



Capítulo 2

Una Breve Introducción a la Criptografía

Seguridad Informática y Criptografía



v 4.1



Material Docente de  
Libre Distribución

Ultima actualización del archivo: 01/03/06  
Este archivo tiene: 15 diapositivas

Dr. Jorge Ramíó Aguirre  
Universidad Politécnica de Madrid

Este archivo forma parte de un curso completo sobre Seguridad Informática y Criptografía. Se autoriza el uso, reproducción en computador y su impresión en papel, sólo con fines docentes y/o personales, respetando los créditos del autor. Queda prohibida su comercialización, excepto la edición en venta en el Departamento de Publicaciones de la Escuela Universitaria de Informática de la Universidad Politécnica de Madrid, España.

Curso de Seguridad Informática y Criptografía © JRA

Capítulo 2: Una Breve Introducción a la Criptografía

Página 35

¿Qué estudiaremos en este libro?

- Si alguna vez ha pinchado en el acceso a una página web segura, por ejemplo para comprar un billete de avión en Internet, mirar el estado de una cuenta corriente en su banco, ... e incluso al introducir su clave cuando accede a hotmail ...
- La comunicación se ha hecho en una plataforma segura conocida como SSL dentro de un protocolo https (secure).
- En esos pocos segundos, tras los que se habrá dado cuenta que aparece un candado en la barra de tareas del navegador, a grandes rasgos ha pasado algo parecido a lo que se mostrará en la última diapositiva de este capítulo.
- Al final del curso, entre otras cosas, deberíamos ser capaces de saber qué es lo que ha pasado, entender los algoritmos utilizados y poder evaluar sus fortalezas y debilidades ☺.

© Jorge Ramíó Aguirre Madrid (España) 2006

## La razón de este capítulo en el libro

La inclusión de este capítulo -a manera de resumen- de lo que se entiende por criptografía y sus aplicaciones en los sistemas de cifra actuales tiene como objetivo ser una introducción general y amplia de las técnicas de protección de la información y que puede utilizarse en dos escenarios:

- Como la primera clase de un curso de criptografía y/o seguridad informática, de forma que el profesor pueda comentar, razonar y debatir con sus alumnos lo que se verá en profundidad en el resto de la asignatura, y servir además como motivación de la misma.
- Como material básico para una charla de aproximadamente una hora en la que el ponente hace un repaso general de estas técnicas y sus aplicaciones. También para la presentación de este tema de la criptografía en otras asignaturas relacionadas con la seguridad pero que sólo pueden dedicarle una hora dentro del temario.

## La criptografía según la RAE



*He aquí una definición no muy afortunada...*

La Real Academia Española define criptografía (del griego: oculto + escritura) como:

*"el ~~arte~~ de ~~escribir~~ con clave ~~secreta~~ o de modo ~~enigmático~~".*

Puede ser interesante y llamativa, pero resulta muy poco ajustada para los tiempos actuales.

→  
vea la siguiente diapositiva

## Imprecisiones de esta definición

- Arte: la criptografía ha dejado de ser un arte: es una ciencia.
- Escritura de documentos: no sólo se escriben mensajes; se envían o se guardan en un computador diversos tipos de documentos y formatos (TXT, DOC, EXE, DLL, JPG, ...).
- Se supone una clave: los sistemas actuales usan una o dos. En varias aplicaciones de Internet entran en juego 4 claves.
- Clave secreta: existirán sistemas de clave secreta que usan una sola clave y sistemas de clave pública (muy importantes) que usan dos: una clave privada (secreta) y la otra pública.
- Representación enigmática: la representación binaria de la información podría ser enigmática para nosotros los humanos pero no para los computadores ☺ ... es su lenguaje natural.

## Una definición más técnica de criptografía

### Criptografía

He aquí una definición más formal... ✓

Rama inicial de las Matemáticas y en la actualidad también de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar, y por tanto proteger, un mensaje o archivo por medio de un algoritmo, usando una o más claves.

Esto dará lugar a diferentes tipos de sistemas de cifra, denominados criptosistemas, que nos permiten asegurar al menos tres de los cuatro aspectos básicos de la seguridad informática: la confidencialidad o secreto del mensaje, la integridad del mensaje y autenticidad del emisor, así como el no repudio mutuo entre emisor (cliente) y receptor (servidor).

Capítulo 2: Una Breve Introducción a la Criptografía Página 40

## Confidencialidad e integridad

**Criptosistema**

*Cualquier medio de transmisión es inseguro*

Estos dos aspectos básicos de la seguridad informática, el de la confidencialidad y el de integridad (además de la disponibilidad del sistema y el no repudio) serán muy importantes en un entorno de intercambio de información segura a través de Internet.

© Jorge Ramío Aguirre Madrid (España) 2006

Capítulo 2: Una Breve Introducción a la Criptografía Página 41

## Tipos de criptosistemas

### Clasificación de los criptosistemas

Según el tratamiento del mensaje se dividen en:

- Cifrado en bloque (IDEA, AES, RSA\* ...) 64 ó 128 bits
- Cifrado en flujo (A5, RC4, SEAL ...) cifrado bit a bit

Según el tipo de claves se dividen en:

- Cifrado con clave secreta **Sistemas simétricos**
- Cifrado con clave pública **Sistemas asimétricos**

(\*) Como veremos en otro capítulo, sistemas como RSA no cifran por bloques propiamente tal: cifran un número único.

© Jorge Ramío Aguirre Madrid (España) 2006

## Criptosistemas simétricos y asimétricos

### Criptosistemas simétricos:

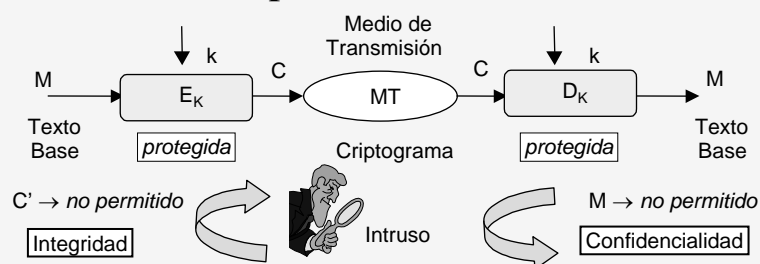
Existirá una única clave (secreta) que deben compartir emisor y receptor. Con la misma clave se cifra y se descifra por lo que la seguridad reside en mantener dicha clave en secreto.

### Criptosistemas asimétricos:

Cada usuario crea un par de claves, una privada y otra pública, inversas dentro de un cuerpo finito. Lo que se cifra en emisión con una clave, se descifra en recepción con la clave inversa. La seguridad del sistema reside en la dificultad computacional de descubrir la clave privada a partir de la pública. Para ello, usan funciones matemáticas de un solo sentido o con trampa.

## Criptosistemas simétricos

### Cifrado con criptosistemas de clave secreta

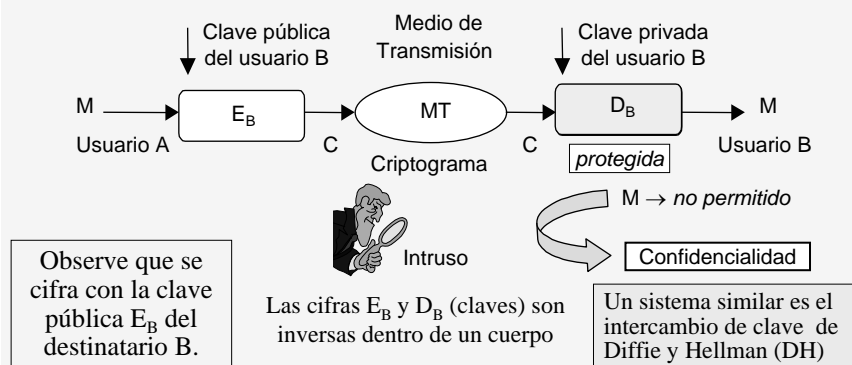


La confidencialidad y la integridad se lograrán si se protegen las claves en el cifrado y en el descifrado. Es decir, se obtienen simultáneamente si se protege la clave secreta.

DES, TDES,  
IDEA, CAST,  
RC5, AES, ...

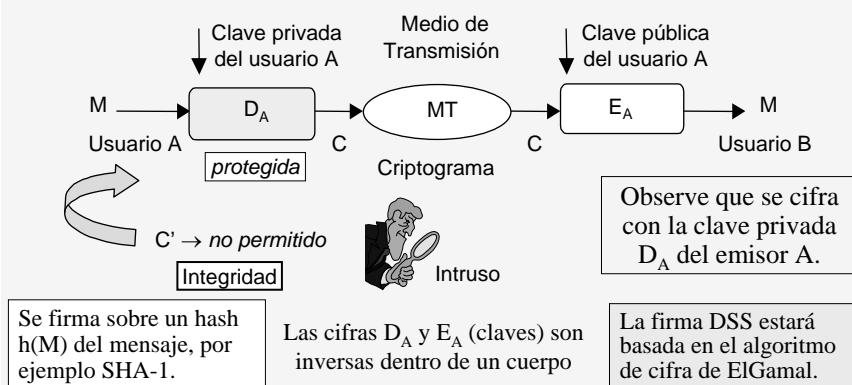
## Criptosistemas asimétricos (parte 1)

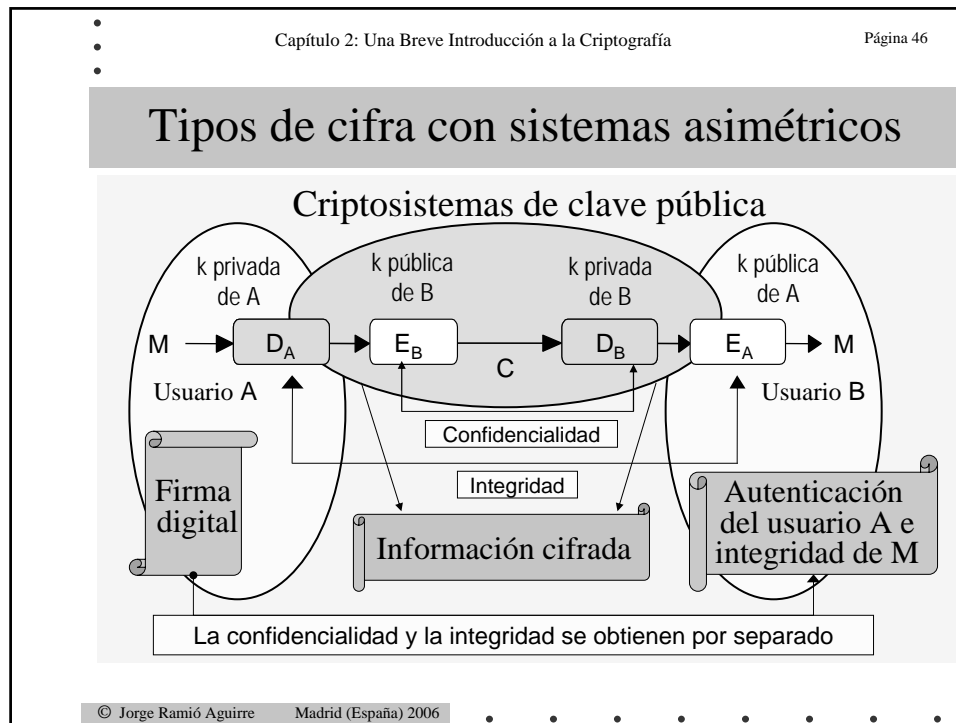
### Cifrado con clave pública del receptor (intercambio de claves RSA)



## Criptosistemas asimétricos (parte 2)

### Cifrado con clave privada del emisor (firma digital RSA)






Capítulo 2: Una Breve Introducción a la Criptografía Página 47

## ¿Qué usar, cifra simétrica o asimétrica?

Los sistemas de clave pública son muy lentos pero tienen un fácil intercambio de clave y cuentan con firma digital.

Los sistemas de clave secreta son muy rápidos pero carecen de lo anterior.

¿Qué hacer?

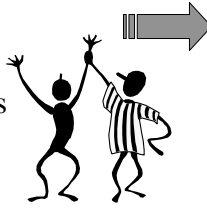


Cifrado de la información:

- Usaremos sistemas de clave secreta

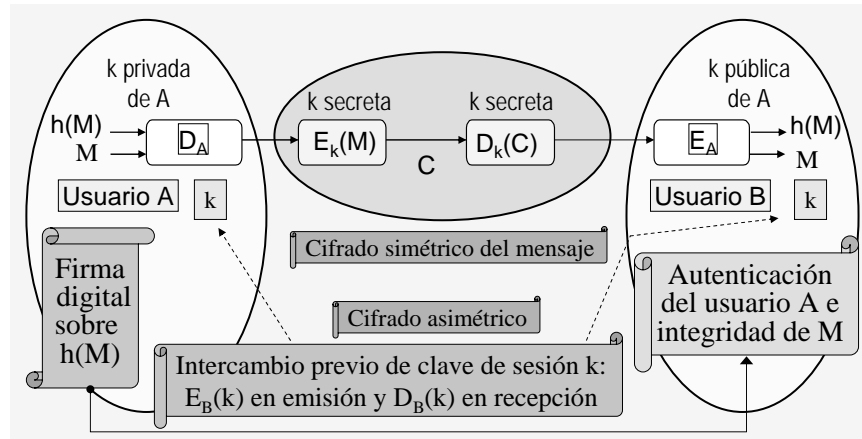
Firma e intercambio de clave de sesión:

- Usaremos sistemas de clave pública



© Jorge Ramío Aguirre Madrid (España) 2006

## Sistema híbrido de cifra y firma digital



Fin del capítulo