DECSAI
Departamento de Ciencias de la Computación e I.A.
Universidad de Granada

Seguridad
Transmisión de datos y redes de ordenadores

Seguridad

Aspectos de la seguridad en redes
- Ataques (activos y pasivos)

Criptografía
- Criptografía de clave secreta
- Criptografía de clave pública

Funciones hash, firmas digitales y certificados

Autentificación

Comunicaciones seguras en Internet
- Cortafuegos
- Redes privadas virtuales
- Seguridad en redes inalámbricas 802.11
- Seguridad en Internet: IPSec & SSL/TLS
- Seguridad en las aplicaciones de Internet (correo electrónico y web)

Apéndice: Intercambio de claves

Seguridad: Motivación

Motivos por los que alguien
podría causar problemas de seguridad:

Adversary	Goal
Student	To have fun snooping on people's e-mail
Cracker	To test out someone's security system; steal data
Sales rep	To claim to represent all of Europe, not just Andorra
Businessman	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 e-mail
Con man	To steal credit card numbers for sale
Spy	To learn an enemy's military or industrial secrets
Terrorist	To steal germ warfare secrets

Seguridad: Aspectos

Aspectos por los que se necesita seguridad:

- Privacidad de la información (p.ej. evitar intrusos).
- Libertad de expresión.
- Derechos de autor (copyright).
- Autentificación (origen y destino fiables).
- Integridad
  (el mensaje ha de recibirse tal como se originó).
- No repudiación
  (una vez enviado un mensaje, el usuario no puede negar su autoría, p.ej. transacciones comerciales).

Seguridad

SEGURIDAD

=

Confidencialidad

+

Integridad

+

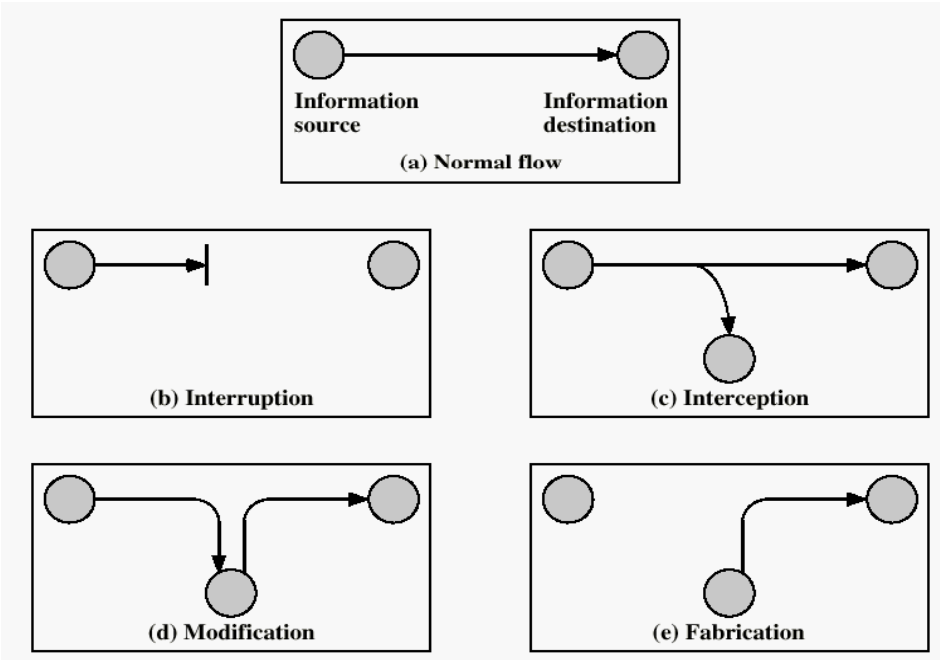
Disponibilidad

+

Autentificación

Seguridad: Ataques

Riesgos (amenazas) ➔ Identificación de vulnerabilidades



Seguridad: Ataques

Ataques pasivos

Difíciles de detectar,
si bien pueden tomarse medidas preventivas.

- **Escuchas** *[eavesdropping]*

  Objetivo: Obtener información.

  Mecanismo: Análisis del tráfico
  (frecuencia y naturaleza de los mensajes).

  vg: Sniffers, scanners, crackers…

Seguridad: Ataques

Ataques activos

"Fáciles" de detectar, aunque difíciles de prevenir:

- **Masquerading = Spoofing**
  (pretender ser quien no se es)

  vg: Direcciones IP (DNS),
  números de secuencias (TCP),
  ataques por repetición [replay],
  MIM [Man in the Middle]…

Seguridad: Ataques

Ataques activos

"Fáciles" de detectar, aunque difíciles de prevenir:

- **Alteración de datos**

  vg: WWW

- **Denegación de servicio** *[denial of service]*

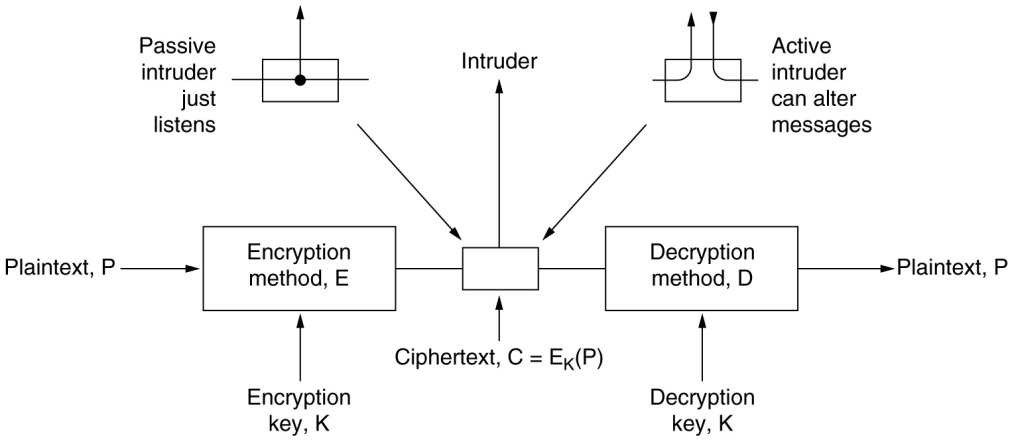
  vg: Ping-of-death, smurf, spam, DDoS (TCP SYN)...

- **Ingeniería social**

Seguridad: "Malware"

- Virus
- Gusanos [worms]
- Caballos de Troya
- Puertas traseras [trap doors]
- Bombas lógicas

Criptografía



Sistema criptográfico de clave secreta.

Criptografía

Ejemplo: Cifrado por transposición

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

Plaintext

pleasetransferonemilliondollarsto
myswissbankaccountsixtwotwo

Ciphertext

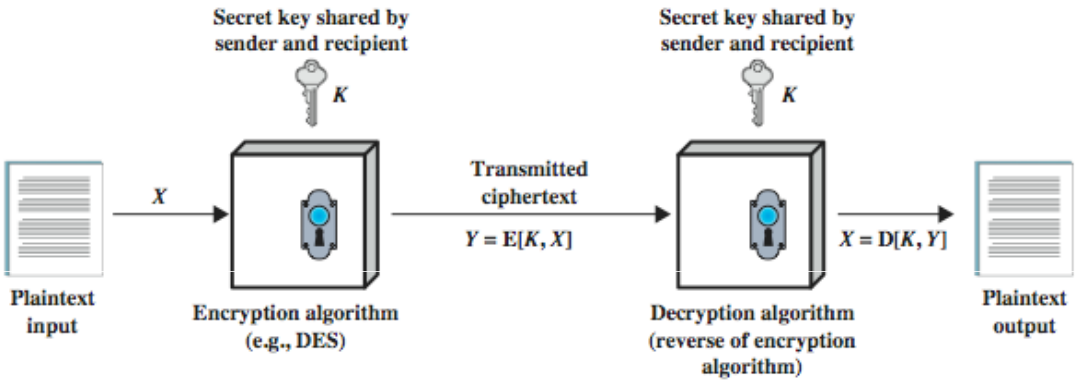
AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUOERIRICXB

Criptografía

Posibles ataques:

- **Criptoanálisis** (basado en el conocimiento de los algoritmos de cifrado y de las características generales de los mensajes).
- **Fuerza bruta** (se analizan todas las posibilidades hasta que se consiga algo).

Criptografía de clave secreta



Requisito:

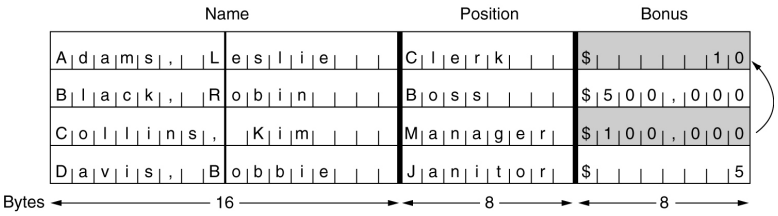
Aunque sea conocido el algoritmo de cifrado, debe ser difícil descifrar el mensaje (aun disponiendo de muchos textos cifrados).

Criptografía de clave secreta

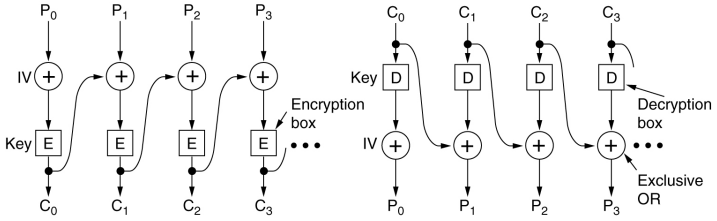
Algoritmos de cifrado en bloque

Bloques de texto de tamaño fijo ⇒ Bloques de texto cifrado.

- Modo ECB [Electronic Code Book]



- Modo CBC [Cipher Block Chaining]:
  Cifrado con encadenamiento

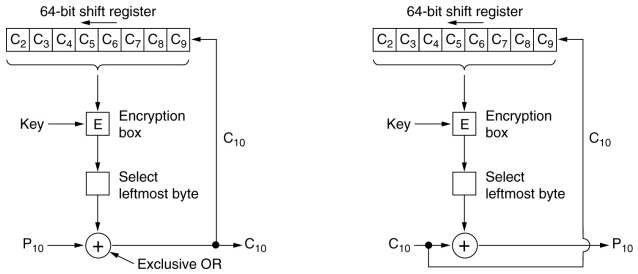


Criptografía de clave secreta

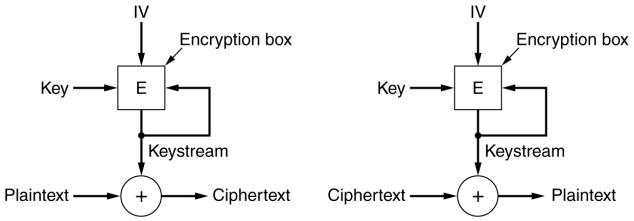
Algoritmos de cifrado en bloque

Bloques de texto de tamaño fijo ⇒ Bloques de texto cifrado.

- Modo CF [Cipher Feedback]: Cifrado con realimentación



- Modo SC [Stream Cipher]



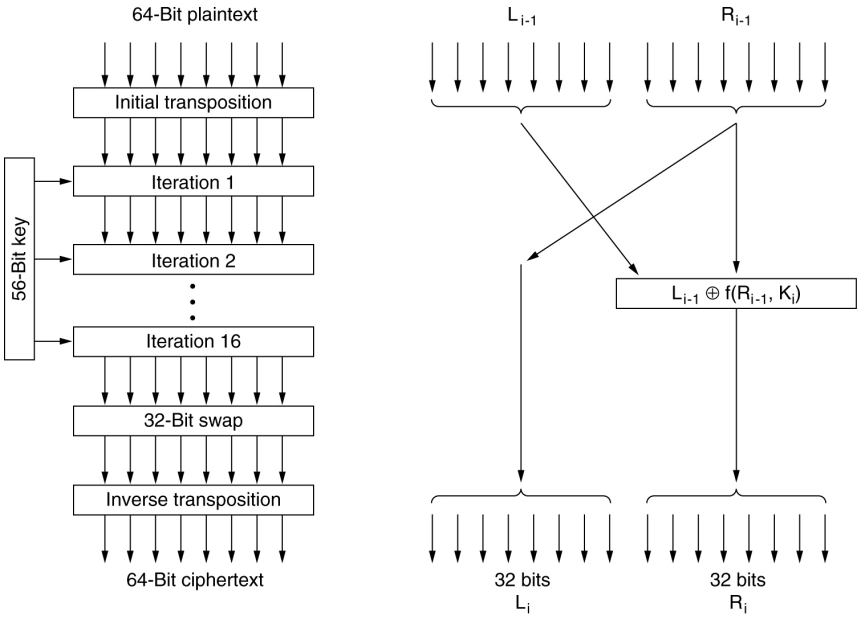
Criptografía de clave secreta

Cipher	Author	Key length	Comments
Blowfish	Bruce Schneier	1–448 bits	Old and slow
DES	IBM	56 bits	Too weak to use now
IDEA	Massey and Xuejia	128 bits	Good, but patented
RC4	Ronald Rivest	1–2048 bits	Caution: some keys are weak
RC5	Ronald Rivest	128–256 bits	Good, but patented
Rijndael	Daemen and Rijmen	128–256 bits	Best choice
Serpent	Anderson, Biham, Knudsen	128–256 bits	Very strong
Triple DES	IBM	168 bits	Second best choice
Twofish	Bruce Schneier	128–256 bits	Very strong; widely used

Criptografía de clave secreta

DES *[Data Encryption Standard], estándar USA*

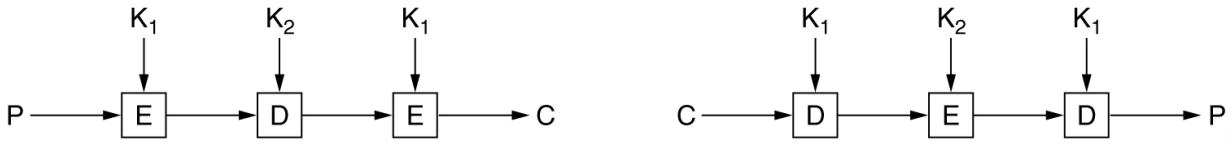
Bloques de 64 bits, clave de 56 bits (inseguro idesde 1998!)



Criptografía de clave secreta

Triple DES *[Data Encryption Standard]*

ANSI X9.17 (1985): 168 bits de clave

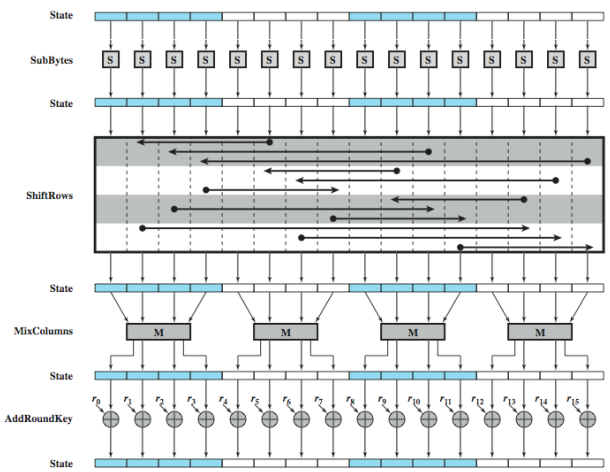


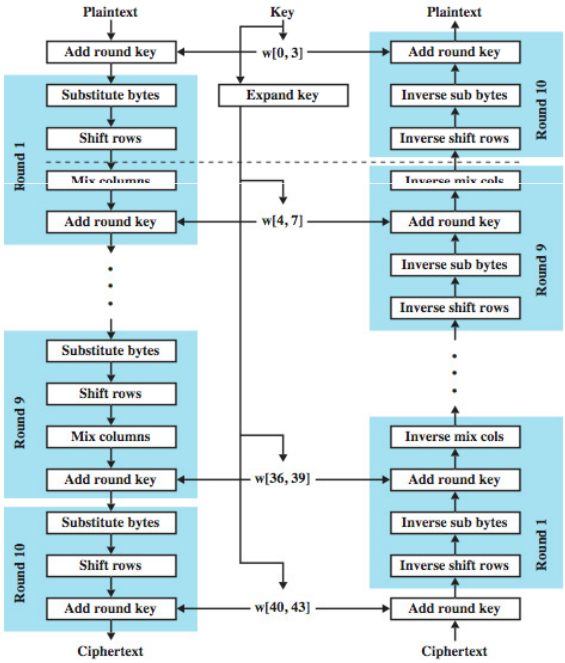
Criptografía de clave secreta

AES *[Advanced Encryption Standard]*

NIST (1997)

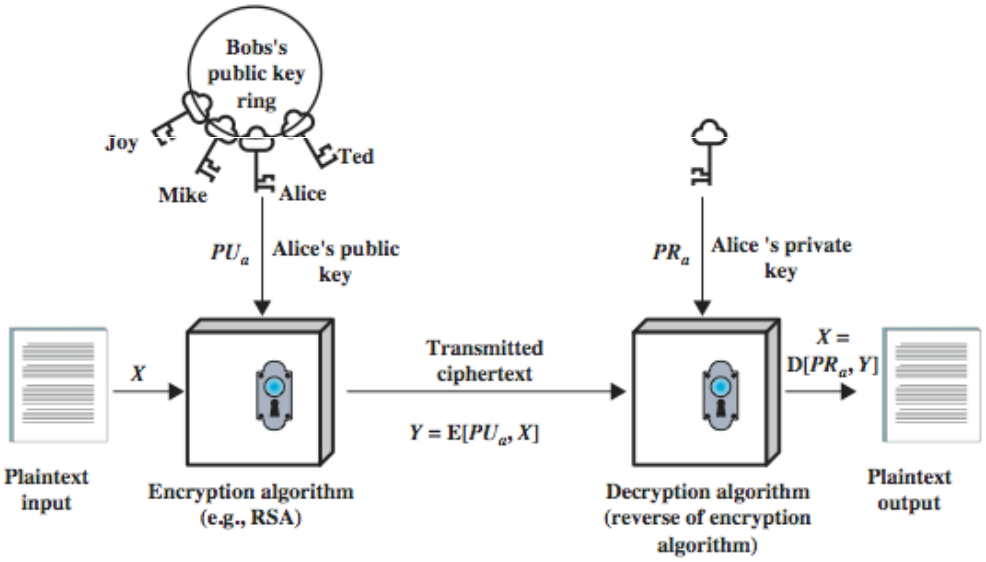
FIPS 197 (2001)





Criptografía de clave pública

Sistema asimétrico con dos claves:



Criptografía de clave pública

Requisitos:

- Debe ser fácil crear un par (clave pública, clave privada).
- Debe existir un algoritmo eficiente para cifrar el texto usando una clave y descifrarlo usando la otra.
- Debe dificultarse al máximo la posibilidad de descubrir la clave privada conociendo la clave pública.
- Debe ser difícil descifrar el texto si sólo disponemos de la clave que se utilizó para cifrarlo y el texto cifrado.

Criptografía de clave pública

Key Generation

Select p, q	p and q both prime
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$d = e^{-1} \bmod \phi(n)$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod n$

Decryption

Ciphertext:	C
Plaintext:	$M = C^d \pmod n$

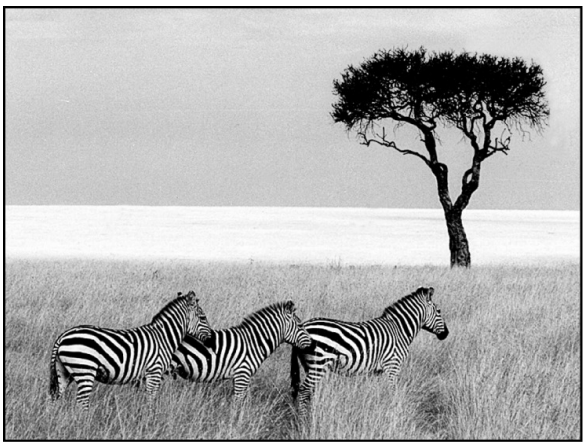
RSA

Rivest, Shamir & Adleman

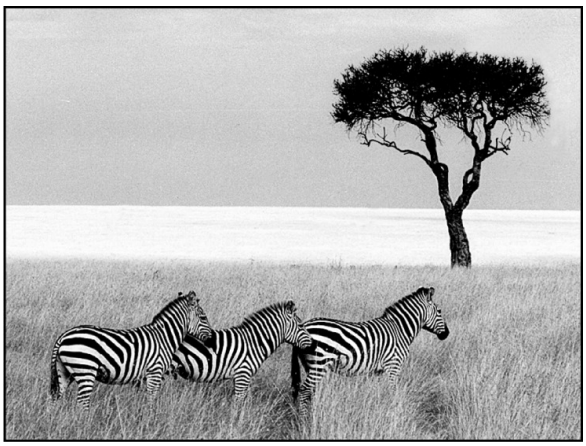
MIT, 1977

Plaintext (P)			Ciphertext (C)		After decryption	
Symbolic	Numeric	P^3	$P^3 \pmod{33}$	C^7	$C^7 \pmod{33}$	Symbolic
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	01	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	05	E
		Sender's computation		Receiver's computation		

Esteganografía



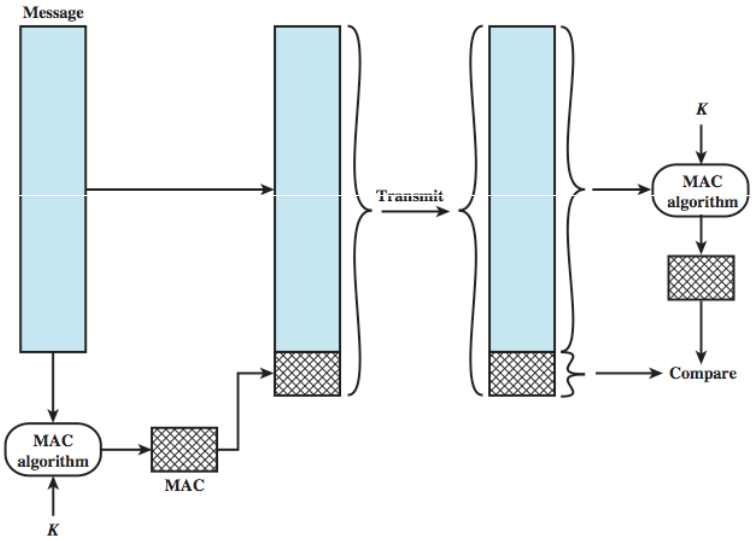
Una foto…



… con cinco obras de Shakespeare.

Funciones hash

Message digests = Message Authentication Codes [MAC]

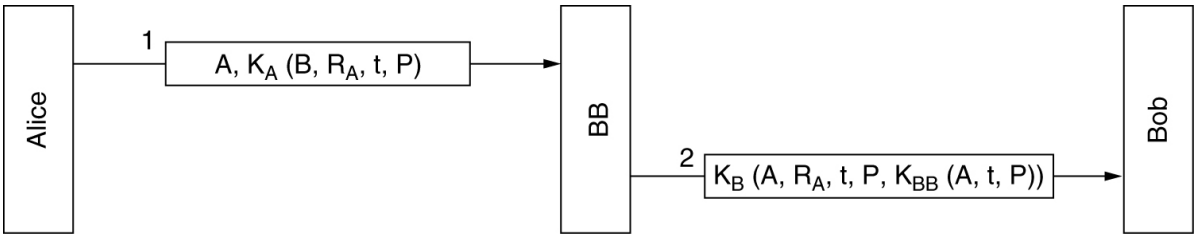


vg: MD5 [Message Digest 5],
SHA-1 [Secure Hash Algorithm – 1]

Firmas digitales

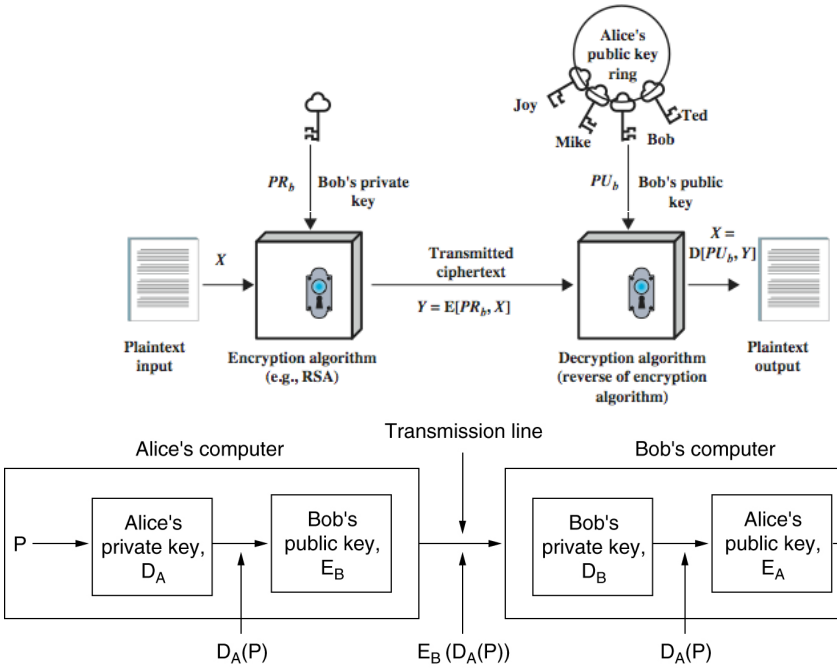
Firmas de clave simétrica

Gran Hermano ("Big Brother")

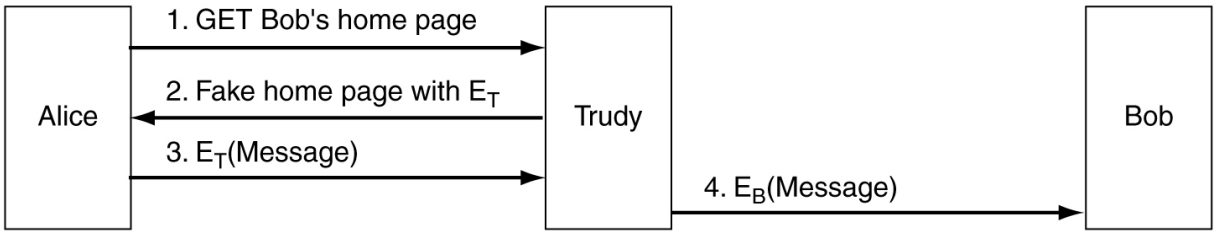


Firmas digitales

Firmas digitales con criptografía de clave pública



Certificados



Intruso en un sistema criptográfico de clave pública

Certificados

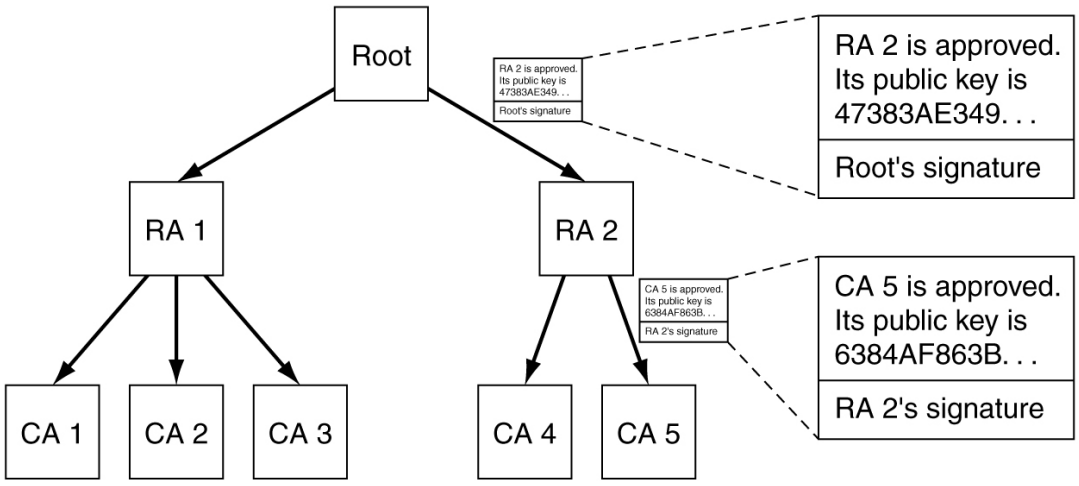
I hereby certify that the public key
19836A8B03030CF83737E3837837FC3s87092827262643FFA82710382828282A
belongs to
Robert John Smith
12345 University Avenue
Berkeley, CA 94702
Birthday: July 4, 1958
Email: bob@superdupernet.com

SHA-1 hash of the above certificate signed with the CA's private key

Certificado digital

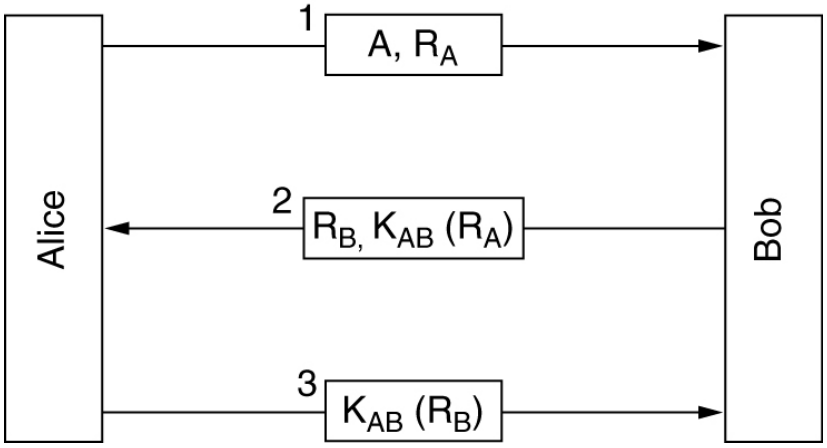
Certificados

Gestión de claves públicas:
Infraestructura de clave pública (PKI)



Autentificación

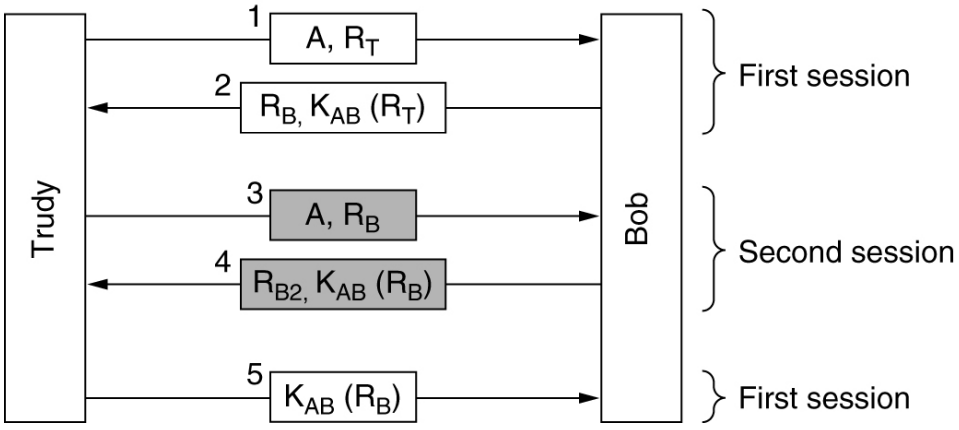
Garantizar que el origen y el destino sean quienes dicen ser…



Autentificación con clave secreta compartida

Autentificación

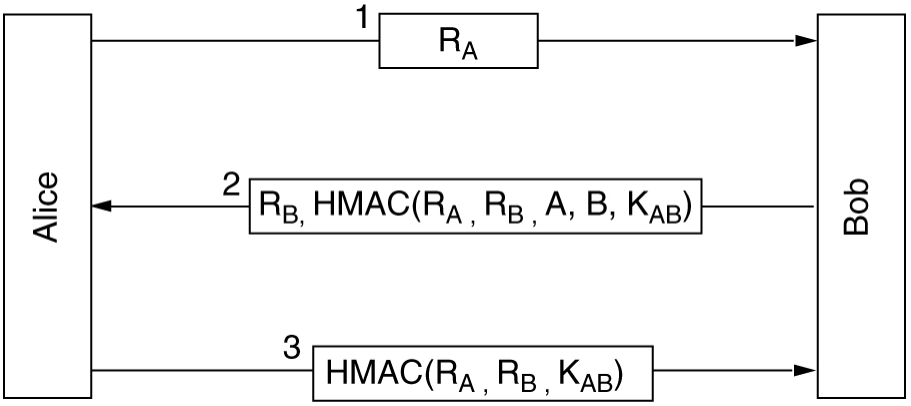
Garantizar que el origen y el destino sean quienes dicen ser…



Problema: Ataque por reflexión

Autentificación

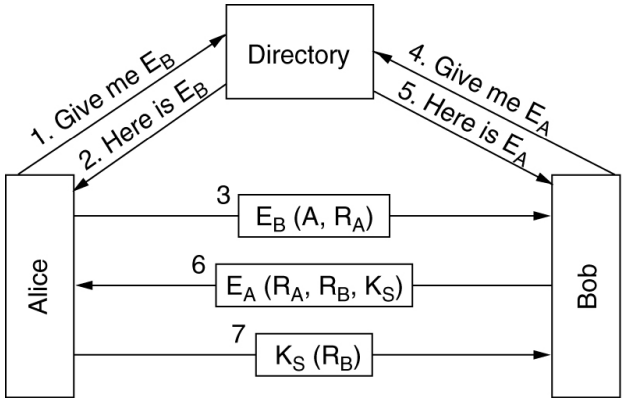
Garantizar que el origen y el destino sean quienes dicen ser…



Solución: HMAC
(Keyed-Hashing for Message Authentication)
RFC 2104

Autentificación

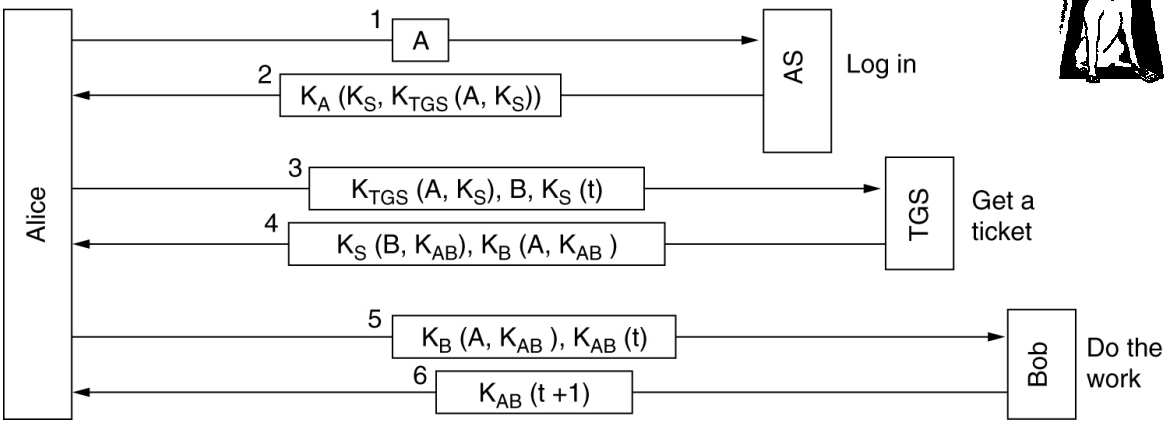
Autentificación basada en criptografía de clave pública



Autentificación mutua

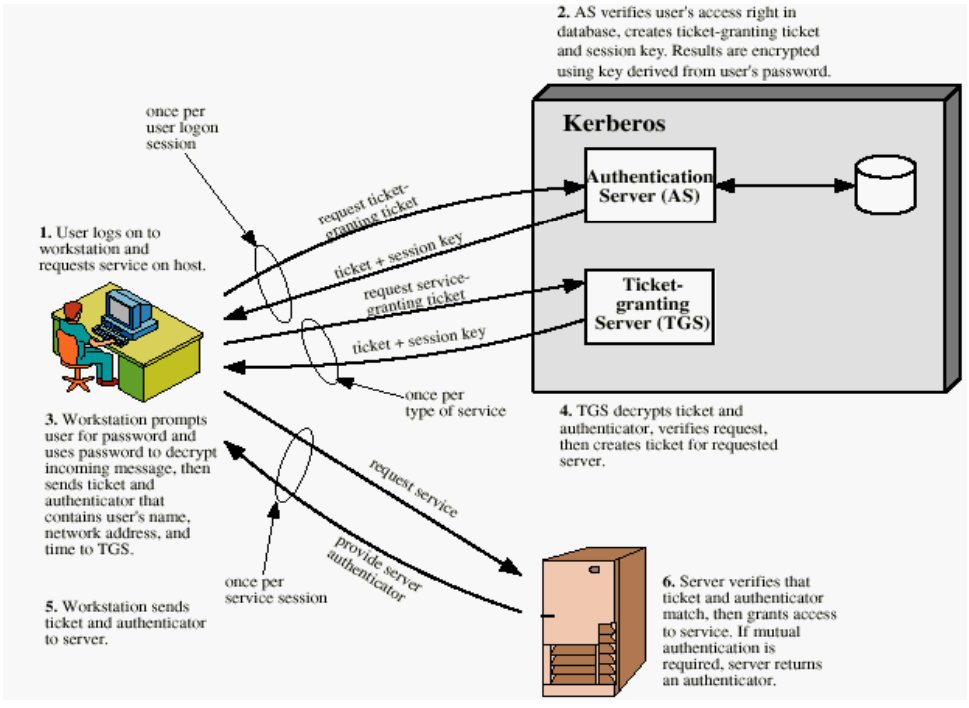
Autentificación

Kerberos



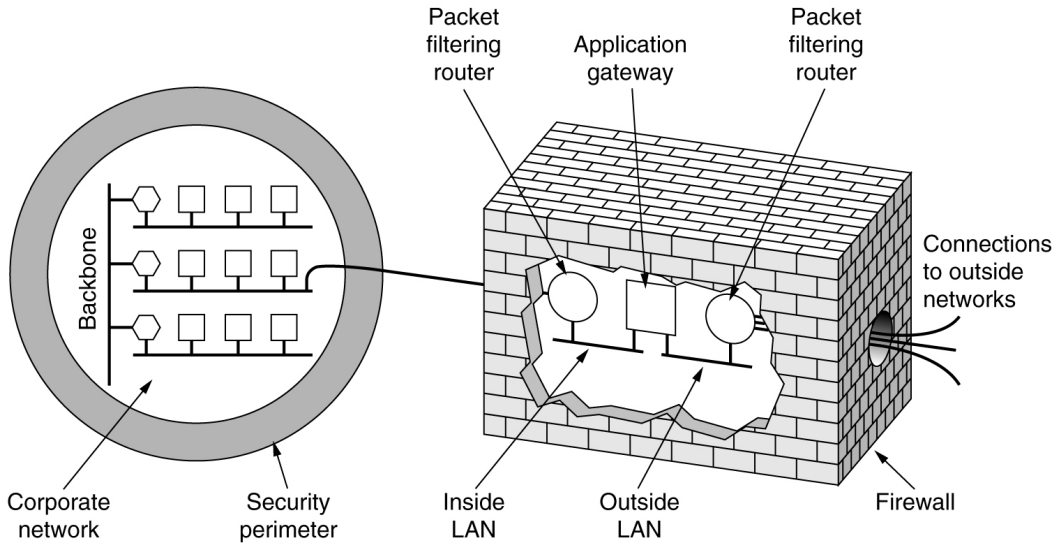
Autentificación

Kerberos



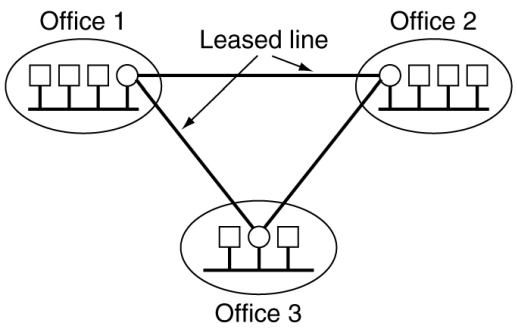
Comunicaciones seguras

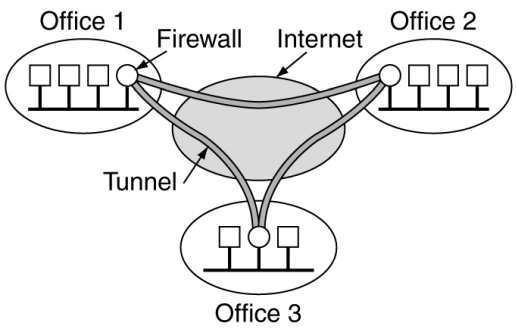
Cortafuegos



Comunicaciones seguras

Redes privadas virtuales

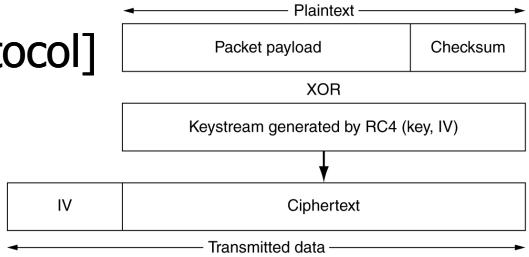




Comunicaciones seguras

Seguridad en redes inalámbricas 802.11

- **WEP** [Wireless Encryption Protocol]
  Inseguro: NO UTILIZAR.

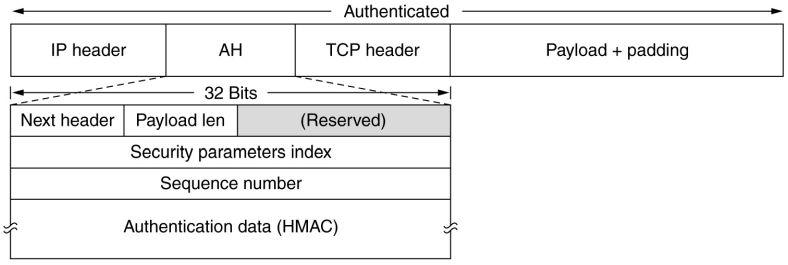


- **WPA** [Wi-Fi Protected Access]
  - Personal Mode = PSK [Pre-Shared Key]:
    Clave compartida (RC4).
    Modo menos seguro, sin servidor de autentificación.
  - TKIP [*Temporal Key Integrity Protocol*], 2002.
    Protocolo de Integridad de Clave Temporal: Contador de secuencia (para prevenir ataques por repetición) y comprobación de integridad [MICHAEL].
  - CCMP [Counter Mode with Cipher Block Chaining Message Authentication Code Protocol] @ WPA2, 2004

Comunicaciones seguras

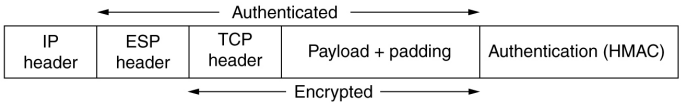
El protocolo IPSec (security extensions for IPv4/v6)

- Cabecera de autentificación

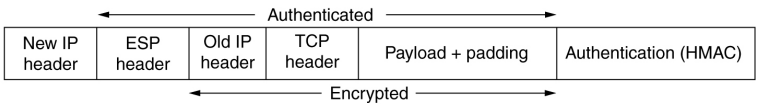


- ESP: Encapsulating Security Payload

Modo de transporte



Modo túnel



- Algoritmo de intercambio de claves

Comunicaciones seguras

SSL [Secure Sockets Layer]
& TLS [Transport Layer Security]

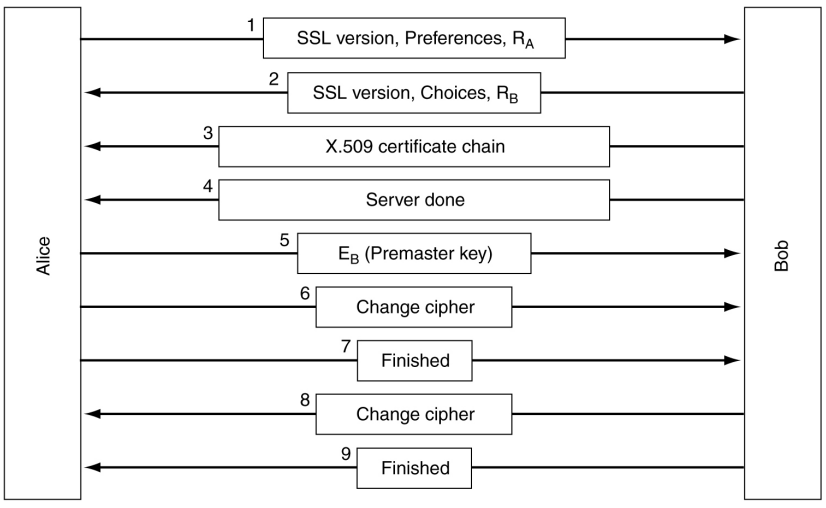
Application (HTTP)
Security (SSL)
Transport (TCP)
Network (IP)
Data link (PPP)
Physical (modem, ADSL, cable TV)

Historia: SSL 3.0 @ Netscape, 1996
TLS 1.0 @ RFC 2246, 1999 ≈ SSL 3.0
TLS 1.1 @ RFC 4346, 2006

Comunicaciones seguras

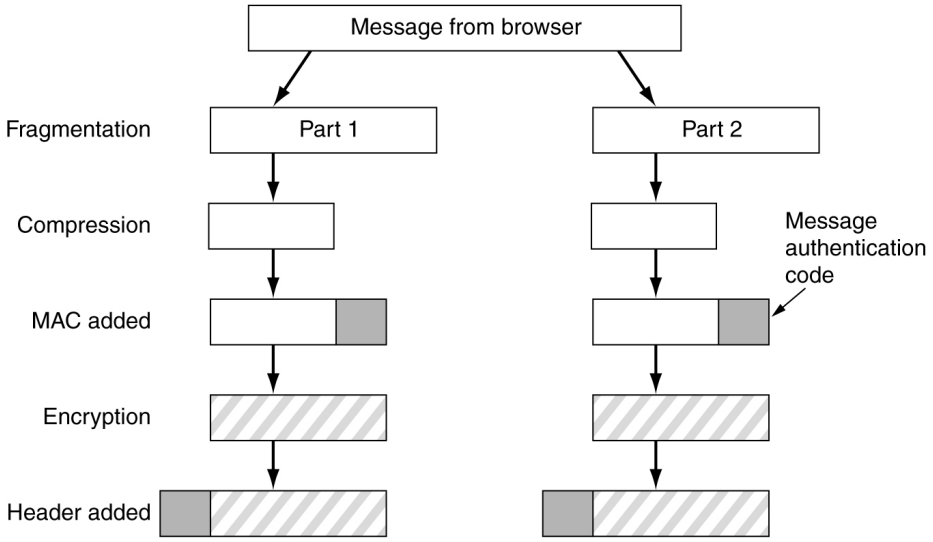
SSL / TLS

Establecimiento de una conexión SSL/TLS

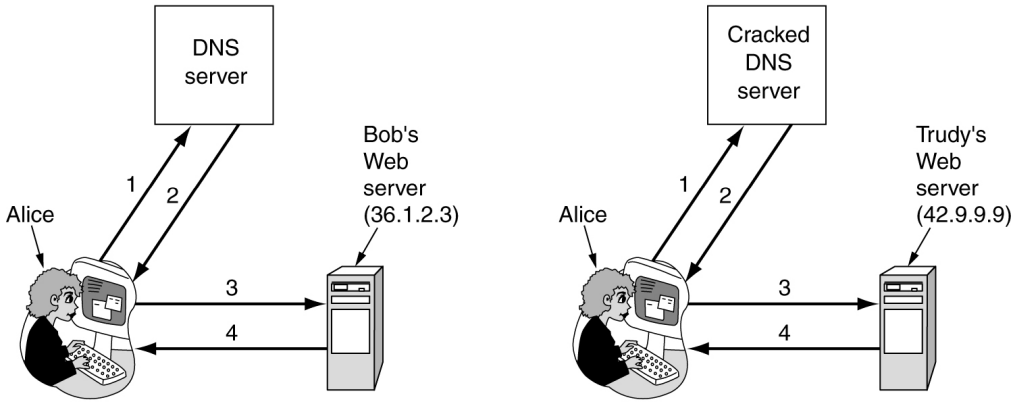


SSL / TLS

Transmisión de datos con SSL/TLS



Servidores de nombres DNS



1. Give me Bob's IP address
2. 36.1.2.3 (Bob's IP address)
3. GET index.html
4. Bob's home page

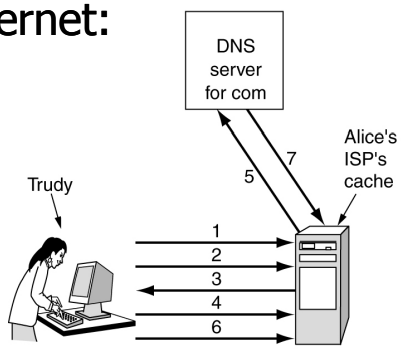
1. Give me Bob's IP address
2. 42.9.9.9 (Trudy's IP address)
3. GET index.html
4. Trudy's fake of Bob's home page

Situación normal vs. Ataque a los servidores DNS

Comunicaciones seguras

Servidores de nombres DNS

Ataque utilizando la infraestructura del proveedor de acceso a Internet:



1. Look up foobar.trudy-the-intruder.com (to force it into the ISP's cache)
2. Look up www.trudy-the-intruder.com (to get the ISP's next sequence number)
3. Request for www.trudy-the-intruder.com (Carrying the ISP's next sequence number, n)
4. Quick like a bunny, look up bob.com (to force the ISP to query the com server in step 5)
5. Legitimate query for bob.com with seq = n+1
6. Trudy's forged answer: Bob is 42.9.9.9, seq = n+1
7. Real answer (rejected, too late)

Self-certifying URL

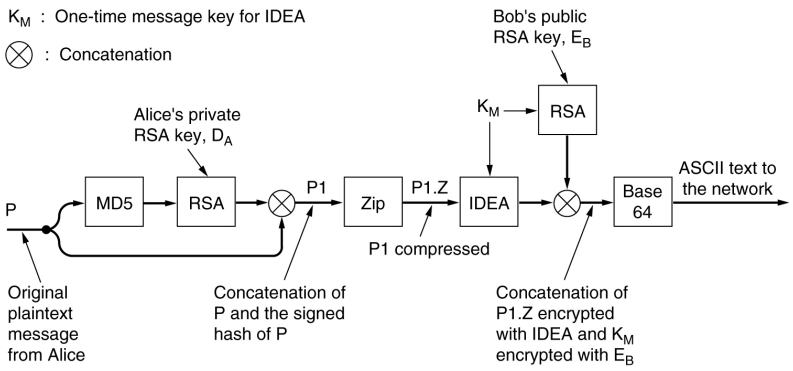
Server | SHA-1 (Server, Server's Public key) | File name

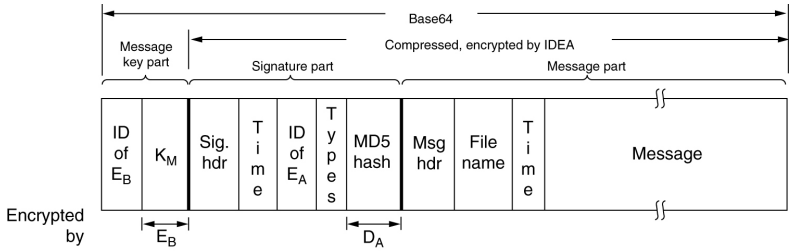
http://www.bob.com:2g5hd8bfjkc7mf6hg8dgany23xds4pe6/photos/bob.jpg

Comunicaciones seguras

Correo electrónico: PGP (Pretty Good Privacy)

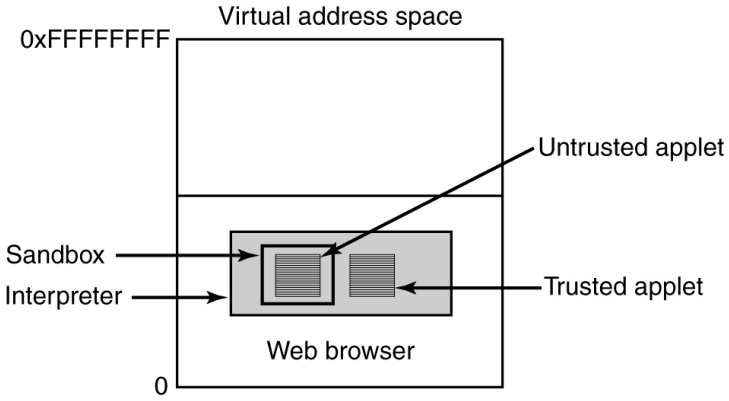
Criptografía, firma digital y compresión





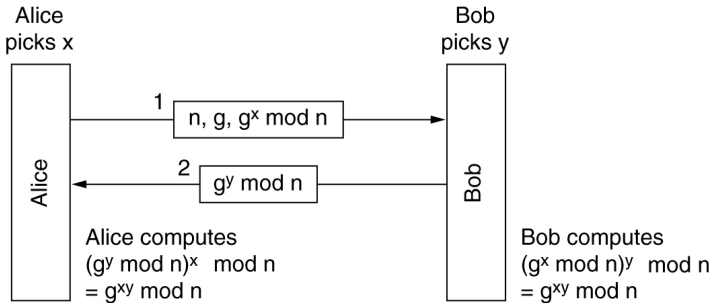
Comunicaciones seguras

Seguridad en los applets Java

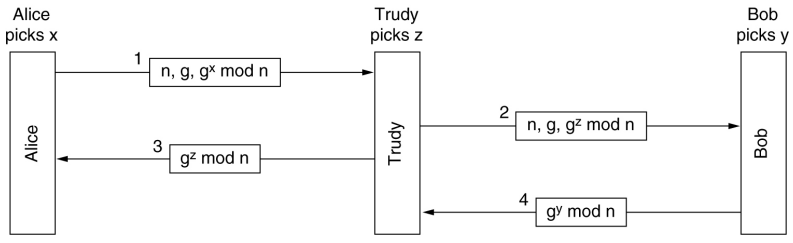


Apéndice
Intercambio de claves

Algoritmo de Diffie-Hellman

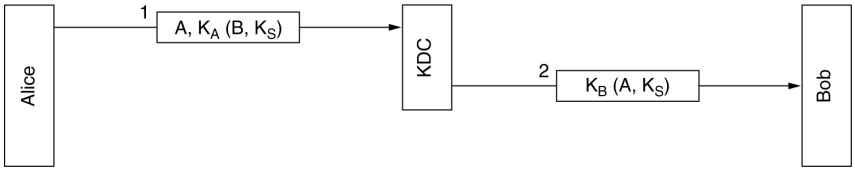


Ataque de un intermediario ("bucket brigade"):

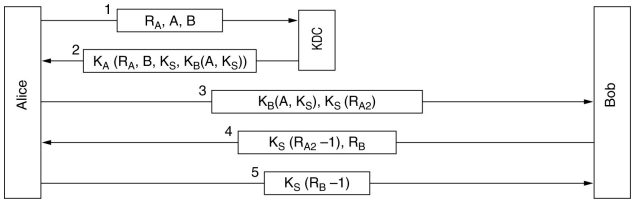


Apéndice
Intercambio de claves

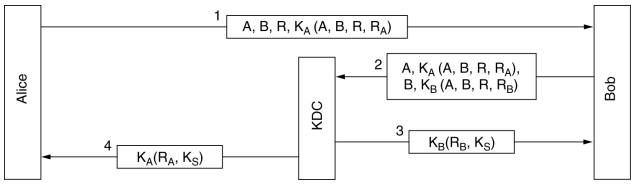
Uso de un centro de distribución de claves (KDC):



- Protocolo de Needham-Schroeder:



- Protocolo de Otway-Rees:



Bibliografía

- Sean Smith & John Marchesini: **The Craft of System Security**. Addison-Wesley Professional, 2007, ISBN 0-321-43483-8.
- John E. Canavan: **Fundamentals of network security**. Artech House, 2001. ISBN 1-58053-176-8.
- Amparo Fúster Savater, Dolores de la Guía Martínez, Luis Hernández Encinas, Fausto Montoya Vitini & Jaime Muñoz Masqué: **Técnicas criptográficas de protección de datos**. RA-MA, 1997. ISBN 84-7897-288-9.
- Jesús E. Díaz Verdejo; Juan Manuel López Soler & Pedro García Teodoro: **Transmisión de datos y redes de computadores**. Prentice-Hall, 2003. ISBN 84-205-3919-8.
- William Stallings: **Comunicaciones y redes de computadores**. Prentice-Hall, 2004 [7ª edición]. ISBN 84-205-4110-9.
- Andrew S. Tanenbaum: **Redes de computadoras**. Prentice-Hall, 2003 [4ª edición]. ISBN 970-260-162-2.