


Fundamentos de criptografía. Protocolos criptográficos



Garantía y Seguridad de la Información.

Servicios de seguridad

- ▶ Los servicios de seguridad son capacidades funcionales que intentan contrarrestar las amenazas a la seguridad
 - ▶ Autenticación
 - ▶ Autorización
 - ▶ Integridad
 - ▶ Confidencialidad
 - ▶ No repudio



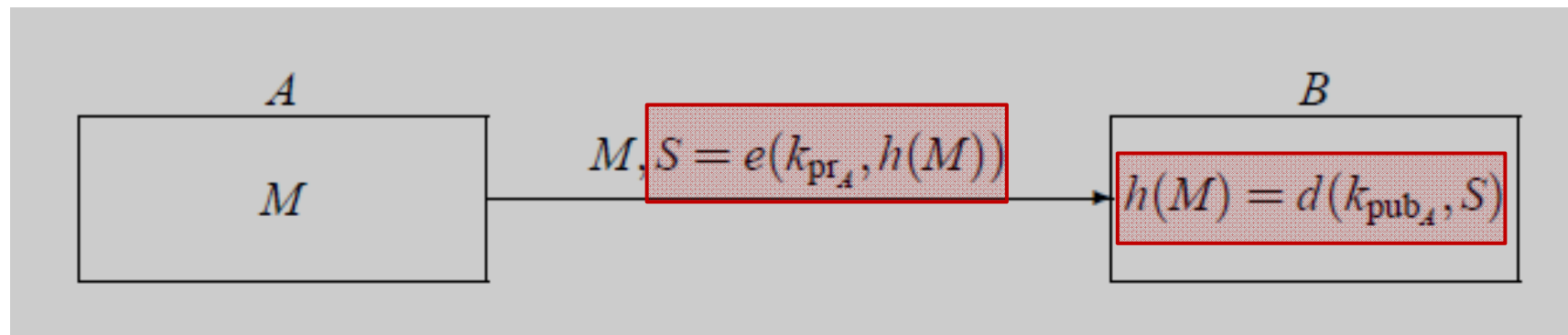
Firma digital



Integridad, No repudio

Firma digital

- ▶ Es un mensaje cifrado con la clave privada del firmante.
- ▶ Lo que se cifra no es el mensaje a firmar, sino solamente su resumen calculado con una función *hash*.



- *B descifra con la clave pública de A y compara su resumen con lo descriptado: si son iguales, nadie ha modificado.*

Firma digital

- ▶ Se ofrecen conjuntamente los servicios de:
 - ▶ **No repudio**, nadie excepto A podría haber firmado el documento
 - ▶ **Autenticidad**, si el documento viene firmado por A, podemos estar seguros de su identidad, sólo él ha podido firmarlo
 - ▶ **Integridad del documento**, en caso de ser modificado, no se generaría la misma función de resumen
- ▶ No ofrece confidencialidad

Infraestructura de clave pública (PKI)

- ▶ ¿Cómo saben emisor y receptor que las claves públicas del otro son las correctas?
 - ▶ Un espía engaña al emisor dándole su propia clave pública, haciéndole creer que se trata de la del receptor.
 - ▶ Si el espía logra interceptar un mensaje puede emplear ahora su clave privada para descifrarlo.

Certificado digital

- ▶ Documento electrónico que usa la firma digital de una tercera parte de confianza
 - ▶ vincular una clave pública con una identidad (nombre de una persona u organización, dirección, e-mail...)
 - ▶ firmado (clave privada) por un tercero de confianza
- ▶ Permite verificar que una clave pública pertenece a un individuo, organización o servicio
 - ▶ Proporciona no repudio

Infraestructura de clave pública (PKI)

- ▶ Existe una entidad de confianza que asegura
 - ▶ La clave pública es de su propietario
- ▶ Firma con su clave privada un documento que afirma “la clave pública de A es k_{pub_A} ”
- ▶ Lo publica para que todos los usuarios lo sepan
- ▶ Este documento es un Certificado de Clave Pública
- ▶ La entidad es una Autoridad de Certificación

Infraestructura de clave pública (PKI) (I)

- ▶ La Autoridad de Certificación (**CA** [Certificate Authority]): **emitir certificados**.
- ▶ La Autoridad de Registro (**RA** [Registration Authority]): **asegurar que el solicitante del certificado es quien dice ser** (físicamente).
- ▶ La Autoridad de Validación (**VA** [Validation Authority]): **comprobar la validez** de los certificados emitidos.
- ▶ Los **repositorios**. Son **almacenes** de certificados.
 - ▶ repositorio de certificados activos
 - ▶ repositorio de listas de revocación de certificados

Infraestructura de clave pública (PKI) (II)

- ▶ El emisor envía su clave pública, junto con el certificado digital al receptor para que descifre el diálogo que van comenzar
 - ▶ autenticación usuario/contraseña,...
 - ▶ El receptor, antes de utilizar la clave pública, necesita comprobar que el emisor es quien dice ser.
 - ▶ El certificado digital ha sido firmado por una CA oficial utilizando su clave privada.
- ▶ El receptor puede verificar el certificado utilizando la clave pública de la CA (la tiene o se conecta con la VA).
 - ▶ Si el certificado es correcto, la clave pública del emisor también lo es y se inicia el diálogo con toda confianza.

Infraestructura de clave pública (PKI) (III)

- ▶ Hay distintos formatos de certificados
- ▶ El más usado es el **X.509**, especificado en la definición del servicio de directorio X.500.
- ▶ Certificado digital (**estándar X.509**):
 - ▶ Quién firma, para quién firma, qué usos tiene la clave (cifrado y firmado, solo firmado, etc.), en qué fecha se firmó, cuándo caduca esa firma, qué algoritmos se han utilizado, etc.

Infraestructura de clave pública (PKI) (IV)

- ▶ Los certificados tienen un período de validez. Si dejan de ser válidos dentro de ese período, es necesario revocarlos.
- ▶ Razones para la revocación:
 - ▶ Se sospecha que la clave privada del usuario está comprometida.
 - ▶ El usuario ya no está certificado por esa AC.
 - ▶ Se sospecha que el certificado de la AC está comprometido.

Infraestructura de clave pública (PKI) (V)

- ▶ **Autoridades de certificación. Características**
 - ▶ Cualquier usuario con acceso a la clave pública de la AC puede verificar la clave pública del usuario que fue certificada.
 - ▶ Sólo la AC puede modificar el certificado sin que esto se detecte.
 - ▶ Se evita la necesidad de un repositorio de acceso común.

Infraestructura de clave pública (PKI) (y VI)

► Vulnerabilidades:

- Un virus en el ordenador puede alterar el depósito de claves e importar claves públicas de **CA fraudulentas**.
- Un **ataque a una CA** podría robar su clave privada.
 - El atacante firma las claves públicas de servidores peligrosos y los clientes se conectarían a ellos confiando en que es una firma legal.



Servicio de autenticación



Servicio de autenticación

- ▶ Autenticación: Nadie ha falsificado la comunicación.
- ▶ **Autenticación de mensaje o autenticación de origen de datos**
 - ▶ confirmar que el emisor, A , de un mensaje es auténtico
 - ▶ *el mensaje no ha sido generado por un tercero Z que quiere hacer creer que lo ha generado A .*
- ▶ **Autenticación de entidad**
 - ▶ confirmar la identidad de un participante A en una comunicación
 - ▶ *no se trata de un tercero Z que dice ser A .*

Autenticación de origen de datos

- ▶ Autenticación de mensaje
 - el mensaje no ha sido generado por un tercero Z que quiere hacer creer que lo ha generado A*
- ▶ Firmas digitales
 - ▶ criptografía asimétrica
- ▶ Códigos de autenticación de mensaje o MAC (Message Authentication Code),
 - ▶ criptografía simétrica

Message Authentication Code, MAC

- ▶ Porción de información utilizada para autenticar un mensaje.
- ▶ Se adjunta una etiqueta o código de autenticación de mensaje (*Message Authentication Code*, MAC) a cada mensaje o paquete.
 - ▶ El mensaje mismo (y el MAC) puede ser cifrado o no

Propiedades del MAC

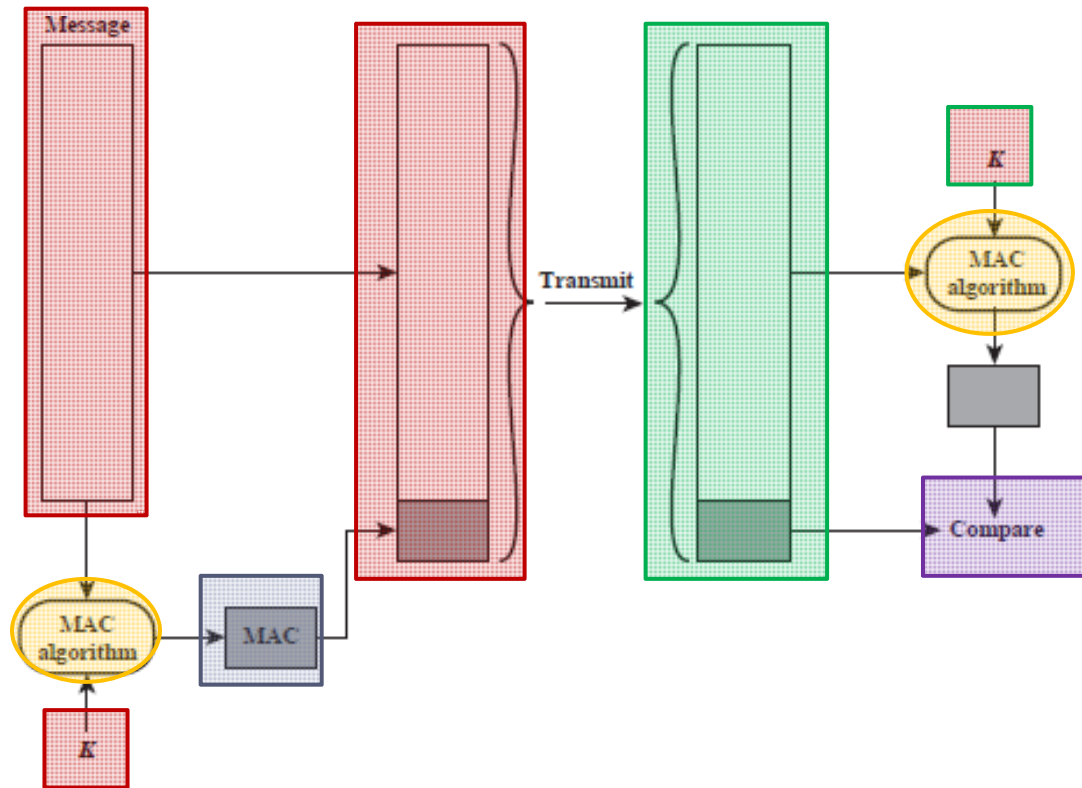
- ▶ Función, a , con dos entradas:
 - ▶ Un mensaje M de longitud arbitraria
 - ▶ Una clave secreta k compartida por el emisor y el receptor del mensaje
- ▶ Obtenemos un código, $C_{MAC} = a(k, M)$, de longitud fija.
 - ▶ **Propiedades de la función a :**
 - ▶ Es computacionalmente inviable encontrar un mensaje $M' \neq M$ que dé el mismo código
 - ▶ Es inviable obtener el código de un mensaje cualquiera sin conocer la clave

Propiedades del MAC

- ▶ Dado un par (M, C_{MAC}) un atacante no puede obtener otro par (M', C_{MAC})
- ▶ El código MAC sirve como prueba de autenticidad del mensaje.
 - ▶ Ese código MAC sólo puede provenir de M
 - Si A envía mensajes a B autenticados con una **clave compartida**, sólo B podrá verificar la autenticidad de estos mensajes.
 - Si A denegase la autoría de un mensaje autenticado, B no podría demostrar delante de un tercero imparcial que el mensaje lo generó A (**pudo generarlo B**)
 - ▶ El no repudio está garantizado por la firma digital

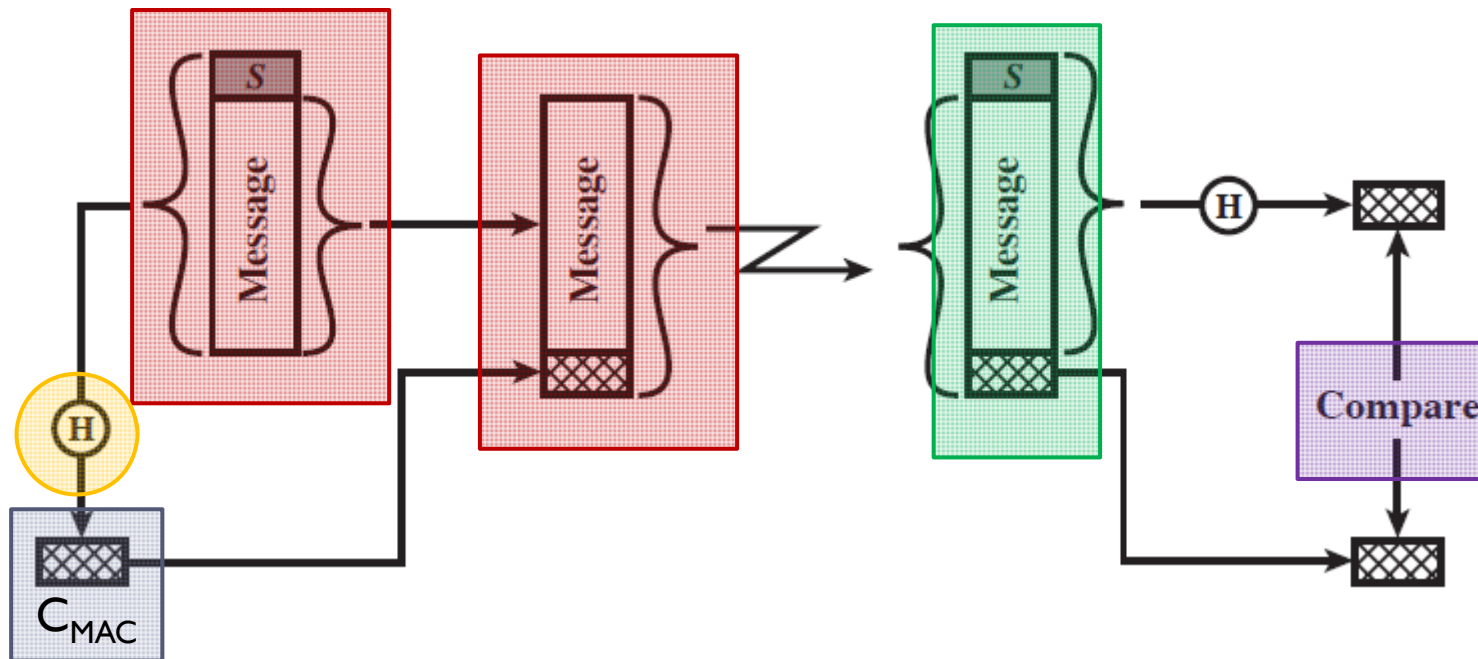
Algoritmos MAC (I)

- ▶ Aplicar al mensaje M un cifrado en bloque en modo CBC con la clave k , tomando el último bloque cifrado como código C_{MAC}



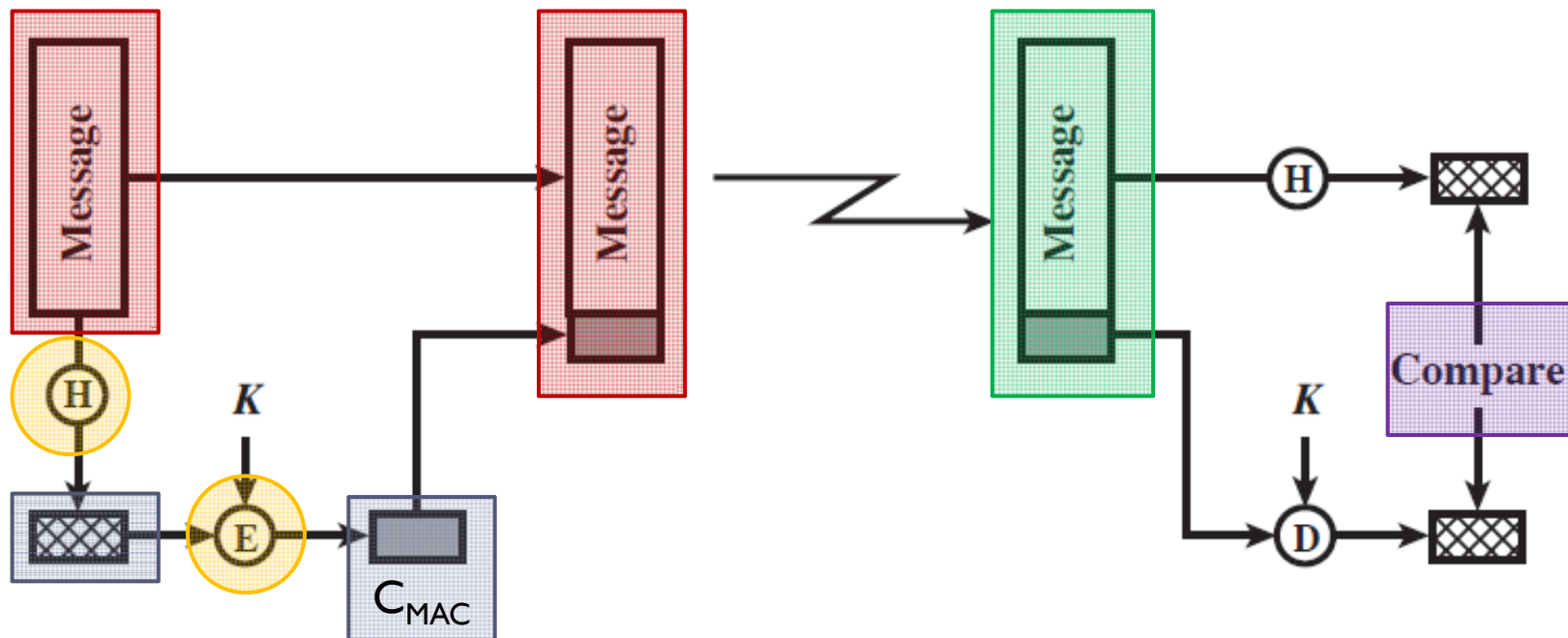
Algoritmos MAC (III)

- Calcular el resumen hash concatenando el mensaje y la clave, S , y el resumen es el código C_{MAC}



Algoritmos MAC (IV)

- Calcular el resumen hash del mensaje y cifrarlo con la clave, K , y el resumen es el código C_{MAC}



Algoritmos MAC (y V)

▶ HMAC

- ▶ Al mensaje se le añade como prefijo una cadena de bits derivada de la clave
- ▶ Se calcula su *hash*
- ▶ Al resultado se le prefija otra cadena de bits derivada de la clave
- ▶ Se vuelve a calcular el *hash*.
- ▶ Elegido como MAC de implementación obligatoria para IPsec
- ▶ Usado en otros protocolos de Internet, como TLS

Autenticación de entidad

- ▶ La autenticación de entidad
 - ▶ confirmar la identidad de un participante A en una comunicación
 - ▶ *no se trata de un tercero Z que dice ser A.*
- ▶ Es un requisito para permitir el acceso a un recurso restringido.
- ▶ Se utiliza cuando en una comunicación una de las partes quiere asegurarse de la identidad de la otra.

Autenticación de entidad (*usuarios*)

- ▶ Para la identificación de un usuario A:
 - ▶ Algo que A *sabe*: una contraseña o una clave privada.
 - ▶ Algo que A *tiene*: una tarjeta con banda magnética o con chip.
 - ▶ Algo que A *es*: alguna propiedad inherente a A, sus características biométricas.
- ▶ Se identifica en tiempo real

Autenticación de entidad (*sistemas*)

- ▶ Los métodos de autenticación tradicionales no son adecuados para su uso en redes de ordenadores
 - ▶ los atacantes supervisan el tráfico de la red para interceptar contraseñas y romper la seguridad del sistema.
- ▶ Enfoques posibles
 - ▶ Centros de distribución clave (KDC). Kerberos.
 - ▶ Infraestructuras de clave pública (PKI).
- ▶ Protocolos AAA
 - ▶ RADIUS
 - ▶ Diameter
 - ▶ SET



Kerberos



Kerberos. ¿Qué es?

- ▶ El sistema Kerberos se desarrolló en la década de 1980 en el Instituto de Tecnología de Massachusetts (MIT) para el Proyecto Athena
- ▶ La versión 4 se lanzó a fines de la década de 1980.

Kerberos. ¿Qué es?

- ▶ Es un protocolo de autenticación en redes de ordenadores.
- ▶ Permite a dos ordenadores en una red insegura demostrar su identidad mutuamente de manera segura.
- ▶ Se basa en criptografía simétrica y requiere un tercero de confianza.

Kerberos

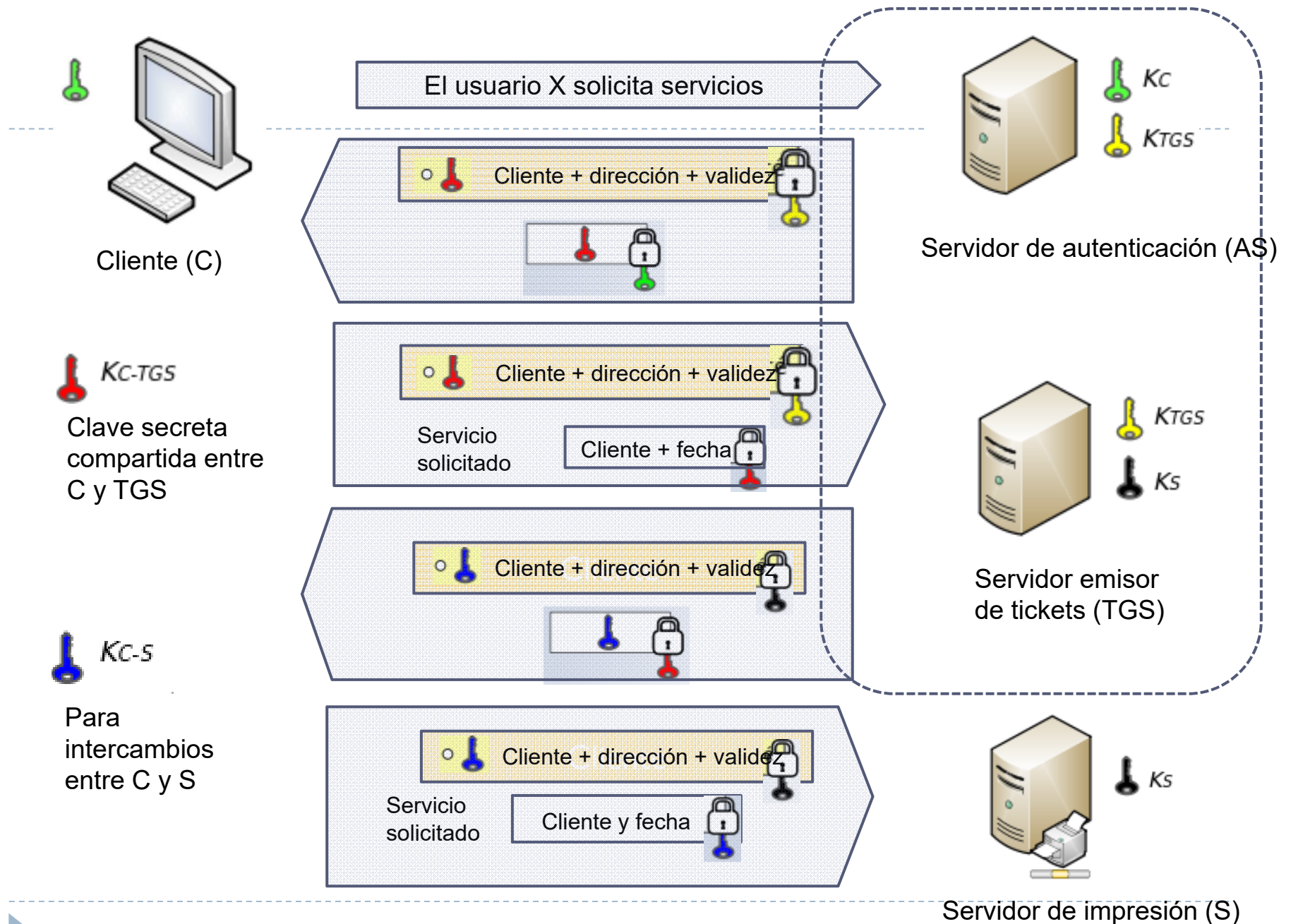
- ▶ Los clientes quieren utilizar servicios de los servidores.
- ▶ Existe un mecanismo central, llamado centro de distribución de claves (KDC)
 - ▶ un servidor de autenticación (AS)
 - ▶ un servidor de autorización, servidor emisor de tickets (TGS)
 - ▶ Los tickets sirven para demostrar la identidad de los usuarios.

Kerberos. ¿Cómo funciona? (I)

- ▶ Cada cliente tiene una clave secreta única que sólo conoce el cliente y el KDC.
 - ▶ El conocimiento de esta clave sirve para probar la identidad del cliente.
- ▶ El AS (servidor de autenticación) tiene registrados a todos los usuarios
- ▶ Cada servidor de servicios (SS) comparte una clave con el AS.

Kerberos. ¿Cómo funciona? (II)

- ▶ El cliente se autentica ante el AS (*autenticación*)
- ▶ Demuestra al TGS (*emisor de tickets*) que está autorizado a recibir un ticket de servicio (y lo recibe)
- ▶ Ya puede demostrar al SS (*servicios*) que ha sido aprobado para hacer uso del servicio.
- ▶ Hace uso de él.



- ▶ El cliente tiene una clave secreta que es conocida por el AS.
- ▶ El AS verifica la identidad del cliente.

-
- ▶ El AS le envía un ticket. Este ticket le autoriza a hacer peticiones al TGS y está cifrado con la clave del TGS y contiene la clave a utilizar entre el cliente y el TGS.
 - ▶ Le envía, también, la clave a utilizar entre el cliente y el TGS, cifrada con la clave del cliente.
 - ▶ El cliente tiene un ticket (que no puede descifrar) y una clave.

- ▶ En la siguiente etapa, el cliente envía el ticket recibido (indescifrable para él) y otro ticket con su identificador y la fecha de emisión, cifrado con la clave secreta compartida entre él y el TGS
- ▶ El TGS recibe esto y puede obtener la clave secreta compartida entre C y TGS y el contenido del ticket, verificando la autenticidad de la petición.

- ▶ El TGS emite un ticket de acceso al servidor cifrado con la clave secreta del servidor y se le envía al cliente, junto con la clave de sesión entre el cliente y el servidor, cifrada con la clave que comparte C y TGS.

- ▶ En la última etapa, el cliente envía el ticket recibido (indescifrable para él) para acceder al servidor y otro ticket con su identificador y la fecha de emisión, cifrado con la clave de sesión entre él y el servidor.
- ▶ El servidor verifica que el ticket es válido y autoriza el acceso al servicio.



Kerberos (paso a paso)

1. Un usuario introduce su nombre de usuario y password en el cliente.
2. El cliente genera una clave hash a partir del password y la usa como la **clave secreta del cliente**.
3. El cliente envía un mensaje en texto plano al AS solicitando servicio en nombre del usuario.
 - ▶ Un mensaje de ejemplo podría ser "El usuario XYZ solicita servicios".
 - ▶ Ni la clave secreta ni el password son enviados, sólo la petición del servicio.

Kerberos (paso a paso)

4. El AS comprueba si el cliente está en su base de datos. Si es así, envía dos mensajes al cliente:

Mensaje A: **Clave secreta TGS/cliente** usando **la clave secreta AS/cliente**.

Mensaje B: Ticket (ID de cliente, dirección de red del cliente, período de validez y **clave secreta compartida por TGS con el cliente**) cifrado usando la **clave secreta TGS/AS**.

Kerberos (paso a paso)

5. Una vez que el cliente ha recibido los mensajes, descifra A para obtener la **clave secreta TGS/cliente**.

Esta clave se usa para las posteriores comunicaciones con el TGS.

El cliente no puede descifrar el mensaje B.

En este momento el cliente ya se puede autenticar ante el TGS.

6. El cliente envía los siguientes mensajes al TGS:

Mensaje C: Ticket del mensaje B y el ID del servicio solicitado.

Mensaje D: Autenticador (compuesto por el ID de usuario en el cliente y una marca de tiempo), cifrado usando la **clave secreta TGS/cliente**.

Kerberos (paso a paso)

7. El TGS descifra el mensaje D (autenticador) usando la **clave secreta TGS/cliente** y envía los siguientes mensajes al cliente:

Mensaje E: Ticket cliente-a-servidor (ID de usuario en el cliente, dirección de red del cliente, período de validez y **clave secreta cliente/servidor** para la duración de la sesión) cifrado usando la clave secreta TGS/servidor.

Mensaje F: La clave secreta cliente/servidor para la duración de la sesión cifrada usando la **clave secreta TGS/cliente**.

Kerberos (paso a paso)

8. El cliente recibe los mensajes E y F, ya tiene suficiente información para autenticarse ante el servidor de aplicaciones. El cliente se conecta al servidor y envía los siguientes mensajes:

Mensaje E del paso anterior.

Mensaje G: un nuevo autenticador que incluye el ID del usuario en el cliente, una marca de tiempo, cifrado usando la **clave secreta cliente/servidor** para la duración de la sesión.

Kerberos (paso a paso)

9. El servidor descifra el ticket usando su propia clave secreta (compartida con TGS) y envía el siguiente mensaje al cliente para confirmar su identidad:

Mensaje H: la marca de tiempo encontrada en el último autenticador recibido del cliente más I, cifrado usando la **clave secreta cliente/servidor** para la duración de la sesión.

Kerberos (paso a paso)

10. El cliente descifra la confirmación usando la clave y comprueba si la marca de tiempo está correctamente actualizada. Si es así, el cliente confiará en el servidor y podrá comenzar a usar el servicio que este ofrece.
11. El servidor provee del servicio al cliente.

Problemas de Kerberos

- ▶ Cualquier programa que lo utilice ha de ser modificado para poder funcionar correctamente
 - ▶ “*kerberización*”
 - ▶ Modificación para comunicación con el KDC.
- ▶ Gran centralización del sistema.
 - ▶ Se ha de disponer en todo momento del servidor Kerberos.
- ▶ Casi toda la seguridad reside en el servidor que mantiene la base de datos de claves.
- ▶ Uso de timestamps como prueba.
 - ▶ Todas las máquinas mínimamente sincronizadas.
- ▶ Utiliza cifrado simétrico con el algoritmo DES.



Aplicaciones para comunicaciones seguras



Otras protecciones con criptografía

- ▶ Introducir seguridad en los protocolos de transporte en una red.
 - ▶ Protocolo SSL o de otros basados en SSL.



Protocollo SSL



Secure Sockets Layer

Protocolo SSL

- ▶ Es un protocolo de seguridad a nivel de transporte
 - ▶ permite establecer conexiones seguras a través de redes inseguras, como Internet
- ▶ Protege las conexiones entre clientes y servidores web con el protocolo HTTP

Protocolo SSL

- ▶ Es un protocolo de seguridad a nivel de transporte
 - ▶ permite establecer conexiones seguras a través de redes inseguras, como Internet
- ▶ Proteger las conexiones entre clientes y servidores web con el protocolo HTTP.
 - ▶ el cliente se ha conectado al servidor auténtico,
 - ▶ puede enviarle datos confidenciales
 - ▶ un número de tarjeta de crédito
 - ▶ nadie más que el servidor sería capaz de ver

Protocolo SSL (TSL)

- ▶ *Transport Layer Security (TLS)*
 - ▶ es el protocolo sucesor de SSL
 - ▶ se lanzó en 1999 como una versión mejorada de SSL 3.0
 - ▶ la versión actual es TLS 1.3 (desde 2018).

Servicios de seguridad proporcionados

- ▶ **Confidencialidad**
 - ▶ una clave para los paquetes del cliente al servidor
 - ▶ otra clave para los paquetes en sentido contrario
- ▶ **Autenticación de entidad.**
 - ▶ el cliente confirma la identidad del servidor mediante firmas digitales y certificados digitales.
- ▶ **Autenticación de mensaje.**
 - ▶ cada paquete va cifrado y puede incorporar un código MAC

Servicios de seguridad proporcionados

- ▶ **Confidencialidad**

- ▶ Cliente y servidor acuerdan qué claves utilizarán para cifrar los datos.
- ▶ Dos claves distintas:
 - ▶ una para los paquetes del cliente al servidor
 - ▶ otra para los paquetes en sentido contrario
- ▶ Intercambio de claves mediante criptografía asimétrica.
 - ▶ El algoritmo concreto para este intercambio también se negocia al inicio de la conexión.

Servicios de seguridad proporcionados

- ▶ **Autenticación de entidad.**
 - ▶ el cliente confirma la identidad del servidor mediante firmas digitales
 - ▶ el cliente necesita conocer la clave pública del servidor
 - ▶ se utilizan certificados digitales.
 - ▶ **la autenticación del cliente frente al servidor.**
 - ▶ normalmente, las aplicaciones utilizan su propio método de autenticación.

Servicios de seguridad proporcionados

- ▶ **Autenticación de mensaje.**
 - ▶ cada paquete va cifrado
 - ▶ y puede incorporar un código MAC
 - ▶ el destinatario comprueba que nadie ha modificado el paquete (integridad).
 - ▶ Las claves secretas para el cálculo de los códigos MAC (una para cada sentido) se acuerdan de forma segura en inicio

Funcionamiento de SSL

- ▶ Existe una negociación inicial para
 - ▶ **autenticar** el servidor y, acaso, el cliente, mediante sus certificados
 - ▶ establecer las **claves** de sesión
 - ▶ establecer las **claves** para el cifrado simétrico de los datos
 - ▶ establecer las **claves** para los códigos MAC

Protocollo SSH

Secure Shell

Protocolo SSH

- ▶ Desarrollado en 1995 por Tatu Ylönen.
- ▶ Es un protocolo de red que permite establecer un canal seguro entre dos dispositivos de red.
- ▶ Diseñado para ofrecer una alternativa segura a Telnet y FTP.

Protocolo SSH

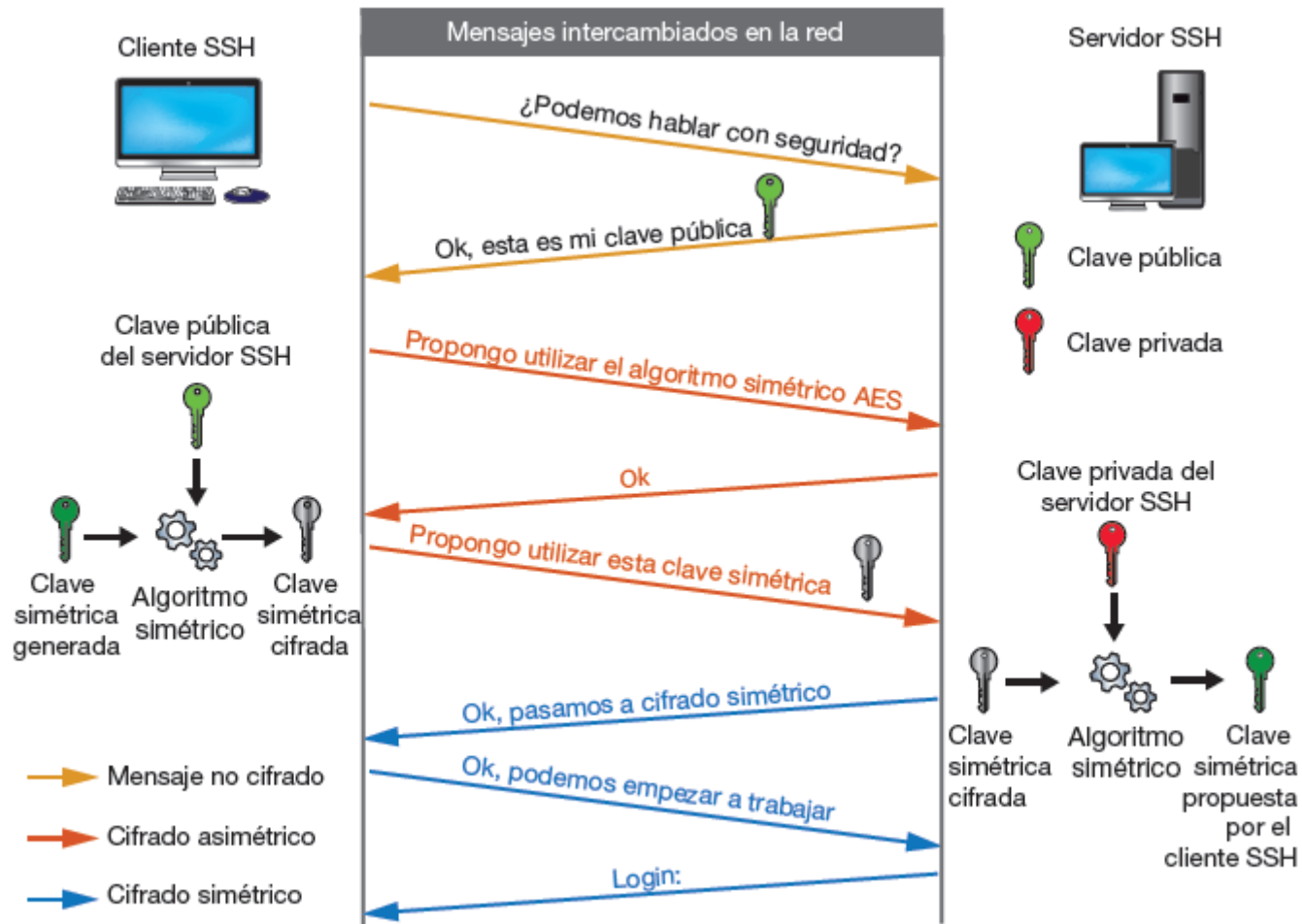
- ▶ Provee los siguientes servicios de seguridad:
 - ▶ **Autenticación:** El cliente puede verificar que se está conectando al servidor al que indicó.
 - ▶ **Confidencialidad:** Los datos intercambiados se transmiten usando cifrado.
 - ▶ **Integridad:** Se verifica la integridad de los datos intercambiados mediante hash.

Esquema básico de cifrado en SSH

- ▶ Criptografía asimétrica en el inicio de la sesión
 - ▶ acordar la clave simétrica aleatoria.
- ▶ Criptografía simétrica durante la transmisión
 - ▶ utilizando la clave simétrica acordada.
- ▶ Se cambia la clave simétrica cada cierto tiempo (minutos)
 - ▶ dificultar más el espionaje de la conversación.

- A quiere establecer una conversación con B
- En A se genera una nueva clave simétrica (CS).
- Para enviársela a B de modo seguro, A la cifra utilizando un algoritmo asimétrico con la clave pública de B.
- Cuando B recibe la CS cifrada, la descifra con su clave privada
- El diálogo sigue cifrando con el algoritmo simétrico acordado y la CS recibida.

Esquema básico de cifrado en SSH



Esquema básico de cifrado en SSH con CA

