Tema 5: Seguridad en redes

Bibliografía:

[Kurose11] Secciones 1.6, 8.1, 8.2 (excepto la introducción) y 8.2.1

Objetivos

- Entender los fundamentos de seguridad en un sistema de redes de computadores
  - La criptografía y sus aplicaciones más allá de la confidencialidad
  - Integridad de los mensajes
  - Autenticación
- Seguridad en la práctica: sockets seguros

Índice

A13

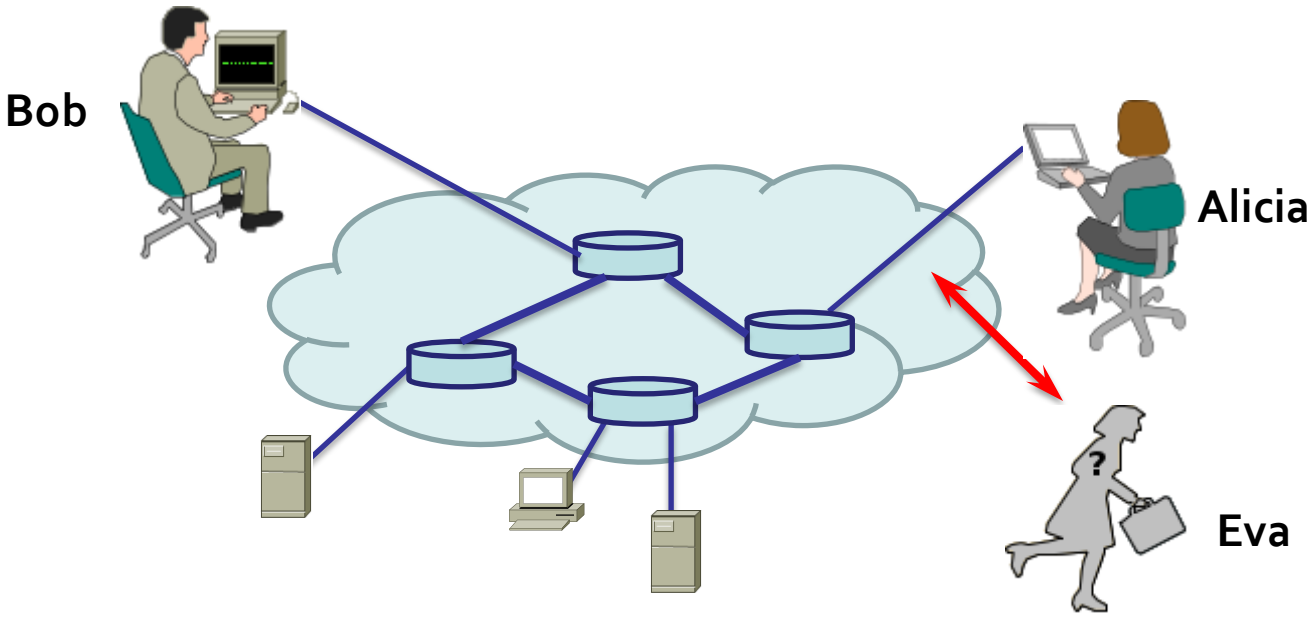
Propiedades (I)

- **Propiedades deseables en una comunicación segura**
  - **Confidencialidad**: el contenido del mensaje disponible únicamente para el emisor y el receptor
    - Solución: mediante cifrado
      - El emisor cifra el mensaje
      - El receptor descifra el mensaje
  - **Autentificación**: emisor y receptor quieren confirmar la identidad de la otra parte
    - Solución: mediante técnicas criptográficas

Propiedades (II)

- **Integridad del mensaje:** contenido del mensaje inalterado durante la transmisión (accidental o intencionadamente)
  - Solución: técnicas adicionales al control de errores empleado en los niveles de transporte y enlace de datos
- **Disponibilidad:** recursos de la red disponibles en cualquier momento (ataques de denegación de servicio)
  - Solución: ???????
- **Control de acceso:** recursos de la red disponibles sólo para los usuarios legítimos
  - Solución: restricción en el control de acceso con mecanismos de autentificación, cortafuegos, etc.

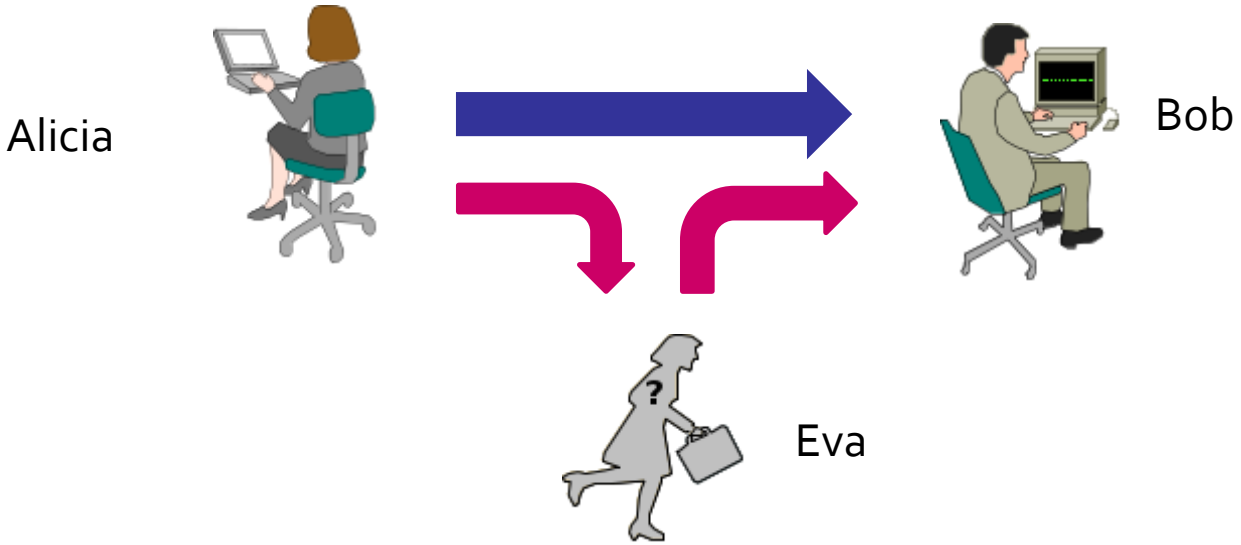
Buenos y malos



- Alicia y Bob pueden ser:
  - 2 routers que quieren intercambiar sus tablas de encaminamiento
  - Un cliente y un servidor que quieren establecer una conexión de transporte segura:
    - Transacciones bancarias on-line
    - Comercio electrónico
    - …

Tipos de malos

- **Intruso pasivo**
  - Puede escuchar y recoger información que circula por la red: contraseñas, información sobre tarjetas de crédito, etc.
- **Intruso activo**
  - Puede eliminar mensajes y/o añadir otros nuevos

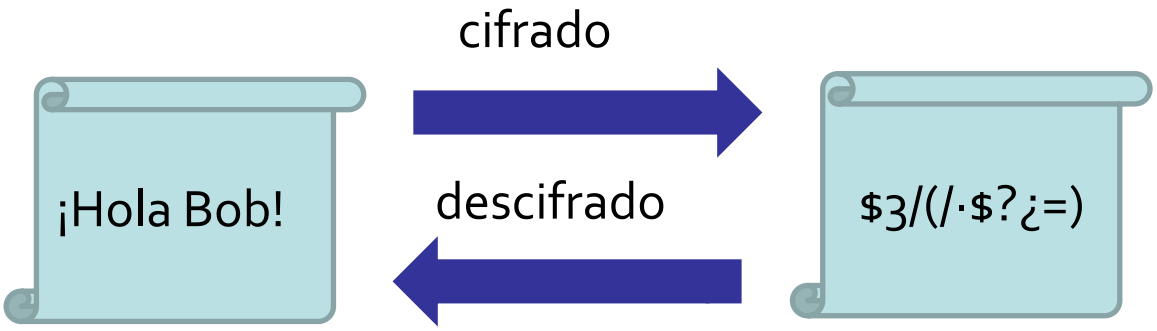


Índice

A13

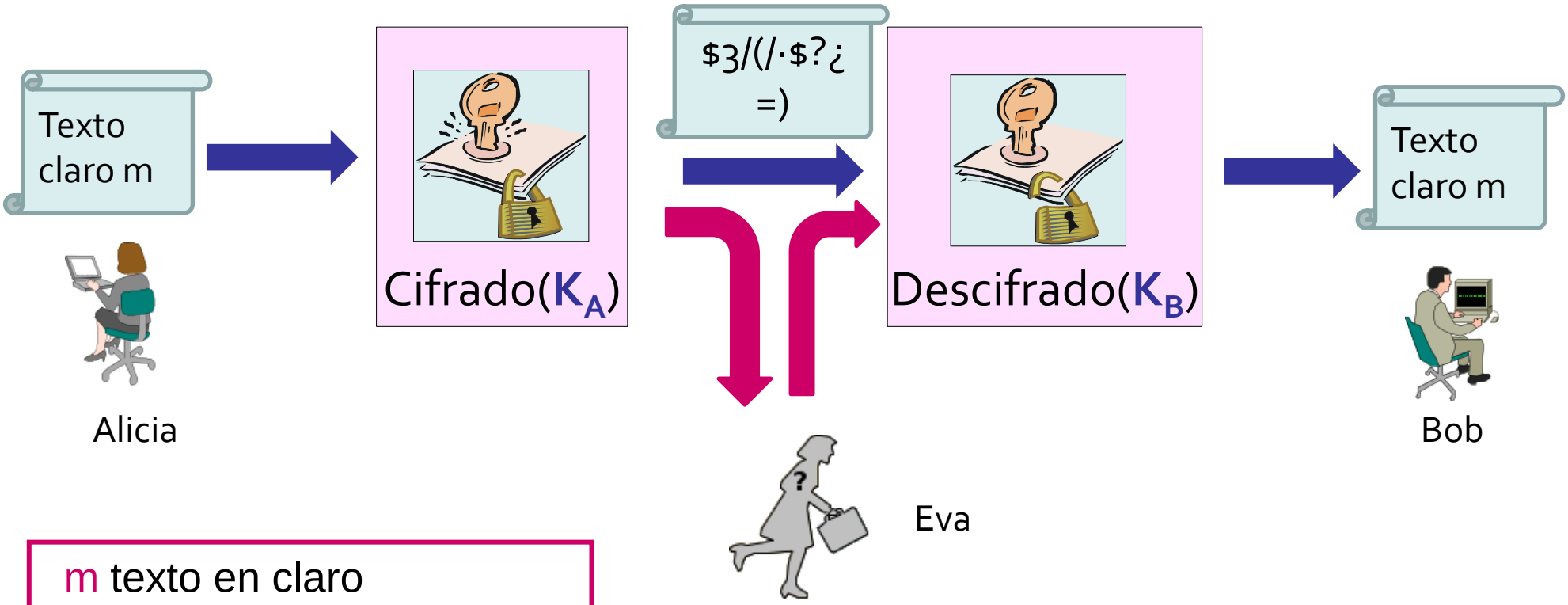
2. Principios de criptografía

- **Criptografía:** ciencia y arte de modificar los datos para que sólo puedan ser conocidos por su emisor y el receptor deseado
  - Datos modificados → cifrado
  - Texto sin modificar → texto nativo o texto en claro



Componentes criptográficos

Para cifrar o descifrar se requiere un algoritmo y una o más claves (K_A, K_B)



m texto en claro
$K_A(m)$ texto cifrado con K_A
$m=K_B(K_A(m))$

Cifrados de sustitución

Cifrado monoalfabético

```
Texto plano:   abcdefghijklmnopqrstuvwxyz
Texto cifrado: mnbvcxzasdfghjklpoiuytrewq
```

Ejemplo:

Texto en claro: hola bob.alice
Texto cifrado: akgm nkn. mgsbc

- ¿K?
- Caso particular: cifrado de César
  - Sustitución cíclica de las letras del alfabeto
  - ¿K?

Cifrados de sustitución

- **Cifrado Monoalfabético**
  - Cifrado de César.
    - Texto claro
    - Cifrado K=11

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	x	y	z
l	m	n	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j	k

  - "Hola clase" → "Saxl nxlep"
- **Cifrado Polialfabético**
  - Texto claro
  - Cifrado K=11
  - Cifrado K=4

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	x	y	z
l	m	n	o	p	q	r	s	t	u	v	x	y	z	a	b	c	d	e	f	g	h	i	j	k
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	x	y	z	a	b	c

  - Ejemplo $C_1C_1C_2C_1C_2C_2$: "Hola clase" → "Saol fxlvp"

Cómo romper un cifrado monoalfabético

- Ataque de sólo texto cifrado
  - Dos aproximaciones:
    - Búsqueda a través de todo el espacio de claves
    - Análisis estadístico

- Ataque de texto en claro conocido
  - En un cifrado monoalfabético pueden identificarse partes de palabras repetidas
- Ataque de texto en claro seleccionado

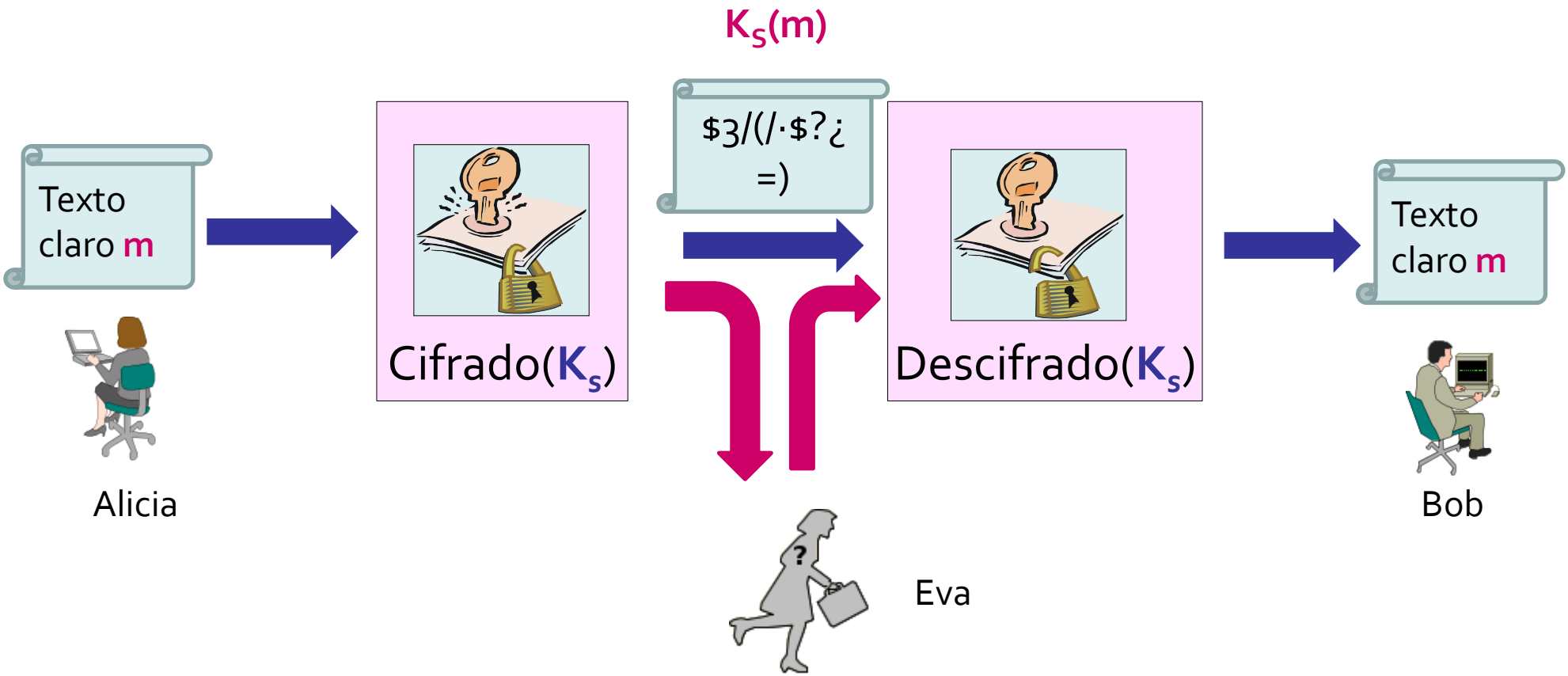
Tipos de criptografía

- Al emplear criptografía
  - El algoritmo suele ser conocido, incluso un estándar
  - Sólo las claves son secretas
- Criptografía de clave simétrica
  - Sólo una clave
- Criptografía de clave pública
  - Dos claves
- Funciones *hash* criptográficas
  - *Sin claves, ¿?*

Índice

A13

Cifrado de clave simétrica o secreta



- Bob y Alicia comparten la misma clave K_S
- Problema: ¿cómo se puede transmitir la clave de forma segura?

Cifrado de bloques (I)

- Bloque específico
  - Equivalencia bloque claro ↔ bloque cifrado

Claro	Cifrado	Claro	Cifrado
000	110	100	011
001	111	101	010
010	101	110	000
011	100	111	001

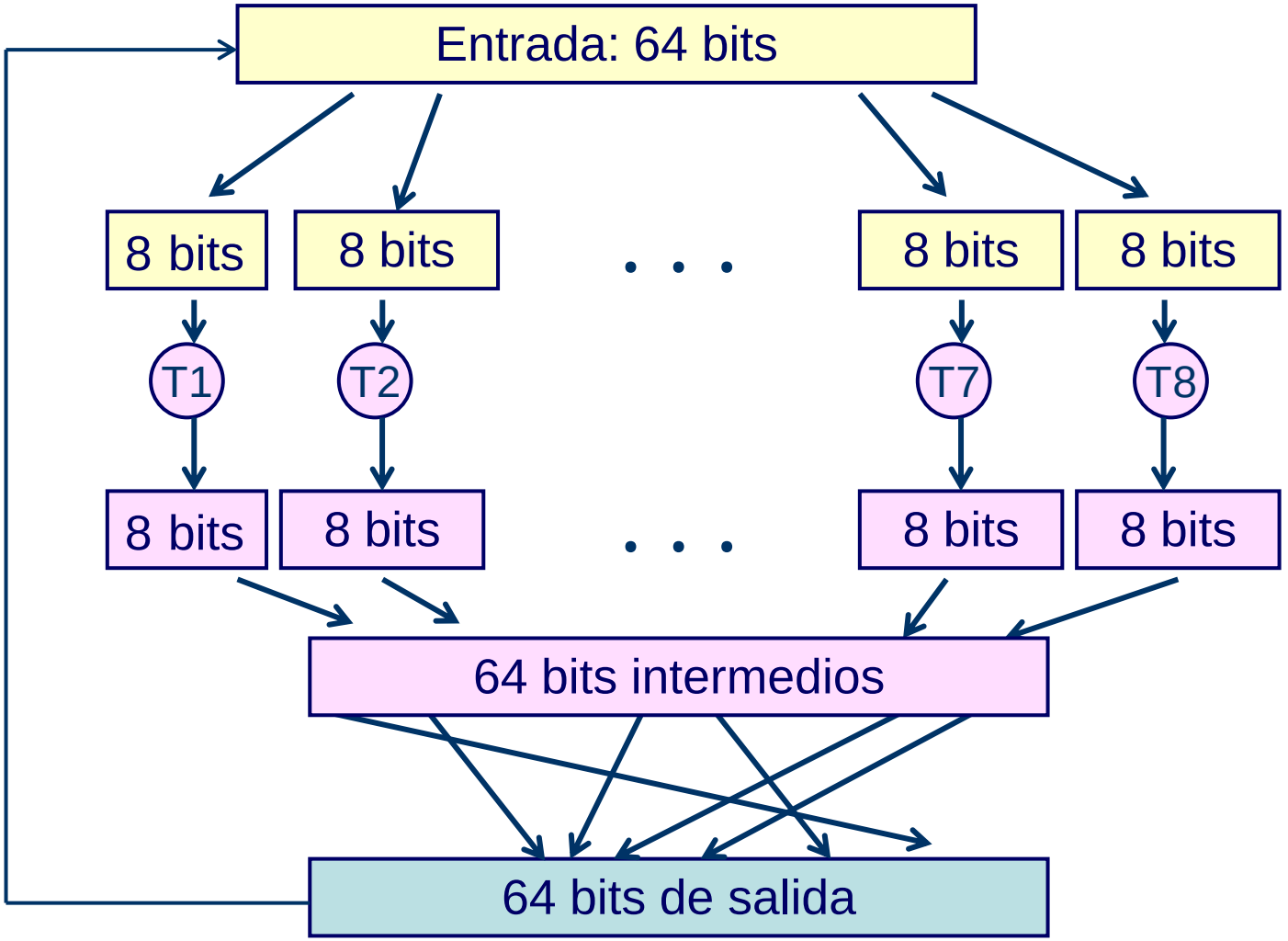
¿Cuál sería el cifrado para 010110001111 ?

  - Inviable para bloques grandes
    - Para bloques de 64 bits sería necesaria una tabla con 2^{64} entradas
    - Se emplean funciones que simulan una permutación aleatoria

Cifrado de bloques (II)

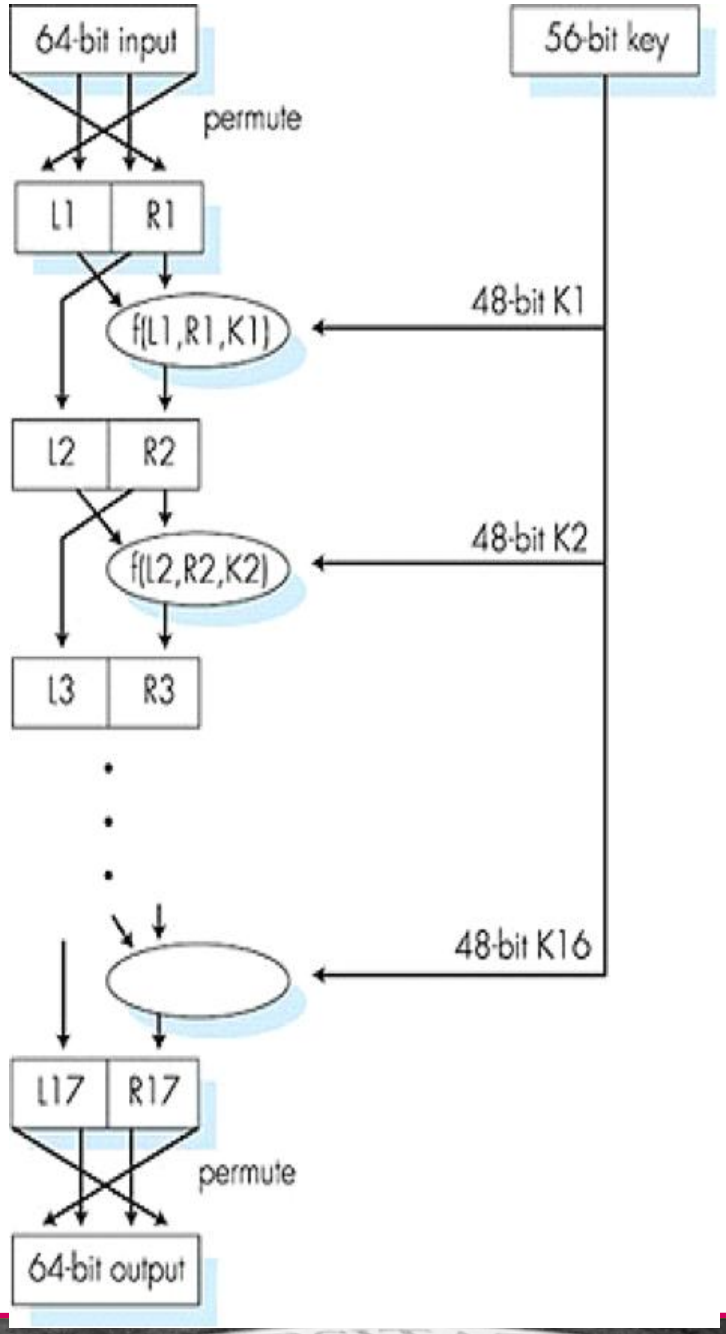
Función prototipo

Bucle de n ciclos



Cifrado de bloques (III)

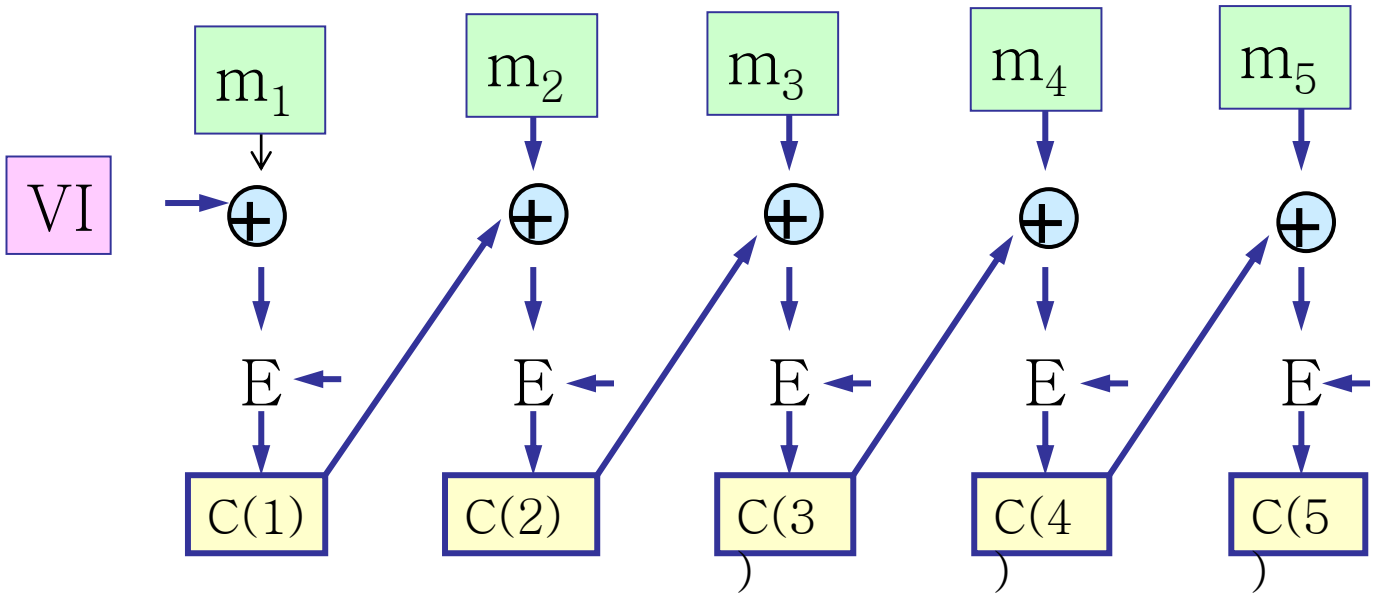
- Las sustituciones y/o el barajado dependen de una clave.
- DES (*Data Encryption Standard*)
  - Bloques 64 bits, clave 56 bits.
- 3DES
  - Clave 168 bits (3x56), se usa como 3 claves de 56 bits
- AES (*Advanced Encryption Standard*)
  - Bloques 128 bits, claves de 128, 192 y 256 bits.



Cifrado de mensajes largos (I)

- Evitar la repetición de bloques
  - Ejemplo: "GET " ó "HTTP/1.1"
- **CBC (*Cipher Block Chaining*)**
  - El emisor genera un **IV** (vector de inicialización) aleatorio y lo envía al receptor (en claro).
  - En vez de cifrar el primer bloque, antes aplica la XOR con el **IV** :
    - $c(1)=K_s(m(1)\ XOR\ IV)$
  - Para cada bloque posterior, aplica a los datos la XOR con el anterior bloque cifrado antes de cifrarlo:
    - $c(i)=K_s(m(i)\ XOR\ c(i-1))$

Encadenamiento de bloques cifrados (CBC)



- Vector de inicialización (VI), c(0)
  - No necesita ser secreto
  - Se cambia en cada sesión, aunque el texto se repita el cifrado será distinto

Clave simétrica: conclusiones

- Permite:
  - Conseguir **confidencialidad** en los mensajes que se transmiten
  - Garantizar la **integridad** de los mensajes
  - Realizar **autentificación**
- Problema:
  - Distribución de una clave común al emisor y al receptor a través de un canal inseguro
- Solución:
  - **Criptografía de clave pública**

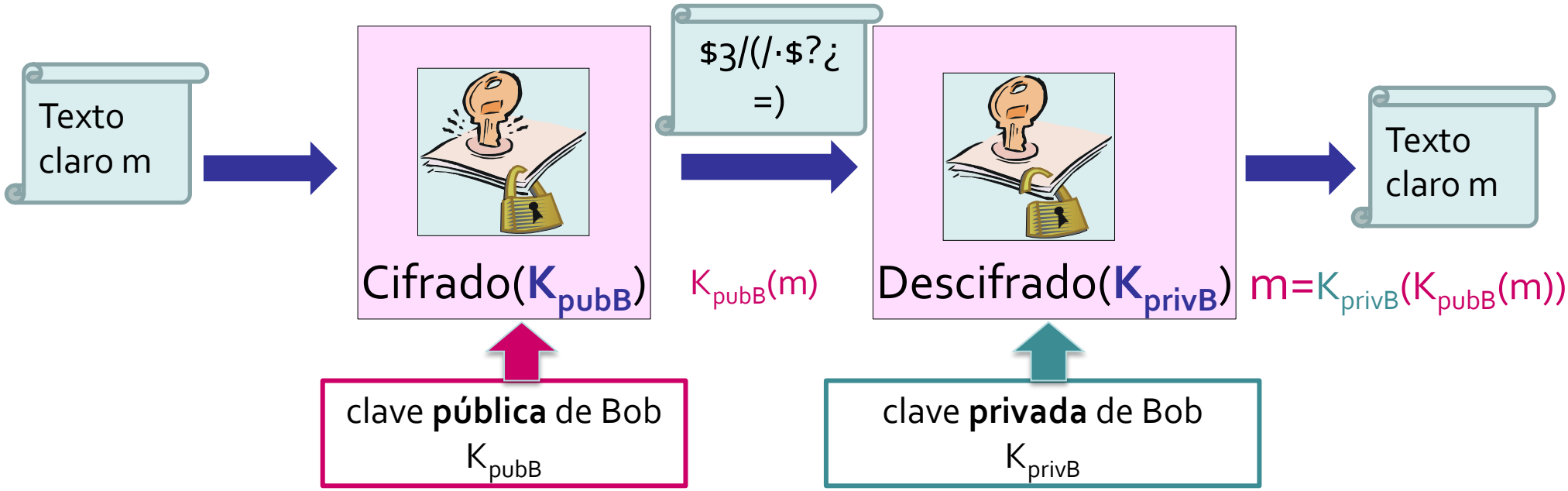
Índice

1. Seguridad en las comunicaciones
2. Principios de criptografía
   i. Criptografía de clave simétrica
   ii. Criptografía de clave pública
3. Integridad de los mensajes
4. Autentificación de terminal
5. Conexiones TCP seguras: SSL

A14

Clave pública: componentes

- Criptografía asimétrica
- Dos claves distintas
  - Pública: disponible para todo el mundo (K_{pub})
  - Privada: la conoce sólo su dueño (K_{priv})
- Cifrado: $m' = K_{pub}(m)$
- Descifrado: $m=K_{priv}(K_{pub}(m))$



Clave pública: autentificación

- Algunos de los algoritmos presentan una interesante propiedad:
  - $K_{pubB}(K_{privB}(m)) = m = K_{privB}(K_{pubB}(m))$
- Cifrar con K_{privB} permite conseguir autentificación y no-repudiación de mensajes
  - **Firmas digitales** (se verán más adelante)

Clave pública: fundamentos

- Mucho más moderna que la criptografía simétrica
  - Primera publicación **Diffie-Hellman**, 1976
- … y mucho más **costosa computacionalmente**
  - Algoritmos basados en asimetrías de problemas matemáticos complejos:
    - **RSA:** aritmética modular de números primos
    - **El Gamal:** problema del logaritmo discreto
    - …
  - Se utiliza en muchos casos para transmitir claves de sesión secretas entre dos sistemas
  - También para conseguir autenticación y no repudio de mensajes (firmas digitales)

Ejemplo: RSA

- p y q son primos muy grandes ($p \cdot q$ del orden de 1024 bits).
- Sea $n=p \cdot q$ y $z=(p-1) \cdot (q-1)$
- Se elige e tal que no tiene ningún múltiplo común con z.
- Se elige d tal que $e \cdot d \mod z = 1$.
- Clave pública = (n, e) ; Clave privada (n, d)
- Cifrado del mensaje m: $c = m^e \mod n$
- Descifrado del mensaje: $c^d \mod n = m^{e \cdot d} \mod n =$
- $= m^{(e \cdot d \mod z)} \mod n = m^1 \mod n = m$
- Para romper el cifrado, hay que averiguar p y q factorizando n.

Clave pública: conclusiones

- El cálculo de este cifrado es muy costoso computacionalmente, por lo que se limita a pequeños bloques de datos:
  - Intercambio de claves secretas
  - Autenticación de terminales
  - Firmas digitales

Índice

1. Seguridad en las comunicaciones
2. Principios de criptografía
   i. Criptografía de clave simétrica
   ii. Criptografía de clave pública
3. Integridad de los mensajes
   i. Funciones hash
   ii. Código de autenticación (MAC)
   iii. Firma digital
   iv. Certificación y distribución de claves
4. Autenticación del punto terminal
5. Conexiones TCP seguras: SSL

A14

3. Integridad y autenticación

- Integridad: Garantizar que el mensaje no se ha modificado en tránsito, accidental o intencionadamente
- Autenticación: Verificar que el origen del mensaje es realmente quién dice ser
- Existen dos tipos de soluciones, basadas en clave secreta o basadas en clave pública

i. Resumen del mensaje

- Cifrar todo el mensaje puede resultar costoso (cálculo y almacenamiento)
- **Solución eficiente**: cifrar un bloque de bits pequeño obtenido a partir del documento (resumen del mensaje), mediante una función (función hash, **H**)
  - Ha de combinarse con otras funciones criptográficas para garantizar la integridad

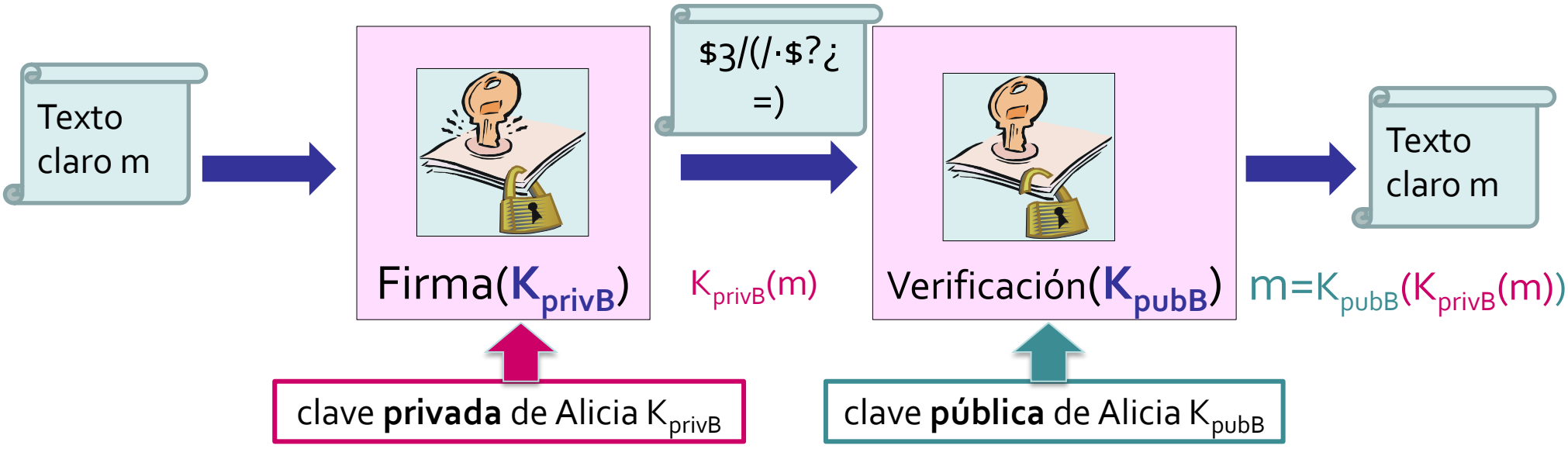
- **Propiedades de H(m)**
  - Salida de longitud fija
  - Fácil de calcular (computacionalmente)
  - Irreversible
  - No se pueden encontrar (computacionalmente) dos mensajes distintos que den el mismo resultado
- Idea similar al *checksum* o a los CRC
- Ejemplos: MD5 (128 bits), SHA-1 (160)

ii. Código de autenticación (MAC)

- Se basa en la existencia de una clave secreta común ***s***. ⟶ Problema de difusión de la clave
- Se genera un MAC (*Message Authentication Code*) que se añade al mensaje
- El receptor evalúa el MAC
- Ejemplo: HMAC:
  - El emisor genera un MAC como el *Hash* (MD5 o SHA-1) del mensaje y de la clave, y lo añade al mensaje.
- Empleado por OSPF (difusión de tablas de encaminamiento.

iii. Firmas digitales

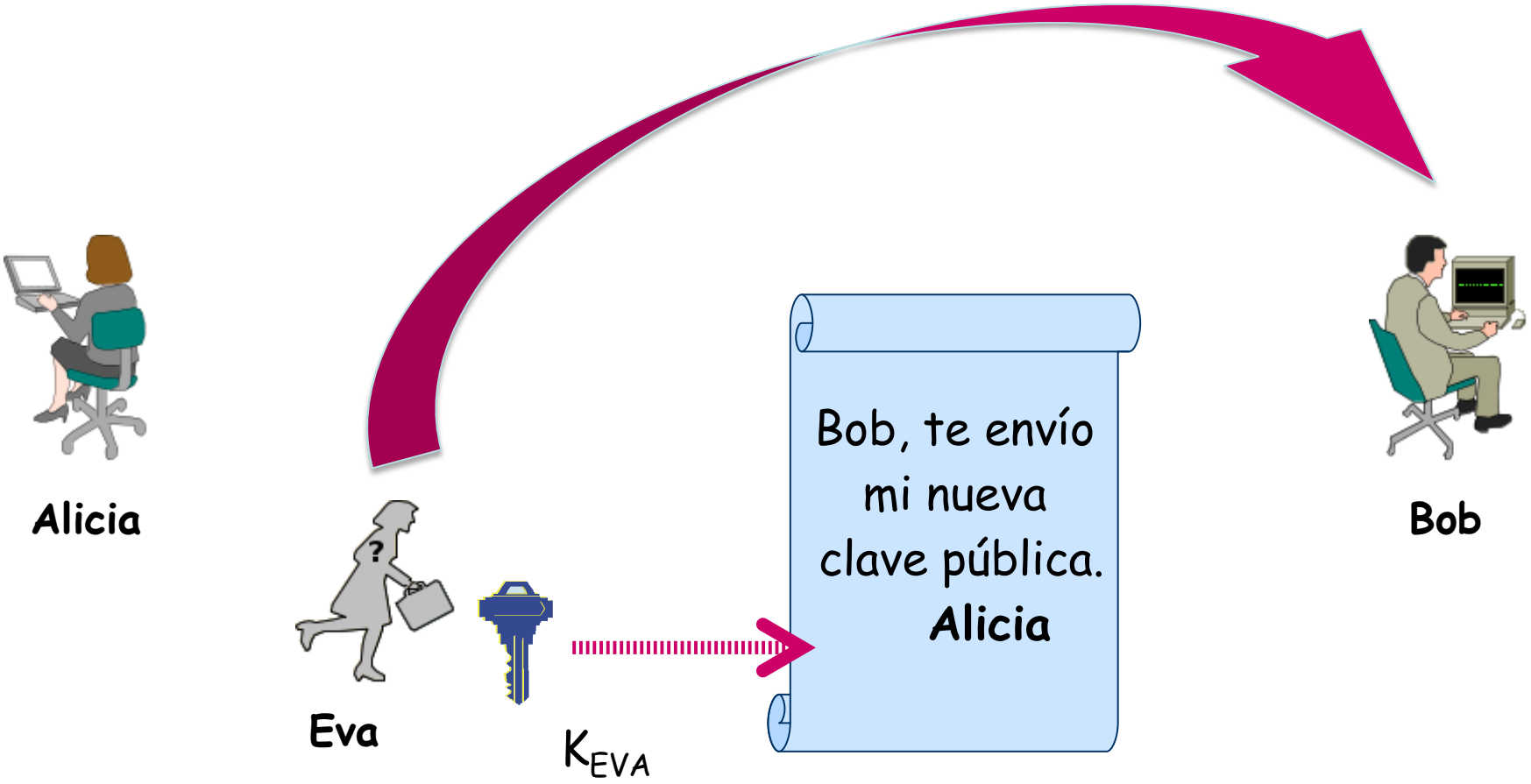
- Basadas en clave pública → Muy costoso.
- Permiten demostrar
  - Quién generó la información
    - Impiden la repudiación del mensaje
  - Que la información no se ha modificado



Firmas digitales con resumen del mensaje

- Para aligerar el coste computacional:
  - Se aplica una función *hash* y se obtiene un resumen del mensaje
  - El resumen se cifra con la clave privada del emisor
- Es el procedimiento más frecuente de firma digital

- ¿Cómo estar seguros de que una clave pública es la correcta?



Certificados digitales (I)

- Sirven para resolver el problema de administrar las claves públicas y para que la identidad del dueño no pueda ser falsificada
  - La identidad del usuario es asegurada por un tercero: la **autoridad certificadora (AC)**
- Partes:
  - Una clave pública
  - La identidad de un implicado
  - La autoridad certificadora

Certificados digitales (II)

clave **privada** de AC

Clave pública
de Bob Pérez

K_{bob}

Clave pública
de Bob Pérez

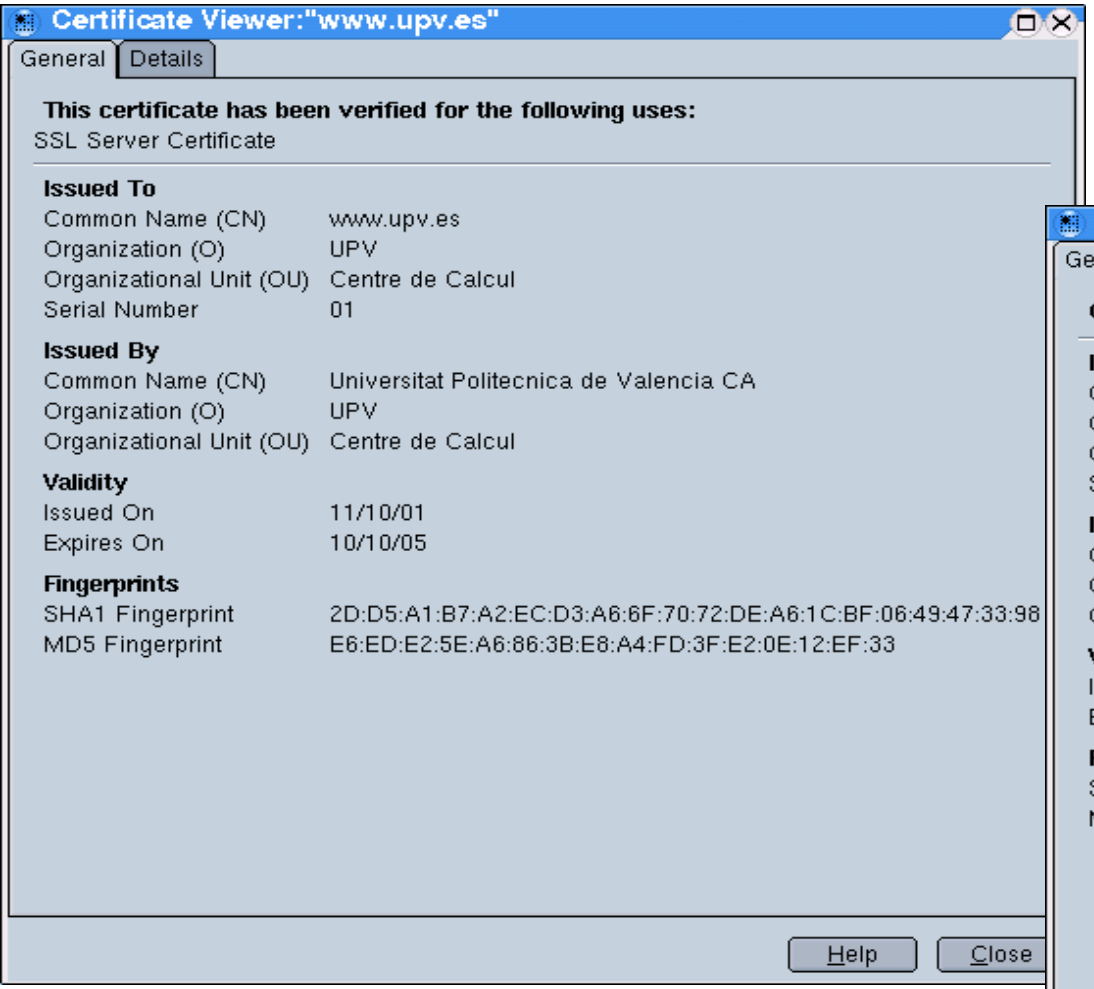
K_{bob}

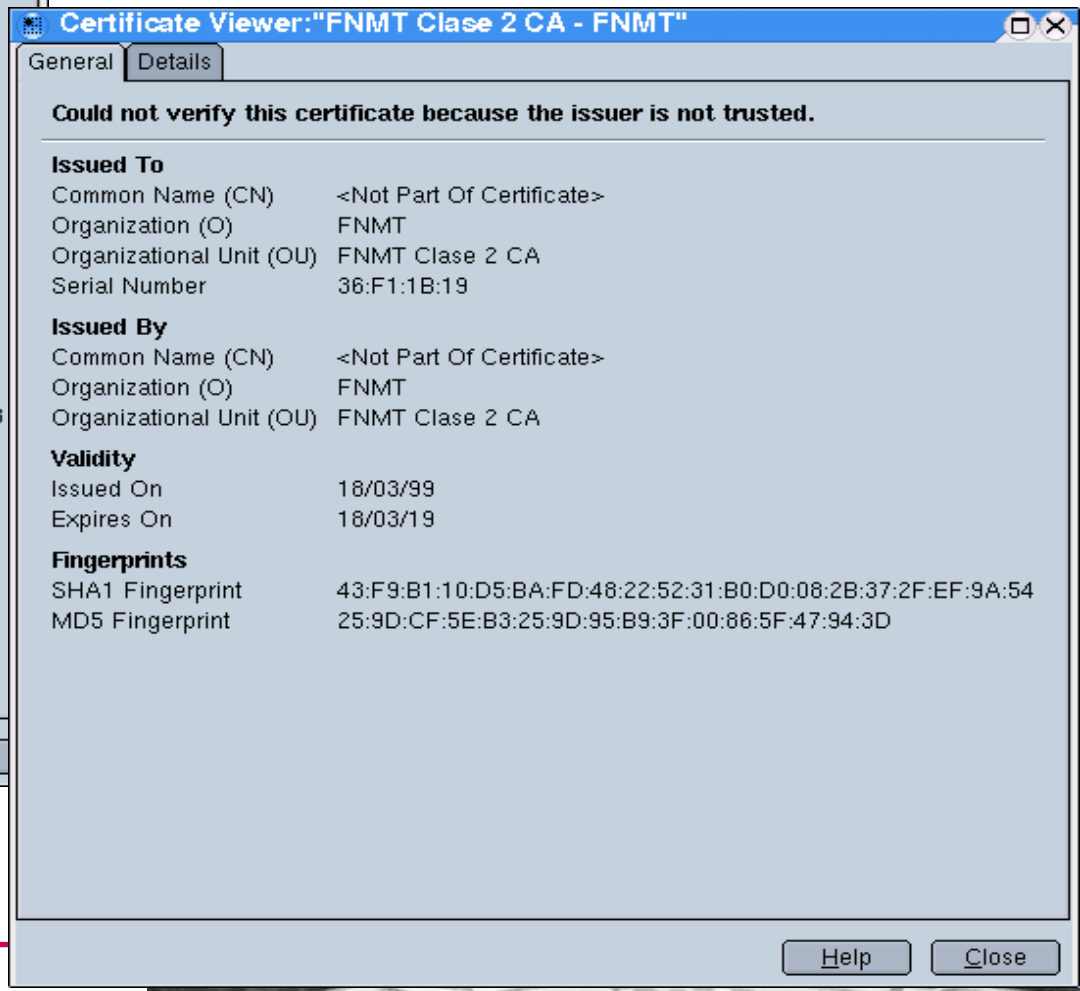
Firma digital de la AC

Bob

Certificado
Bob Pérez

Certificados de un navegador





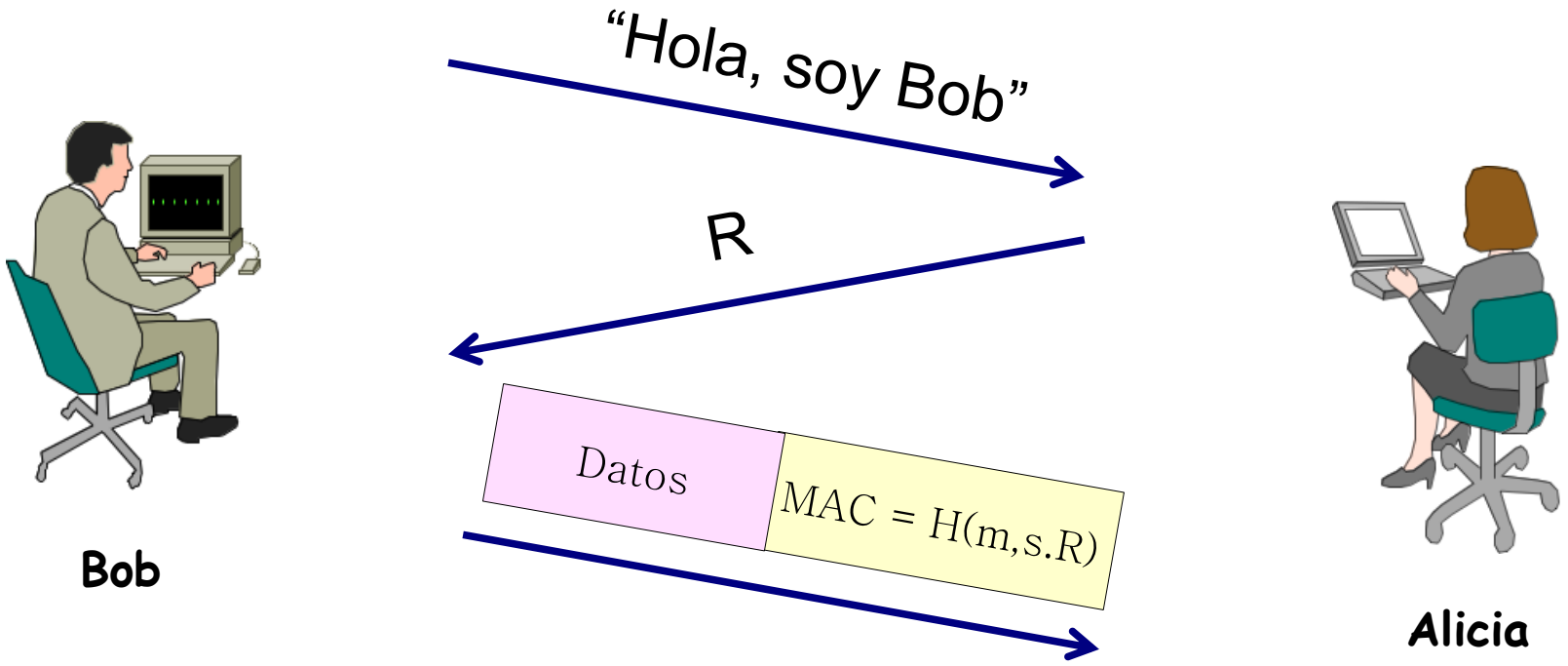
Índice

A14

4. Autentificación del punto terminal

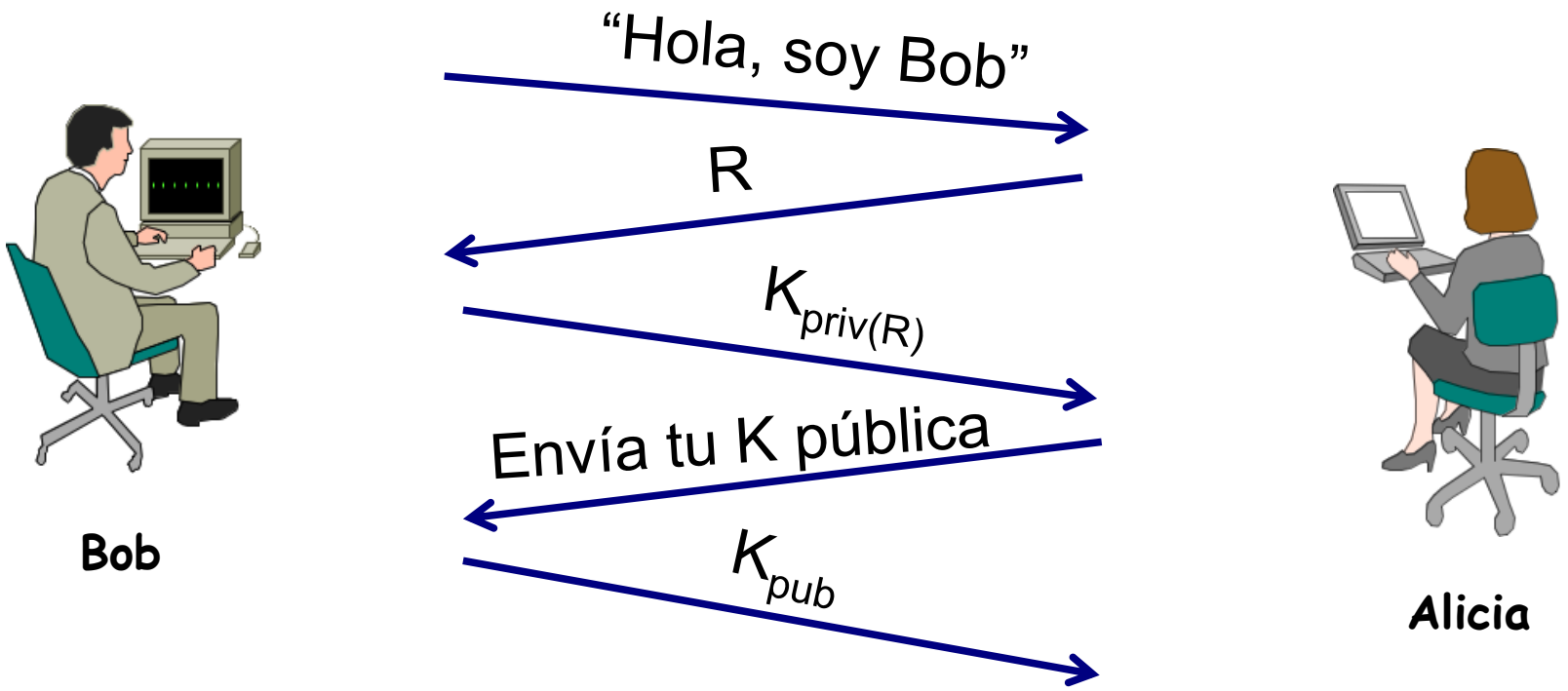
- ¿Cómo es posible saber que el otro extremo es quién afirma ser?
  - Ataques por reproducción
  - Ataques por interposición
- Reproducción:
  - Enviar copia de mensajes válidos anteriores
    - Solución: **números distintivos**

Números distintivos



- R se genera aleatoriamente para cada conexión.
- El MAC se genera como *Hash* del mensaje, la clave secreta y R

Autenticación por clave pública



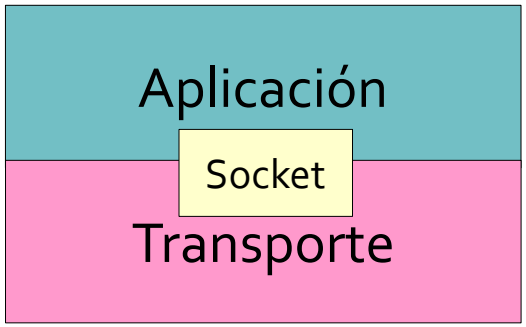
- ¿Suplantación? → Ataques de interposición
  - Certificados digitales.

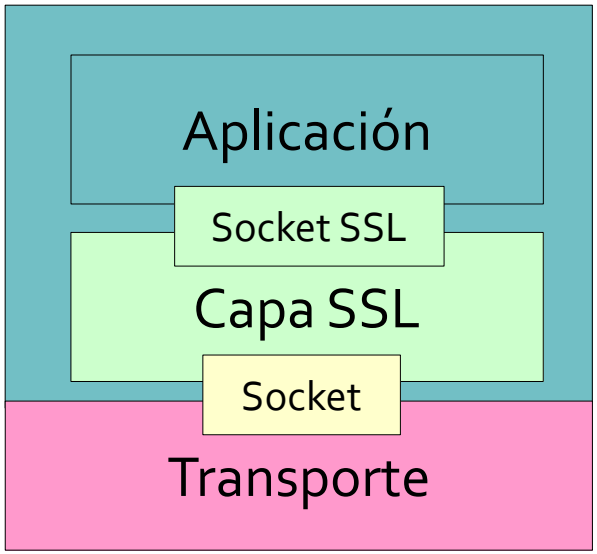
Índice

A15

- ***Secure Sockets Layer* (SSL)**
  - Protocolo de seguridad ampliamente utilizado
    - Soportado por la mayoría de los navegadores y lectores de correo
  - Diseñado originalmente por Netscape (1993)
  - Versión actual 3.0
  - Muy parecido a TLS (*Transport Layer Security*), RFC 5246

SSL y TCP/IP





- Agrega confidencialidad, integridad y autenticación a TCP
  - Con clases y librerías para trabajar en C y en Java de forma similar al API de los *sockets*
  - Se definen puertos estándar diferentes de los habituales

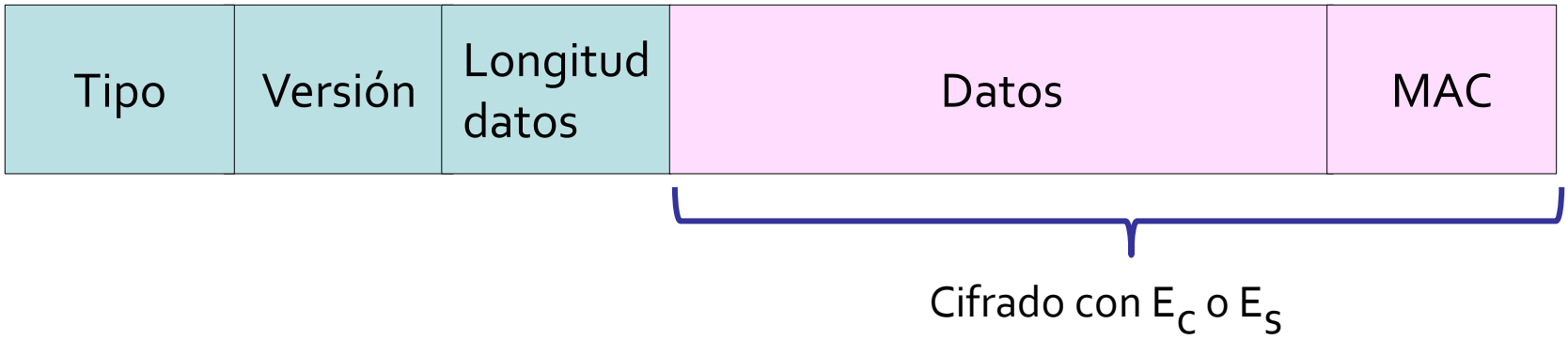
SSL simplificado - Etapas

- Fase de acuerdo
  - Autentificación de C y S mediante certificados
  - Deducción de las claves: a partir de un secreto compartido generan un conjunto de claves de sesión
- Transferencia de datos
  - Divididos en registros
- Cierre de la conexión
  - De forma segura
    - ¿Por qué es necesario si ya existe un cierre a nivel de TCP?

- Fase de acuerdo
  - Establecimiento de la conexión TCP
  - El cliente envía su número distintivo y sus cifrados permitidos.
  - El servidor envía su número distintivo y selecciona de entre ellos:
    - Un cifrado simétrico, uno de clave pública y un algoritmo MAC
  - El servidor envía su certificado
  - El cliente selecciona la clave pre-maestra PMS y la envía cifrada al servidor.

- **Deducción de claves**
  - A partir de la PMS se obtiene la clave maestra (MS) en cada extremo
  - La MS genera cuatro claves distintas:
    - Dos claves de cifrado E_c y E_s
    - Dos claves de MAC M_c y M_s
    - En caso de CBC, dos IV
- El cliente envía un MAC de todos los mensajes de acuerdo.
- El servidor envía un MAC de todos los mensajes de acuerdo.

- **Registros SSL**
  - Los datos se fragmentan en registros



  - El MAC se calcula sobre los 4 campos anteriores, la clave MAC ***M*** y un número de secuencia que se incrementa en cada registro
  - El campo ***tipo*** permite cerrar la conexión de forma segura.
    - Aunque va sin cifrar, está cubierto por el MAC.