UNIVERSIDAD PONTIFICIA ICAI ICADE COMILLAS MADRID

Seguridad Informática

Capítulo 04: Criptografía simétrica

Titulación: Ingeniero en Informática.
Curso 5º - Cuatrimestral (2007-2008)

Javier Jarauta Sánchez
Rafael Palacios Hielscher
José María Sierra

Tema 04: Criptografía simétrica

- Introducción y conceptos básicos
- Historia de la criptografía
- Criptosistemas
- Algoritmos y claves
- Criptografía de clave secreta (simétrica)
- Tipos de cifrado: Bloque y flujo
- Algoritmos simétricos: DES, 3DES, IDEA, AES, CAST, BLOWFISH, RC2, RC5, RC4
- Aplicaciones: SSL, IPSec
- Situación actual y futuro de la criptografía

Conceptos Básicos

Modelo ISO 7498/2 Riesgos-Servicios-Mecanismos

Riesgo	Solución	Servicio
¿Quién tiene acceso a …?	Tarjeta de identidad	Control de acceso
¿Cómo puedo garantizar que soy quien digo ser?	Fotos en carnets identidad	Autenticación
¿Cómo se garantiza que solo aquellos a los que se ha autorizado tienen acceso a la información?	Entrega en mano. Firma del destinatario a la recepción	Confidencialidad
¿Cómo puedo saber que la información no ha sido manipulada?	Sobres y paquetes sellados	Integridad
¿Cómo me aseguro que las partes que intervienen en una transacción no nieguen haberlo hecho?	Testigos, notarios, correos certificados	No repudio

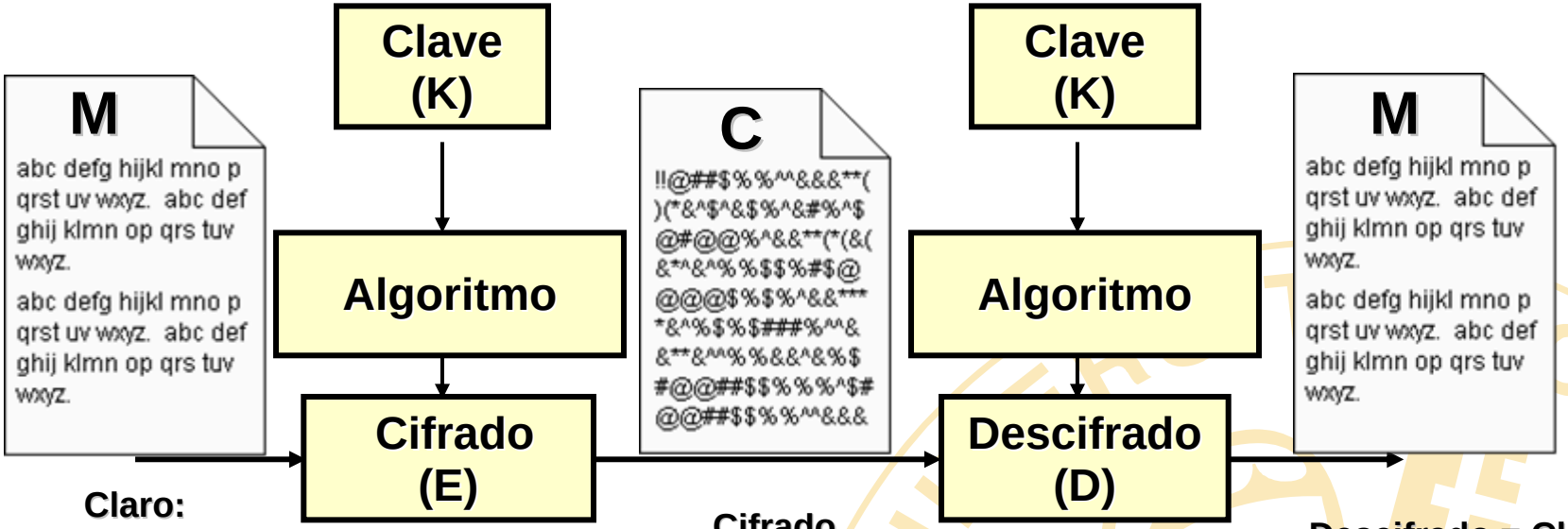
Introducción y conceptos básicos

- ISO 7498/2: Riesgos-Servicios-Mecanismos
- Estados y vulnerabilidad de la información:
  - Mientras se Procesa, Transmite, Almacena
- Criptología: Criptografía y Criptoanálisis
  - El arte y ciencia de mantener mensajes seguros
  - El arte y ciencia de romper mensajes seguros
- Criptosistema
  - Conjunto de dispositivos de cifrado y descifrado, acompañado de un protocolo de transmisión de claves
- Algoritmos criptográficos
  - La función matemática del proceso de cifrado y descifrado, junto con la interrelación con las claves
- Claves
  - Parámetros que inicializan y personalizan los algoritmos

Definiciones

- Servicios de seguridad básicos:
  - **Autenticación**: Asegurar que el origen de la información es quien dice ser
  - **Confidencialidad**: Impedir que la información sea vista por quien no debe
  - **Integridad**: Asegurar que la información no se modifica cuando se transmite o almacena
  - **No repudio**: Impedir que alguien niegue haber realizado una transacción cuando efectivamente lo ha hecho

Criptosistema o Sistema Criptográfico



Claro:

Texto
Voz
Datos

$E_K(M) = C$

Cifrado
Criptograma:

Texto
Voz
Datos

$D_K(C) = M$

Descifrado = Claro:

Texto
Voz
Datos

----------Canal Seguro----------

$E_{K1}(M) = C$

$D_{K2}(C) = M$

$D_{K2}(E_{K1}(M)) = M$

$D_K(E_K(M)) = M$

Criptoanálisis: Tipos de ataques

Punto de partida: Se conoce el Algoritmo

Principal objetivo: Obtener la Clave

TIPOS DE ATAQUES

1.Por texto cifrado

2. Por texto claro conocido

3. Por texto claro seleccionado

4. Por texto claro seleccionado adaptativo

Si el algoritmo es fuerte

! ATAQUE POR FUERZA BRUTA ¡

Historia: Criptografía Clásica

Historia - Métodos Clásicos

- Ocultación
  - Ocultar mensajes dentro de otros
- Sustitución
  - Cada carácter del texto claro se sustituye por otro en el texto cifrado, según reglas precisas que varían según el método
  - Para descifrar se vuelve a sustituir
  - Cuatro tipos: Monoalfabética, Polialfabética, Homofónica, Poligrámica
- Transposición
  - Los caracteres no cambian su significado, sino que alteran sus posiciones respectivas del texto en claro, según patrones que difieren según el método.
  - P.ej. Poner texto horizontal en vertical
  - Requiere mucha memoria.

Historia de la criptografía

- Métodos de ocultación
  - Steganografía: Ocultación de mensajes en otros mensajes (tinta invisible, marcas de agua, sustitución de bits menos significativos en imágenes...)

- Métodos antiguos
  - La escítala lacedemonia: Método espartano de transposición (Siglo V a. de C.)

Escítala lacedemonia

Texto Claro: LA_ESCITALA_FUE_LA_PRIMERA

Algoritmo: 3 filas x 8 columnas

L	E	I	L	F	_	P	M	A
A	S	T	A	U	L	R	E	_
_	C	A	_	E	A	I	R	_

Texto Cifrado: LEILF_PMAASTAULRE__CA_EAIR_

Historia - Sistemas Clásicos

- Sustitución monoalfabética
  - Siglo I a. de C. Cifrado de Cesar
- Sustitución homofónica
  - 1401. Duque de Mantua
- Sustitución polialfabética
  - 1568. Inventado por León Battista
  - 1586. Cifrado de Vignère
- Sustitución poligráfica: Cifra varias letras juntas
  - 1854 Playfair cipher (I Guerra Mundial)

Historia - Sistemas Clásicos

Cifrado de Cesar

Texto Claro	V	I	N	I		V	I	D	I		V	I	N	C	I		C	A	E	S	A	R		D	I	X	I	T
Clave	D	D	D	D		D	D	D	D		D	D	D	D	D		D	D	D	D	D	D		D	D	D	D	D
Tx Cifrado	Y	L	P	L		Y	L	G	L		Y	L	P	F	L		F	D	H	V	D	U		G	L	A	L	W

Método: Sustitución biunívoca de una letra
Algoritmo: Desplazar el alfabeto n posiciones (n=3)
Clave: D
Variante: Utilizar diferentes claves (n= 5, 20,...)
Variante: Utilizar permutaciones (26! =4.03 10^{26})

Sustitución homofónica

Método: Sustitución simple, pero un carácter claro puede dar lugar a varios cifrados
Algoritmo: A podría corresponder a D, G o Q
Clave: n = 3, 6, 17

Historia - Sistemas Clásicos

Sustitución Polialfabética - Cifrado de Vignère

Texto Claro	P	A	R	I	S		B	I	E	N		V	A	L	E		U	N	A		M	I	S	A
Clave	F	R	A	N	C		I	A	F	R		A	N	C	I		A	F	R		A	N	C	I
Tx Cifrado	U	R	R	U	U		J	I	J	E		V	N	N	M		U	R	R		M	U	U	I

Método: Múltiples sustituciones simples
Algoritmo: Cada letra se sustituye por otra según la clave
Clave: FRANCIA
Periódicos Longitud L= Nº de letras de la clave (7)
Seguridad: Mas cuanto mayor es la clave

Sustitución poligráfica

Método: Cifra varias letras juntas, normalmente 2
Algoritmo: Matriz de 5 x 5 sin repetir letras
Clave: palabra inicial

Cifrado de Vignère (mod 27)

Texto Claro

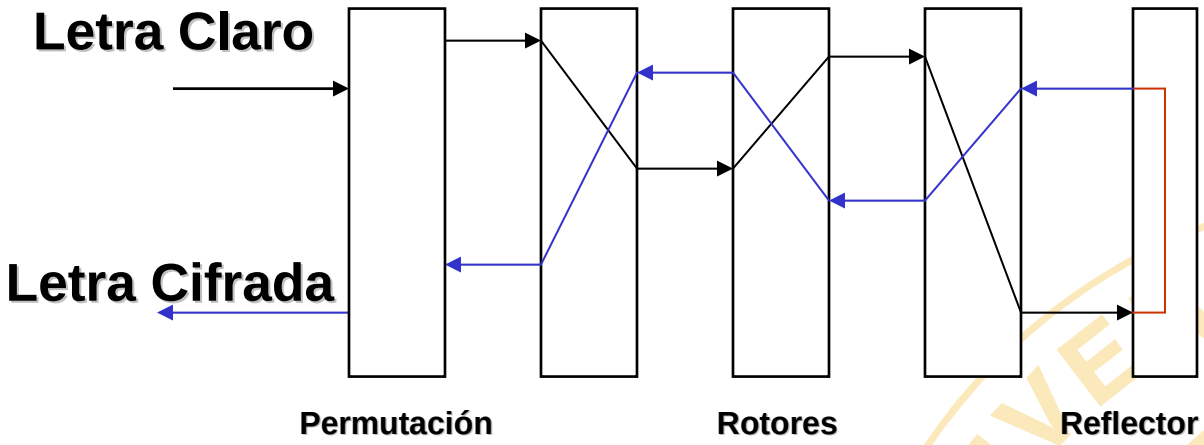
Clave

	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7
1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
3	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
4	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
5	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
6	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
7	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
8	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
9	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
0	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
1	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
2	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
3	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
4	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
5	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
6	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ
7	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O
8	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P
9	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q
0	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R
1	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S
2	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T
3	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U
4	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V
5	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W
6	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X
7	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y

Historia - Sistemas Clásicos

- One-Time Pad: Incondicianalmente seguro
  - 1917. Cifrado de Vernam
  - Es Vignère con longitud clave k=longitud mensaje m)
- Transposición: (confusión y difusión)
  - 1949 Shannon demostró el secreto perfecto
- La máquina Hagelin (USA)
  - 6 rotores de 26, 25, 23, 21, 19 y 17 pins
  - Vignère de periodo 101.405.850
- La máquina Enigma. (Alemania-Japón)
  - 1923. Scherbius. Electromecánica
  - 3 rotores y un reflector

Enigma



Utilizada por Alemanes en II Guerra Mundial

Clave: - Configuración de rotores

- Posición inicial de rotores

- Permutación inicial

Descifrada por Polacos

Historia: Criptografía Moderna

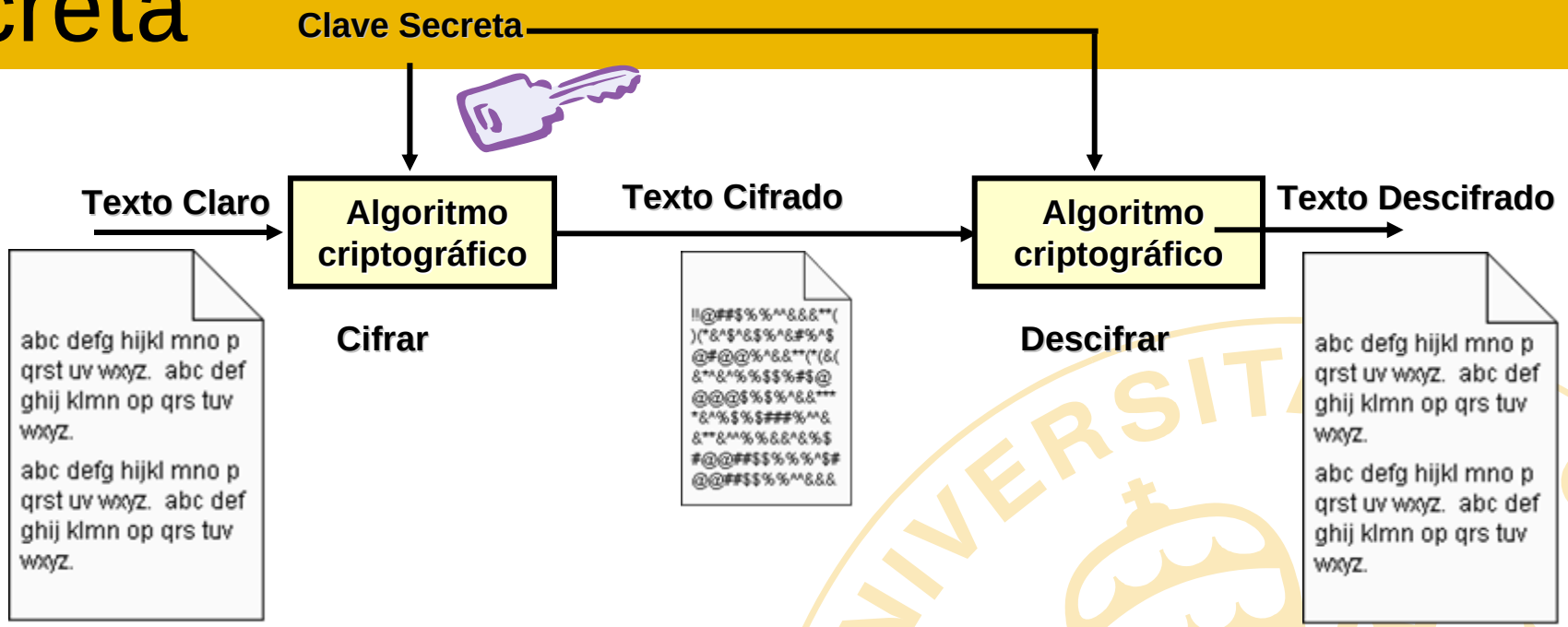
Historia de la criptografía

- Data Encryption Standard (DES)
  - 1970. NBS
  - 1974. Lucifer IBM (clave de128 bits)
  - 1975. DEA IBM (Clave de 56 bits)
  - 1976. DES Estandar NIST para EEUU
- International Data Encryption Alg (IDEA)
  - 1991. Eurocrypt. Lai, Massey y Murphy
- Advanced Encryption Standard (AES)
  - Oct 2000. Rijndael seleccionado por NIST

Tipos de algoritmos criptográficos

- Simétricos. Clave Secreta
  - Utiliza la misma clave para cifrar y descifrar
  - La seguridad está en la clave no en el algoritmo
  - Las claves hay que distribuirlas en secreto
  - Si una clave está comprometida, puede descifrarse todo el tráfico con la misma
  - Aumento del número de claves: n(n-1)/2 para n usuarios
  - Permiten altas velocidades de cifrado
  - Tipos de Algoritmos
    - Flujo (o serie): operaciones con OR-Exclusive
    - Bloque: Modos ECB, CBC

Algoritmos Simétricos o de Clave Secreta



- Utiliza La misma clave para cifrar y descifrar
- La segurida se basa en mantener secreta la clave, no el algoritmo.
- Se necesita compartir las claves entre transmisor-receptor.
- Fortaleza: Velocidad de cifrado
- Debilidades: Gestión de claves
- Tipos: Algoritmos de serie y de bloque
- Ejemplos: DES, 3DES, RC4, CAST, IDEA, AES.

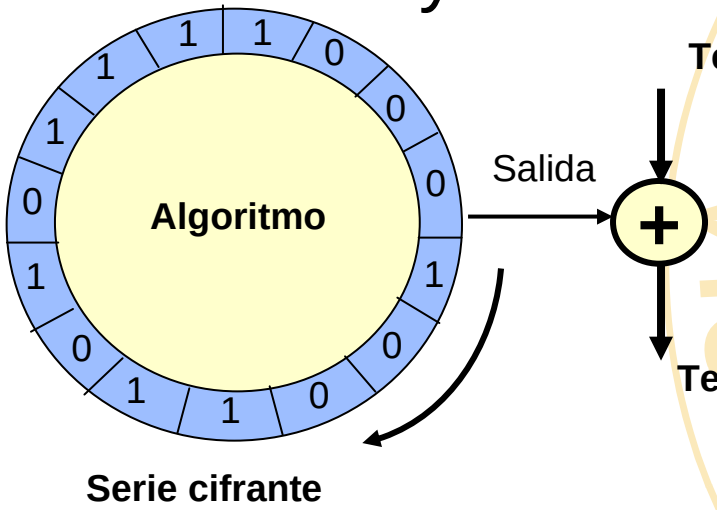
Criptografía de Clave Secreta (Simétrica)

Criptografía de clave secreta

- Tipos de algoritmos simétricos
  - De serie cifrante (flujo)
  - De bloque
- Tipo de sincronización
  - Auto sincronizable
- ¿Es mejor dar a conocer el algoritmo o mantenerlo secreto?
  - Entornos militares y estratégicos: secreto
    - Ej. OTAN. Ej. A5 de GSM
  - Entornos civiles: conocido
    - Ej. DES. Ej. AES

Algoritmos de serie cifrante

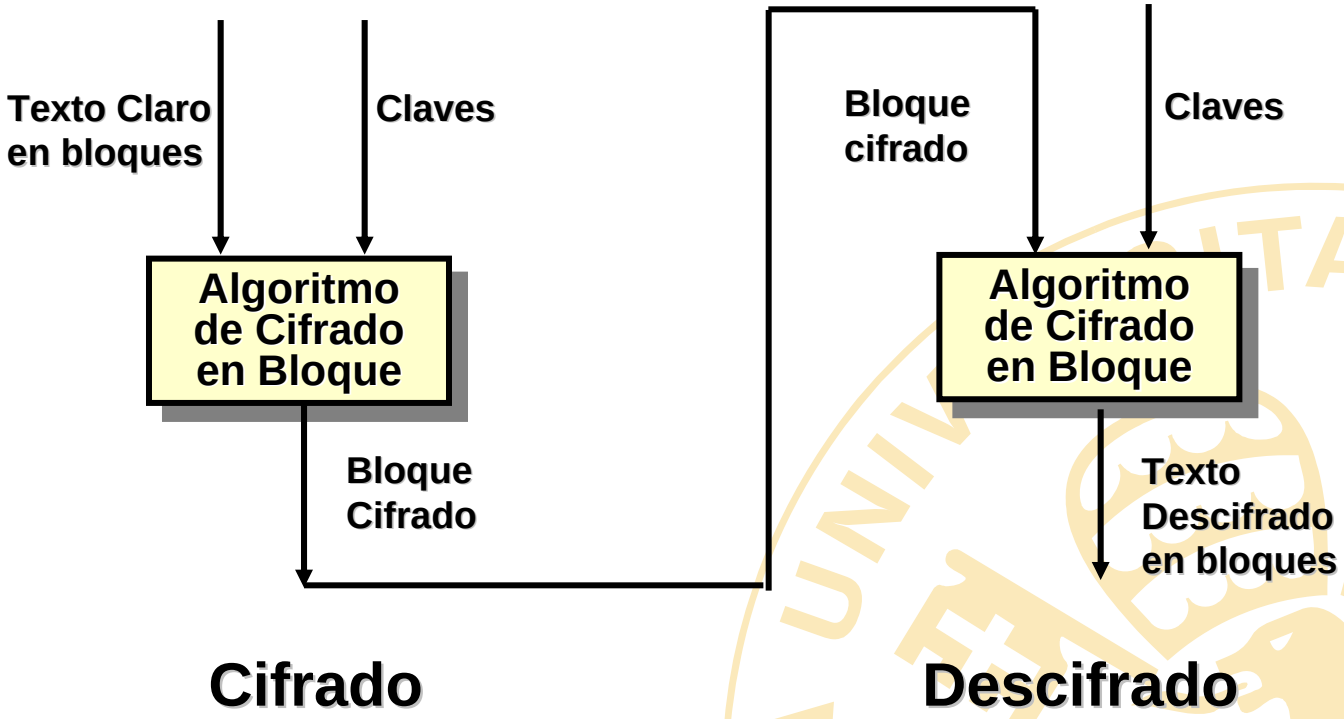
- El texto claro se digitaliza y cada bit se cifra mediante una OR Exclusive con un bit de la serie cifrante
- La serie cifrante ha de ser muy larga, pseudo-aleatoria y no lineal
- Tipos de cifradores de flujo
  - Síncronos y auto-sincronizables



Algoritmos de cifrado en Bloque

- El algoritmo de cifrado transforma x bits del texto claro en x bits del texto cifrado.
- Cada bit del texto claro tiene efecto en cada bit del texto cifrado.
- Cada bloque es independiente, no hay influencia entre bloques.
- Bloques de texto claro idénticos, producen bloques de texto cifrado idénticos.
- Un error en el texto cifrado influye solo en su bloque
- Tipos de Algoritmos de Bloque
  - DES Electronic Code Book (ECB)
  - DES Cipher Block Chaining (CBC)

Cifrado en bloque



El algoritmo DES y 3DES

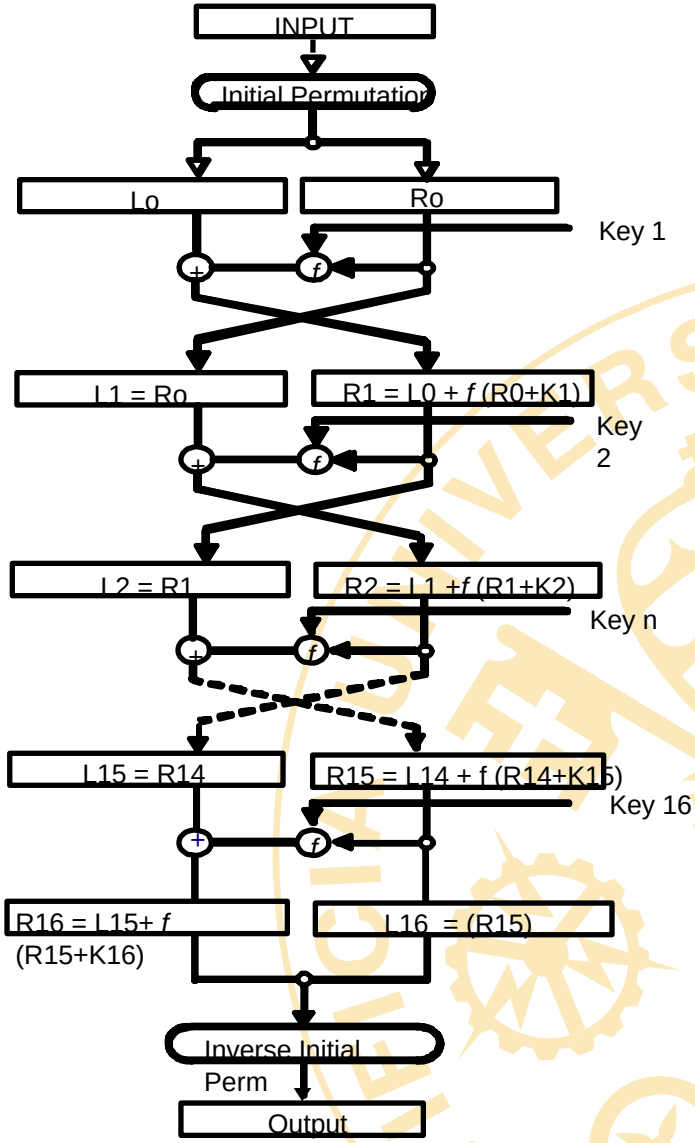
- Está basado en Lucifer de IBM (1975)
- Se aprueba como estándar en 1977 por NIST, ANSI 3.92 (DEA),
- Utiliza claves de 56 bits y 8 de paridad (64 bits)
- Utiliza técnicas básicas de:
  - Transposición, le confiere propiedades de difusión
  - Sustitución, le confiere propiedades de confusión
  - Operaciones lógicas bolenas (Or-exclusivo)
- Es un algoritmo de cifrado en bloques de 64 bits
- Realiza 16 iteraciones para cifrar un bit
- En cada iteración utiliza 48 bits de los 64 de la clave
- Se utiliza en diferentes modos: ECB, CBC
- Mediante los modos CFB y OFB se cifra en serie
- Existía un modo con clave de 40 bits (muy débil), el único exportable de EEUU hasta el año 2000
- La Electronic Frontier Foundation (www.eff.org) construyó un craqueador que lo rompe en 3 días

Algoritmo DES

- Realiza una permutación inicial del bloque según una función derivada de la clave.
- Realiza un conjunto de sustituciones usando 8 S-boxes (matrices de 4 x 16) seguidas de una permutación.
- Divide el bloque de 64-bit permutado en dos partes de 32-bit y expande los 32 bits a 48 bits.
- Cifra la parte derecha con 48 de los 56 bits originales de la clave.
- Repite 16 veces el conjunto completo de funciones, con una clave de cifrado diferente cada vez.
- Realiza una permutación final, que es la inversa de la permutación realizada inicialmente.

1. Permutación inicial
2. Transformación de la clave
3. Permutación de expansión
4. Descripción de la iteración
5. Sustitución en la S-Box
6. Permutación en la P-Box
7. Permutación Final
8. Potencia del DES

DES: Diagrama del proceso



Otros algoritmos simétricos

- **RC2:**
  - Diseñado por Ron Rivest para RSA y no ha sido publicado
  - Cifrado de bloque de 64 bits con claves de longitud variable
  - Tres veces más rápido que DES
- **RC4:**
  - Diseñado en 1987 por Ron Rivest para RSA
  - En septiembre de 1994 alguien puso el código en Internet
  - Cifrado en serie con claves de longitud variable
  - Diez veces más rápido que DES
- **RC5**:
  - Diseñado por Ron Rivest y analizado por RSA Labs.
  - Cifrado de bloque con claves de 40 a 2040 (típico 128)
  - Variable en número de iteraciones, recomendadas 12

Otros algoritmos simétricos

- **CAST**:
  - Diseñado en Canadá por C. Adams y S. Tavares (Entrust)
  - Utiliza claves de 40 a 128 bits (típico 128)
  - Cifrado de bloque, utiliza 6 S-boxes, muy rápido
- **BLOWFISH**:
  - Diseñado por Bruce Schneier
  - Claves de 40 a 448 (típico 128)
  - Es muy sencillo (5k) y optimizado para software actual
- **IDEA**:
  - Diseñado por James Massey
  - Claves de 128 bits. Es dos veces más rápido que el DES.
  - Patentado por Ascom-Tech AG.
  - Muy utilizado en Europa

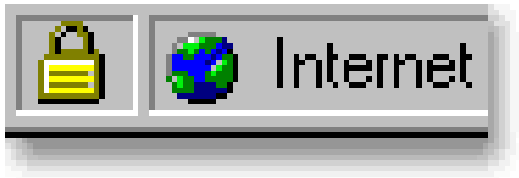
Otros algoritmos simétricos

- **AES**:
  - En Enero 1997 NIST solicitó algoritmos para sustituir al DES
  - En Agosto 1998 se pre-seleccionaron 15 algoritmos
  - En Abril de 1999 se seleccionaron 5 finalistas: MARS, RC6, Rijndael, Serpent y Twofish
  - En Octubre de 2000 se seleccionó Rijndael como AES - FIPS 197
  - Diseñado en Bélgica por Joan Daemen y Vincent Rijmen (Univ Leuven)

  - Algoritmo de cifrado en bloques de 128 bits
  - Puede utilizar diferentes tamaños de clave. 128, 192 y 256
  - Se aceptan implantaciones en software, firmware, hardware o mixtas
  - Para información sensible “no clasificada”

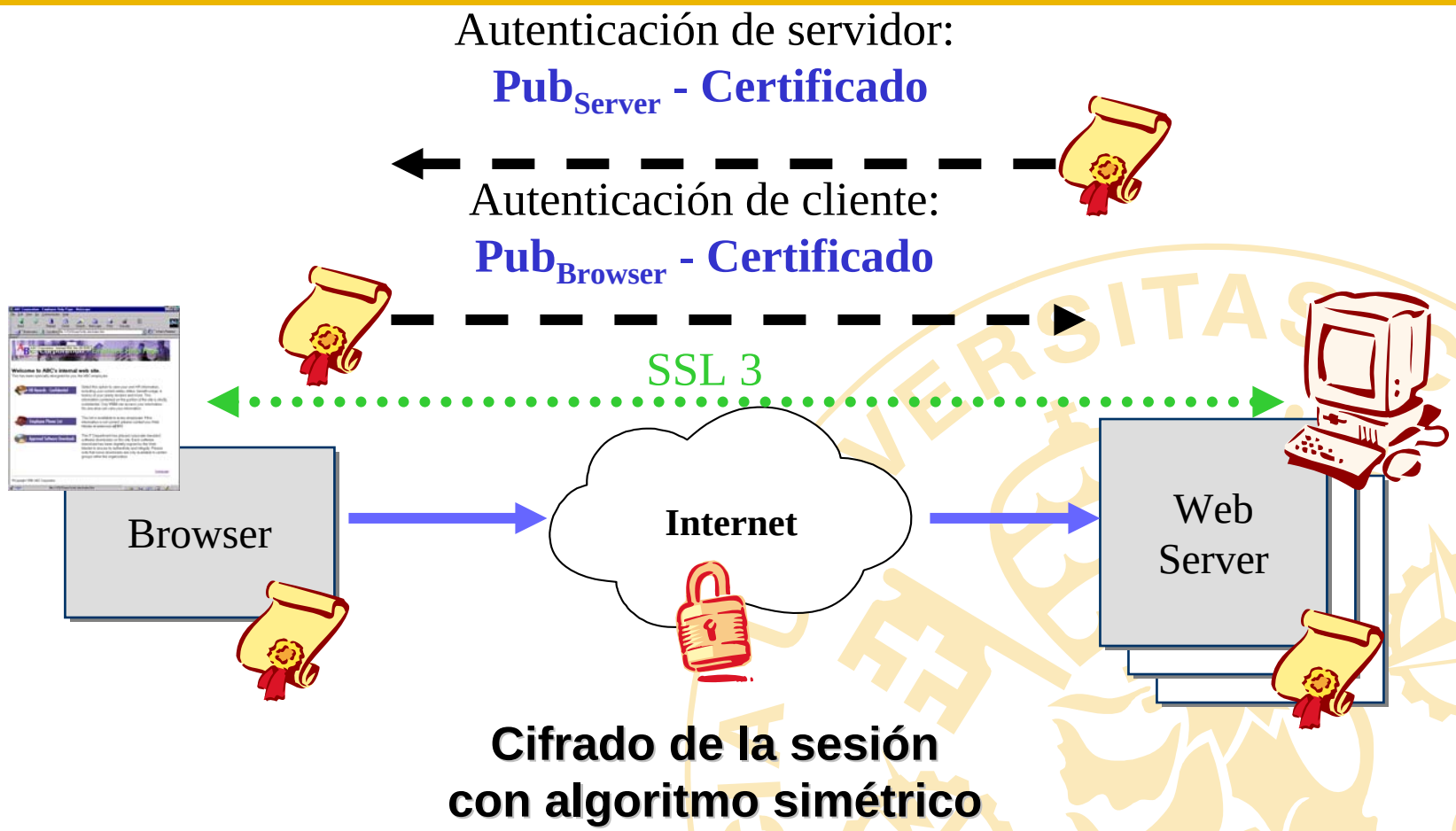
Aplicaciones reales

Aplicación: SSL

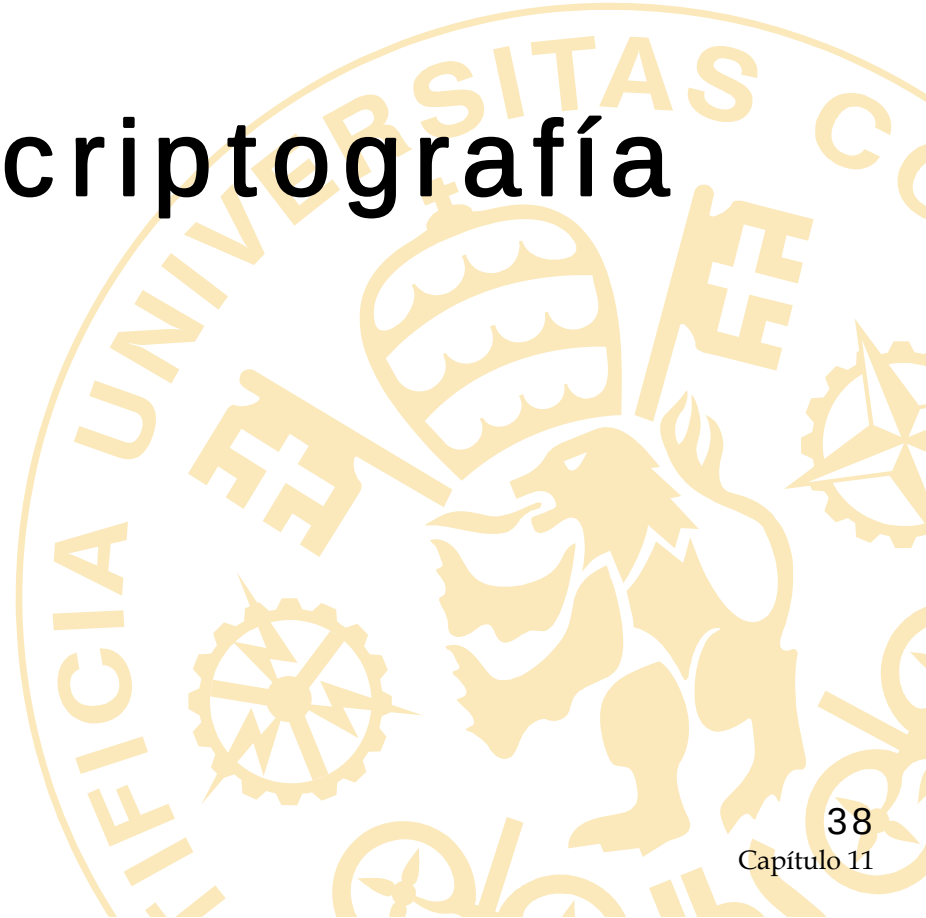


- SSL - Secure Sockets Layer. Estandar de facto para los navegadores
- Actualmente conocido también como TLS Transport Layer Security
- El navegador cliente inicia una sesión https:
- El Web Server envía al navegador su certificado y solicita (si procede) el certificado del cliente
- Se utiliza un algoritmo simétrico para el cifrado de datos una vez establecido el tunel seguro

SSL - Secure Sockets Layer



El futuro de la criptografía



Situación actual y futuro

- Amplia utilización en Internet e Intranet: SSL
- Redes Privadas Virtuales (VPN): IPSec
- Combinación de criptografía simétrica y asimétrica en comunicaciones
- Cifrado de datos en discos duros de PC, tarjetas de PDA, memorias USB…
- Nuevos algoritmos basados en criptografía cuántica