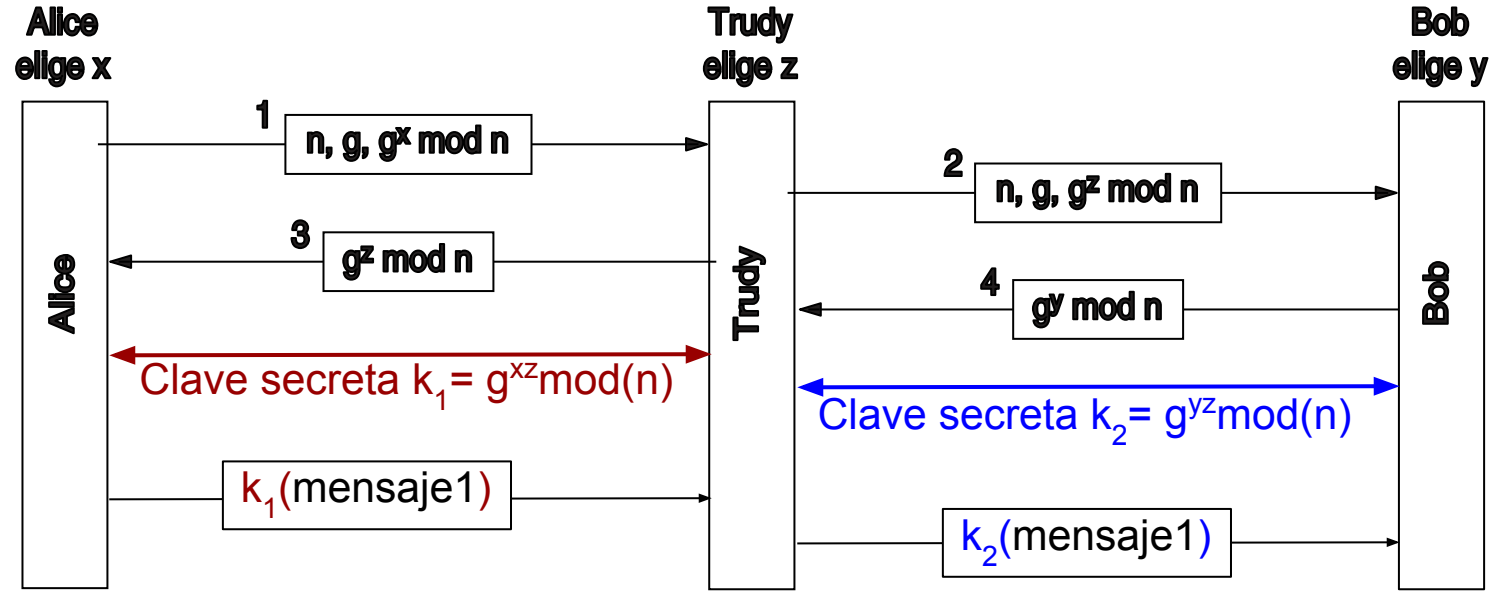
- **n** y **g** debe cumplir ciertas condiciones y son públicos.
- Fundamento: Es muy difícil calcular **x** a partir de $g^x \bmod(n)$.
- La clave secreta común es $g^{xy} \bmod(n)$

Figura obtenida de: A. Tanenbaum, D. Wetherall, "Redes de computadoras", Quinta edición (2012), pag. 717

[1] En criptografía o temas de seguridad, “muy difícil de calcular” significa que con el mejor algoritmo conocido, un cluster poderoso tardaría miles de años en resolver el problema.

Protocolo de intercambio de claves Diffie-Hellman

- Desventaja: vulnerable al ataque “man-in-the-middle”



Trudy puede leer y (si quiere) modificar todos los mensajes entre Alice y Bob, sin que ellos lo sepan.

Figura basada en: A. Tanenbaum, D. Wetherall, "Redes de computadoras", Quinta edición (2012), pag. 717

IEEE 802.11 - Seguridad

- Problemas:
  - Autentificación e intercambio de clave de sesión.
  - Cifrado: Para evitar la “escucha” de datos
- Autentificación e intercambio de clave:
  - WPA: WiFi Protected Access
    - WPA 1: Versión inicial
    - WPA 2: Incluido con el estándar 802.11i.
  - WEP: Wired Equivalent Privacy.
    - Se ha probado que puede quebrantarse
- Cifrado:
  - DES (Data Encryption Standard)
  - AES (Advanced Encryption Standard)

IEEE 802.11 - Seguridad

- **WEP** (Wired Equivalent Privacy)
  - Creado por un comité (Diferente procedimiento para creación de algoritmos de encriptación y autentificación del NITS[1]).
  - Claves de 32 bits.
  - Puede romperse en menos de un minuto.
- **WPA** (WiFi Protected Access):
  - WPA corporación (Enterprise):
    - Útil en empresas. Hay un servidor de autenticación. Cada usuario tiene su usuario y contraseña. Protocolo EAP.
  - WPA personal o WPA PSK (Pre-shared key):
    - No hay servidor de autentificación. Un usuario y contraseña para todos.
    - Basado en una clave simétrica (o compartida).

[1]NIST: National Institute of Standards and Technology

- **WPA**

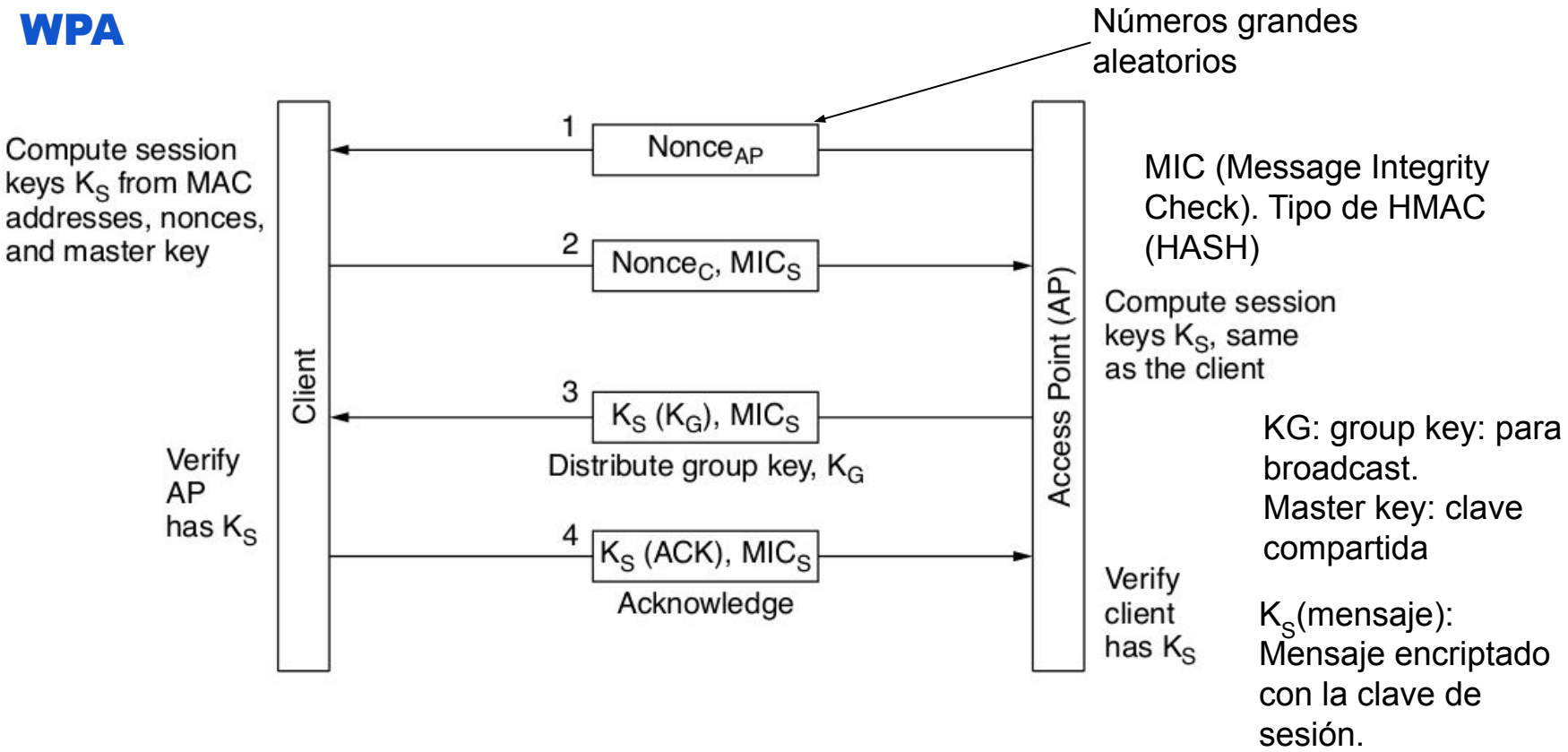
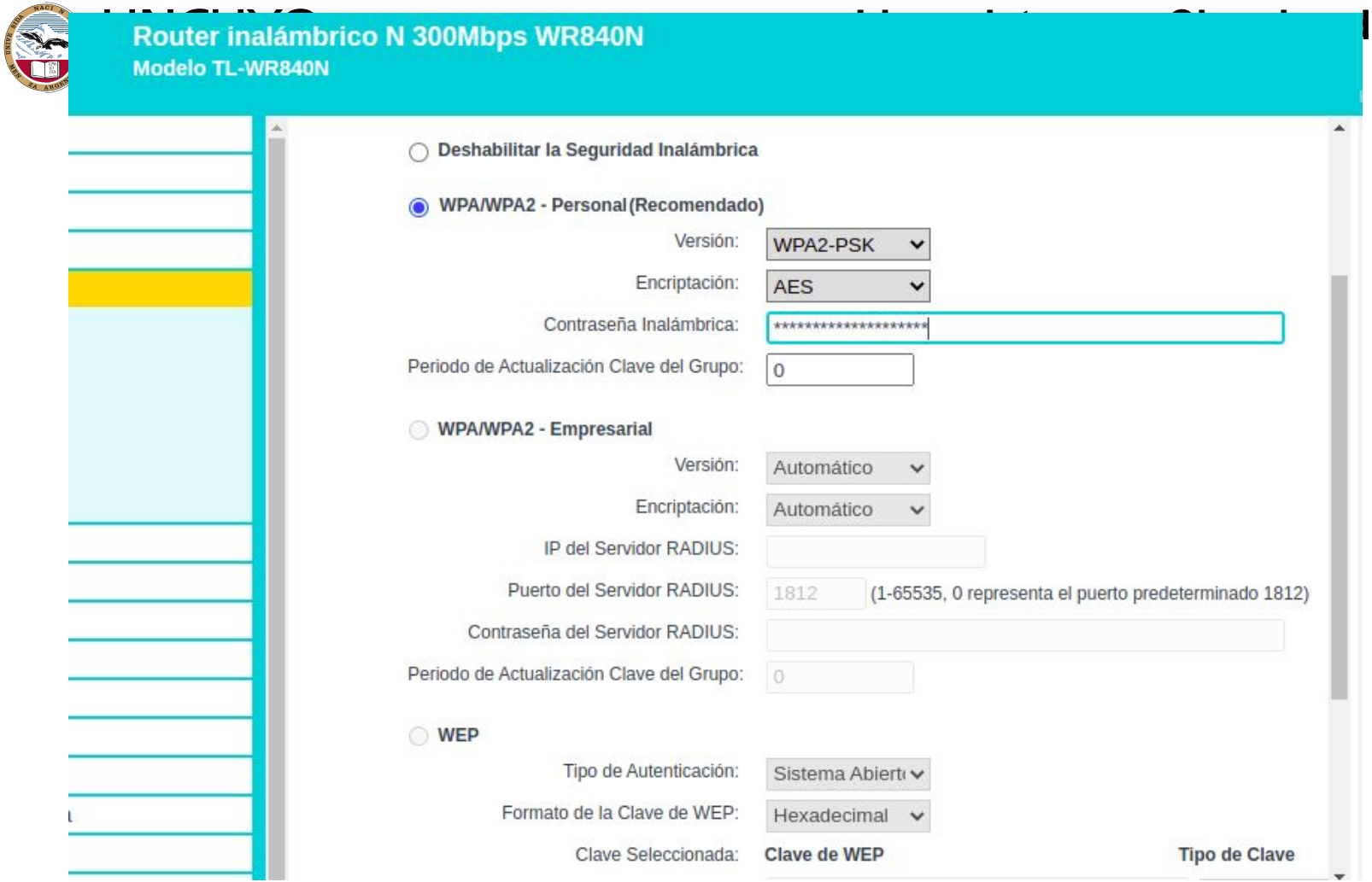


Figura obtenida de A. Tanenbaum, D. Wetherall, "Redes de computadoras", 6° edición (2012), pag. 828

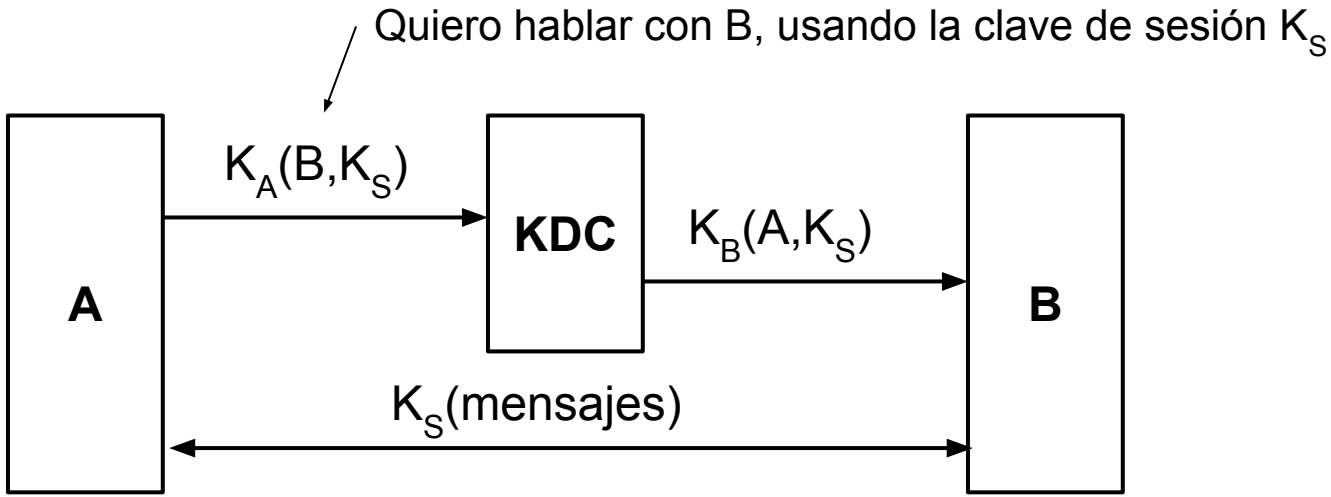
Seguridad en redes inalámbricas
Protocolo WPA3 (Wi-Fi Protected Access)

- Claves 192 bits.
- Seguro aún con claves débiles.
- Permitir dispositivos IoT sin pantalla ni teclado (escaneando QR con otro dispositivo).


Router inalámbrico N 300Mbps WR840N
Modelo TL-WR840N
Deshabilitar la Seguridad Inalámbrica
WPA/WPA2 - Personal (Recomendado)
Versión:
WPA2-PSK
Encriptación:
AES
Contraseña Inalámbrica:
Periodo de Actualización Clave del Grupo:
0
WPA/WPA2 - Empresarial
Versión:
Automático
Encriptación:
Automático
IP del Servidor RADIUS:
Puerto del Servidor RADIUS:
1812
(1-65535, 0 representa el puerto predeterminado 1812)
Contraseña del Servidor RADIUS:
Periodo de Actualización Clave del Grupo:
0
WEP
Tipo de Autenticación:
Formato de la Clave de WEP:
Hexadecimal
Clave Seleccionada:
Clave de WEP
Tipo de Clave

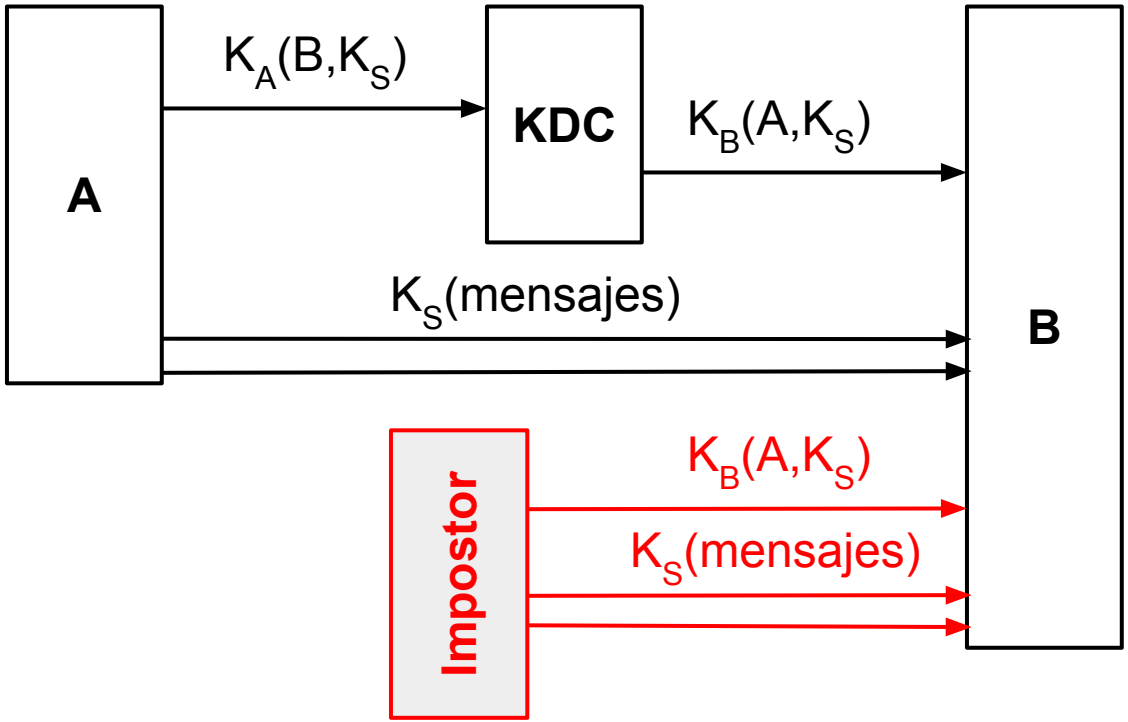
Centro de distribución de claves

- Permite intercambio de claves y autentificación.
- KDC (Key distribution center o Centro de distribución de claves).
  - Tiene una clave compartida con cada posible usuario.



Centro de distribución de claves

- Ataque de repetición: el atacante escucha mensajes válidos y los repite



Protocolos de autentificación: Kerberos

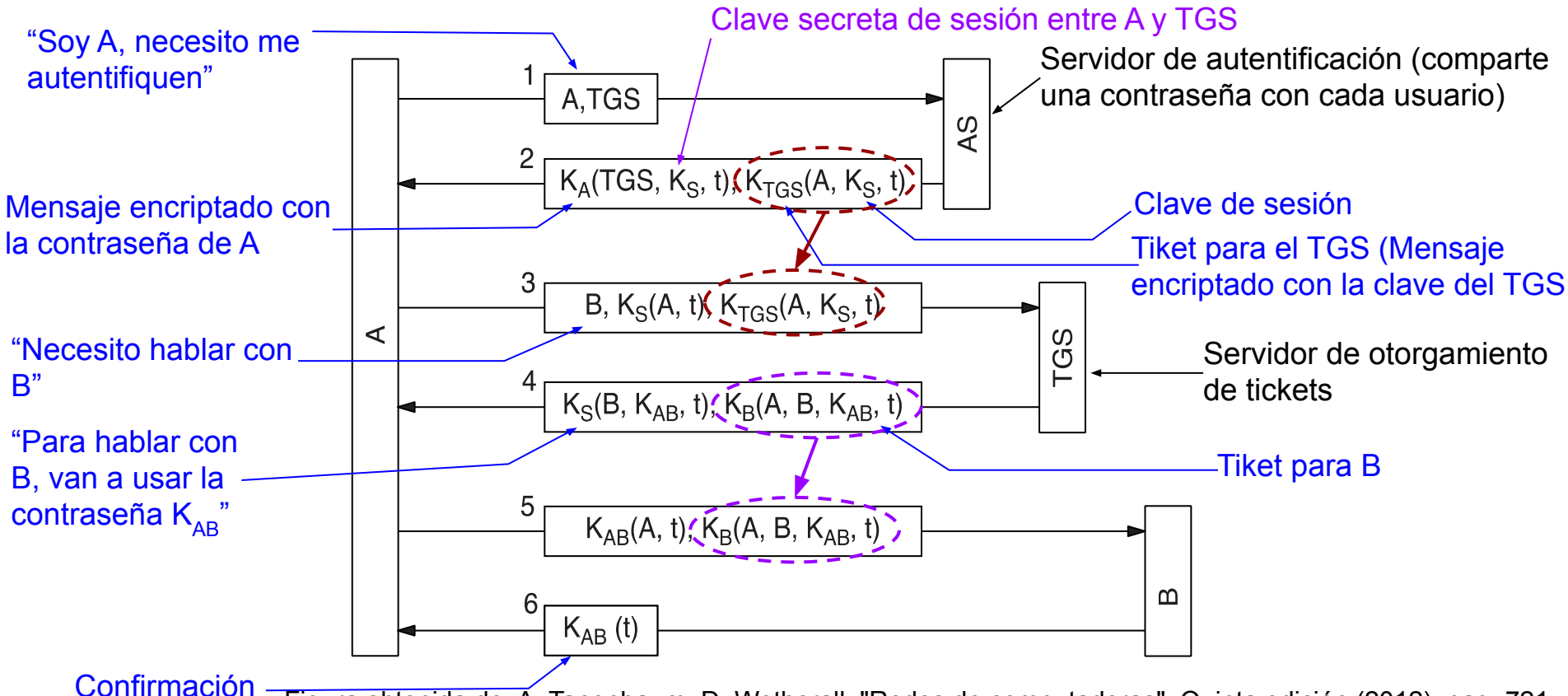
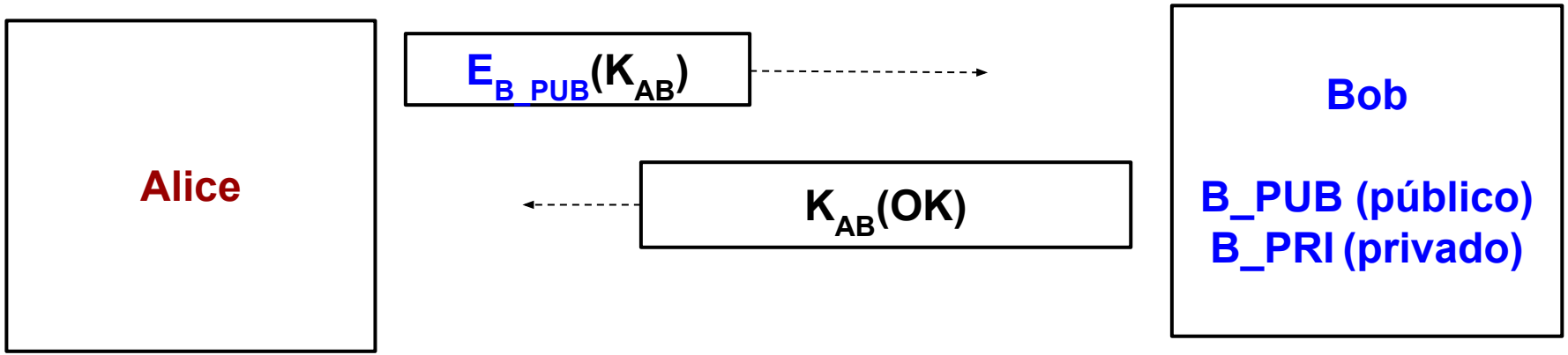


Figura obtenida de: A. Tanenbaum, D. Wetherall, "Redes de computadoras", Quinta edición (2012), pag. 721

Protocolos de autentificación: Kerberos

- Desarrollado por el MIT, código abierto y gratuito.
- Versión actual: 5 (se ha actualizado constantemente al detectar vulnerabilidades)
- Una vez autenticado, A puede pedir tickets para comunicarse con otros usuarios sin pasar nuevamente por el AS.
  - Si ahora quiere hablar con C, se comunica con el TGS.
  - La contraseña K_S sirve para toda la comunicación entre A y el TGS.
- La computadora que A utilice sólo pedirá la contraseña cuando llegue el mensaje 2, y dicha contraseña sólo será necesaria pocos milisegundos.
  - Una vez verificado el mensaje 2, no se vuelve a utilizar la contraseña A (para proteger la contraseña de A).
  - El protocolo sobreescribe la contraseña de A inmediatamente después de desencriptar el mensaje 2, para evitar que alguien pueda robarla.

Intercambio de clave secreta compartida mediante encriptación de clave pública



Problema: ¿Cómo sabe Alice que habla con Bob? ¿Como sabe Alice que B_PUB es la clave pública de Bob y no la clave pública de un impostor?

Faltan varios elementos para que este sistema sea seguro. Un esquema seguro es TSL o SSL (final de la presentación).

Temario

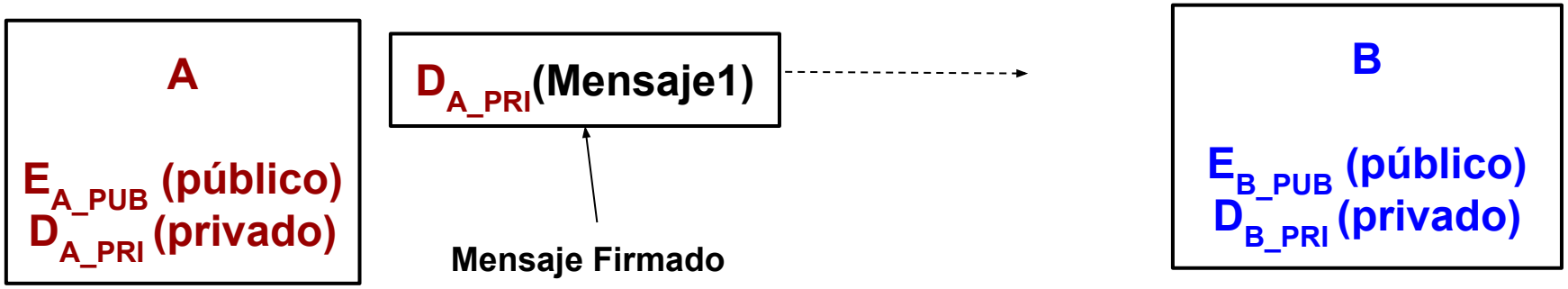
- Problemas de seguridad en redes de computadoras
- Criptografía
- Generación de claves secretas compartidas
- **Firmas digitales y certificados**
- Implementaciones de seguridad

Firmas digitales

- Mismos objetivos: equivalente a una firma escrita.
- Tres condiciones:
  - Que el receptor pueda verificar la identidad del transmisor.
  - Que el emisor no pueda repudiar más tarde el contenido del mensaje.
  - Que el receptor no haya podido elaborar el mensaje él mismo.
- Dos estratégias:
  - Firmas de clave pública.
  - Firmas de clave simétrica:

Firmas de clave pública

Objetivo: Autenticar al emisor. Que B sepa que fue realmente A quien envió el mensaje.

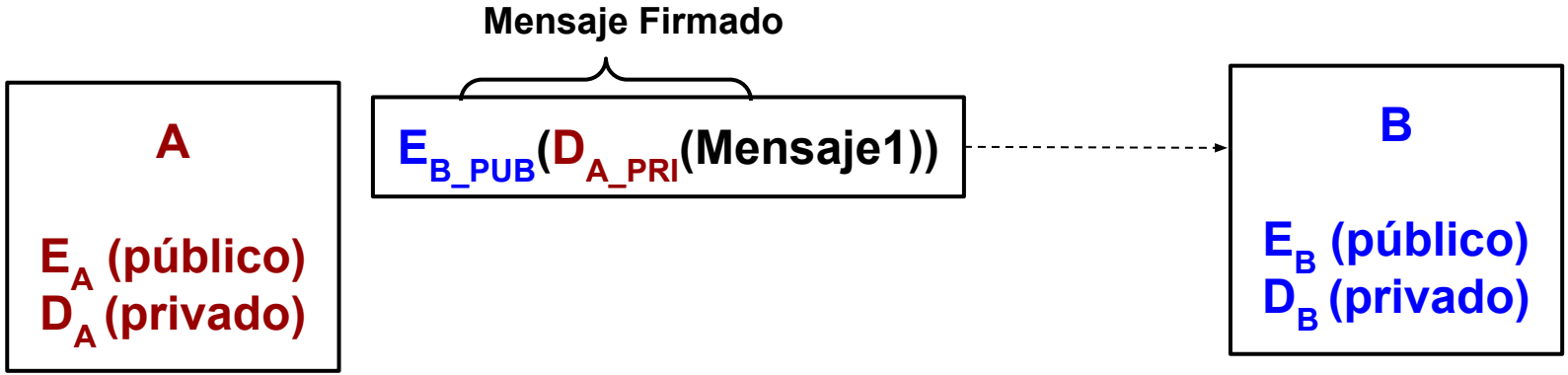


Requisito necesario: El algoritmo de encriptación de clave pública debe cumplir: D(E(P))=P y E(D(P))=P

$E_{A\_PUB}(D_{A\_PRI}(Mensaje1))=Mensaje1$

D_{A_PRI}**(Mensaje1)** es la prueba de que solo A lo pudo generar.

Firmas de clave pública + encriptación



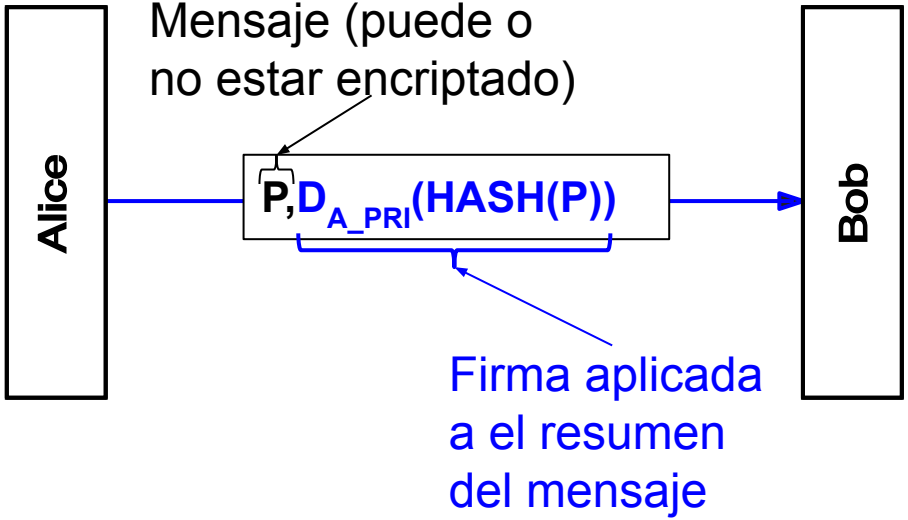
$D_{B\_PRI}(E_{B\_PUB}(D_{A\_PRI}(Mensaje1))=D_{A\_PRI}(Mensaje1)$
$E_{A\_PUB}(D_{A\_PRI}(Mensaje1))=Mensaje1$

$D_{A\_PRI}(Mensaje1)$ es la prueba de que solo A lo pudo generar.

Firma de resúmenes de mensajes

- Desventaja de las firmas de clave pública:
  - Aplicar D en el emisor E en el receptor a **todo el mensaje** puede ser computacionalmente costoso.
- Autentificación mediante resúmenes de mensajes: No se firma todo el mensaje, **se firma un resumen del mismo,** obtenido mediante una **función HASH**.
- Se requiere una función de resumen o **función HASH**, que cumpla:
  - Dado el mensaje P, es computacionalmente económico y rápido calcular la función HASH o **HASH(P)**.
  - Dado HASH(P), es imposible calcular P.
  - Dado P, nadie puede encontrar P′ de tal manera que HASH(P′) = HASH(P).
  - Un cambio en la entrada de incluso 1 bit produce una salida muy diferente.
- Ejemplos: Algoritmos SHA, MD5.

Firma de resúmenes de mensajes



Acciones que realiza Bob:

1) Aplica E_A al resumen firmado: $E_{A\_PUB}(D_{A\_PRI}(HASH(P))=HASH(P)$
2) Aplica la función HASH al mensaje recibido P: HASH(P)
3) Compara el resultado de los pasos 1 y 2.

Bob se asegura que:

- El mensaje proviene de Alice (Solo Alice conoce D_A).
- El mensaje no fue alterado por el camino.

Figura obtenida de: A. Tanenbaum, D. Wetherall, "Redes de computadoras", Quinta edición (2012), pag. 690

Firma de resúmenes de mensajes: SHA-1 y SHA-2

- Desarrollado por la NSA en 1993.
- Genera un mensaje H de 160 bits a partir de texto plano de cualquier longitud.

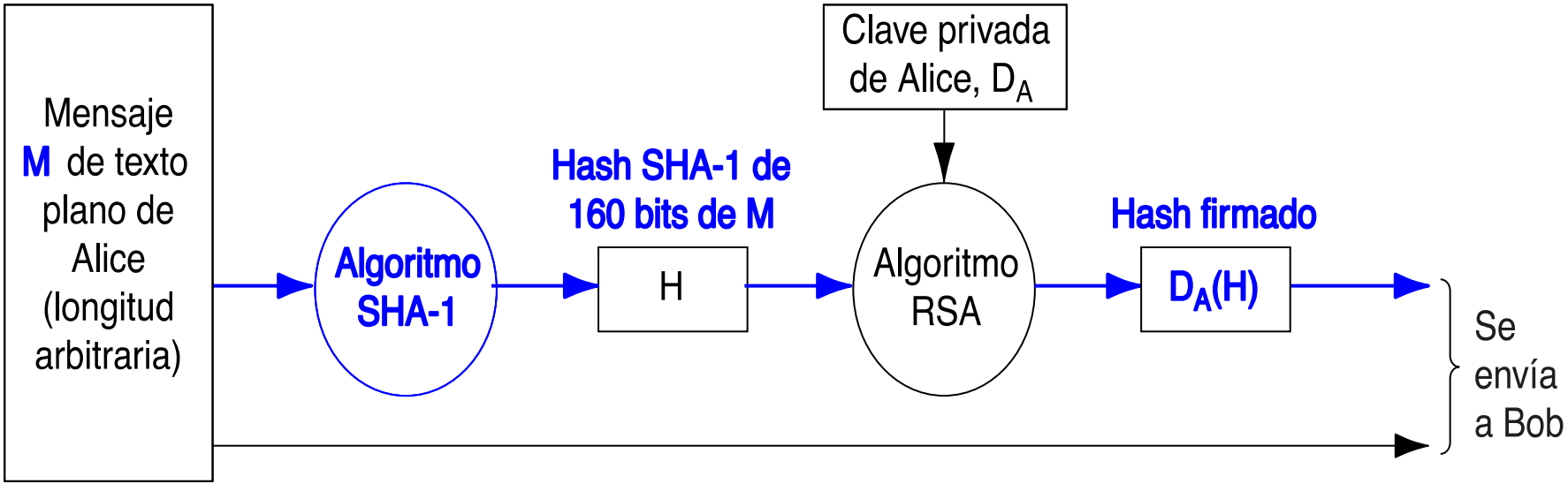
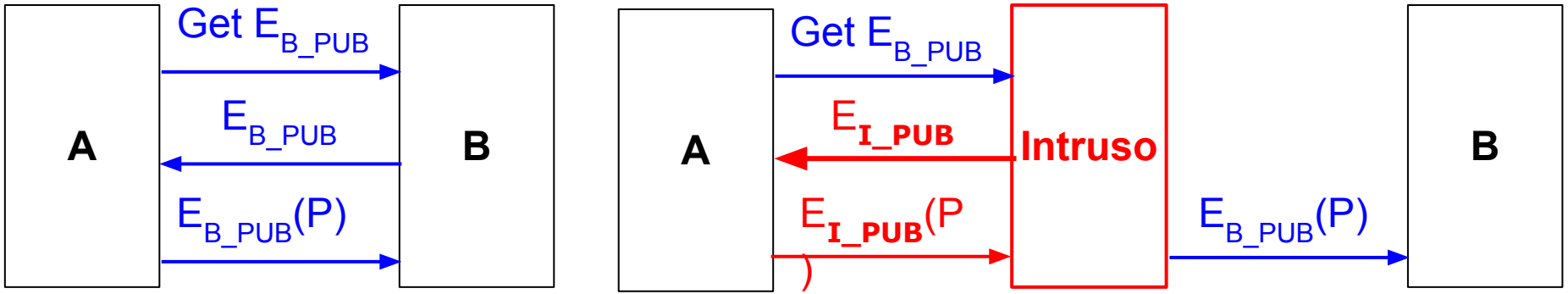


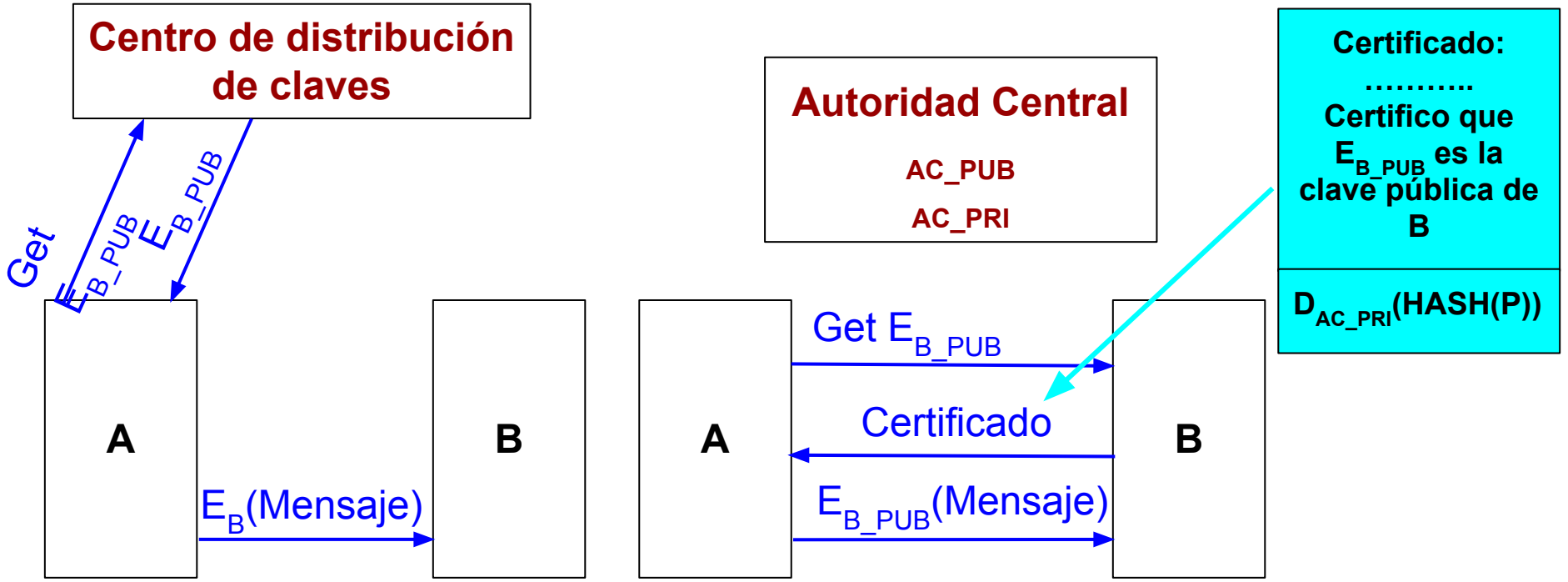
Figura obtenida de: A. Tanenbaum, D. Wetherall, "Redes de computadoras", Quinta edición (2012), pag. 690

Administración de claves públicas

- A quiere comunicarse con B. A necesita la clave pública de B. ¿Como sabe A que la clave pública que obtiene de B (E_{B_PUB}) es realmente la clave pública de B?
  - **Solución: Centro de distribución de claves o Certificados**



Administración de claves públicas



Administración de claves públicas

- Solución 1: Centro de distribución de claves que envíe claves bajo demanda.
  - Cuello de botella. Si falla, falla la seguridad de Internet.
- Solución 2: Autoridades de certificación.
  - Emiten certificados que certifican que una clave pública pertenece a determinada persona (o DNS cuando se usa DNSsec, o una IP, etc.).
  - Se calcula el HASH-1 (contenido del certificado resumido) y **se firma con la clave privada de la autoridad de certificación**.
    - Solo la autoridad de certificación conoce su clave privada.
    - Los navegadores conocen las claves públicas de las autoridades de certificación.
    - **Un intruso no conoce la clave privada de la autoridad de certificación, por lo que no puede generar la firma.**

Administración de claves públicas: Certificados

Dueño:
ebankpersonas.bancopatagonia.com.ar

Clave pública:
c2 e7 21 f6 20 d0 fd ……..

Autoridad de Certificación:
DigiCert

Firma de la Autoridad de Certificación:
67:70:AA:00:DE:68:7F:0B:F4……..

Un certificado puede enlazar una clave pública con:

- **un nombre (empresa, persona, etc). Uso más común.**
- **Un atributo: edad, pertenecer a un curso, etc. (solo el poseedor de la clave privada podrá desencriptar mensajes).**

Firma (HASH del contenido del certificado) encriptado con la clave privada de la autoridad de certificación

$$DA_{AC\_PRI}(HASH(\text{contenido certificado}))$$

Ver certificados Chrome: Clic en el candado, luego en “certificado”.
Ver certificados en Firefox: Clic en el candado, luego en flecha al lado de “conexión segura”, luego en “más información”, luego en “seguridad”, luego en “ver certificado”.

Estándar X.509

- Estándar (ITU-T) que indica cómo debe escribirse un certificado (campos que debe tener). Versión actual: 3

Campo	Significado
Versión	Qué versión de X.509.
Número de serie	Este número más el nombre de la CA identifican el certificado de manera única.
Algoritmo de firma	El algoritmo utilizado para firmar el certificado.
Emisor	El nombre X.500 de la CA.
Periodo de validez	Los tiempos inicial y final del periodo de validez.
Nombre del sujeto	La entidad cuya clave se va a certificar.
Clave pública	La clave pública del sujeto y la ID del algoritmo que la utiliza.
ID del emisor	Un ID opcional que identifica al emisor del certificado en forma única.
ID del sujeto	Un ID opcional que identifica al sujeto del certificado en forma única.
Extensiones	Se han definido muchas extensiones.
Firma	La firma del certificado (firmada por la clave privada de la CA).

Figura obtenida de: A. Tanenbaum, D. Wetherall, "Redes de computadoras", Quinta edición (2012), pag. 696

Infraestructuras de claves públicas

- ¿Quién es la **autoridad de certificación (SA)**?
  - No puede ser una autoridad central, si se cae, se cae la seguridad de todo internet.
  - No puede haber una sola clave privada (muchas SA que usen la misma clave), la probabilidad de que sea robada sería alta (sería botín demasiado atractivo de robar).
  - **Solución: PKI** (Public Key Infrastructure o Infraestructura de Clave Pública).
- PKI (Public Key Infrastructure): Define la estructura de funcionamiento y estándares para protocolos y documentos.
  - El único requisito es conocer la clave privada del Raíz

Infraestructuras de claves públicas: Ejemplo

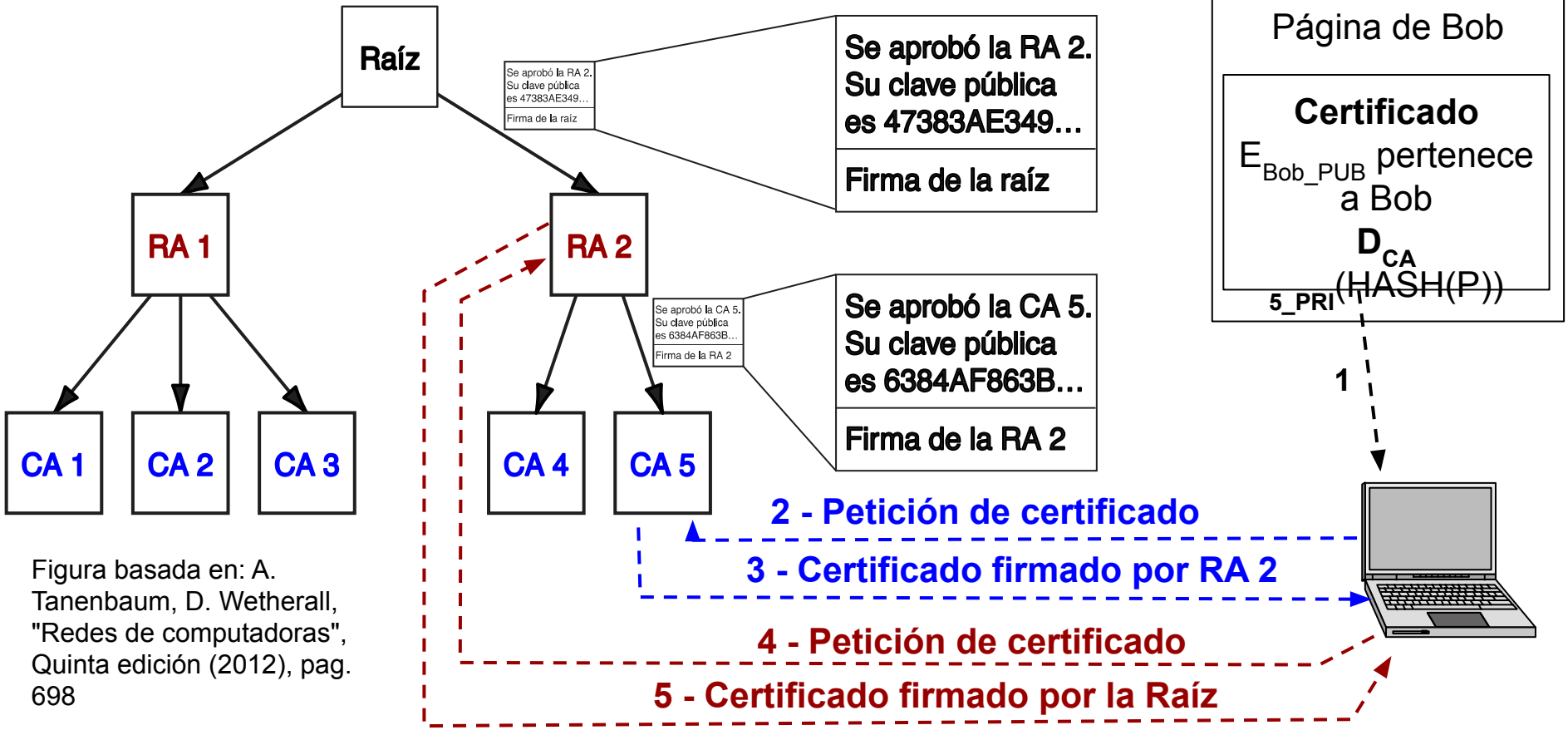
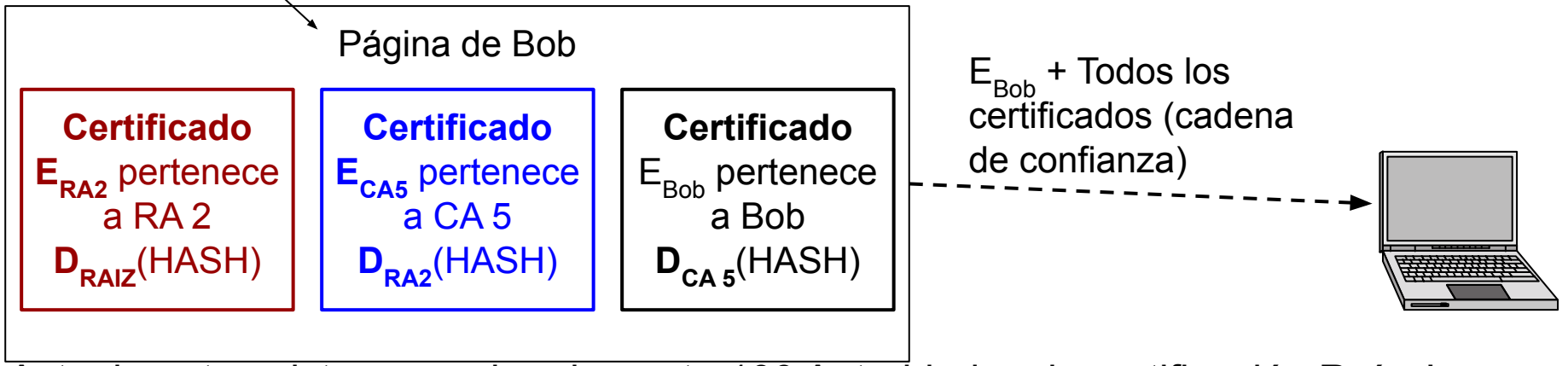


Figura basada en: A. Tanenbaum, D. Wetherall, "Redes de computadoras", Quinta edición (2012), pag. 698

Infraestructuras de claves públicas: Ejemplo

Almacena todos los certificados hasta la raíz



Actualmente existen aproximadamente 100 Autoridades de certificación Raíz. Los navegadores y aplicaciones que utilizan Internet las conocen [1]

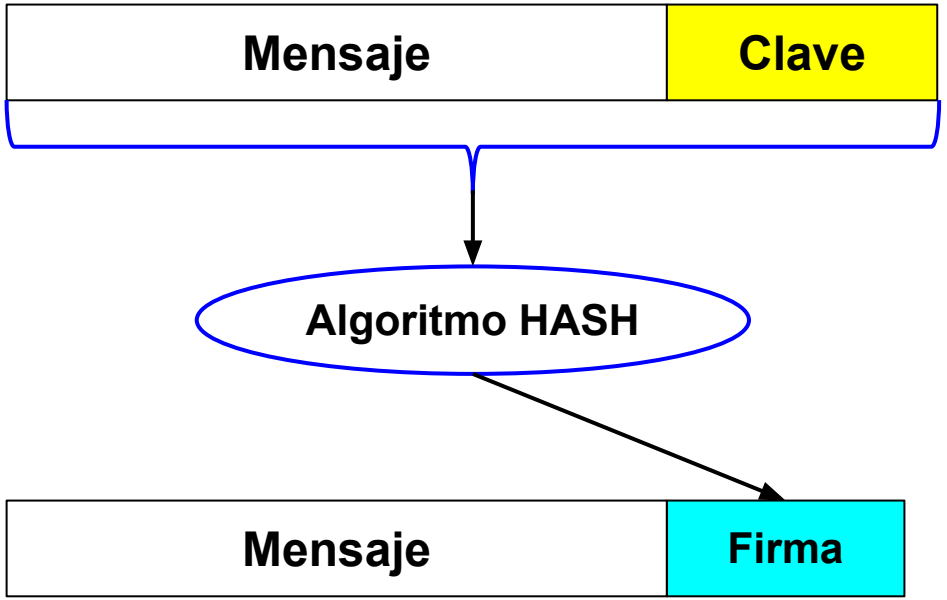
[1] Google Chrome: Acerca de Google Chrome (o similar) -> Configuración Avanzada -> Privacidad y Seguridad -> Gestionar Certificados -> Autoridades.
Firefox: Preferencias -> Privacidad y Seguridad -> Ver certificados -> Autoridades

Firmas de clave simétrica

- Firmar mensajes con clave pública **es muy robusto pero computacionalmente costoso**.
  - Muy útiles y robustos para certificar la identidad de un servidor.
  - Si se envían muchos paquetes firmados, puede hacer lenta la comunicación.
- **Firmas de clave simétrica**: Los paquetes se firman con una clave simétrica.
  - Fundamento: Solo el emisor y el receptor conocen la clave, por lo que solo el emisor pudo haber firmado el paquete.
  - Objetivo: Integridad + Autenticación del emisor.
  - **Ventaja: Menor costo computacional que la firma de clave pública**.
  - Desventaja: Deben intercambiar primero la clave compartida secreta.
- Ejemplo: HMAC

Firmas de clave simétrica Firmas de clave simétrica sin autoridad central: HMAC

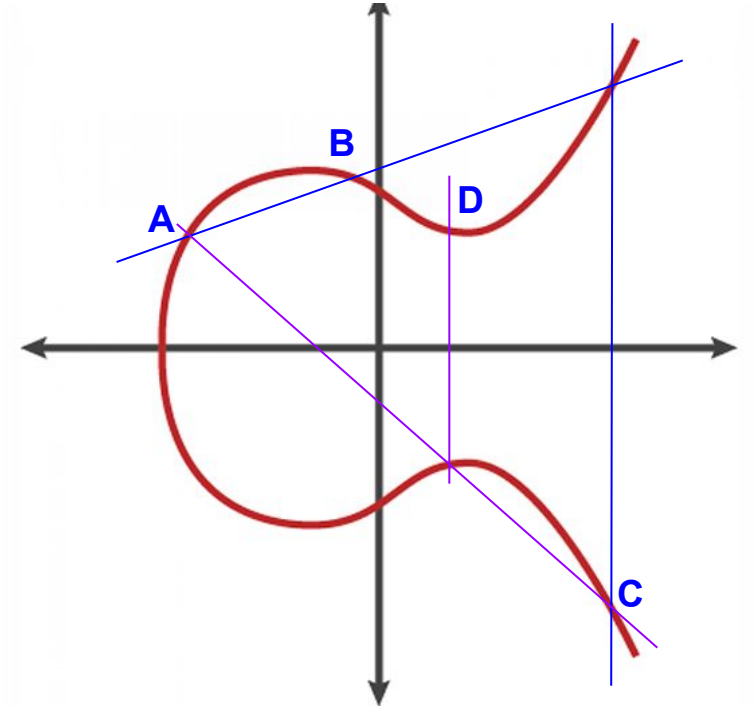
- Al paquete se le añade la clave secreta compartida y se aplica un algoritmo HASH.
- Utilizado por **IPsec**.



Curvas elípticas: Ejemplo con ECDH (Elliptic Curve Diffie Hellman)

Curva elíptica:
$y^2=(x^3+ax+b)$
Se define un álgebra para curvas elípticas

- Alice y Bob eligen una curva elíptica (coeficientes a y b) y un punto generador (A)
- Alice elige un entero n_A y Bob un entero n_B. Que actúan como claves privadas.
- Alice aplica el proceso n_A veces llegando al punto Z_A.
- Bob aplica el proceso n_B veces llegando al punto Z_B.



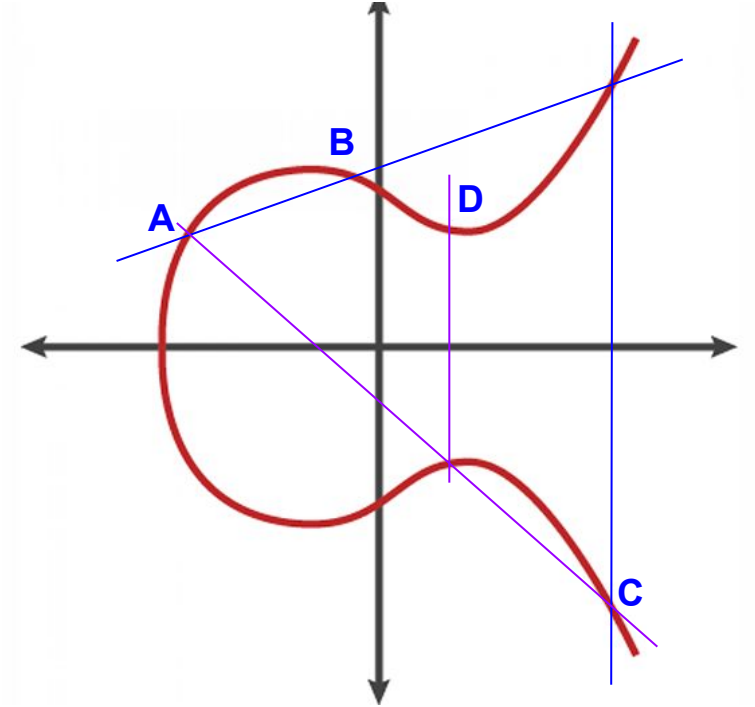
Curvas elípticas: Ejemplo con ECDH (Elliptic Curve Diffie Hellman)

- Alice comparte Z_A y Bob comparte Z_B.

Fundamento:

Conociendo n_A y n_B es fácil llegar a Z_A y Z_B, pero el **proceso inverso es muy difícil**.

- Alice toma Z_B y aplica el proceso n_A veces.
- Bob toma Z_A y aplica el proceso n_B veces.
- **Ambos llegan al mismo punto final**.



Temario

- Problemas de seguridad en redes de computadoras
- Criptografía
- Generación de claves secretas compartidas
- Firmas digitales y certificados
- **Implementaciones de seguridad**

Componentes de seguridad: Firewalls

- Filtro de paquetes.
  - Paquetes salientes (pueden contener información confidencial de la empresa, personas, etc.).
  - Paquetes entrantes (pueden contener malware).
- Inspecciona todos los paquetes (bloqueando o permitiendo).
  - Orígenes y destinos (IPs y puertos).
  - Contenido de las peticiones HTTP.
  - Protocolos o aplicaciones.
  - Si un paquete que proviene de un servidor web externo es respuesta a una petición generada por una máquina interna.
- Verifica si los paquetes cumplen un conjunto de reglas.
  - Si las cumplen, siguen su camino.
  - Si no las cumplen, se descartan.

Componentes de seguridad: Firewalls

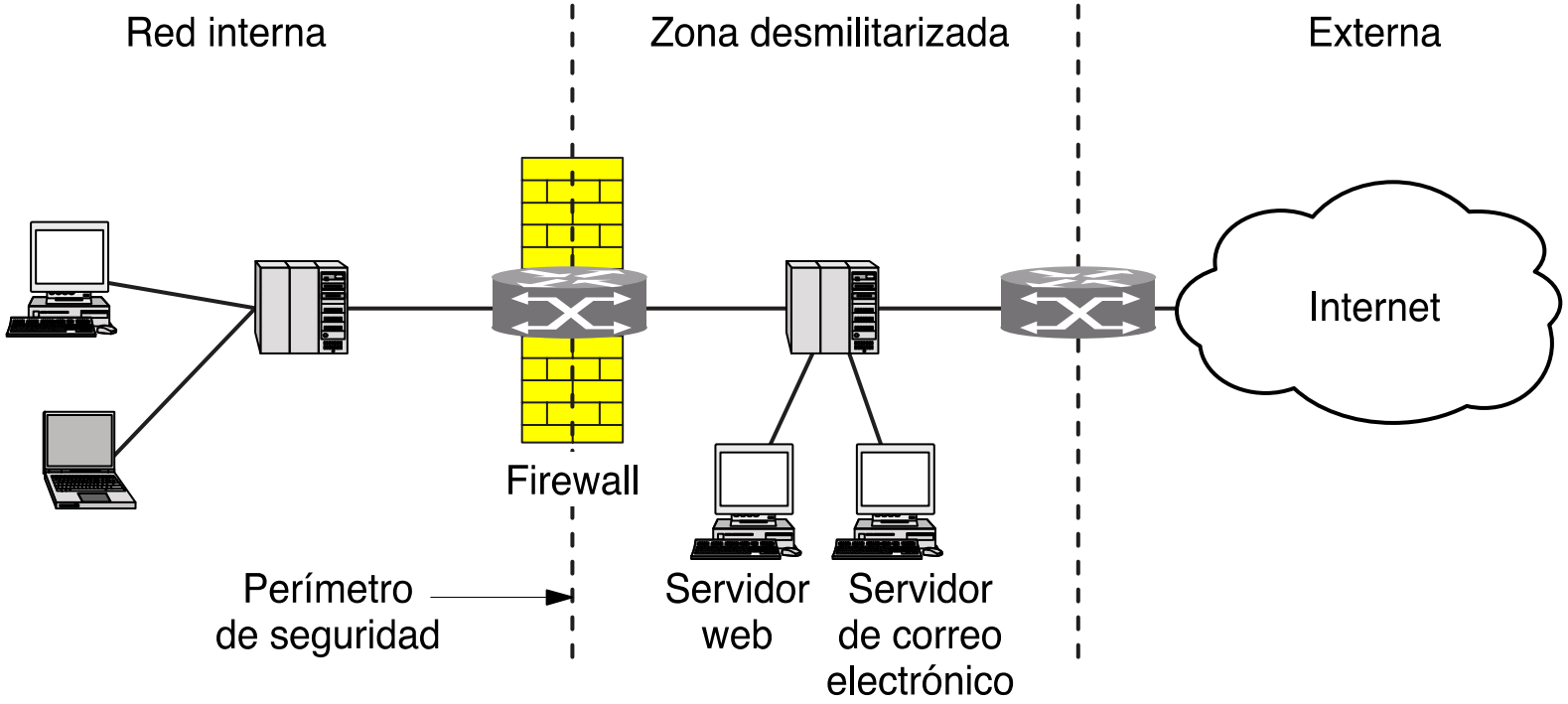


Figura obtenida de: A. Tanenbaum, D. Wetherall, "Redes de computadoras", Quinta edición (2012), pag. 704

Componentes de seguridad: Firewalls

- Desventajas:
  - No pueden inspeccionar tráfico encriptado.
    - Incompatible con IPsec y las VPNs.

- Ejemplo: **IPtables**
  - Aplicación que permite configurar el Firewall del núcleo de Linux.
- **ufw** (Uncomplicated Firewall).
  - Herramienta que permite configurar las IPtables.
- **Gufw**: Interfaz gráfica de ufw.

IDS (Intrusion Detection System)

- Buscan patrones usuales de un ataque:
  - Escaneo de puertos.
  - Ataque ssh de fuerza bruta (intentar con muchas contraseñas comunes).
  - Buscar firmas de ataques conocidos.
- Tipos de IDS según donde actúan:
  - HIDS (Host-based IDS): Actúan en el host.
  - NIDS (Network IDS): Actúan en la red.
- Tipos de IDS según su funcionamiento:
  - IDS basados en **firmas**: Detectan comportamiento de expoits conocidos.
    - Ejemplo: Mensaje con 10 bytes al puerto 53 (DNS).
  - IDS basados en **comportamiento anómalo**: Aprenden el comportamiento de una computadora (tipo tráfico, frecuencia, tamaño de paquetes, etc.) y buscan comportamiento anómalo.

IPsec

- Motivación: gran cantidad de ataques basados en IP spoofing o análisis de tráfico basado en el contenido de los paquetes IP.
- En IPv6 es obligatorio (es un encabezado adicional). En IPv4 es opcional.
- Tres servicios:
  - **Autentificación** + **Integridad**: Agrega un encabezado llamado AH (Authentication Header) con un hash firmado HMAC.
  - **Autentificación** + **Integridad** + **cifrado**: Agrega un encabezado llamado EPS Encapsulado de la carga útil de seguridad (ESP, Encapsulating Security Payload.
  - **Intercambio de claves**.
- Orientado a conexión.
  - La conexión unidireccional se denomina “Asociación de seguridad” (SA).
  - Para seguridad en ambas direcciones, se necesitan dos SA.

IPsec

- Asociación de seguridad queda identificada por 3 parámetros:
  - IP destino.
  - Índice de parámetros de seguridad (identifica la AS dentro del destino).
  - Identificador del protocolo de seguridad: AH o ESP.

Encabezado AH (Authentication Header)

- Provee **integridad**, **autentificación** y **protección ante ataques de repetición** (utilizando un número de secuencia).
- HMAC (Hash Message Authentication Code): Hash de los siguientes datos:
  - Carga útil del paquete IP
  - Datos que no cambian del encabezado IP (direcciones IP para evitar IP spoofing, etc.)
  - Clave secreta compartida.

Encabezado AH (cabecera de autenticación)

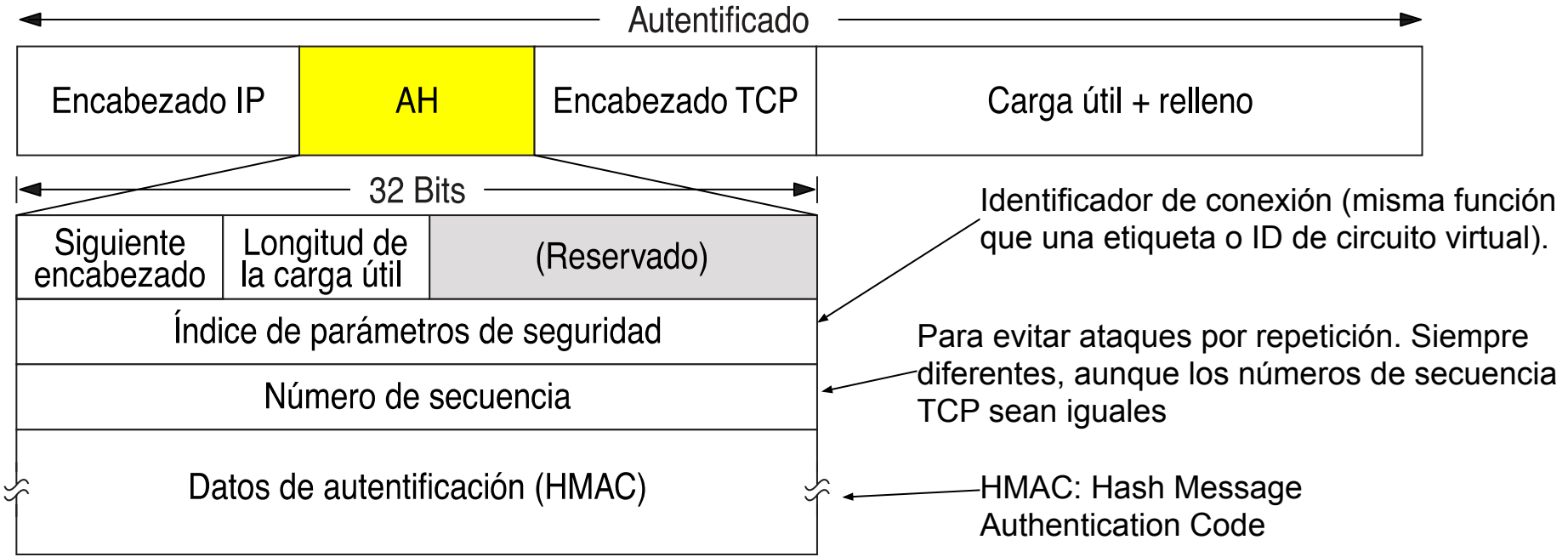


Figura obtenida de: A. Tanenbaum, D. Wetherall, "Redes de computadoras", Quinta edición (2012), pag. 702

IPsec: Encabezado ESP (Encapsulating Security Payload)

- Dos modos:
  - Modo de transporte.
    - Agrega un encabezado IPsec luego del encabezado IP. El campo protocolo del encabezado IP debe indicar que sigue un encabezado IPsec.
    - Las IPs origen y destino no se encriptan.
  - Modo túnel.
    - El paquete IP se encapsula dentro de otro paquete (incluso las IPs).
    - Útil cuando el origen y/o el destino no son el origen o destino final (usualmente el origen y/o destino son firewall).

IPsec: Protocolo ESP en modo transporte

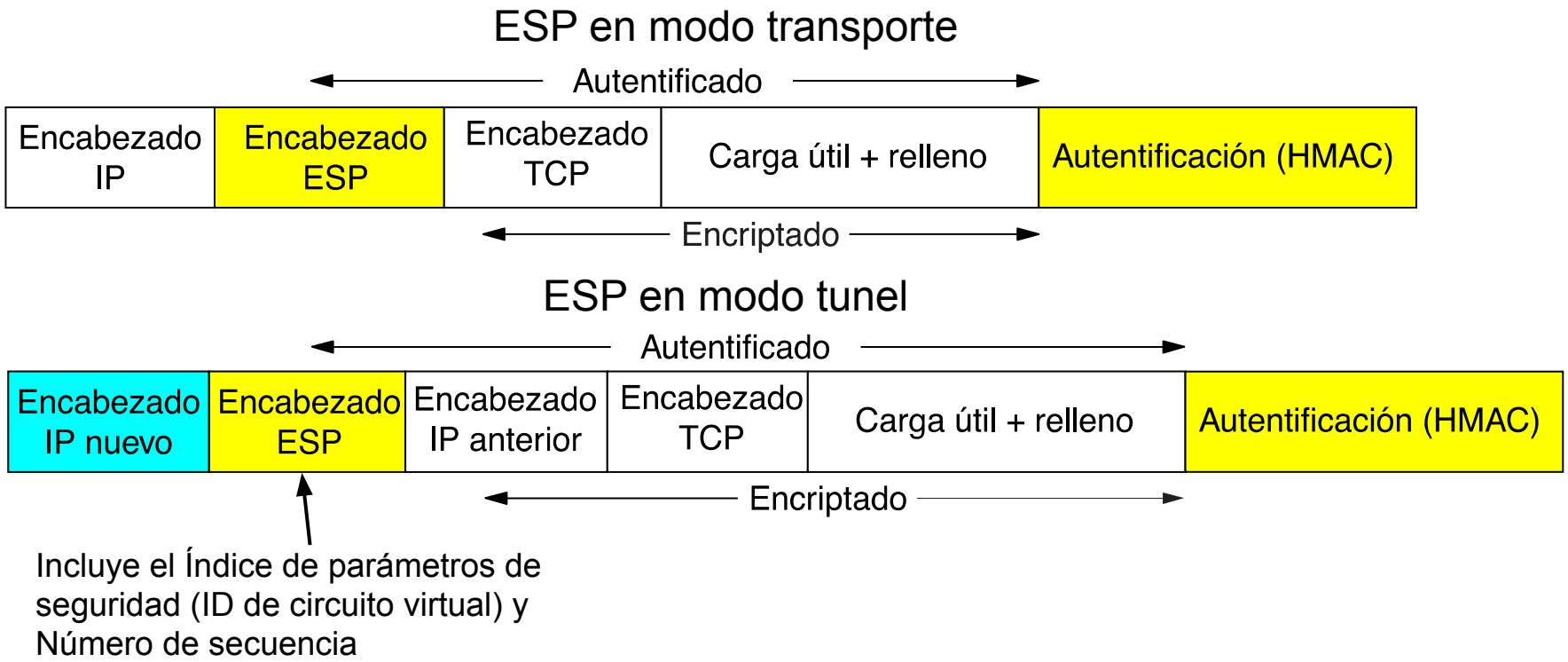


Figura obtenida de: A. Tanenbaum, D. Wetherall, "Redes de computadoras", Quinta edición (2012), pag. 703

DNSsec (DNS seguro)

- Basado en **firmas de clave pública** para lograr autentificación e integridad.
- Toda la información que envía el servidor DNS se firma para que el receptor pueda verificar identidad.
- Servicios:
  - **Autentificación e integridad**: que el cliente pueda verificar el origen de los datos: servicio principal (mediante la firma).
  - **Distribución de claves públicas** (además de la IP asociada a un nombre de dominio, el servidor DNS puede proveer la clave pública del mismo).
- Aún no implementado al 100%.

DNSsec (DNS seguro)

Ejemplo de una respuesta enviada por el servidor DNS que usa DNSsec:

Nombre del dominio	Tiempo de vida	Clase	Tipo	Valor
bob.com.	86400	IN	A	36.1.2.3
bob.com.	86400	IN	KEY	3682793A7B73F731029CE2737D...
bob.com.	86400	IN	SIG	86947503A8B848F5272E53930C...

- Se utiliza PKI (infraestructura de clave pública) con cadena de confianza (se adapta naturalmente a la infraestructura DNS).
- Key: clave pública de Bob.
- SIG: firma.

Figura obtenida de: A. Tanenbaum, D. Wetherall, "Redes de computadoras", Quinta edición (2012), pag. 703

SSL (Secure Sockets Layer) y TLS (Transport Layer Security)

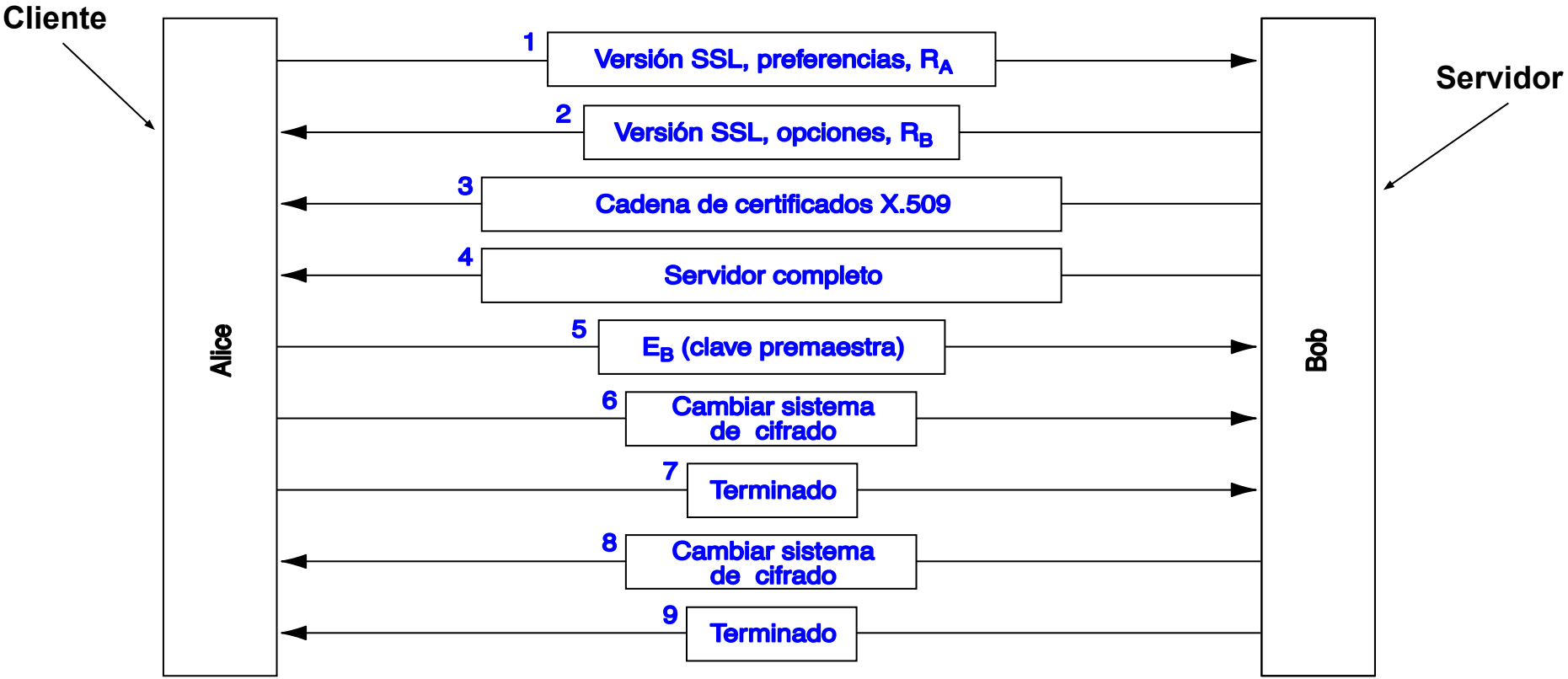
- Servicio que hace que la conexión entre dos sockets sea segura, implementando mecanismos de seguridad.
- Puede ser una capa adicional o estar implementado en las aplicaciones.
- Implementa:
  - Negociación de parámetros.
  - Autentificación del servidor por parte del cliente.
  - Encriptación
  - Integridad datos.
- **No impone modificar** ni hacer consciente a las **aplicaciones** de los mecanismos de seguridad (HTTP sobre SSL se llama HTTPS, puerto 443)

Aplicación (HTTP)
Seguridad (SSL)
Transporte (TCP)
Red (IP)
Enlace de datos (PPP)
Física (módem, ADSL, TV por cable)

SSL (Secure Sockets Layer) y TLS (Transport Layer Security)

- SSL
  - Implementado por Netscape Communications Corp.
  - Utilizado (e implementado) por la mayoría de los navegadores actuales.
  - Dos subprotocolos:
    - Establecimiento de conexión
    - Utilización de la conexión
- TLS:
  - Implementación de SSL (versión 3) realizada por la IETF (RFC 5246).
  - Poseen diferencias que los hacen incompatibles.
- Usualmente los navegadores implementan ambos.

SSL: subprotocolo de establecimiento de conexión



SSL: subprotocolo de establecimiento de conexión

- Aclaraciones figura anterior:
  - Preferencias (mensaje 1): preferencias sobre algoritmos criptográficos y de compresión.
  - Opciones (mensaje 2): algoritmos que Bob selecciona de las preferencias que indicó Alice.
  - Servidor completo (mensaje 4): Bob puede enviar peticiones a Alice. Cuando termina, envía un mensaje a Alice para indicarle que terminó de enviar sus mensajes.
  - Clave premaestra: se utiliza para crear, junto con R_A y R_B, una clave de sesión.
- ¿Cómo autentifica el servidor al cliente?
  - En el mensaje 4, pidiéndole su certificado.
  - Si el cliente no tiene certificado (lo más usual), se realiza mediante un usuario contraseña (fuera del alcance de SSL).

Servicios SSL

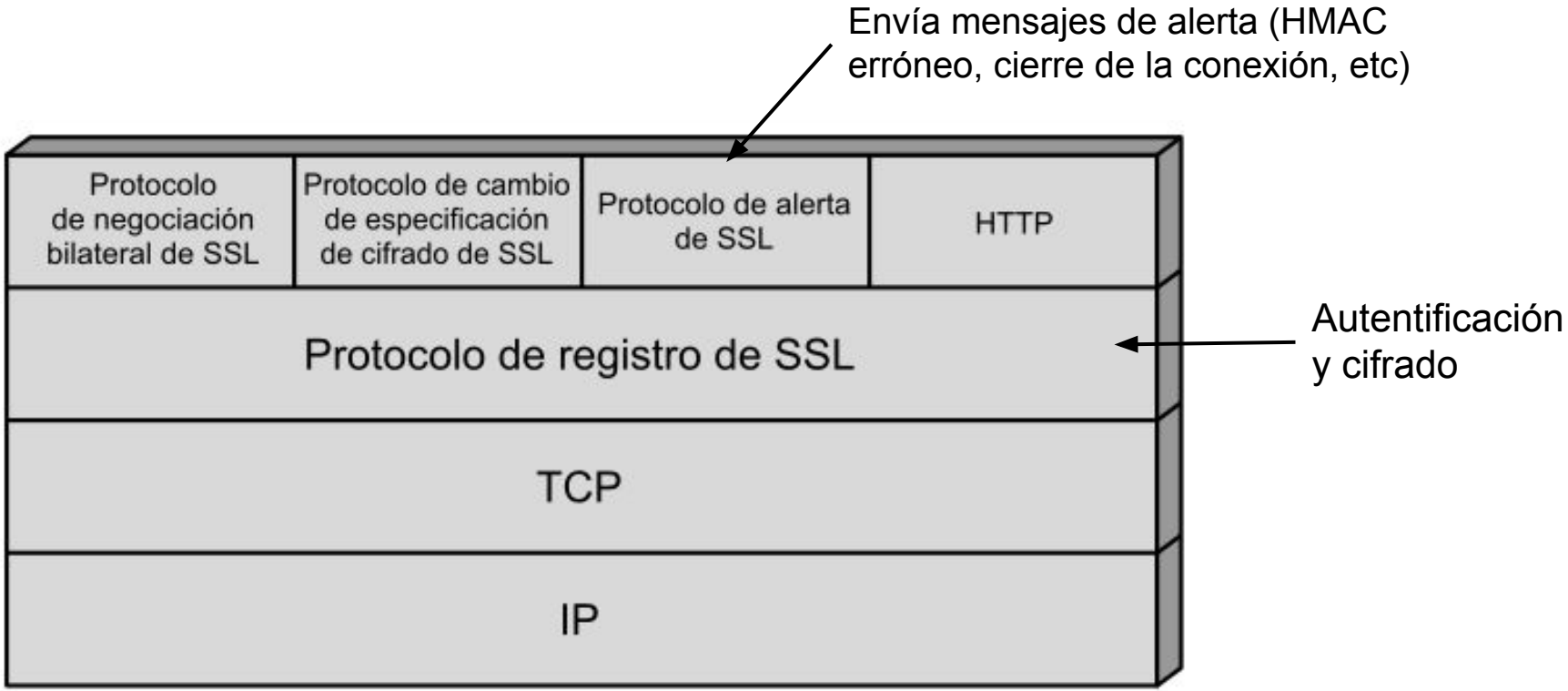


Figura obtenida de: William, Stallings: “Data and Computer Communications”, 8ed, 2007, pag. 750

Elementos de seguridad en redes en el modelo TCP/IP

Aplicación	Autentificación de clientes que no poseen certificados (usuario y contraseña).
SSL	Encriptación. Autentificación, Integridad (firmas, certificados)
Transporte	
Red	IPsec Firewall *, IDS*
Enlace	WPA, AES, Triple DES.
Física	Protección física de enlaces.

* Los firewall y los IDS actúan en todas las capas.

Bibliografía

- A. Tanenbaum, D. Wetherall, "Redes de computadoras", Sexta edición. 2021.
- https://nmap.org/