Seguridad y Alta Disponibilidad:
Criptografía

IES Gonzalo Nazareno
CONSEJERÍA DE EDUCACIÓN

Jesús Moreno León

jesus.moreno.edu@
juntadeandalucía.es

Septiembre 2012

Transparencias adaptadas del material del libro:

Redes de computadores: un enfoque descendente basado en Internet, 2ª edición.Jim Kurose, Keith Ross

Criptografía

Etimológicamente, criptografía proviene de dos palabras del griego:

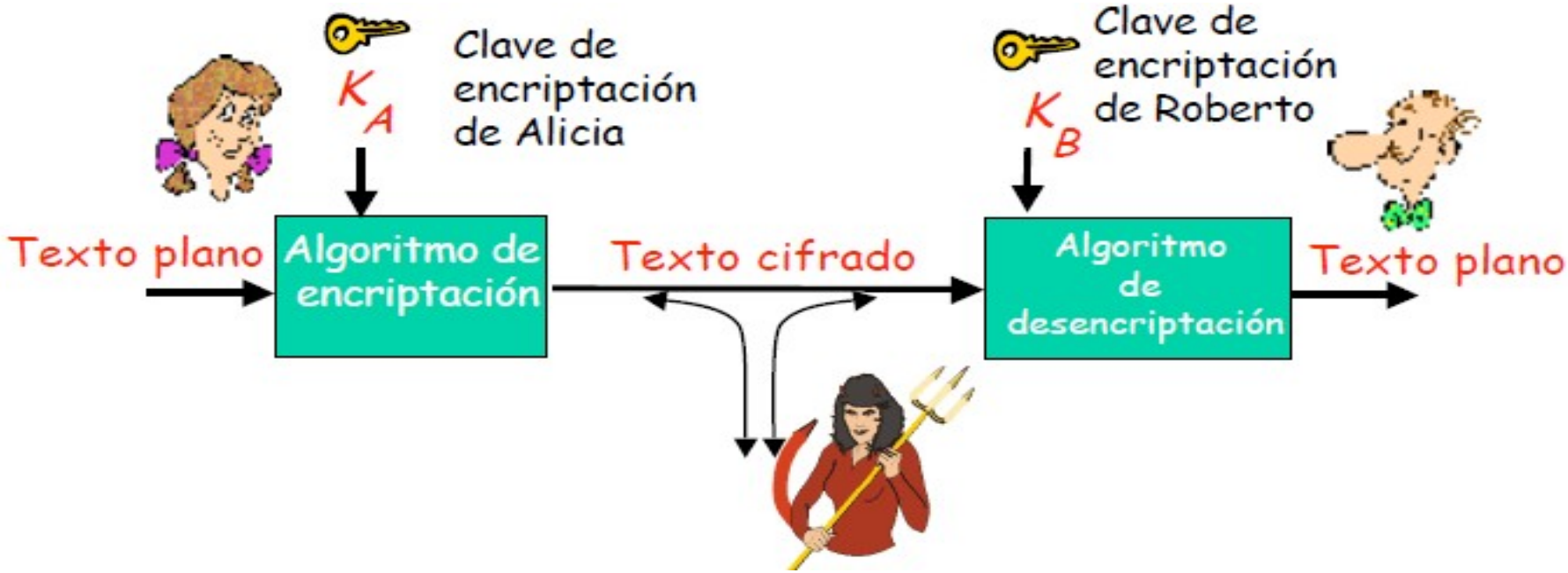
- Cripto → escondido
- Grafía → escritura

Es la ciencia que estudia el diseño de códigos secretos y la interpretación de mensajes cifrados.

Historia de la criptografía y su desarrollo en Europa

Ejercicios básicos

El lenguaje de la criptografía



- Criptografía **clave simétrica**: claves del emisor y receptor, idénticas
- Criptografía **clave pública**: cada usuario tiene una clave pública conocida por todos y una clave privada, que es secreta

¿Cuáles son los equivalentes de Roberto y Alicia en seguridad informática?

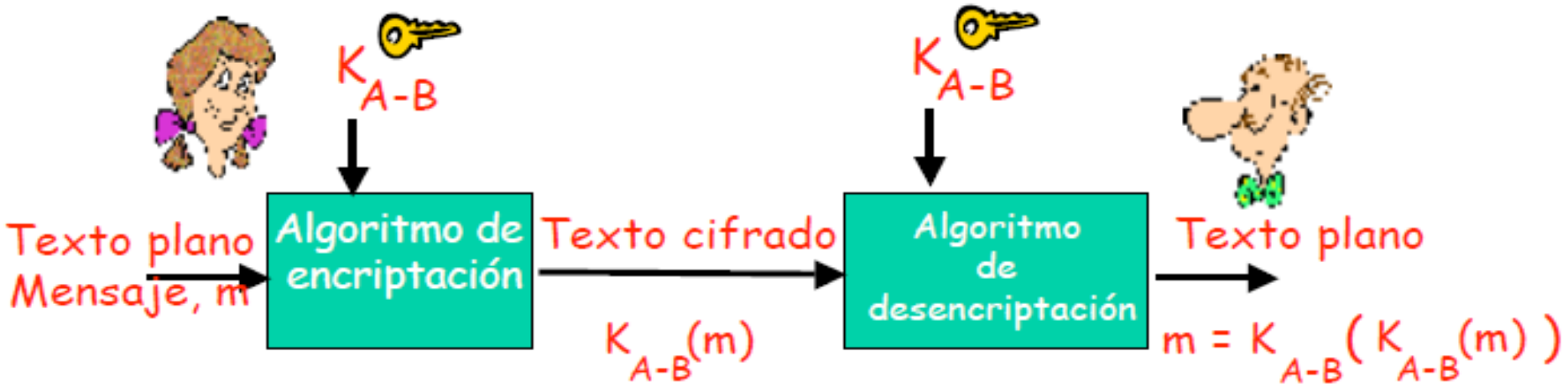
- Robertos y Alicias de la vida real
- Navegador / servidor de Internet para transacciones electrónicas
- Cliente / servidor de banco online
- Servidores DNS
- Routers que intercambian tablas de encaminamiento
- ...

Hay muchos chicos malos por ahí... ¡y chicas!

¿Qué puede hacer un chic@ mal@?

- Escuchar a escondidas → interceptar mensajes
- Insertar activamente mensajes
- Suplantación → puede falsear la dirección origen de un paquete
- Secuestro → apoderarse de la conexión eliminando a uno de los participantes e insertarse él en su lugar
- Denegación de servicio: impedir que el servicio se utilizado por otros
- ...

Criptografía de clave simétrica



Roberto y Alicia comparten la misma clave (simétrica) K_{A-B}

Antes de poder comunicarse deben ponerse de acuerdo en el valor de la clave

Criptografía de clave simétrica

Algoritmos de cifrado simétricos:

- DES
- TripleDES
- AES

Ver para creer...

- El proyecto OpenSSL es un esfuerzo colaborativo para desarrollar un toolkit libre y gratuito que implementa SSL y TLS, así como herramientas y bibliotecas relacionadas con la criptografía
- Ciertos programas de una máquina, como OpenSSH o el navegador, hacen uso de las funciones que OpenSSL les suministra
- Entre las herramientas que incorpora se encuentra el programa **openssl**, que se utiliza desde la línea de comandos

Ver para creer...

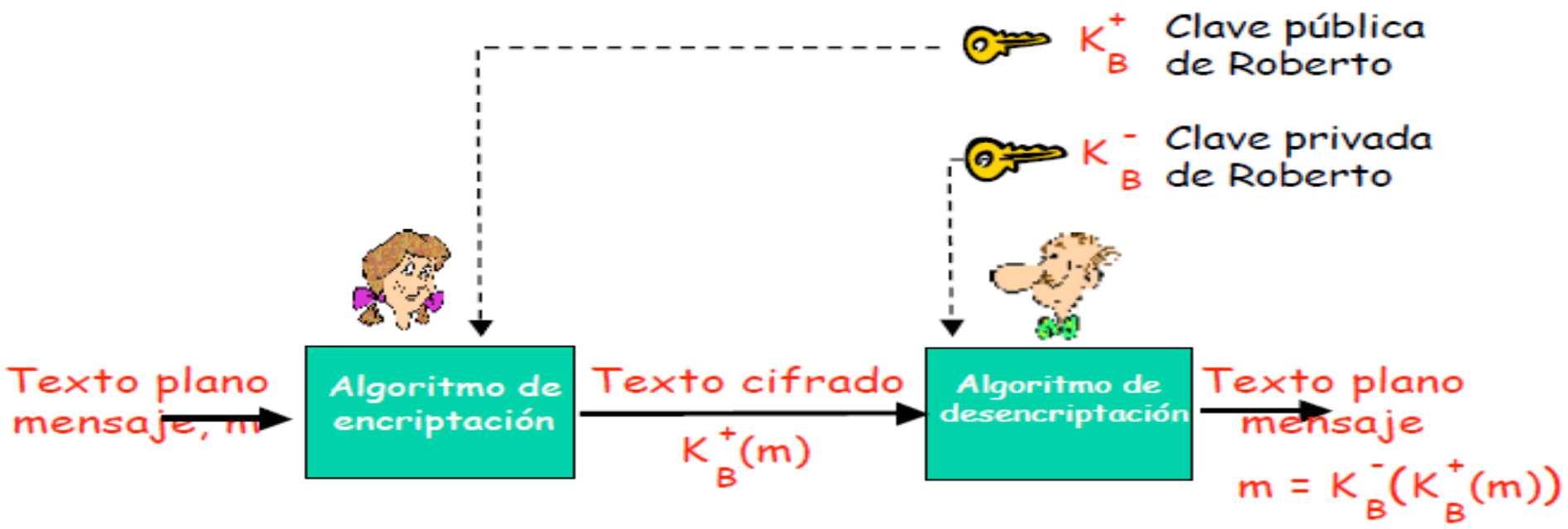
- Cifrado con Triple DES:

```
$ openssl des3 -in texto.txt -out texto.cifrado
```

- Descifrado con Triple DES

```
$ openssl des3 -d -in texto.cifrado -out texto.descifrado
```

Criptografía de clave pública



Emisor y receptor no comparten clave secreta

Clave de encriptación es pública y conocida por todos

Clave de desencriptación es privada, conocida sólo por el receptor

Criptografía de clave pública

Algoritmos de encriptación de clave pública:

- DSA
- RSA

Ver para creer...

- Generar clave privada RSA:

```
$ openssl genrsa -out privada.key 1024
```

- Obtener la clave pública RSA:

```
$ openssl rsa -in privada.key -pubout -out publica.key
```

Ver para creer...

- Codificar un texto con la clave pública:

```
$ openssl rsautl -in texto.txt -out texto.cifrado -inkey
  publica.key -pubin -encrypt
```

- Decodificar un texto con la clave privada:

```
$ openssl rsautl -in texto.cifrado -out texto.descifrado
  -inkey  privada.key  -decrypt
```