

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

Seguridad en los Sistemas Informáticos

Tema 5: Criptografía

Grado en Ingeniería Informática

Departamento de Ingeniería Informática
Universidad de Cádiz

Curso 2024–2025

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

- 1 Fundamentos
- 2 Tipos de sistemas criptográficos
- 3 Criptografía de clave simétrica
- 4 Criptografía de clave asimétrica
- 5 Algoritmos de huella digital
- 6 Protocolos
- 7 Aplicaciones de la criptografía

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

1 Fundamentos

- Historia y conceptos
- Criptosistemas

2 Tipos de sistemas criptográficos

3 Criptografía de clave simétrica

- Cifrado por sustitución
- Cifrado por transposición
- Cifrado producto
- Algunos modos de operación
- DES
- AES

4 Criptografía de clave asimétrica

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

Definición de la RAE

- La palabra **Criptografía** proviene del griego Cripto que significa oculto y Grafía que significa escritura.
- Su definición es «Arte de escribir con clave secreta o de un modo enigmático».

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

Definición correcta

Rama inicial de las Matemáticas y en la actualidad de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar un mensaje o archivo por medio de un algoritmo, usando una o más claves. Esto da lugar a diferentes tipos de criptosistemas que permiten asegurar cuatro aspectos fundamentales de la seguridad informática:

- confidencialidad,
- integridad,
- disponibilidad,
- no repudio de emisor y receptor.

Otras definiciones

- Criptanálisis** es el conjunto de técnicas empleadas para la ruptura de los códigos criptográficos.
- Criptología** se emplea para agrupar tanto a la Criptografía como al Criptanálisis.
- Esteganografía** ocultación en el interior de una información, aparentemente inocua, otro tipo de información (cifrada o no). Ejemplo: *chaffing and winnowing*.

Breve repaso histórico (I)

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

- En el siglo V antes de J.C. se usaban técnicas de cifrado para proteger a la información: **escítala**.



Fuente: <https://es.wikipedia.org/wiki/Esc%C3%ADtala#/media/Archivo:Skytale.png>

Breve repaso histórico (II)

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

- Los mayores avances se lograron en la Segunda Guerra Mundial: los países en conflicto tenían un gran número de técnicos encargados de romper los mensajes cifrados de los teletipos (máquina ENIGMA).
- Puntos de inflexión:
 - 1948 Estudio de Claude Shannon sobre la Teoría de la Información: «A Mathematical Theory of Communication».
 - 1974 Estándar de cifrado DES.
 - 1976 Estudio de W. Diffie y M. Hellmann sobre la aplicación de funciones de un solo sentido a un modelo de cifrado (cifrado de clave pública): «New directions in Cryptography».

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

1 Fundamentos

- Historia y conceptos
- Criptosistemas

2 Tipos de sistemas criptográficos

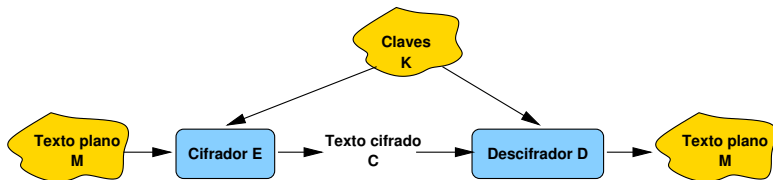
3 Criptografía de clave simétrica

- Cifrado por sustitución
- Cifrado por transposición
- Cifrado producto
- Algunos modos de operación
- DES
- AES

4 Criptografía de clave asimétrica

Notación

Un **criptosistema** se puede definir con una quintupla (M, C, K, E, D) .



$$E(k, M) = E_k(M) = C$$

$$D(k, C) = D_k(C) = M$$

$$D(k, E(k, M)) = D_k(E_k(M)) = M$$

Rendimiento y flexibilidad

- Algoritmo de cifrado/descifrado rápido y fiable.
- Posibilidad de transmitir ficheros por una línea de datos, almacenarlos o transferirlos.
- No debe existir retardo debido al cifrado o descifrado.

Fortaleza

- **La seguridad del sistema deberá residir solamente en el secreto de una clave y no de las funciones de cifrado.**
- La fortaleza del sistema se entenderá como la imposibilidad computacional (tiempo de cálculo en años que excede cualquier valor razonable) de romper el cifrado o encontrar la clave secreta a partir de otros datos de carácter público.

Generales

- 1 Debe ser imposible recuperar del criptograma el texto inicial o la clave.
- 2 Las claves deben ser fáciles de recordar y de modificar.
- 3 El criptosistema debe ser comunicable con los medios de transmisión habituales.
- 4 La complejidad del proceso de descifrado debe corresponderse con el beneficio obtenido.

Seguridad por diseño

- Todo criptosistema se divide en una parte pública (algoritmos de cifrado y descifrado) y otra privada (claves).
- El criptosistema debe ser seguro suponiendo que el enemigo conoce la parte pública.

Concepto

Aquel que el texto cifrado no proporciona ninguna información sobre el texto original, incluso cuando el criptoanalista conozca:

- El texto cifrado.
- El algoritmo criptográfico empleado.
- El espacio de claves.
- La forma en que una clave determina la transformación del texto original.

Condición necesaria y suficiente

$$p(C, M, K) = p(C, M', K')$$

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

Probable

Cuando aún no se ha demostrado la seguridad del mismo, pero que de momento no ha sido roto.

Práctica o rompible

El criptosistema se considera seguro contra aquellos enemigos que tengan insuficiente tiempo y/o recursos.

Teórica o irrompible

El criptosistema se considera seguro contra cualquier enemigo que tenga recursos y tiempo ilimitados.

Condiciones

- Mensaje con 25 caracteres formado por letras mayúsculas.
- Existen 26^{25} (aproximadamente 10^{35}) combinaciones.
- Realizando 10^{10} operaciones/segundo, requiere 10^{11} años.
- ¿Es rompible? Cuidado con el criptoanalista y el crecimiento de la velocidad de los ordenadores.

Evento	Probabilidad
Caernos un rayo	2^{33}
Ganar la primitiva	2^{23}
Ganar la primitiva y caernos un rayo	2^{56}

Cuadro: Ejemplos de probabilidades

Condiciones

- Mensaje con 25 caracteres formado por letras mayúsculas.
- Existen 26^{25} (aproximadamente 10^{35}) combinaciones.
- Realizando 10^{10} operaciones/segundo, requiere 10^{11} años.
- ¿Es rompible? Cuidado con el criptoanalista y el crecimiento de la velocidad de los ordenadores.

Evento	Probabilidad
Caernos un rayo	2^{33}
Ganar la primitiva	2^{23}
Ganar la primitiva y caernos un rayo	2^{56}

Cuadro: Ejemplos de probabilidades

Tipos de criptosistemas

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

Simétricos (o de clave privada)

- Emplean una única clave, utilizada y compartida en secreto por emisor y receptor.
- Pueden usar cifrado *de bloque* (dentro de un *modo de operación*) o *de flujo*.

Asimétricos (o de clave pública)

- Cada usuario genera un par de claves, la *pública* (conocida por todos) y la *privada* (conocida por sólo él mismo).
- Usa «funciones trampa» fáciles de aplicar en una dirección, pero muy difíciles de invertir sin la clave de descifrado. Ejemplo: factorización, logaritmo, etc.
- Puede requerir división en bloques si el texto es largo (sólo ciertos modos de operación sirven).

Cifrado simétrico: distribución de claves

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

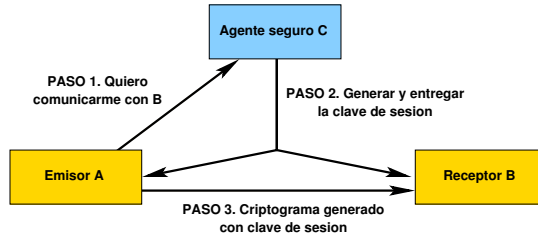
Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía



Tipos de claves

De sesión Sólo se usa durante la conexión que se establece entre dos sistemas a comunicar. Cada clave sólo se usa una vez.

Permanente Cada agente tiene una y la comparte con el servidor para distribuir las claves de sesión.

Cifrado asimétrico: confidencialidad

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

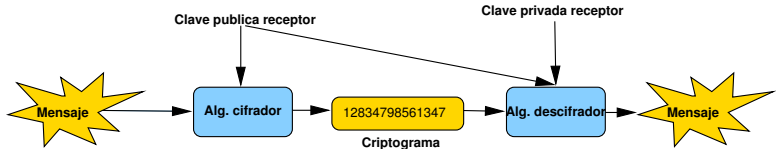
Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía



$$D_{K_{priv}}(E_{K_{pub}}(M)) = M$$

K_{priv} y K_{pub} pertenecen al receptor.

Cifrado asimétrico: autenticidad

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

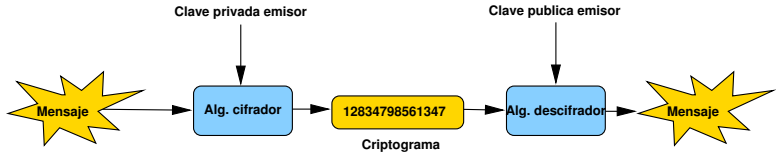
Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía



$$D_{K_{pub}}(E_{K_{priv}}(M)) = M$$

K_{priv} y K_{pub} pertenecen al emisor.

Cifrado asimétrico: ambos

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

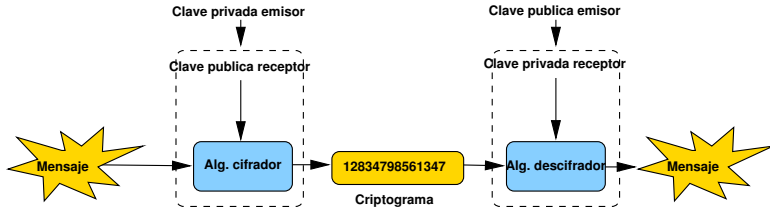
Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía



Ventajas

- Simetría: la clave sirve para cifrar y para descifrar.
- Existen implementaciones hardware.
- Son los métodos a emplear cuando no existe un canal de comunicación (copias de seguridad).
- Asegura la confidencialidad de la información.

Inconvenientes

- La autenticación se basa en la confianza mutua entre receptor y emisor.
- Gestión de claves: para N personas se necesitan $N \times (N - 1)/2$ claves. Cada persona tiene que recordar $N - 1$ claves.
- Distribución de las claves.

Ventajas

- Asegura la confidencialidad de la información.
- No necesita un canal seguro para distribuir la clave pública.
- Gestión de claves sencilla: para N personas, se requieren $2N$ claves, donde cada usuario sólo tiene que recordar una única clave.
- Garantiza la autenticación (firma digital).

Inconvenientes

- 10000 veces más lento que los simétricos.
- Requieren de un canal de comunicación.

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

Características

Se cifra carácter a carácter según un flujo continuo de claves.

Ventajas

- Rapidez.
- Baja propagación de errores.

Inconvenientes

- Susceptibilidad de inserción y modificación del mensaje.

Esquema de funcionamiento

Un flujo de claves cifra un flujo de caracteres

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

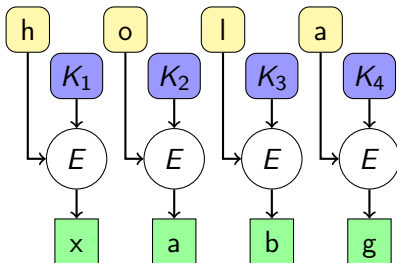
Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía



Normalmente, F es XOR, y el flujo de claves se genera a partir de una clave proporcionada por el usuario. En RC4, por ejemplo, la clave determina una permutación del vector usado para cifrar.

Cifrado Vernam (no periódico, polialfabético)

Antepasado de los cifrados de flujo actuales

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

Características

- Diseñado por Gilbert Vernam, presenta secreto perfecto.
- El cifrado/descifrado consiste en realizar la función XOR.
- La clave permitía obtener una secuencia binaria y aleatoria S que se almacenaba en una cinta que alimentaba un teletipo. Esa clave era igual de larga que el mensaje y sólo se usaba una vez (*one time pads*).

Ejemplo de cifrado Vernam

Por simplificar, usamos suma modular

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

Ejemplo

M = HOY ES FIESTA

Secuencia aleatoria = 76 16 82 48 44 3 14 54 48 13 42

M	h	o	y	e	s	f	i	e	s	t	a
M	7	15	25	4	19	5	8	4	19	20	0
+S	76	16	82	48	44	3	14	54	48	13	42
=Suma	83	31	107	52	63	8	22	58	67	33	42
=mod 27	2	4	26	25	9	8	22	4	13	6	15
C	c	e	z	y	j	i	v	e	n	g	o

Características

- Operan sobre cadenas de un tamaño fijo (bloques).
- Cada bloque se cifra con la misma clave.
- Se integran en un *modo de operación* (ver NIST SP 800-38A).

Ventajas

Inmunidad frente a la inserción de símbolos.

Inconvenientes

- Baja velocidad.
- Facilidad de propagación de errores.
- Problemas en mensajes con estructura muy regular.

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

1 Fundamentos

2 Tipos de sistemas criptográficos

3 Criptografía de clave simétrica

- Sistemas clásicos
 - Cifrado por sustitución
 - Cifrado por transposición
 - Cifrado producto
 - Algunos modos de operación
- Sistemas modernos
 - DES
 - AES

4 Criptografía de clave asimétrica

Sustitución: descripción y tipos

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

Definición

Cambiar un carácter por otro según una regla.

Objetivo: generar confusión

Mezclar los elementos del mensaje, aumentando la complejidad de la dependencia funcional entre clave y criptograma. Es decir, el criptoanalista no debe ser capaz de predecir qué ocurrirá al criptograma cambiando un carácter en el texto en claro.

Tipos

Simple Según permutación del alfabeto de entrada.

Homofónica Aleatorio entre varias posibilidades.

Polialfabética Usa varios alfabetos.

Poligrámica Sustituye varios caracteres de una vez.

Definición

Sustitución simple que usa un alfabeto rotado p posiciones hacia delante.

$$\begin{aligned}\text{Cifrado} &\rightarrow c_i = E(m_i) = m_i + p \pmod{A} \\ \text{Descifrado} &\rightarrow m_i = D(c_i) = c_i - p \pmod{A}\end{aligned}$$

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
ñ	o	p	q	r	s	t	u	v	w	x	y	z	
14	15	16	17	18	19	20	21	22	23	24	25	26	

$p = 3$ (**Método de César**)

M = EL PATIO DE MI CASA ES PARTICULAR

Definición

Sustitución simple que usa un alfabeto rotado p posiciones hacia delante.

$$\begin{aligned}\text{Cifrado} &\rightarrow c_i = E(m_i) = m_i + p \pmod{A} \\ \text{Descifrado} &\rightarrow m_i = D(c_i) = c_i - p \pmod{A}\end{aligned}$$

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
ñ	o	p	q	r	s	t	u	v	w	x	y	z	
14	15	16	17	18	19	20	21	22	23	24	25	26	

$p = 3$ (**Método de César**)

M = EL PATIO DE MI CASA ES PARTICULAR

C = HÑ SDWLR GH OL FDVD HV SDUWLFXÑDU

Ventajas

- Sencillo.
- Rápido.
- Clave fácil de recordar (número o letra).

Desventajas

- Fácil de descifrar:
 - Letra con más apariciones.
 - Grupos de letras del lenguaje (*Sherlock Holmes*, «The Adventure of the Dancing Men»).
 - Espacio de claves reducido (sólo 27 posibilidades en español).

Enunciado

Descifrar el siguiente criptograma:

C = LZAH LZ BTH WYBLIH XBL KLILYOH ZLY CHROKH

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
ñ	o	p	q	r	s	t	u	v	w	x	y	z	
14	15	16	17	18	19	20	21	22	23	24	25	26	

Enunciado

Descifrar el siguiente criptograma:

C = LZAH LZ BTH WYBLIH XBL KLILYOH ZLY CHROKH

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
ñ	o	p	q	r	s	t	u	v	w	x	y	z	
14	15	16	17	18	19	20	21	22	23	24	25	26	

clave = 7

M = ESTA ES UNA PRUEBA QUE DEBERIA SER VALIDA

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

Enunciado

Cifre el siguiente mensaje usando el método ROT5:

M = TU ESFUERZO SERA RECOMPENSADO

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
ñ	o	p	q	r	s	t	u	v	w	x	y	z	
14	15	16	17	18	19	20	21	22	23	24	25	26	

Ejercicio 1: Método de César

Cifre el siguiente mensaje usando el método de César:
M = LAS VACACIONES SE ACERCAN

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13
ñ	o	p	q	r	s	t	u	v	w	x	y	z	
14	15	16	17	18	19	20	21	22	23	24	25	26	

Otras permutaciones para sustituciones simples

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

Usar una palabra clave

Una palabra clave genera el inicio del diccionario, y el resto se completa con las que faltan, en orden.

criptografia → **criptogafbdehjklnmñqsuvwxyz**

Usar un salto entre letras

Se va saltando n posiciones por el alfabeto, y añadiendo las letras por las que se pase.

3 → **adgjmoruxbehknpsvycfijñqtzw**

Características

- Tratan de «aplanar» la distribución de probabilidad.
- A cada carácter pueden corresponderle varios caracteres, según su frecuencia en el lenguaje.

Ejemplo

- Alfabeto de entrada: a (40 %) y b (60 %)
- Alfabeto de salida: a, b, c, d y e
- $a \rightarrow \{b, c\}$
- $b \rightarrow \{a, d, e\}$
- Entonces: abba \rightarrow cdab

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

Ventajas

- Aplana la distribución de probabilidad.

Desventajas

- Complicado de definir.
- Requiere usar un alfabeto de salida mayor.
- Sigue siendo vulnerable a análisis de frecuencias (aunque requiere más mensajes).

Características

- Generalización del método César.
- La clave consiste en **N** claves de cifrado por sustitución simple, que se usan consecutivamente y de manera cíclica para todo el mensaje.

Ejemplo

CLAVE = prueba = 16 18 21 4 1 0

M	h	o	y	e	s	f	i	e	s	t	a
N	7	15	25	4	19	5	8	4	19	20	0
+K (periódico)	16	18	21	4	1	0	16	18	21	4	1
=Suma	23	33	46	8	20	5	24	22	40	24	1
=mod 27	23	6	19	8	20	5	24	22	13	24	1
criptograma	w	g	s	i	t	f	x	v	n	x	b

Características

- Se cifra por digramas (bloques de dos caracteres).
- Si el texto en claro tiene un número impar de elementos se rellena con una letra establecida para que su longitud sea par.
- Si M1M2 están en la misma fila, C1C2 son los dos caracteres de la derecha.
- Si M1M2 están en la misma columna, C1C2 son los caracteres de abajo.
- Si M1M2 están en filas y columnas distintas, C1C2 son los caracteres de la diagonal, desde la fila de M1.

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

Ejemplo

La clave es CLASE

C	L	A	S	E
B	D	F	G	H
I/J	K	M	N/Ñ	O
P	Q	R	T	U
V	W	X	Y	Z

M = AH OR AD EB ES ER MA SF AC IL. ¿Cuál sería el criptograma?

Ejemplo

La clave es CLASE

C	L	A	S	E
B	D	F	G	H
I/J	K	M	N/Ñ	O
P	Q	R	T	U
V	W	X	Y	Z

M = AH OR AD EB ES ER MA SF AC IL. ¿Cuál sería el
criptograma?

C = EF MU LF CH CE AU RF AG SL KC

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

Definición

- También denominado **permutación**.
- Consiste en reordenar los caracteres del mensaje.

Objetivo: generar difusión

Dispersar las propiedades estadísticas del lenguaje sobre todo el criptograma.

Definición

- Se establece el número de columnas.
- Se escribe el texto en filas. Por ejemplo, con 5 columnas:

c_1	c_2	c_3	c_4	c_5
c_6	c_7	c_8	c_9	c_{10}
c_{11}	c_{12}	...		

- Si el texto no es múltiplo del número de columnas establecidos se completa con otros caracteres.
- El criptograma se obtiene leyendo en columnas. En el ejemplo anterior sería, $C = c_1, c_6, c_{11}, c_2, c_7, \dots$
- A veces se emplea una palabra clave de la misma longitud deseada que indica el orden de establecer las columnas.

Transposición por columnas: ejemplo

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

Ejemplo

- Clave = TORMENTA \rightarrow TORMENA \rightarrow 7 columnas
- M = ATAQUE POSTPUESTO HASTA LAS DOS AM

T	O	R	M	E	N	A
7	5	6	3	2	4	1
A	T	A	Q	U	E	P
O	S	T	P	U	E	S
T	O	H	A	S	T	A
L	A	S	D	O	S	A
M	X	X	X	X	X	X

- Criptograma = PSAAX UUSOX QPADX EETSX TSOAX
ATHSX AOTLM

Definición

- Similar al de columnas, pero se establece el número de filas.
- Se escribe el texto en columnas. Por ejemplo, con 3 filas:

c_1	c_4	...
c_2	c_5	...
c_3	c_6	...

- El criptograma se obtiene leyendo en filas.
- Si el texto no es múltiplo del número de filas establecidos se completa con otros caracteres.
- También se puede emplear una palabra clave de la misma longitud deseada que indica el orden de establecer las filas.
- ¿Qué criptograma se obtiene para el mensaje = ATAQUE POSTPUESTO HASTA LAS DOS AM, con clave = TORMENTA?

Descripción

- Fijado el número de columnas o de filas, según se desee, la transcripción del mensaje a criptograma se realiza siguiendo un patrón geométrico:
 - Diagonales empezando por el extremo superior derecho o izquierdo.
 - Cuadrados desde dentro hacia fuera o viceversa.
 - Espiral desde el centro hacia fuera, o viceversa.
 - etc.

Transposición inversa

- Consiste en transmitir el mensaje a la inversa, es decir, primero el último carácter, después el penúltimo y así sucesivamente.
- Si $c_1 c_2 c_3 \dots c_N$ es el mensaje claro, su criptograma sería $c_N c_{N-1} \dots c_3 c_2 c_1$.

Transposición por desplazamiento

- Consiste en realizar un desplazamiento de los caracteres a la izquierda o a la derecha.
- Si $c_1 c_2 c_3 \dots c_N$ es el mensaje claro, su criptograma con un desplazamiento unitario a la derecha sería $c_N c_1 c_2 \dots c_{N-1}$.

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

Descripción

- Es una combinación de varias operaciones: sustitución, transposición, operaciones lógicas (XOR), operaciones aritméticas (suma, producto, etc.), otras funciones reversibles, etc.
- Es lo empleado en la mayor parte de los sistemas actuales.

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

Ejercicio 2: Cifrado producto

Cifrado producto: ROT13, transposición inversa y doble desplazamiento a la derecha. Usar bloques de 4 caracteres.

M = TRABAJOENEQUIPO

- 1 Dividir el mensaje en bloques (rellenar el último con X).
- 2 Cada estudiante opera con dos bloques (1º y 2º, 2º y 3º, 3º y 4º, 4º y 1º).
- 3 El criptograma es la concatenación de los criptogramas de cada bloque.

Modo Electronic Codebook (ECB)

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

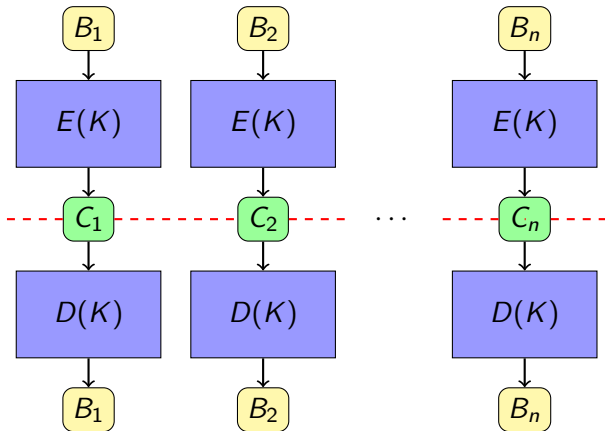
Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía



SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

- Paralelizable y sencillo.
- Un error de comunicación de un bloque cifrado sólo le afecta a él (50 % de los bits aleatoriamente).
- Mismo bloque en claro → mismo bloque cifrado.
- Mantiene las distribuciones de los datos.
- Vulnerable a ataques de repetición y a reordenado.

Modo Cipher Block Chaining (CBC)

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

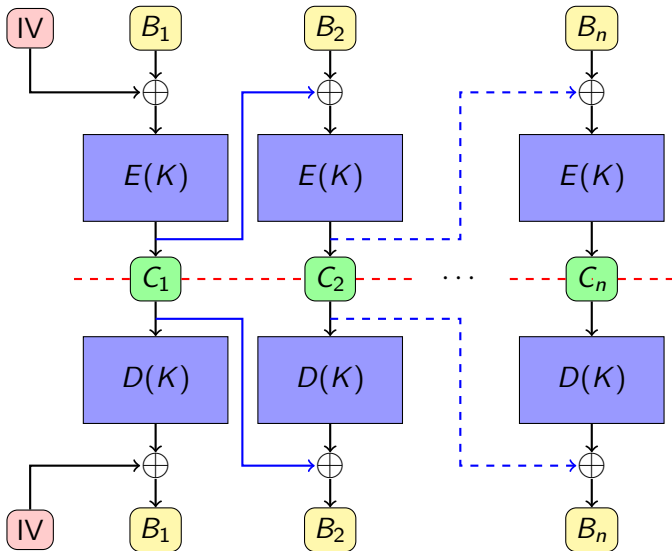
Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía



SSI T5

Grado en Ingeniería Informática

Fundamentos

Tipos de sistemas criptográficos

Criptografía de clave simétrica

Criptografía de clave asimétrica

Algoritmos de huella digital

Protocolos

Aplicaciones de la criptografía

- Cifrado no paralelizable (aunque sí el descifrado).
- Poco útil para acceso aleatorio (ficheros, por ejemplo).
- Todo bloque depende de sus anteriores: no es posible reordenar sin que se note.
- Convierte el cifrado de bloque en cifrado de flujo, donde los caracteres y el flujo de claves se corresponden con los bloques del texto cifrado.
- Mismos bloques cifrados para mismo texto si clave e IV permanecen iguales.
- Se resincroniza: un error en un bloque cifrado afecta a dicho bloque (50 % bits, aleatorio) y al siguiente (justo donde se dio el fallo), pero no más.
- El IV debe ser impredecible y protegerse ante modificaciones por el adversario, ya que le permite modificar el primer bloque descifrado.

Modo Output Feedback (OFB)

Aquí suponemos que el IV es del tamaño de un bloque

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

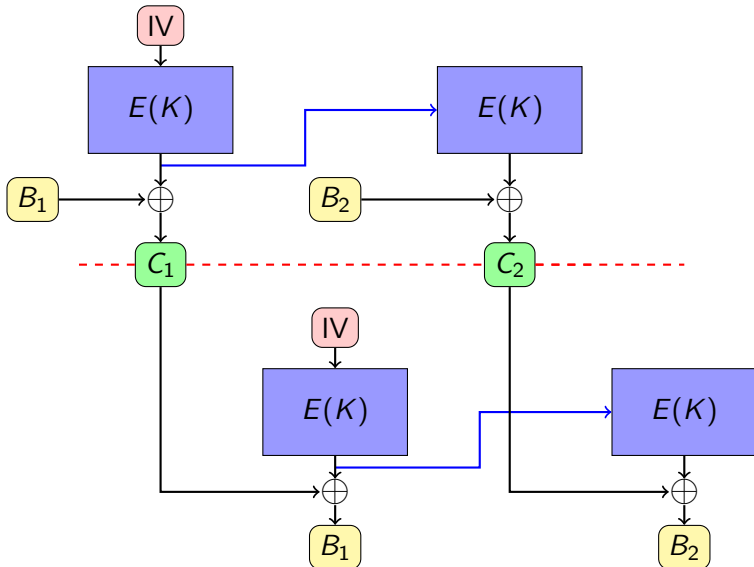
Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía



- No directamente paralelizable, aunque puede precalcularse el flujo de claves.
- Generan las claves de un cifrado en flujo mediante un cifrado en bloque.
- Un error en un bloque cifrado sólo afecta a su carácter.
- Mismo texto cifrado para mismo IV/clave.
- Mismo flujo de claves para mismo IV: no deben repetirse los IV para una misma clave, o un atacante puede hacer XOR entre dos flujos que usen los mismos IV para debilitar el cifrado.
- Se recupera de errores en bits, pero si se borran bits, pierde la alineación del texto respecto de las claves.
- **No** puede usarse con cifrado asimétrico: sólo se cifra, no se descifra.

Modo Counter (CTR)

Versión de OFB pero con contadores en vez de realimentación

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

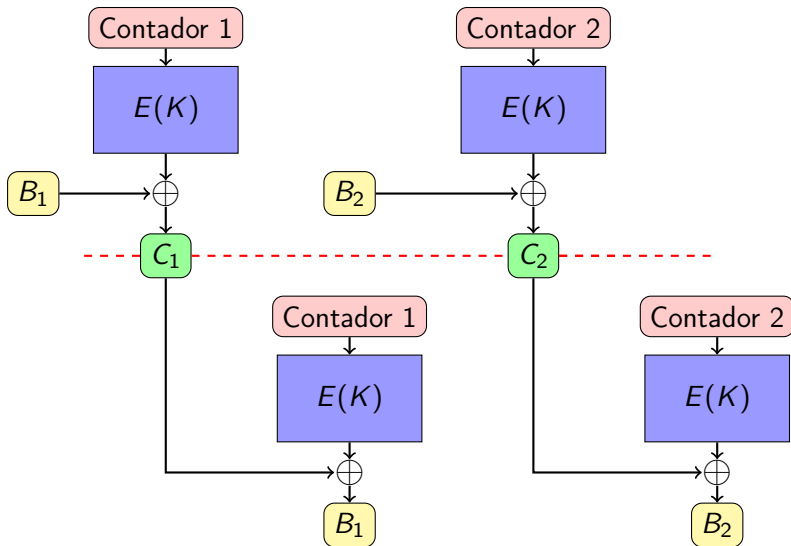
Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía



SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

- Más fácil de paralelizar.
- Acceso directo más sencillo.
- No deben repetirse los valores de los contadores para una misma clave.
- Suele usarse la función incremento, posiblemente con un prefijo único (*nonce*).
- Resto de propiedades de OFB.

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

1 Fundamentos

2 Tipos de sistemas criptográficos

3 Criptografía de clave simétrica

- Sistemas clásicos
 - Cifrado por sustitución
 - Cifrado por transposición
 - Cifrado producto
 - Algunos modos de operación
- Sistemas modernos
 - DES
 - AES

4 Criptografía de clave asimétrica

Data Encryption Standard

Algoritmo de cifrado en bloque desarrollado por el gobierno de los EEUU como un intento de crear un estándar para las comunicaciones.

Historia

- 1972 NBS propone a varias empresas desarrollar un algoritmo criptográfico para uso público que fuese el estándar, sin éxito.
- 1974 Segundo llamamiento, acude IBM con LUCIFER.
- 1976 NBS lo adopta llamándolo DES (su verdadero nombre es DEA en EEUU y DEA1 en el resto), cambiando las claves de 128 a 56 bits.

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

Tamaño de bloque y clave

- Bloques de 64 bits.
- Claves de 8 bytes (con 8 bits de paridad).
- Fácil implementación en un circuito integrado.

Normas ANSI

- X3.92: Descripción del algoritmo.
- X3.108: Descripción de los modos de operación.

DES: esquema

Red Feistel: opera sobre una mitad e intercambia

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

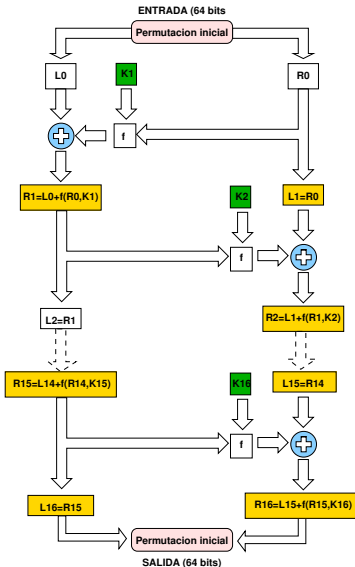
Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

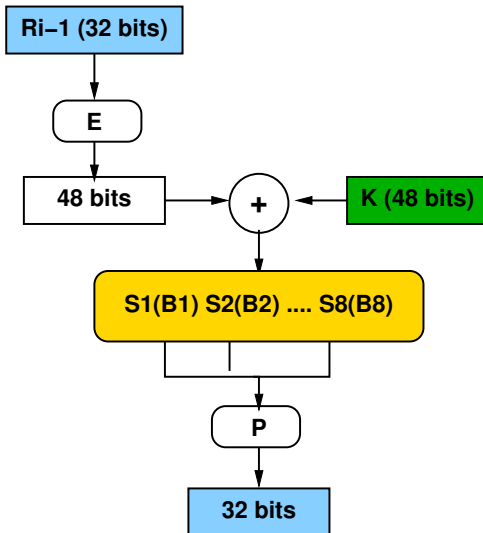
Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

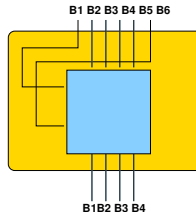


FUNCION F (DES)



Funcionamiento

- Reciben un bloque de 6 bits, de manera que el primero y el sexto seleccionan una fila, y el resto indican una columna de una matriz.
- Esa matriz contiene un número de 4 bits (del 0 al 15), que es el resultado de la caja.
- Los resultados de todas estas cajas, se concatenan formando un bloque de 32 bits.



DES: generación de subclaves

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

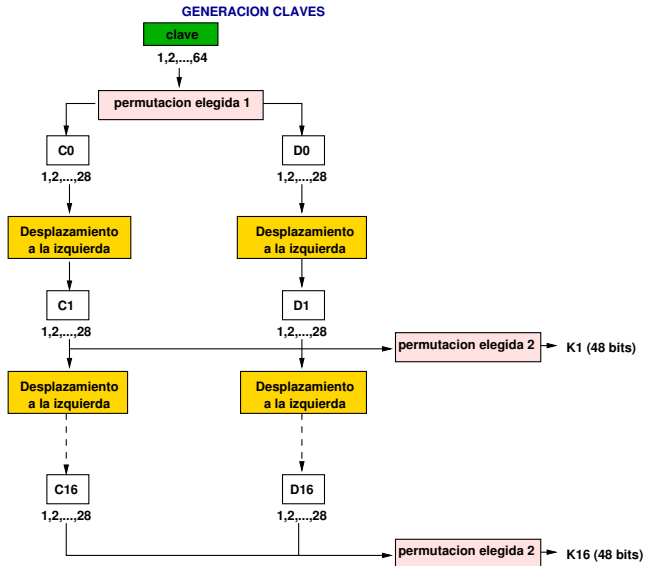
Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía



Descifrado

Igual al cifrado, pero las subclaves se usan en orden inverso: primero k_{16} y por último k_1 .

Seguridad

Combina confusión y difusión, pero:

- Claves cortas.
- ¿Por qué las cajas S?
- Tiene claves débiles (4, 2^{28}) y semidébiles (28), es decir, una clave genera las mismas 16 claves internas o bien 2 claves repetidas 8 veces.

Doble DES

- Emplea dos claves de 64 bits (56 bits reales cada una).
- $C = E(k_2, E(k_1, M))$
- En 1981, Merkle y Hellman, demuestran que es igual que emplear una clave de 57 bits.

Triple DES

- $C = E(k_1, D(k_2, E(k_1, M)))$
- Es igual que emplear una clave de 112 bits.

DES deja de ser estándar

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

Ataques realizados

- 29 enero 1997** 8000 ordenadores en Internet rompen la clave en 96 días. Sólo necesitan recorrer el 25 % del espacio de claves. Se evalúan 7.000 millones de claves/seg.
- 13 enero 1998** Un ataque distribuido por distributed.net lo rompe en 39 días. Sólo recorre el 88 % del espacio de claves. Se evalúan 34.000 millones de claves/seg.
- 13 julio 1998** Se construye una máquina (200.000\$) que rompe la clave en 56 horas. Se evalúan 90.000 millones de claves/seg.
- 18 enero 1999** 100.000 ordenadores en Internet junto con la «DES Cracker» rompen la clave en 22 horas. Se recorre el 22 % del espacio de claves, evaluando 245.000 millones de claves/seg.
- 1997** El NIST no certifica al DES.

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

Historia de la selección

- 1997 NIST convoca un nuevo concurso.
- 1998 Se presentan 15 algoritmos.
- 1999 Se seleccionan 5 finalistas.
- 2000 Aplicando criterios de seguridad, eficiencia y fácil implementación, se escoge el algoritmo Rijndael (Rijmen y Daemen) como el nuevo AES (*Advanced Encryption Standard*).
- 2001 Se convierte en el Estándar nº 197 sobre Procesamiento de Información Federal (FIPS 197).

Diferencias con el proceso anterior

El proceso de selección, revisión y estudio fue abierto a todo el mundo. Es software libre.

Tamaños de clave y de bloque

- Variables (128 - 256 bits o múltiplos de 4 bytes).
- Determinan el número de iteraciones (*rondas*): 9, 11 y 13 ciclos para claves de 128, 192 y 256 bits respectivamente.

Otros aspectos

- No es de tipo Feistel.
- Fácil de implementar en procesadores de 8 y 32 bits: sustitución, transposición, desplazamiento, XOR y sumas.

Pasos

- 1 Sustitución de bytes: cada byte de cada bloque se sustituye según una tabla de sustitución (caja S). Objetivo: confusión.
- 2 Desplazamiento de filas: transposición de desplazamiento de filas. Objetivo: difusión.
- 3 Mezclar columnas: desplazamiento de columnas a la izquierda con XOR. No se realiza la última iteración. Objetivo: difusión.
- 4 Añadir clave: XOR con una subclave obtenida de la clave maestra (expansión y selección). Objetivo: confusión.

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

1 Fundamentos

2 Tipos de sistemas criptográficos

3 Criptografía de clave simétrica

- Cifrado por sustitución
- Cifrado por transposición
- Cifrado producto
- Algunos modos de operación
- DES
- AES

4 Criptografía de clave asimétrica

- RSA

5 Algoritmos de huella digital

Historia

- Fue desarrollado en 1978 por Ronald Rivest, Adi Shamir y Leonard Adleman.
- Patentado por los laboratorios RSA hasta el 20 de septiembre de 2000. Esta empresa fue la que subvencionó los ataques al DES de 1997 a 1999 (DES Challenge).

Estado actual

- Es uno de los más difundidos, y es considerado como un estándar en la criptografía de clave pública.

Requisitos

- Se buscan dos algoritmos de cifrado y descifrado, tal que:

$$D(k_{priv}, E(k_{pub}, M)) = M$$

$$D(k_{pub}, E(k_{priv}, M)) = M$$

- Consideramos cada mensaje M como un número, y todas las operaciones de cifrado y descifrado son operaciones aritméticas.
- Conseguir que los algoritmos de cifrado E y descifrado D sean los mismos \rightarrow exponenciación en aritmética modular.

Cifrado y descifrado

- M es el mensaje original y C el cifrado.
- Clave pública: (e, n) , privada: (d, n) .
- Cifrado: $C = M^e \bmod n$
- Descifrado: $M = C^d \bmod n$

Condición a cumplir

$$C^d \bmod n = (M^e \bmod n)^d \bmod n = M^{ed} \bmod n = M$$

RSA: funcionamiento (II)

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

Ejemplo

- $M = 19$
- Clave pública = $(5, 119)$
- Clave privada = $(77, 119)$

Cifrado

$$C = 19^5 \bmod 119 = 66$$

Descifrado

$$M = 66^{77} \bmod 119 = 19$$

Generación de claves

- ① Cada usuario elige dos números primos grandes, p y q .
- ② Calculamos el número $n = pq$, que todos conocen.
- ③ Calculamos $\phi(n) = (p - 1)(q - 1)$.
- ④ Calculamos la clave pública e , que es un gran número entero que es primo respecto al número $\phi(n)$, es decir, $\text{mcd}\{e, \phi(n)\} = 1$.
- ⑤ Se determina d tal que $ed \text{ mód } \phi(n) = 1$. Esto es equivalente a: $ed \equiv 1 \text{ (mód } \phi(n))$ y $d \equiv e^{-1} \text{ (mód } \phi(n))$. Puede usarse el algoritmo de Euclides extendido, por ejemplo.
- ⑥ $k_{\text{pub}} = (e, n)$
- ⑦ $k_{\text{priv}} = (d, n)$

Ejemplo de generación de claves

- ① Seleccionar dos números primos, $p = 17$ y $q = 11$.
- ② Calcular $n = pq = 17 \times 11 = 187$.
- ③ Calcular $\phi(n) = (p - 1)(q - 1) = 16 \times 10 = 160$.
- ④ Calcular e , que sea primo respecto al número $\phi(n) = 160$, es decir, $\text{mcd}\{e, 160\} = 1$. Además, e debe ser menor que $\phi(n)$. Se elige $e = 7$.
- ⑤ Determinar d tal que $ed \equiv 1 \pmod{\phi(n)}$ y $d < 160$, $7d \equiv 1 \pmod{160}$. El valor correcto es $d = 23$ porque $7 \times 23 = 161 = (1 \times 160) + 1$; d puede calcularse mediante el algoritmo de Euclides extendido.
- ⑥ $k_{pub} = (7, 187)$
- ⑦ $k_{priv} = (23, 187)$

Seguridad

- Todo radica en una buena elección de p y q (longitud mínima de 500 bits). Unos primos seguros se consiguen eligiendo un número r primo grande, de modo que $p = 2r + 1$ y $q = 2p + 1$ sean primos y $\text{mcd}\{p - 1, q - 1\}$ es pequeño. Por ejemplo con $r = 1019$, obtendríamos $p = 2039$ y $q = 4079$, ambos primos y con un $\text{mcd}\{2038, 4078\} = 2$ pequeño.
- Existen claves débiles: $M^e \bmod n = M$.
- Existen claves privadas parejas, es decir, un mensaje cifrado tiene más de una clave de descifrado.
- Ataques de intermediario: evitable con certificados digitales o con anillos de confianza.

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

Ejercicio 3: RSA

Si estamos empleando un sistema de cifrado RSA con clave pública $(17, 187)$, ¿cuál sería la codificación del bloque 15 que queremos transmitir?

Características

- Emplea las funciones de dispersión o de comprobación aleatoria (*hash*, *checksum* o *message digest*).
- El fichero se reduce a un **resumen criptográfico** o huella digital de tamaño fijo:
 - MD5: 128 bits.
 - SHA-1: 160 bits.
 - SHA-2: SHA-224, SHA-256, SHA-384 y SHA-512 bits. Actualmente, son los hashes más fuertes en GnuPG.
 - SHA-3: nuevo algoritmo hash. Se cree que es seguro pero todavía no ha sido oficialmente introducido en el estándar OpenPGP; no soportado por GnuPG (https://www.gnupg.org/faq/gnupg-faq.html#define_sha).
- Son funciones irreversibles: se pierde información del mensaje original y es imposible reconstruirlo.

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

Utilidad

- Las funciones *hash* se utilizan principalmente para garantizar la autenticidad de la información.
- Por ejemplo, si queremos verificar si un archivo ha sido manipulado con el tiempo, podemos aplicarle una función *hash* el día 1 y el día 30. Si los *hashes* de salida de la función son iguales, el archivo no habrá sido modificado. Sin embargo, si el *hash* del día 30 es diferente al inicial, el archivo habrá sido modificado, aunque la modificación sea tan pequeña como un simple bit.
- Se usan en la firma digital o la tecnología *blockchain*.

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

- 1 Fundamentos
- 2 Tipos de sistemas criptográficos
- 3 Criptografía de clave simétrica
 - Cifrado por sustitución
 - Cifrado por transposición
 - Cifrado producto
 - Algunos modos de operación
 - DES
 - AES
- 4 Criptografía de clave asimétrica
- 5 Algoritmos de huella digital

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

- *Transport Layer Security* (TLS) y su predecesor *Secure Socket Layer* (SSL) son protocolos de la capa de aplicación en el modelo TCP/IP.
- Ofrecen servicios de seguridad a otros protocolos y aplicaciones.
- Una de las aplicaciones de TLS es en el protocolo HTTPS, permitiendo crear conexiones seguras.

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

- Protocolo de la capa de Internet.
- Ofrece servicios de seguridad a un nivel bajo.
- Si una aplicación quiere garantizar la integridad o confidencialidad de los datos puede usar los servicios ofrecidos por IPSec sin implementar ningún protocolo.

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

- *Secure Shell* (SSH) es un protocolo de la capa de aplicación.
- Permite crear una conexión remota con la consola de administración de una máquina.
- Garantiza la confidencialidad e integridad de los datos.
- Además, permite crear túneles entre el cliente y el servidor.

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

- 1 Fundamentos
- 2 Tipos de sistemas criptográficos
- 3 Criptografía de clave simétrica
 - Cifrado por sustitución
 - Cifrado por transposición
 - Cifrado producto
 - Algunos modos de operación
 - DES
 - AES
- 4 Criptografía de clave asimétrica
- 5 Algoritmos de huella digital

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

Definición (ISO 7498-2)

La firma electrónica son los datos añadidos a un conjunto de datos que permiten al receptor probar el origen y la integridad de los datos, así como protegerlos contra falsificaciones.

Garantiza:

- Integridad
- Autenticidad
- Confidencialidad (opcional)
- No repudio

Firma electrónica (II)

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

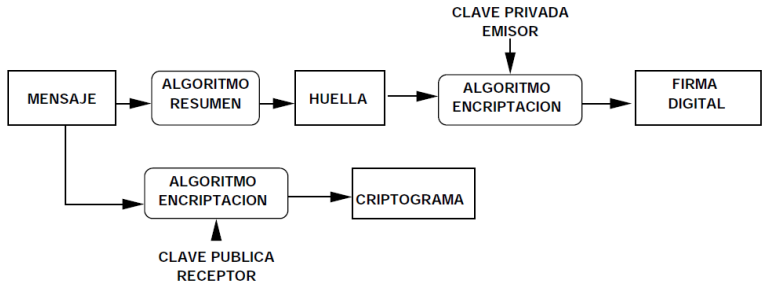
Aplicaciones
de la
criptografía

Cifrado

- Se obtiene la huella digital del mensaje en claro, y esta se cifra con la clave privada del emisor, obteniendo la firma digital del mensaje.
- El mensaje en claro se cifra con la clave pública del receptor.
- El receptor recibe el mensaje cifrado y la firma digital.

Descifrado

- El mensaje se descifra con la clave privada del receptor y, a continuación, el receptor obtiene la huella digital del mensaje que ha recibido.
- La firma digital se descifra con la clave pública del emisor.
- Se compara las dos huellas digitales.



SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

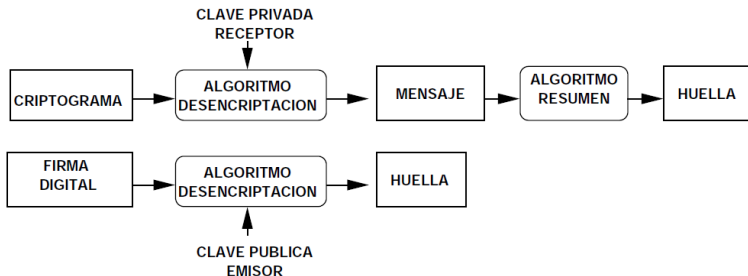
Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía



SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

- 1 Fundamentos
- 2 Tipos de sistemas criptográficos
- 3 Criptografía de clave simétrica
 - Cifrado por sustitución
 - Cifrado por transposición
 - Cifrado producto
 - Algunos modos de operación
 - DES
 - AES
- 4 Criptografía de clave asimétrica
- 5 Algoritmos de huella digital

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

- Un certificado digital es un documento electrónico que permite vincular una clave pública con la identidad real de su creador.
- Este documento debe llevar la firma digital de un notario electrónico para que sea fiable.

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

1 Fundamentos

2 Tipos de sistemas criptográficos

3 Criptografía de clave simétrica

- Cifrado por sustitución
- Cifrado por transposición
- Cifrado producto
- Algunos modos de operación
- DES
- AES

4 Criptografía de clave asimétrica

5 Algoritmos de huella digital

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

- 1 Fundamentos
- 2 Tipos de sistemas criptográficos
- 3 Criptografía de clave simétrica
 - Cifrado por sustitución
 - Cifrado por transposición
 - Cifrado producto
 - Algunos modos de operación
 - DES
 - AES
- 4 Criptografía de clave asimétrica
- 5 Algoritmos de huella digital

SSI T5

Grado en
Ingeniería
Informática

Fundamentos

Tipos de
sistemas
criptográficos

Criptografía
de clave
simétrica

Criptografía
de clave
asimétrica

Algoritmos
de huella
digital

Protocolos

Aplicaciones
de la
criptografía

Características

- No tienen un sistema descifrador.
- Son funciones criptográficas unidireccionales que no tienen inversa.
- No interesa el mensaje en claro.

Utilidad

Almacenamiento de contraseñas: crypt