



CONCEPTOS DE SEGURIDAD EN REDES

Objetivos



- Conceptos y terminología Básica de Seguridad
- Modelo de seguridad en redes
- Conceptos de Criptografía
- Cifrado simétrico
- Criptografía de Clave Pública
 - Hash
 - Firmas Digitales
 - Certificados
- Seguridad IP
 - IPSEC
- Seguridad en la WEB
 - SSL

Definiciones




- **Seguridad Informática:** nombre genérico para el conjunto de herramientas diseñado para proteger los datos
- **Seguridad de Red:** medidas para proteger los datos durante su transmisión.
- **Seguridad de Internet:** Consiste de medidas para determinar, prevenir, detectar, y corregir violaciones a la seguridad que involucren transmisión de la información

Arquitectura de seguridad OSI



- ITU-T X.800 Security Architecture for OSI
 - define una forma sistemática de enmarcar y proveer requerimientos de seguridad
 - nos provee de una útil, aunque abstracto, visión general de los conceptos que veremos

Conceptos de la arquitectura de SI



- X.800 considera tres aspectos de la seguridad de la información
 - ataque a la seguridad
 - servicio de seguridad
 - mecanismo de seguridad

Ataques y amenazas a la seguridad



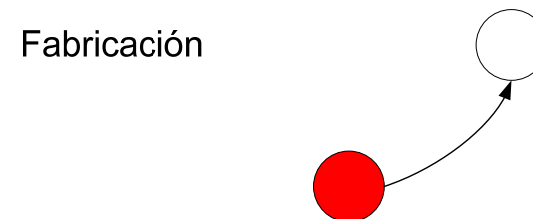
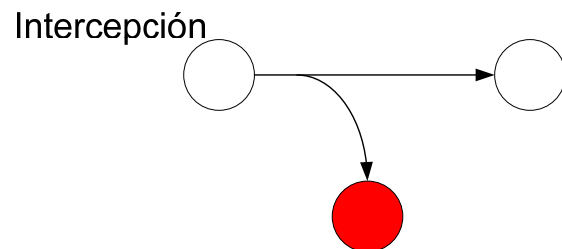
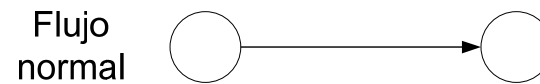
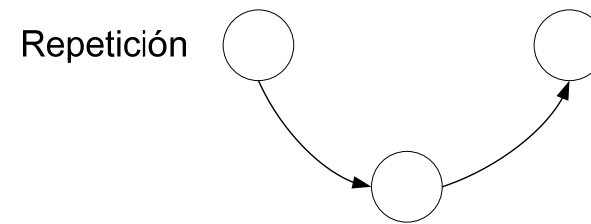
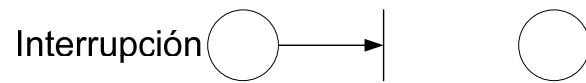
- **Amenaza:** peligro posible que puede explotar una vulnerabilidad
- **Ataque:** Acto deliberado para eludir los servicios de seguridad y violar la política de seguridad de la información
- La seguridad de la información trata de cómo prevenir ataques, o de ocurrir éstos, detectar ataques en sistemas basados en información
- Existe un amplio rango de ataques

Ataques a la seguridad



- **Ataques pasivos:** escuchas o monitoreo de transmisiones para:
 - obtener el contenido de los mensajes, o
 - monitorear el flujo del tráfico
- **Ataques activos:** modificaciones al flujo de datos, con el objeto de:
 - enmascararse bajo la identidad de otro
 - reproducir mensajes anteriores
 - modificar mensajes en tránsito
 - denegación del servicio (DOS - denial of service)

Ataques a la seguridad



Servicios de seguridad



- Un *servicio de seguridad* es algo que mejora la seguridad de los sistemas de procesamiento de datos y las transferencias de información en una organización
- Se ocupan de responder ante ataques a la seguridad
- Hacen uso de uno o más *mecanismos de seguridad* para proveer dicho servicio

Servicios de seguridad



- **Autenticación** – seguridad de que la entidad que se comunica es quien dice ser
- **Control de acceso** – prevención del acceso no autorizado a los recursos
- **Confidencialidad** – protección de los datos frente a su revelación no autorizada
- **Integridad** – seguridad de que los datos se reciben tal cual son enviados por el emisor
- **No repudio** – protección frente a la posibilidad de que el emisor (o el receptor) nieguen la transmisión de un mensaje
- **Disponibilidad** – posibilidad de acceder en forma no-interrumpida a un servicio

Mecanismos de seguridad



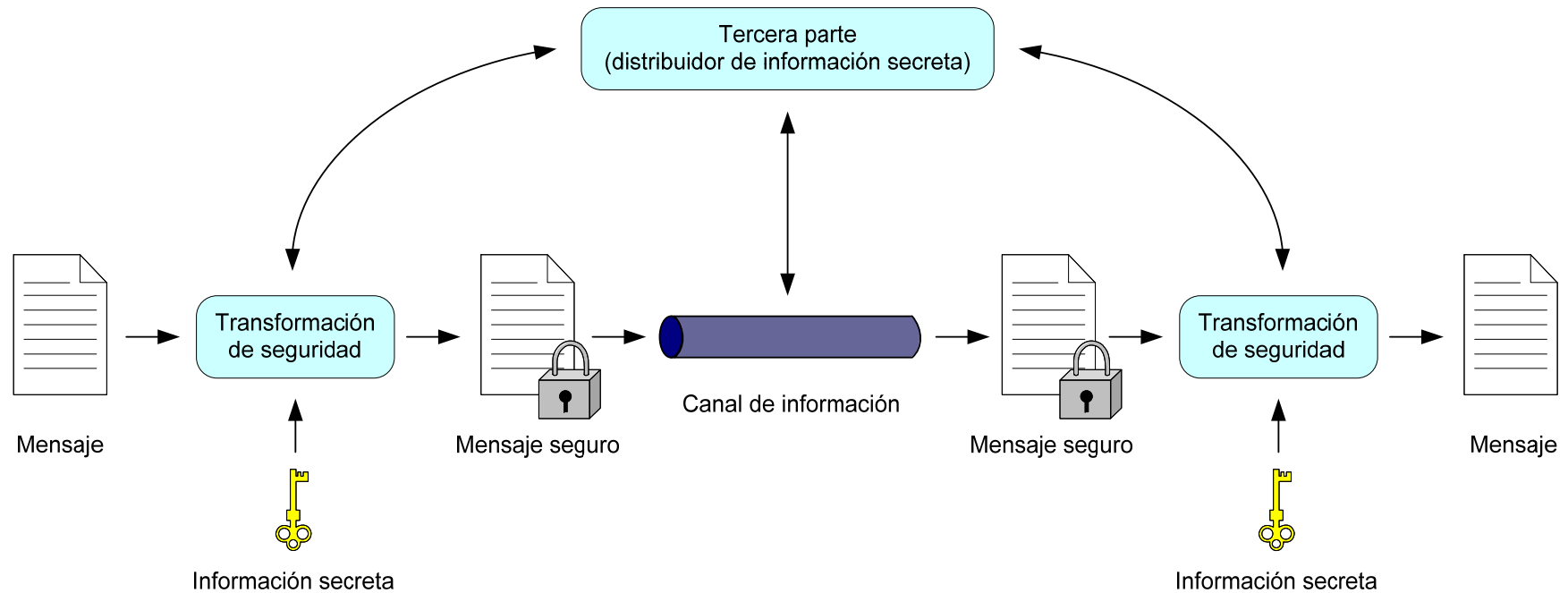
- Un mecanismo diseñado para detectar, prevenir, o recuperarse de un ataque a la seguridad
- No existe un único mecanismo que dé soporte a todas las funciones requeridas
- Sin embargo, un mecanismo en particular se aplica en muchos de los mecanismos en uso: las *técnicas criptográficas*

Mecanismos de seguridad



- Mecanismos de seguridad específicos:
 - **cifrado**, **firma digital**, control de acceso, **integridad de los datos**, **intercambio de autenticación**, relleno de tráfico, control de ruteo, **notarización**
- Mecanismos de seguridad generales:
 - funcionalidad fiable, detección de acciones, informes para la auditoría de seguridad, recuperación

Modelo de seguridad en redes

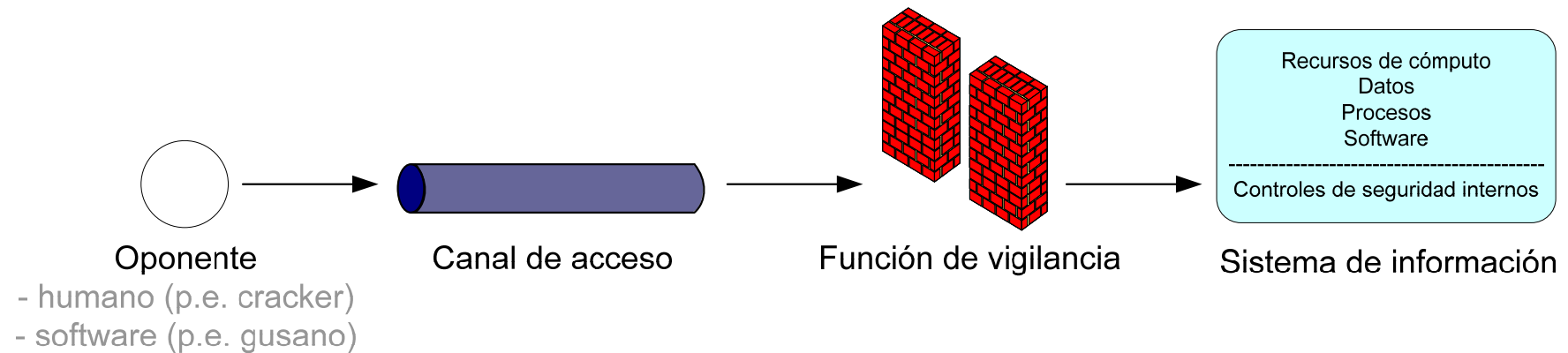


Modelo de seguridad en redes



- El uso de este modelo requiere:
 - Diseñar un algoritmo adecuado para la transformación de seguridad
 - Generar la información secreta (claves) usadas por el algoritmo
 - Desarrollar métodos para compartir y distribuir la información secreta
 - Especificar un protocolo para los dos interlocutores para obtener un servicio concreto de seguridad

Modelo de seguridad en el acceso



- Amenazas de acceso a la información: captura o alteración de datos por parte de usuarios que no deberían tener acceso a dichos datos
- Amenazas al servicio: explotación de fallos del servicio en los computadores para impedir el uso por parte de los usuarios legítimos

Modelo de seguridad en el acceso



- Para dar seguridad a este modelo se va a requerir el uso:
 - Sistemas de autenticación
 - Sistemas de autorización
 - Sistemas de monitoreo

Criptografía



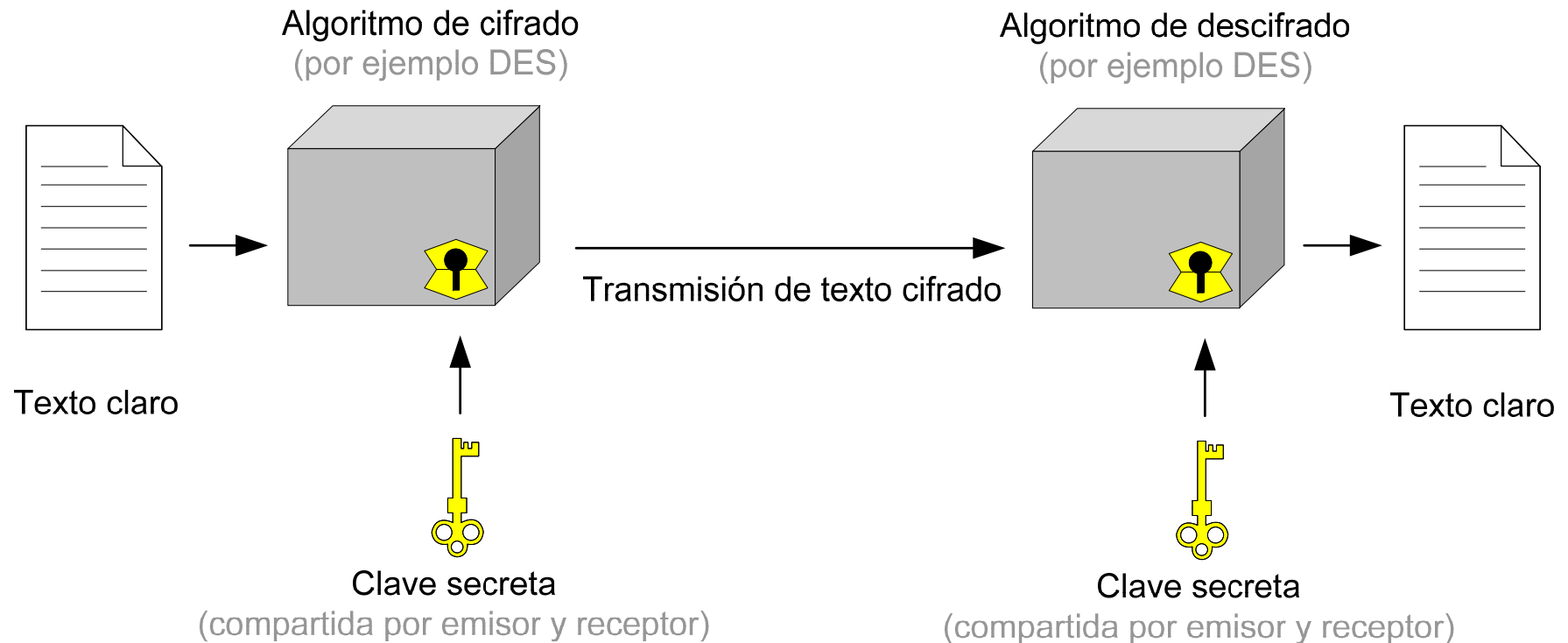
- Podemos clasificarla según tres dimensiones diferentes:
 - El tipo de operaciones utilizadas para transformar el texto claro en texto cifrado
 - El número de claves usadas
 - cifrado convencional o simétrico (una sola clave)
 - cifrado asimétrico o de clave pública (dos claves)
 - La forma en que se procesa el texto claro
 - cifrado de bloques
 - cifrado de flujo

Cifrado convencional (cifrado simétrico)



- Un esquema de cifrado convencional tiene cinco componentes:
 - Texto claro
 - Algoritmo de cifrado
 - Clave secreta
 - Texto cifrado
 - Algoritmo de descifrado
- La seguridad depende de que la clave sea secreta, no de que el algoritmo lo sea

Cifrado Convencional (Cifrado Simétrico)



Algoritmos de cifrado simétrico



- Los algoritmos de cifrado simétrico más comúnmente usados son los *cifradores de bloque*
- Un cifrador de bloque procesa una entrada de texto claro de tamaño fijo y genera un bloque de texto cifrado del mismo tamaño para cada texto claro
- Los más importantes son
 - DES (Data Encryption Standard)
 - 3DES
 - RC5
 - IDEA
 - AES

Esquemas de cifrado



- Cifrado de bloque

- Divide el texto claro en bloques de igual tamaño, los cuales son procesados en orden por el algoritmo de cifrado

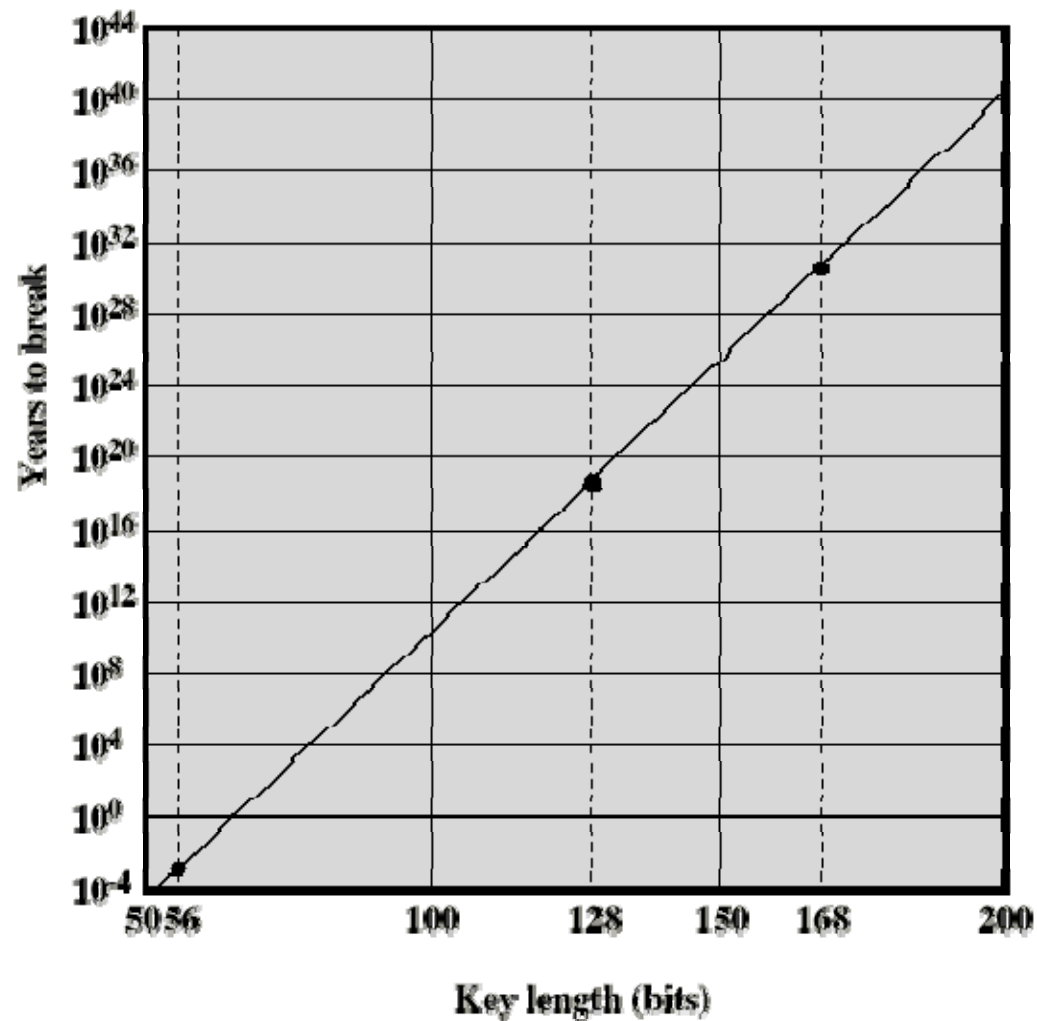
- Cifrado de flujo

- El texto claro se procesa dinámicamente como una única ristra de caracteres

Ataques por fuerza bruta

Tamaño de clave (bits)	Número de claves alternativas	Tiempo requerido (a 10^6 Iteraciones/ μ s)
32	$2^{32} = 4.3 \times 10^9$	2.15 milisegundos
56	$2^{56} = 7.2 \times 10^{16}$	10 horas
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{18} años
168	$2^{168} = 3.7 \times 10^{50}$	5.9×10^{30} años

Ataques por fuerza bruta



Otros cifradores de bloque



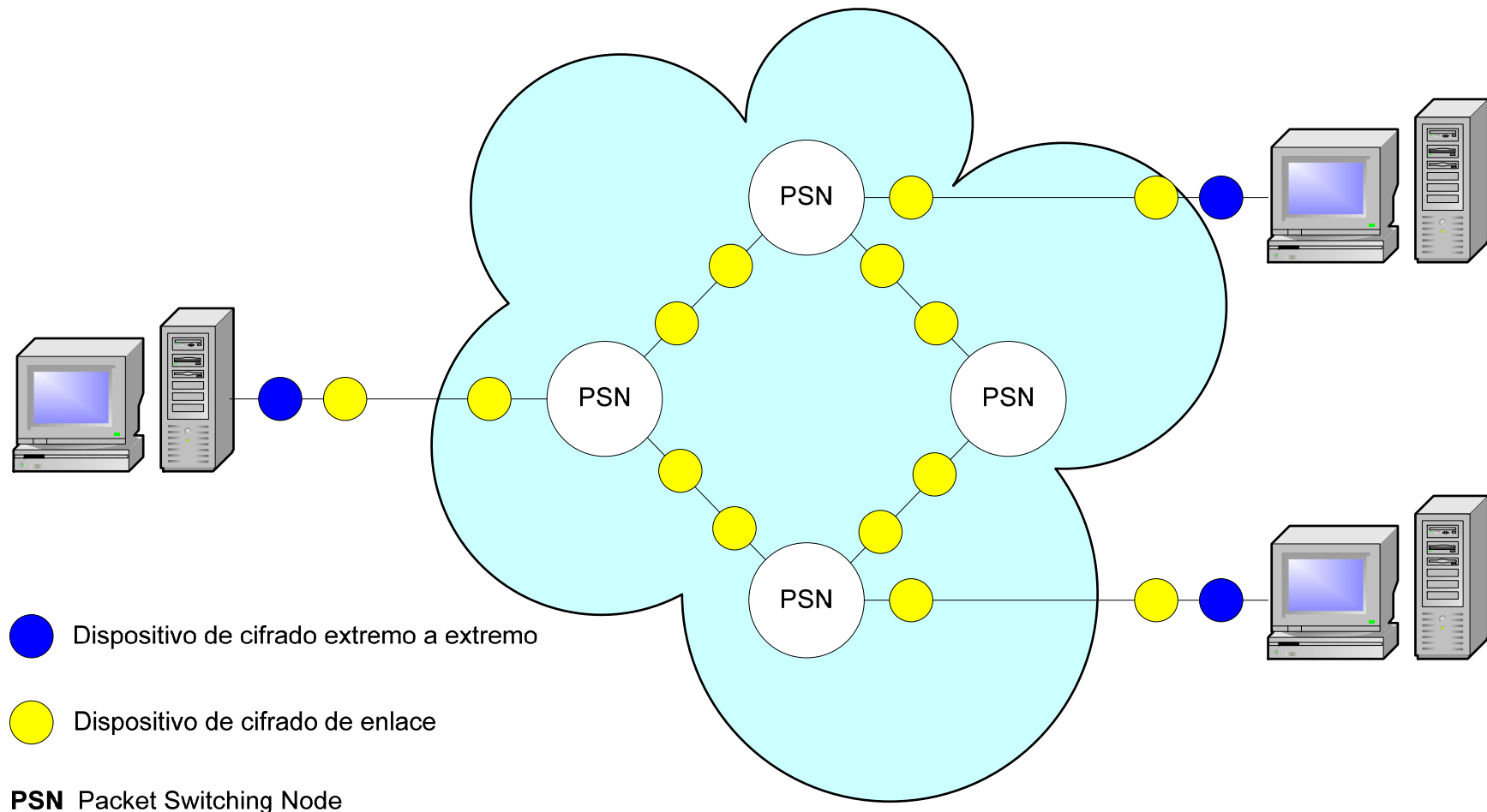
- DES y 3DES
 - Longitud de clave 56 y 168 bits
- Advanced Encryption Standard (AES)
 - Tan robusto como el 3DES
 - Más eficiente (es muy rápido comparado con 3DES)
- International Data Encryption Algorithm (IDEA)
 - Longitud de clave de 128 bits
 - Usado en PGP
- Blowfish
 - Simple implementación
 - Rápida ejecución
 - Corre en menos de 5KB de memoria

Dispositivos de cifrado



- Un enfoque potente para contrarestar las amenazas es el cifrado
- Al usar cifrado hay que decidir qué cifrar y dónde situar los engranajes del cifrado
 - Cifrado de enlace
 - Muchos dispositivos de cifrado
 - Alto nivel de seguridad
 - Se descifra cada paquete en cada salto
 - Cifrado extremo a extremo
 - El emisor cifra y el receptor descifra
 - La carga útil está cifrada
 - El encabezado está en claro
 - Alta seguridad
 - Se requiere ambos, cifrado de enlace y cifrado extremo a extremo

Dispositivos de cifrado



Distribución de claves



- Para que el cifrado simétrico funcione, ambas partes deben tener la misma clave
- Esta clave debe protegerse del acceso de terceros y cambiarse frecuentemente, de ser posible
- La distribución de claves se puede realizar de diferentes maneras
 1. Una clave puede ser elegida por A y enviada a B físicamente
 2. Una tercera parte puede seleccionar la clave y enviarla físicamente a A y B
 3. Si A y B usaron una clave previamente, una parte puede transmitir la nueva clave a la otra cifrada con la anterior
 4. Si A y B tienen una conexión cifrada con una tercera parte C, C puede distribuir la clave, a través de esos enlaces, a A y B

Distribución de claves



➤ Clave de sesión

- Los sistemas finales involucrados establecen una conexión lógica
- Mientras dure ésta, los datos se cifran con una clave de sesión de un sólo uso
- Al finalizar la sesión, la clave se destruye

➤ Clave permanente

- Usadas por ambas partes, a los efectos de distribuir las claves de sesión

Autenticación



- Sirve para verificar que:
 - Los mensajes provienen de la fuente correcta
 - No se alteró su contenido
 - A veces, que fueron enviados en determinado tiempo o secuencia
- Protección contra ataques activos (falsificación de datos y/o transacciones)

Enfoques para autenticación



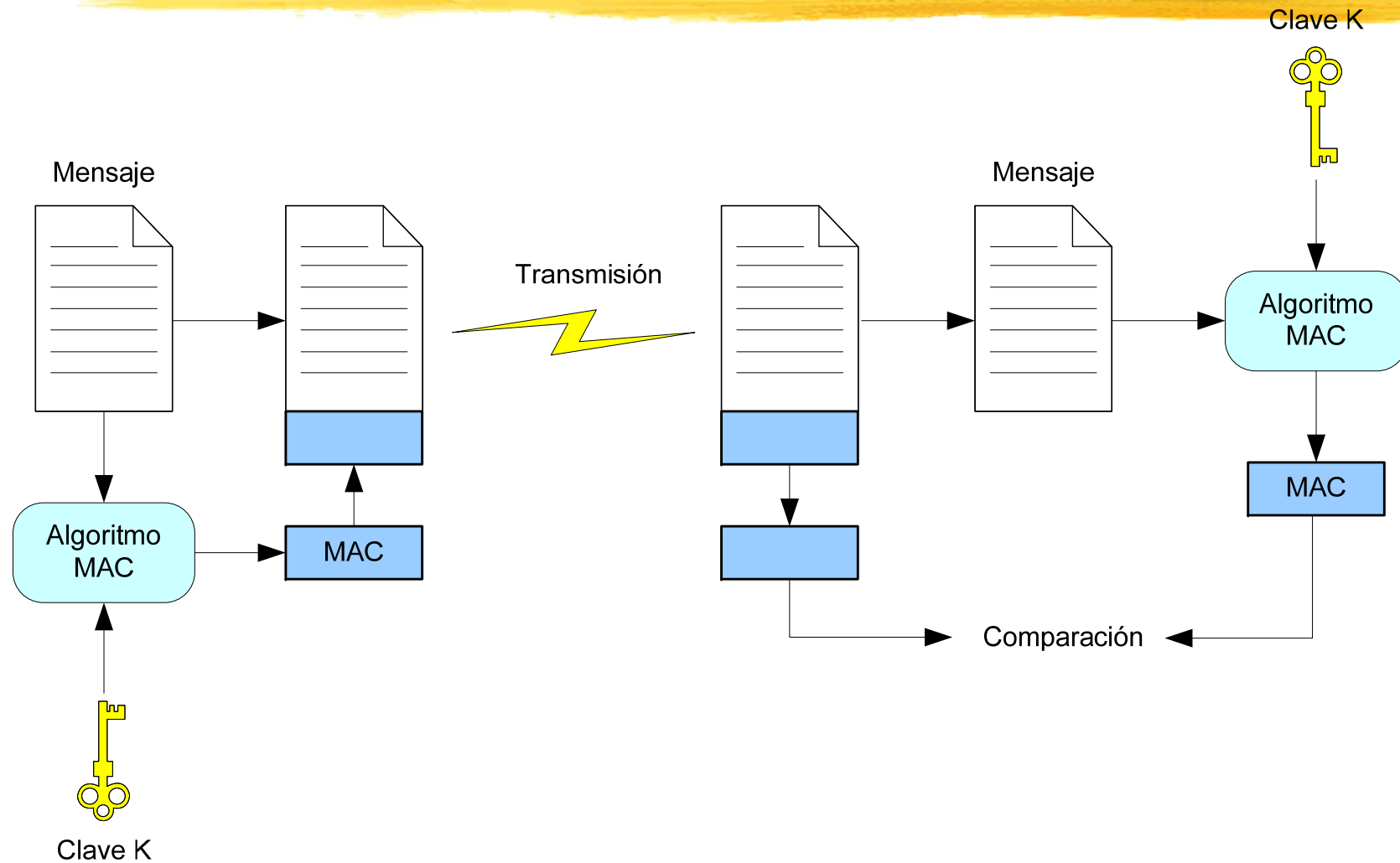
- Autenticación usando cifrado convencional
 - sólo emisor y el receptor deberían conocer la clave
 - si se incluyen *timestamps* se protege contra ataques de repetición
- Autenticación de mensajes sin cifrado
 - una referencia de autenticación se genera y agrega a cada mensaje. El mensaje en sí mismo no se cifra
- Código de Autenticación de Mensajes (MAC)
 - se calcula el MAC como una función del mensaje y la clave
- Función hash unidireccional
 - se calcula como una función del mensaje

Autenticación MAC



- Las partes comparten un secreto (K) común
- Se calcula $MAC(M) = F(K, M)$ y se envía con el mensaje
- Esto garantiza al receptor del mensaje:
 - que el mensaje no fue alterado
 - que el emisor es el indicado
 - si se incluye números de secuencia, que la secuencia es apropiada

Autenticación MAC



Función hash unidireccional



- Es una alternativa al MAC
- Acepta como entrada un mensaje de tamaño variable M y produce un resumen del mensaje de tamaño fijo $H(M)$ como salida
- Para autenticar un mensaje, el resumen se envía con el mensaje, con lo cual se verifica la autenticidad del resumen

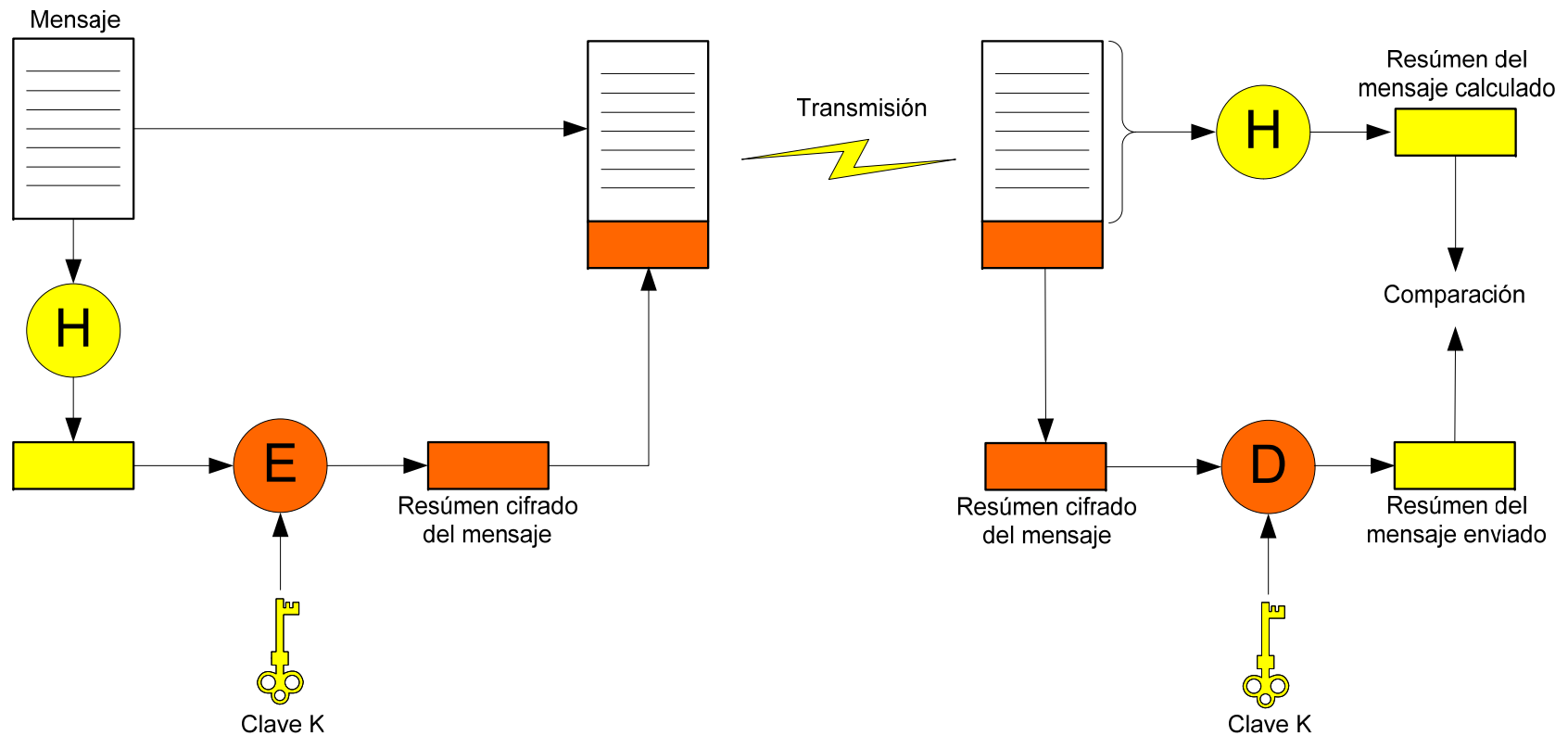
Funciones HASH seguras



	SHA-1	MD5	RIPEMD-160
Longitud de resumen	160 bits	128 bits	160 bits
Longitud de bloque	512 bits	512 bits	512 bits
Numero de pasadas	80 (4 de 20)	64 (4 de 16)	160 (5 pares de 16)
Tamaño de mensaje	$2^{64}-1$ bits	∞	∞

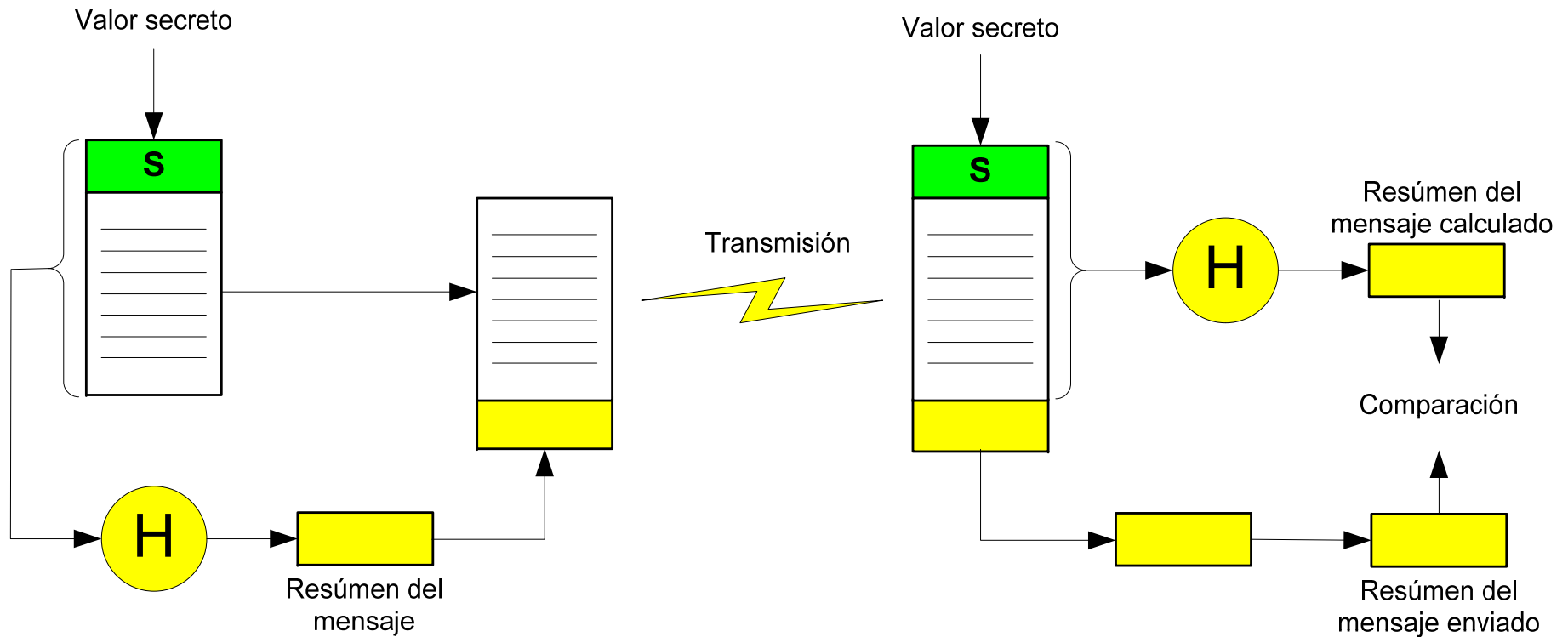
Función hash unidireccional

- Usando cifrado convencional



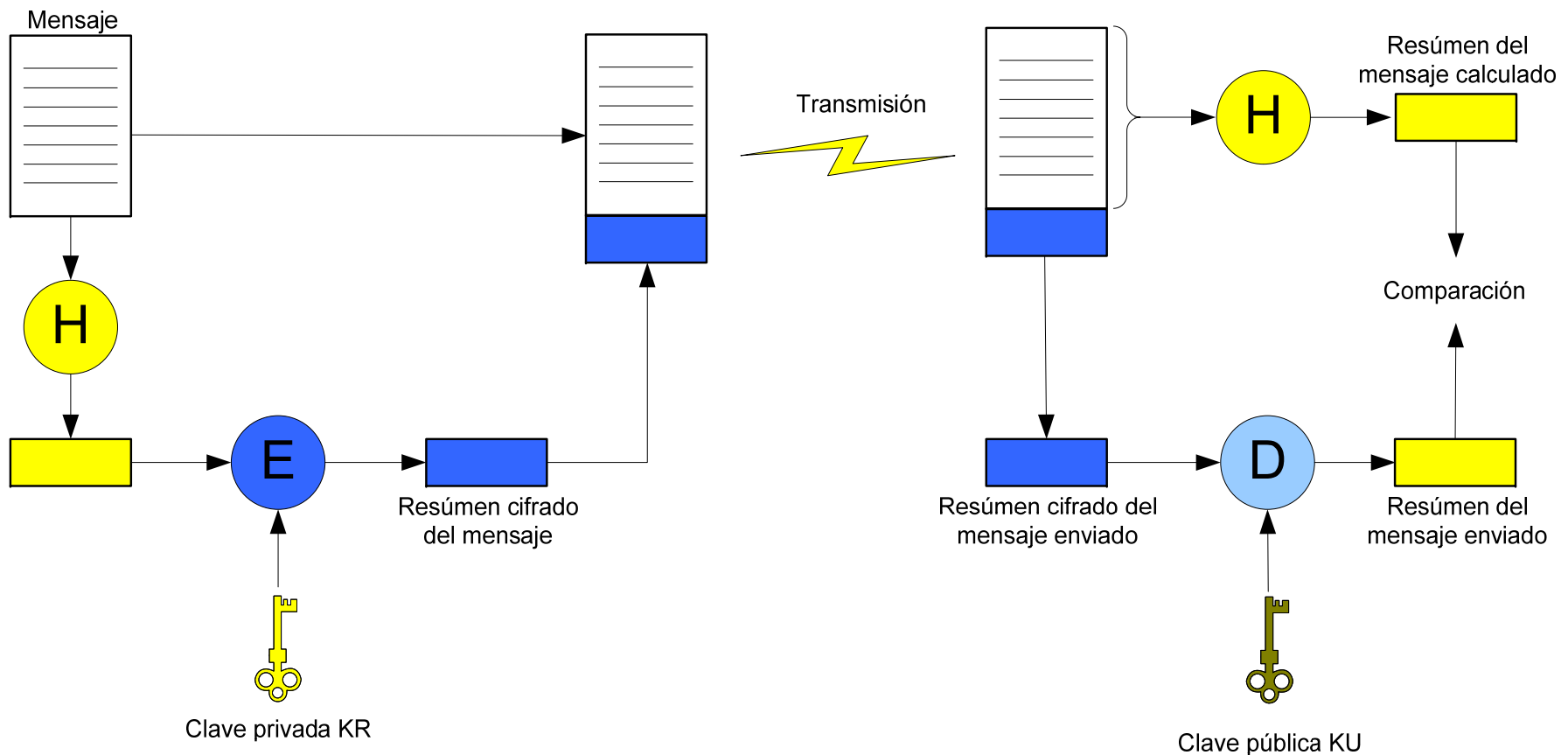
Función hash unidireccional

- Usando un valor secreto



Función hash unidireccional

- Usando cifrado de clave pública



La realidad...



- En el año 2004, MD5 se vio seriamente comprometido
 - Se ideó un método de generación de colisiones de hash
 - El ataque demandó 1 hora de cálculo
 - En un clúster IBM P690
 - Se recomendó usar SHA-1 en su lugar
- En el año 2005, SHA-1 se pudo romper por ataques distintos a fuerza bruta
 - Demostraron rupturas en menos de 2^{69} operaciones
 - Los últimos ataques lograron debilitarlo hasta 2^{63} operaciones
 - Se recomendó usar WHIRPOOL

Criptografía de clave pública



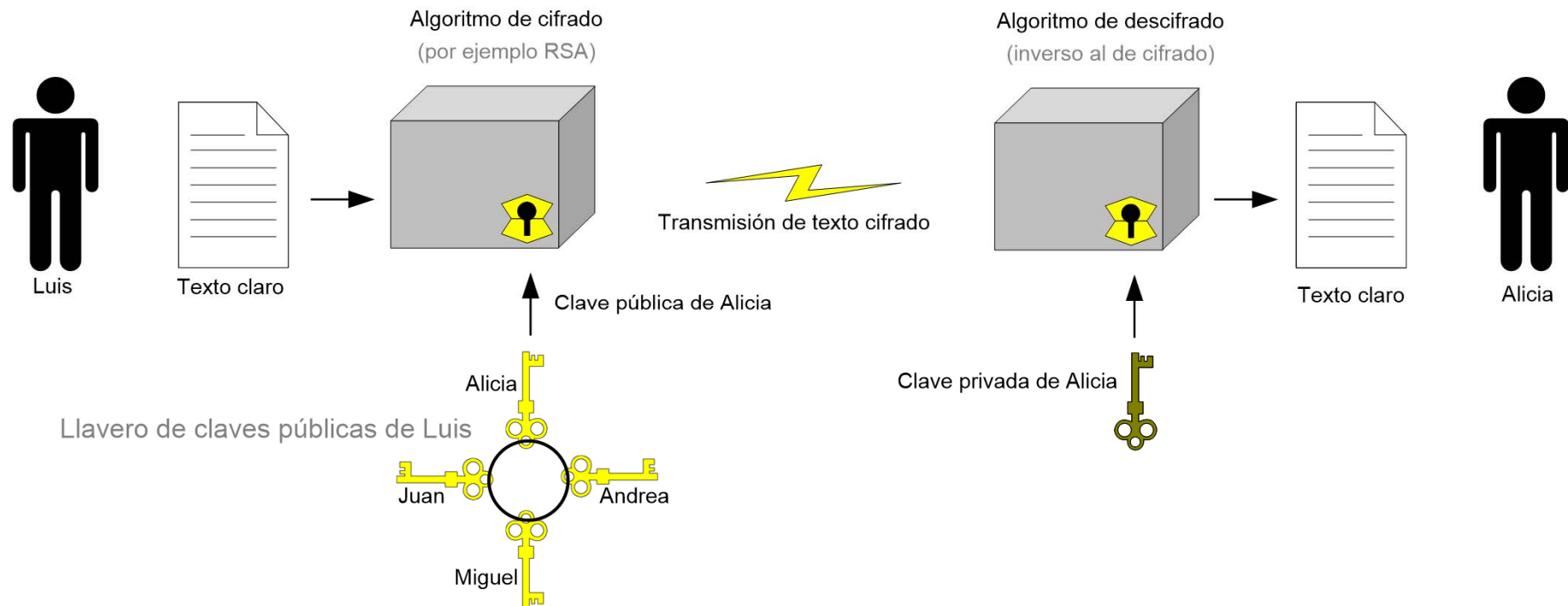
- Se utiliza en aplicaciones de:
 - **Cifrado/Descifrado:** El emisor cifra un mensaje con la clave pública del receptor
 - **Firma digital:** El emisor "firma" un mensaje con su clave privada
 - **Intercambio de claves:** Dos partes cooperan para intercambiar una clave de sesión.
- El esquema tiene seis ingredientes
 - Texto claro
 - Algoritmo de cifrado
 - Claves
 - una clave privada, que sólo su propietario conoce
 - una clave pública, conocida por todos los interlocutores
 - Texto cifrado
 - Algoritmo de descifrado

Cifrado/Descifrado Asimetrico



- Cada participante posee una pareja de claves
- Lo que se cifra con una de ellas, se descifra con la otra
- Si se cifra un mensaje con la clave pública (cualquier interlocutor puede hacerlo) se proporciona confidencialidad
- sólo el propietario de la clave privada podrá leer el mensaje

Cifrado/Descifrado Asimetrico



Requerimientos

- En términos computacionales:
 - Debe ser fácil para una parte B el generar una pareja de claves (clave pública K_{Ub} , clave privada K_{R_b})
 - Debe ser fácil para un emisor A que conozca la clave pública de un receptor B generar el texto cifrado C a partir de un mensaje M, es decir, **$C = E_{K_{UB}}(M)$**
 - Debe ser fácil para un receptor B descifrar el texto cifrado resultante usando su clave privada y recuperar M, es decir, **$M = D_{K_{RB}}(C) = D_{K_{RB}}[E_{K_{UB}}(M)]$**

Requerimientos



- Debe ser imposible determinar una clave privada (KR_b) conociendo su pareja pública (KU_b)
- Debe ser imposible recuperar un mensaje M , conociendo KU_b y el texto cifrado C
- Cualquiera de las claves puede ser usada para el cifrado, mientras se utilice la otra para el descifrado:

$$M = D_{KRb}[E_{KU_b}(M)] = D_{KU_b}[E_{KRb}(M)]$$

Algoritmos de clave pública



- Los más utilizados son:

- **RSA**

- Desarrollado por Ron Rives, Adi Shamir y Len Adleman en el MIT, en 1977
 - Es un cifrador de bloque
 - El más ampliamente implementado

- **Diffie-Hellman**

- Se utiliza para intercambio de clave seguro
 - Se basa en la computabilidad de logartimos discretos

Algoritmo RSA

Veamos un ejemplo:

- Seleccionamos $p=17$ y $q=11$
 - Por tanto: $n=17 \times 11=187$; $\phi(n)=16 \times 10=160$
- Elegimos $e = 7$
 - Entonces $d=23$ satisface la ecuación indicada anteriormente

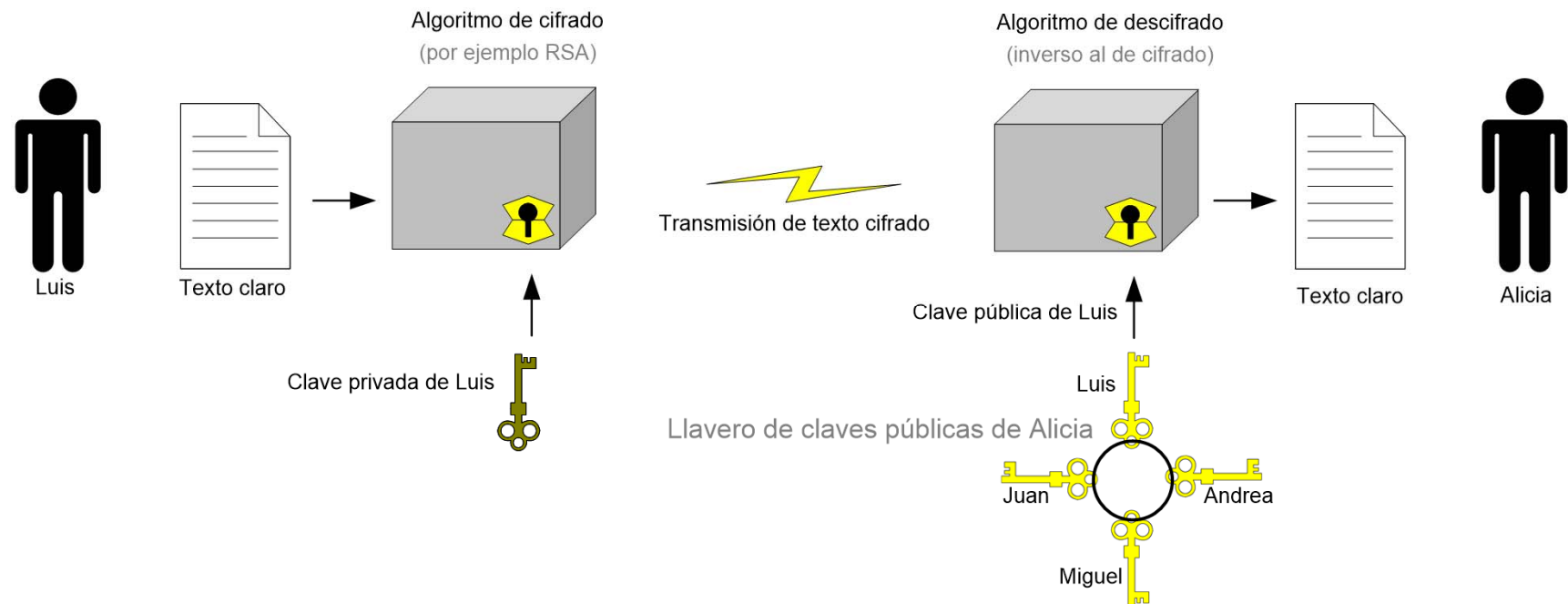


Firma Digital



- Cada participante posee una pareja de claves
- Lo que se cifra con una de ellas, se descifra con la otra
 - Si se cifra un mensaje con la clave privada de la pareja (sólo puede hacerlo el propietario de la pareja) se proporciona *autenticación de origen*
- ¿Por qué no proporciona confidencialidad?

Firma Digital



Firmas digitales



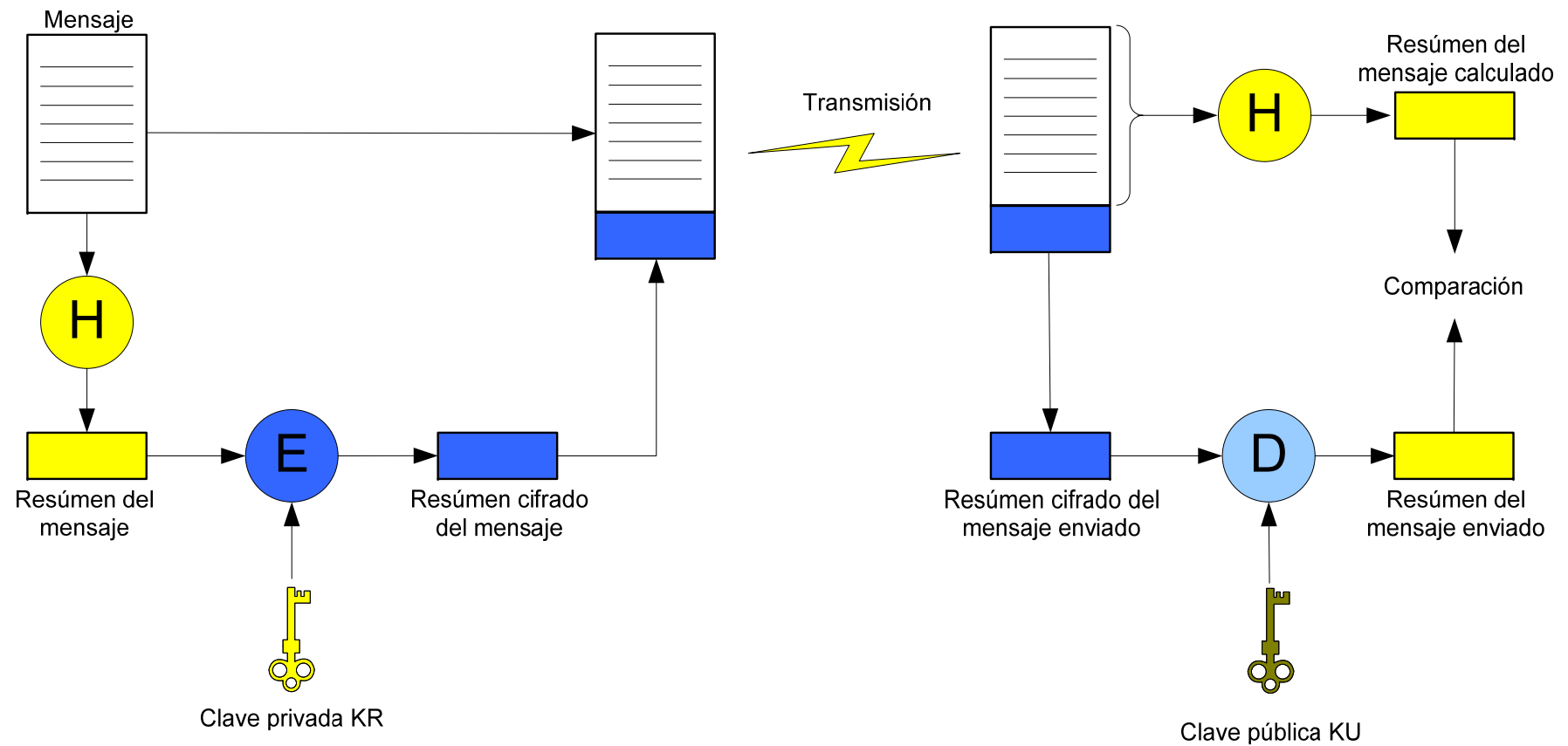
- Esto presenta ciertas desventajas
 - Requiere mayor espacio de almacenamiento, si se desea almacenar un mensaje en claro y su correspondiente versión cifrada y autenticada
 - Requiere recursos de cómputo, si se desea ahorrar espacio y almacenar solamente la versión cifrada y autenticada del mensaje
- Convendría cifrar un pequeño bloque de bits que sea función del mensaje.

Firmas digitales



- Resulta de utilizar un esquema de clave pública cifrando un resumen del mensaje, y no el mensaje en sí
- Proporciona autenticación sin confidencialidad
- El resumen sin cifrar el nombre de *autenticador*
- El resumen cifrado es la *firma digital* del mensaje

Firmas digitales



Gestión de claves



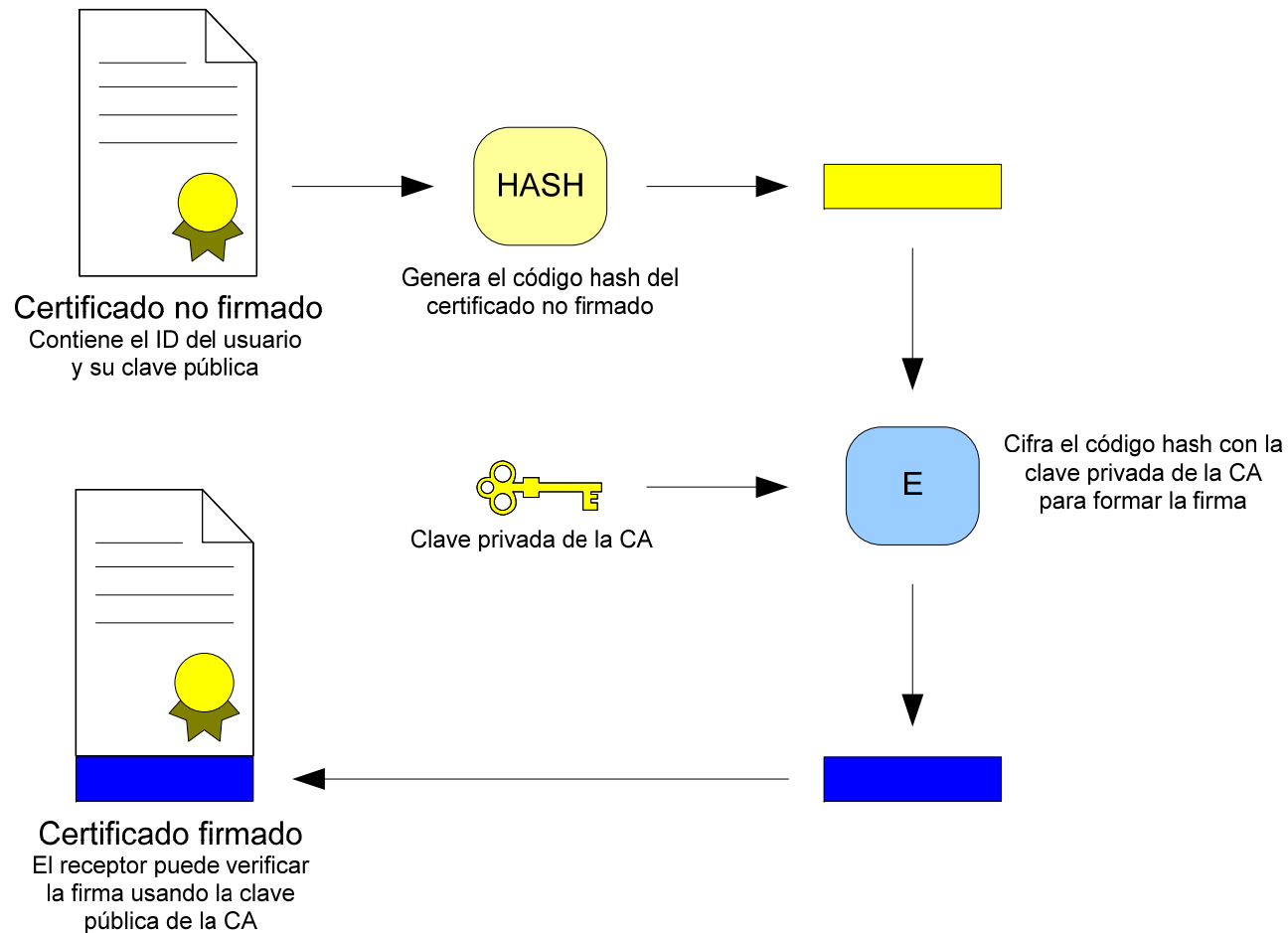
- Es una de las principales funciones del cifrado de clave pública. Involucra
 - El uso del cifrado de clave pública para la distribución de claves secretas
 - La distribución de claves públicas

Certificados de clave pública



- Como vimos, la base del cifrado de clave pública es el hecho de que la clave pública es pública
 - Por tanto, cualquiera podría falsificar ese dato público
 - Hasta ser descubierto el engaño, el daño podría estar consumado
- La solución es el Certificado de Clave Pública
 - Consiste en una clave pública y un identificador de usuario firmados por una tercera entidad confiable
 - Quienquiera que necesite la clave de éste usuario, puede solicitar el certificado y verificar que es válida por medio de la firma fiable de la entidad

Certificados de clave pública



Distribución de claves secretas



- Las partes deben acordar una forma de compartir una clave secreta que nadie más conozca
- Una alternativa es el intercambio Diffie-Hellman
 - No proporciona autenticación
- Otra es el uso de certificados de clave pública:
 - Se prepara un mensaje
 - Se cifra el mensaje mediante cifrado convencional con una clave de sesión
 - Se cifra la clave de sesión con la clave pública del receptor
 - Se añade la clave cifrada al mensaje cifrado y se envía

Introducción a la Seguridad IP



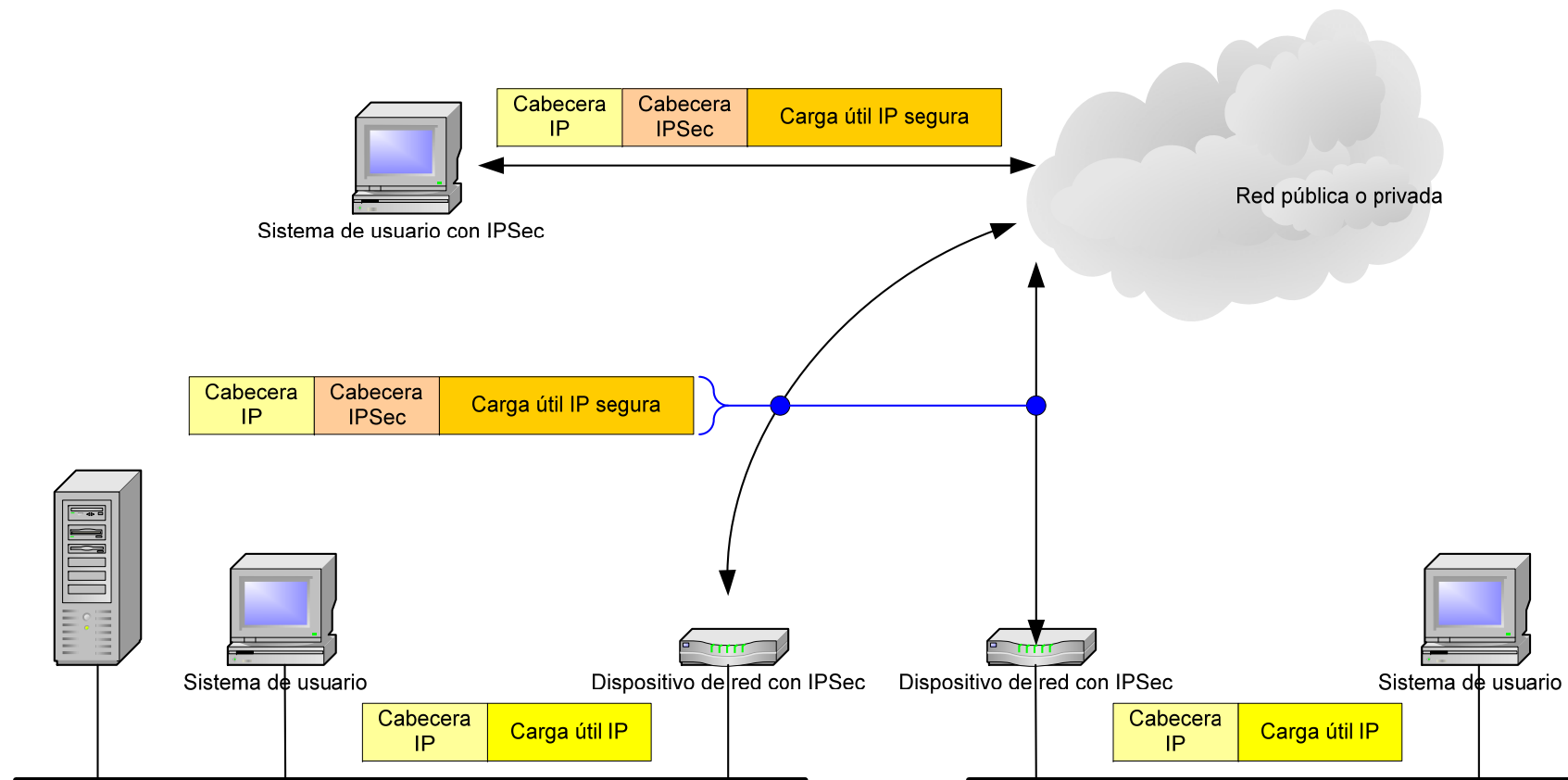
- En 1994 el IAB publicó un informe sobre la necesidad de una mayor y mejor seguridad en Internet
- Trataba sobre la necesidad de proteger la infraestructura de red contra
 - Observaciones
 - Control no autorizado
 - Suplantaciones de identidad y revelación de información
- La nueva generación de IP (IPv6) resuelve estas cuestiones con características propias del protocolo
- La solución a la generación actual se denomina IPSec

Introducción a la Seguridad IP



- Aplicaciones de IPSec
 - Conexión segura entre oficinas sucursales a través de Internet
 - Acceso remoto seguro a través de Internet
 - Establecimiento de conexión extranet e intranet con socios
 - Mejora de la seguridad en el comercio electrónico
- La característica principal de IPSec es ofrecer soporte a estas aplicaciones cifrando y/o autenticando **todo** el tráfico en el nivel de IP

Introducción a la Seguridad IP



Introducción a la Seguridad IP



➤ Beneficios de IPSec

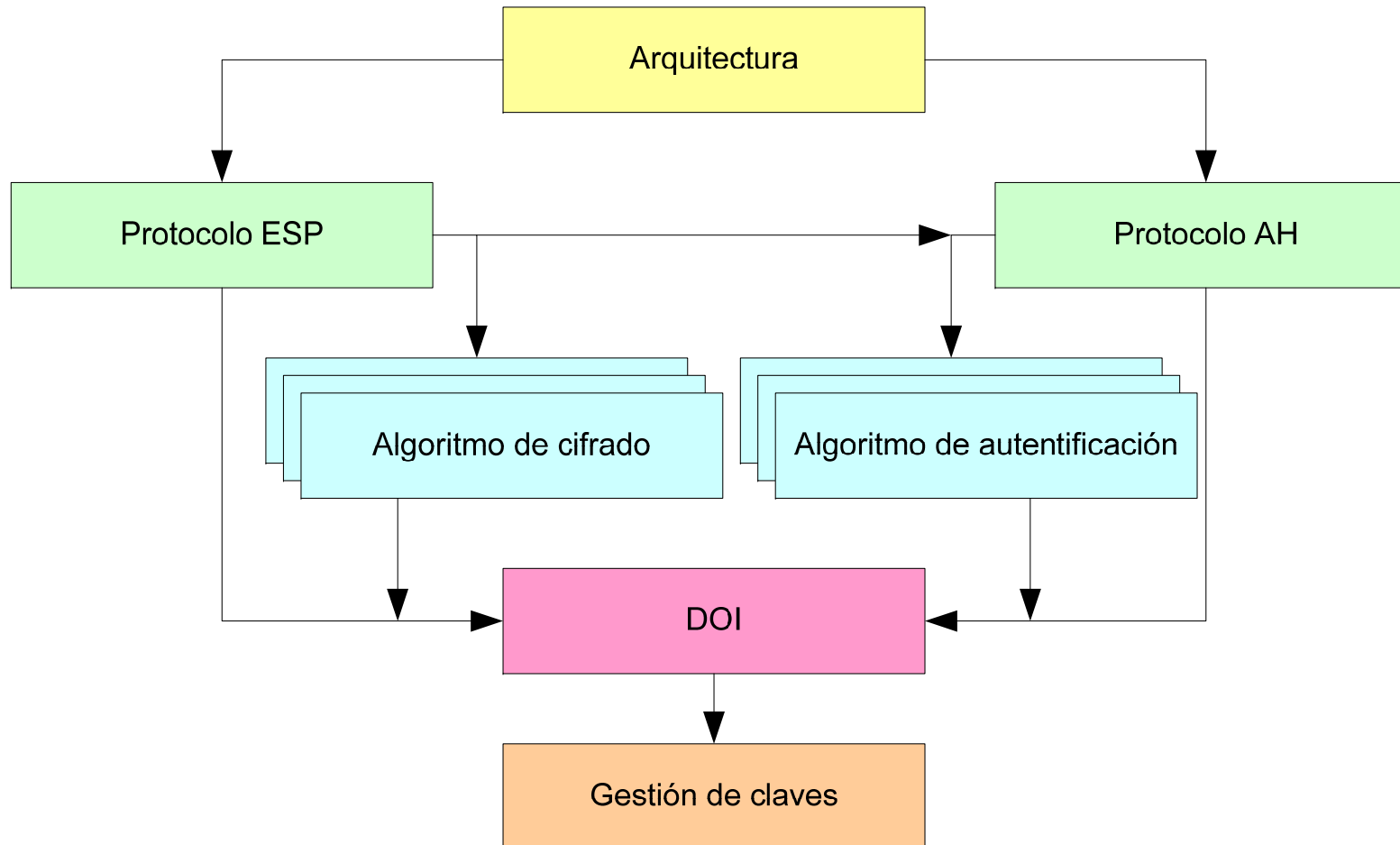
- Si se implementa en el router, puede proporcionar seguridad a todo el tráfico que lo atraviesa sin afectar al tráfico interno
- Es seguro en un firewall si se obliga a que todo el tráfico exterior use IPSec y el cortafuegos es el único punto de acceso
- Es transparente a las aplicaciones (está debajo de la capa de transporte)
- Puede ser transparente a usuarios finales
- Proporciona seguridad a usuarios individuales si es necesario

Servicios IPSec



- Control de acceso
- Integridad sin conexión
- Autenticación de origen de datos
- Rechazo de paquetes reenviados
- Confidencialidad (cifrado)
- Confidencialidad limitada del flujo de tráfico

Arquitectura de Seguridad IP



Cabecera de Autenticación



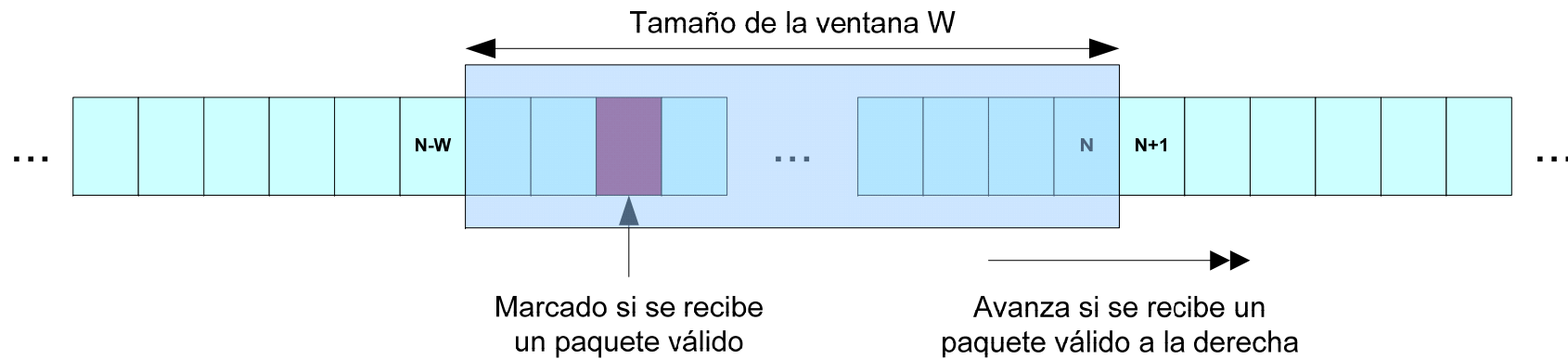
- Proporciona soporte para la integridad de los datos y la autenticación (mediante MAC) de paquetes IP
- Protege contra ataques de repetición

Cabecera de Autenticación

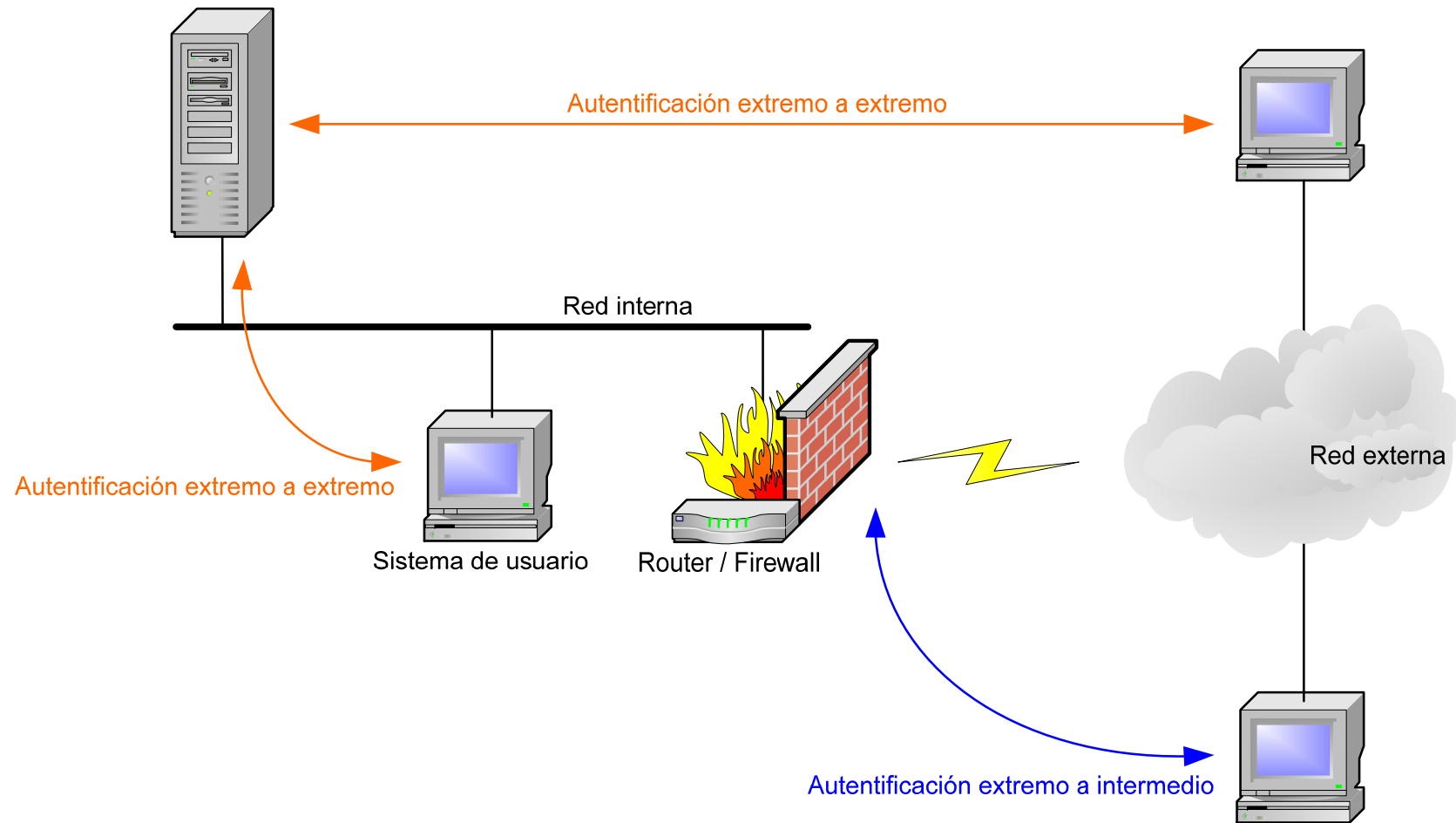


- Como IP es no fiable y no orientado a conexión, IPSec debe proporcionar tales servicios
 - Para ello implementa un protocolo de ventanas deslizantes con una ventana de tamaño $W=64$ y autenticación MAC
 - Si el paquete cae dentro de la ventana y es nuevo (y auténtico) se marca la ranura correspondiente en la ventana
 - Si el paquete cae a la derecha de la ventana y es nuevo (y auténtico) la ventana avanza
 - Si el paquete cae a la izquierda de la ventana o falla la autenticación, se descarta el paquete. Se puede registrar
 - La autenticación se realiza mediante un MAC truncado conocido como ICV (Integrity Check Value)

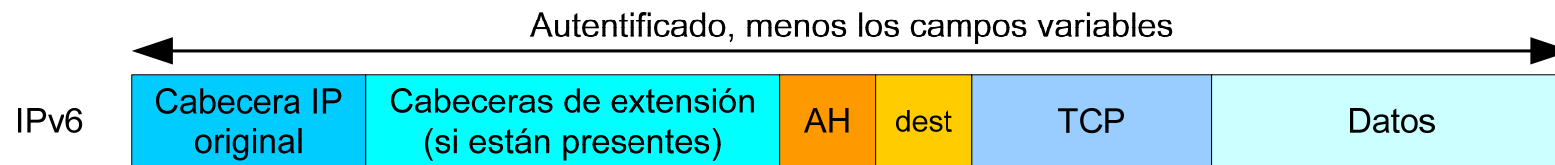
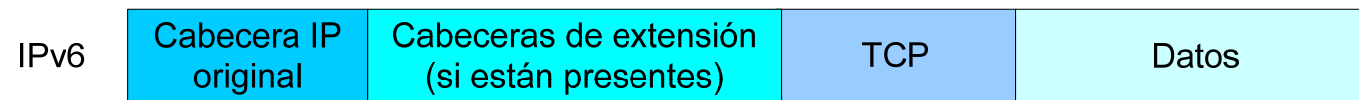
Cabecera de Autenticación



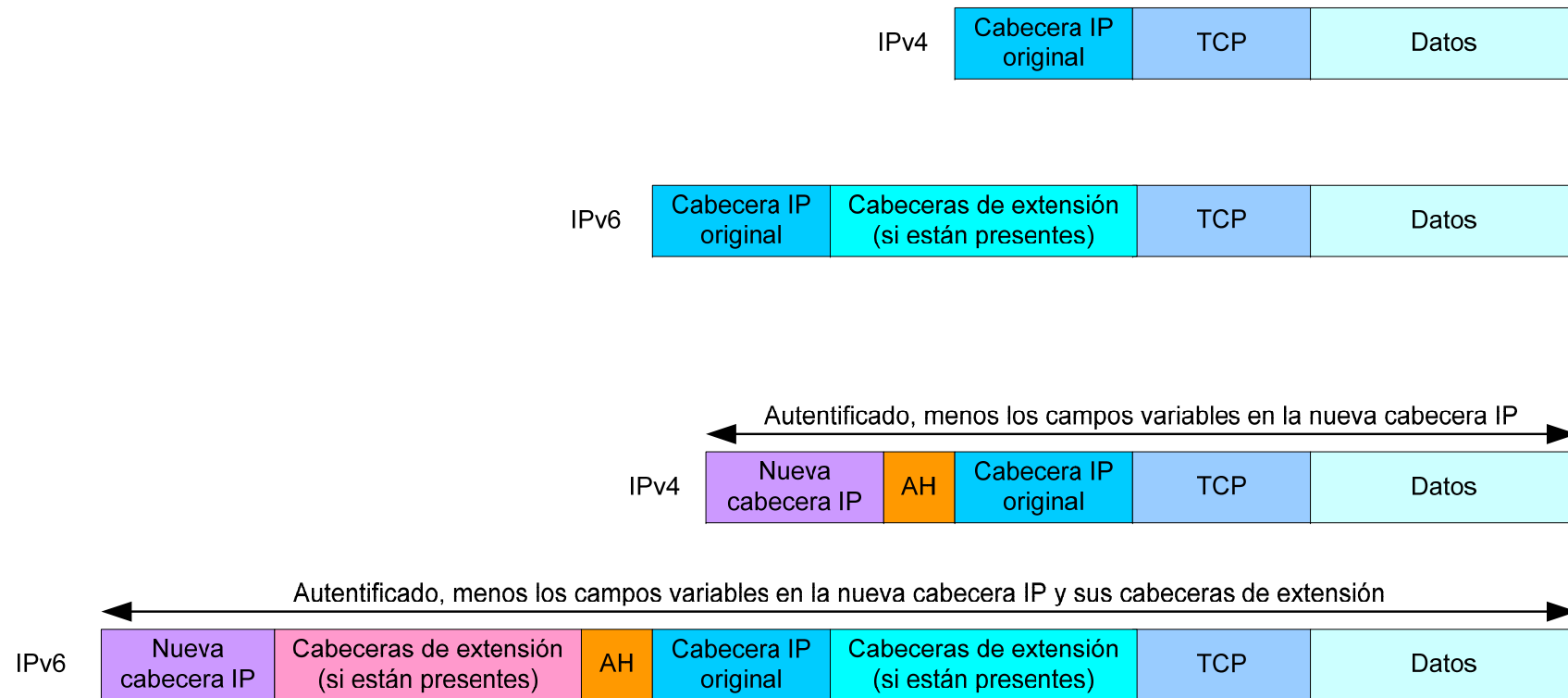
Modo transporte / Modo túnel



AH en modo transporte



AH en modo túnel



Encapsulating Security Payload



- Proporciona servicios de confidencialidad
 - Confidencialidad del contenido del mensaje
 - Confidencialidad limitada del flujo de tráfico
- Puede ofrecer los mismos servicios de autenticación que AH

Algoritmos usados por ESP



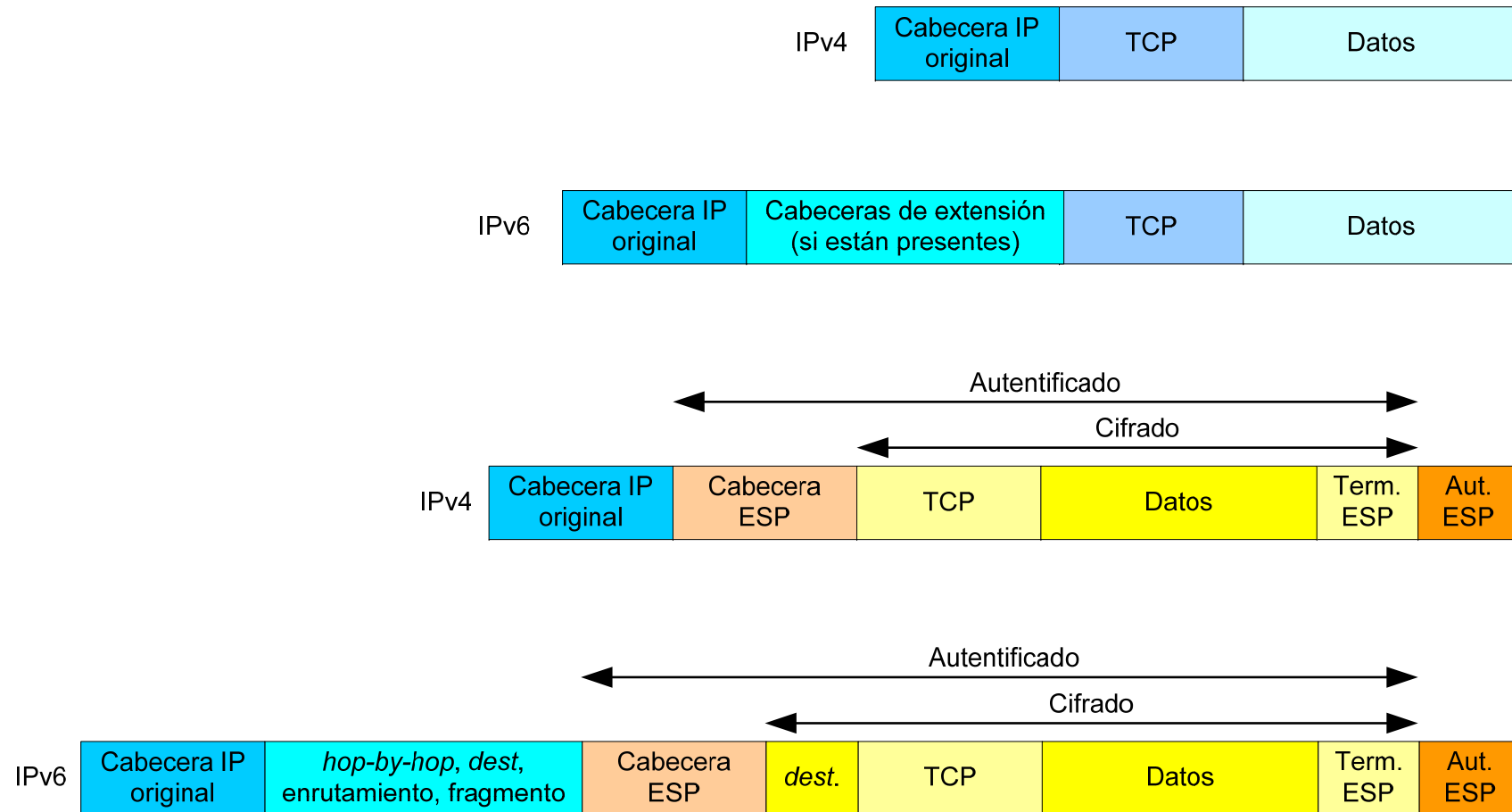
➤ Cifrado:

- 3DES
- RC5
- IDEA
- Triple IDEA
- CAST
- Blowfish

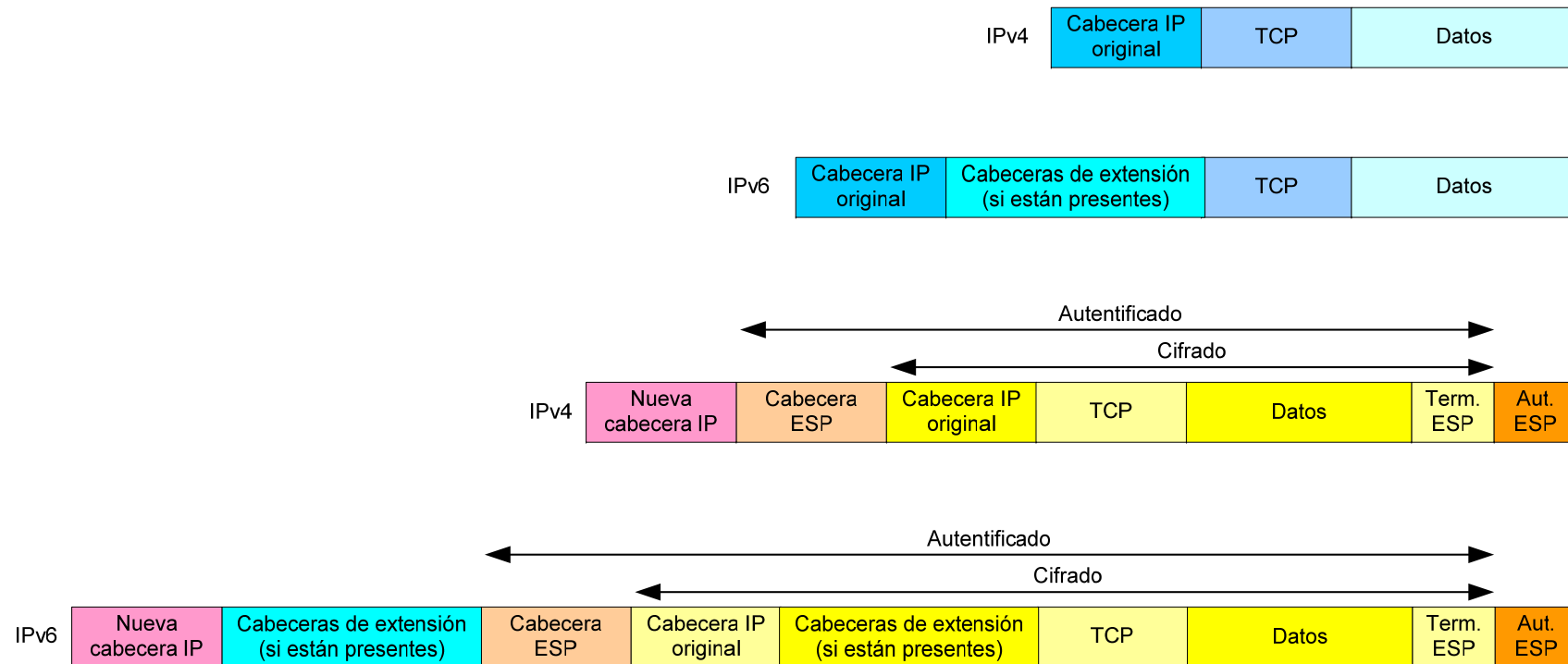
➤ Autenticación:

- HMAC-MD5-96
- HMAC-SHA-1-96

ESP en modo transporte



ESP en modo túnel

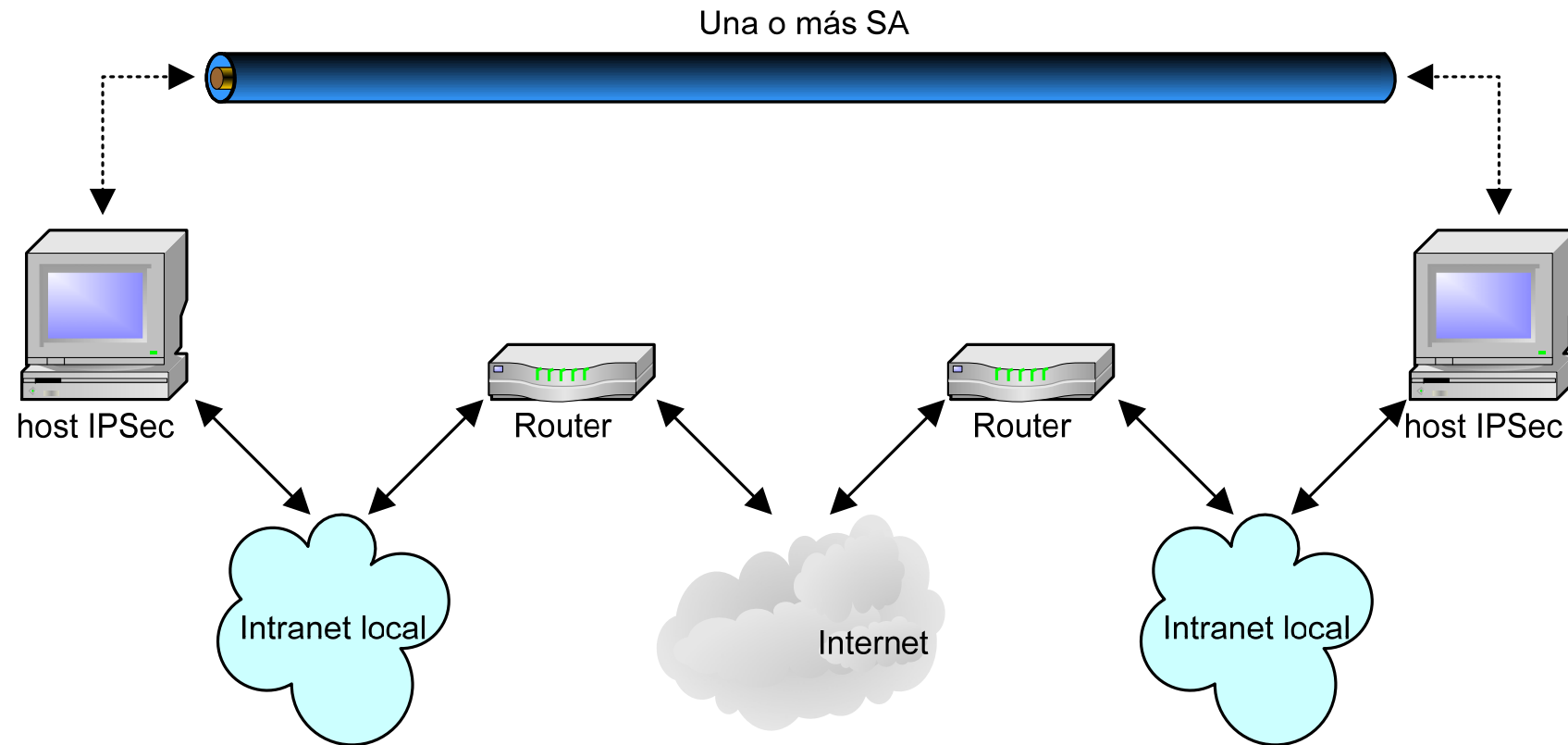


Modo transporte / Modo túnel

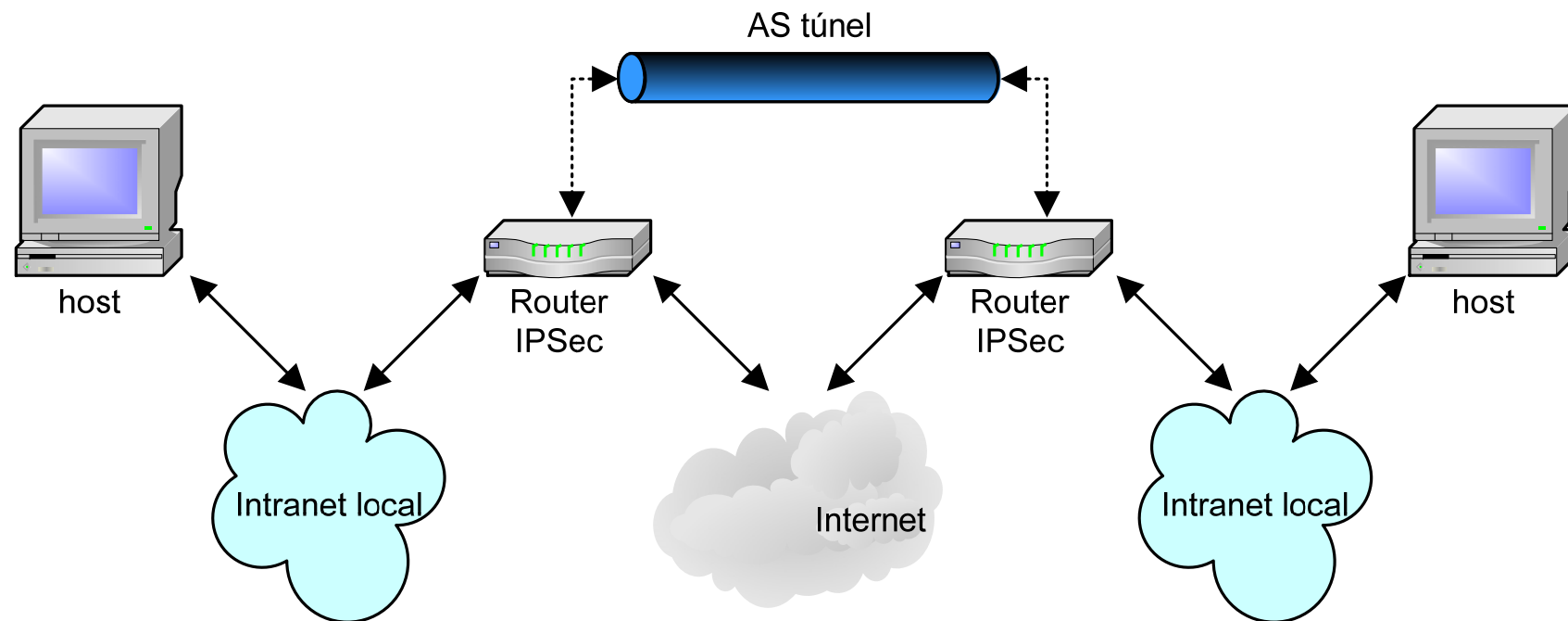


	modo transporte	modo túnel
AH	Autentifica la carga útil de IP y las partes seleccionadas de la cabecera IP y de las cabeceras de extensión IPv6	Autentifica todo el paquete IP interno y las partes seleccionadas de la cabecera IP exterior y las cabeceras de extensión IPv6
ESP	Cifra la carga útil de IP y cualquier cabecera de extensión IPv6 que siga a la cabecera ESP	Cifra el paquete IP interior
ESP/AH	Cifra la carga útil de IP y cualquier cabecera de extensión IPv6 que siga a la cabecera ESP. Autentifica la carga útil de IP, pero no la cabecera	Cifra el paquete IP interior. Autentifica el paquete IP interior.

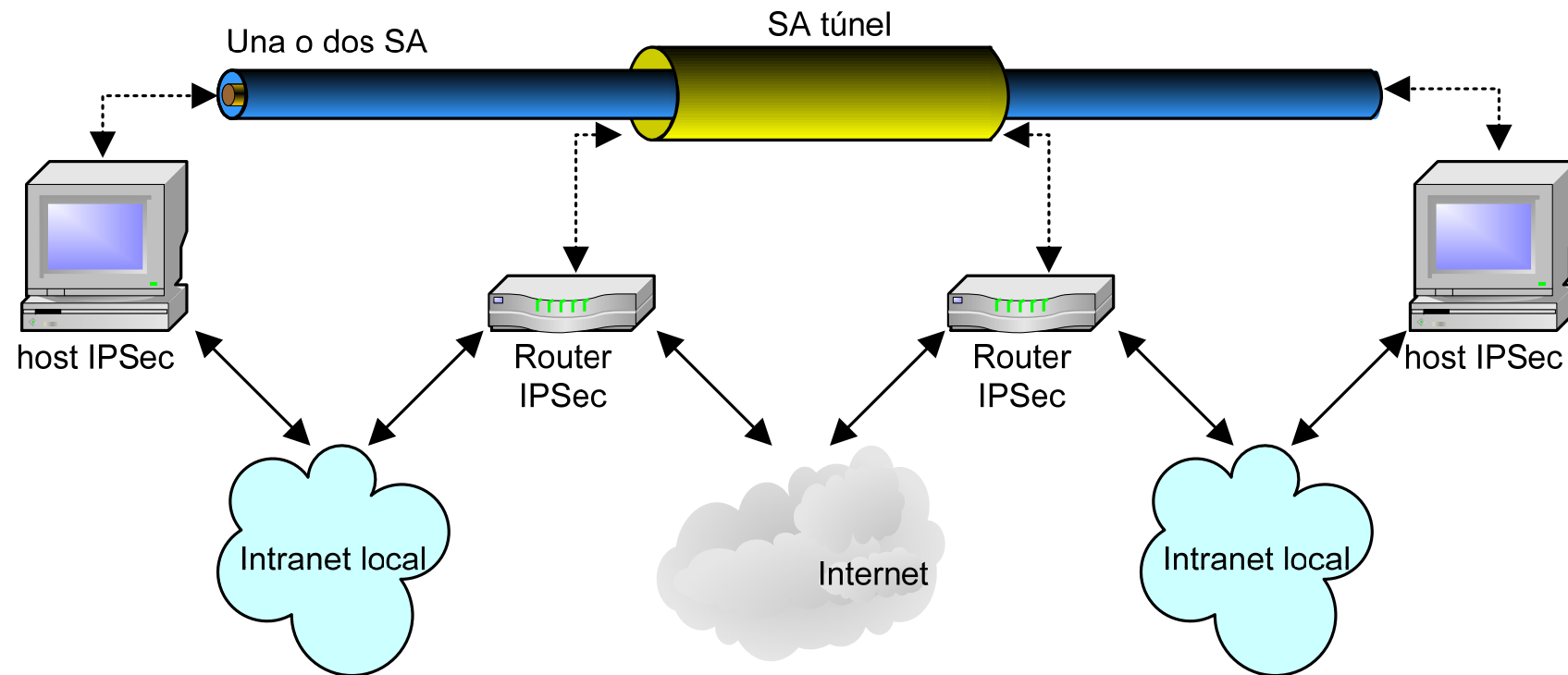
Ejemplo de uso



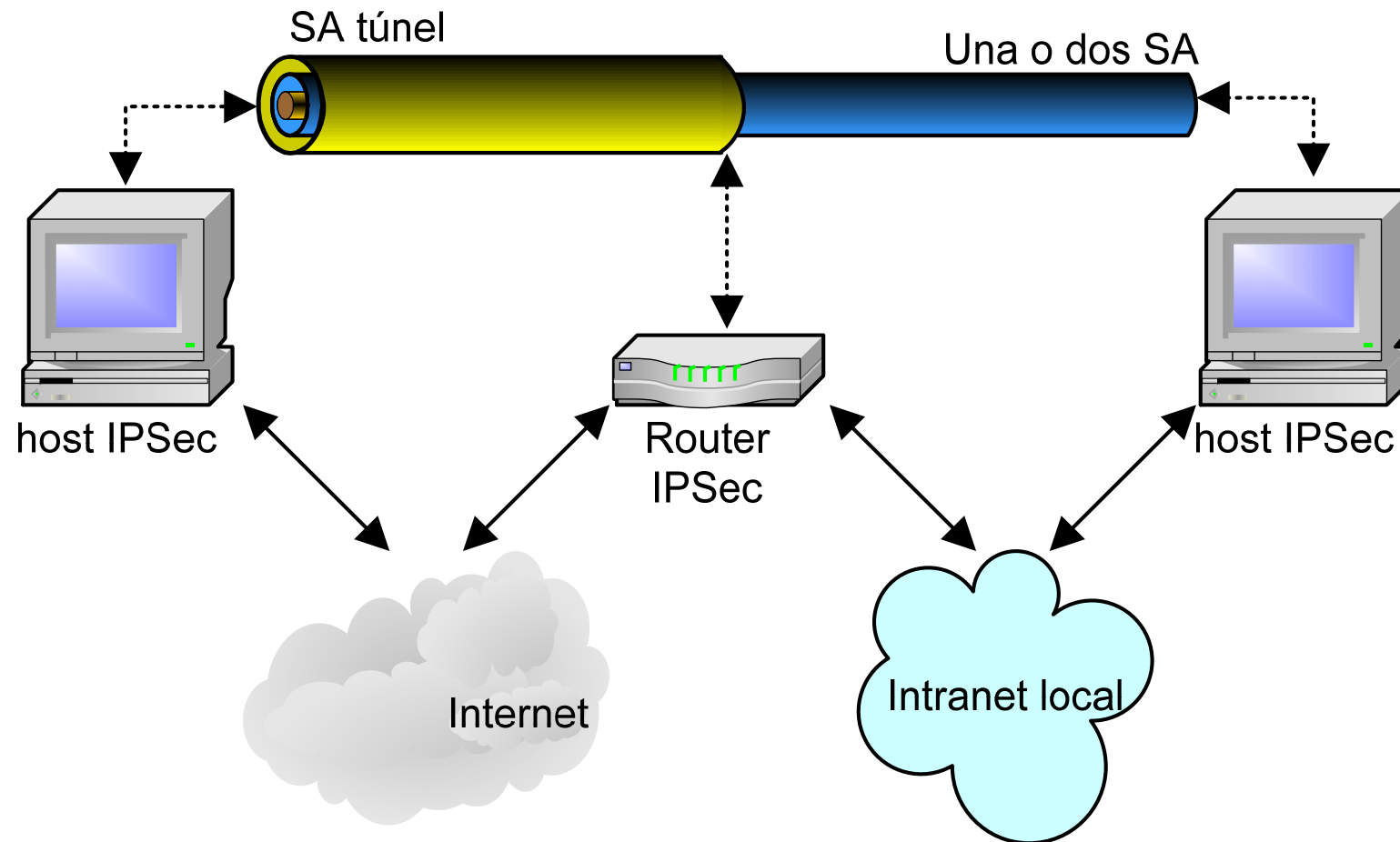
Ejemplo de uso



Ejemplo de uso



Ejemplo de uso



Seguridad en la web



- La web presenta retos que generalmente no se aprecian en el contexto de la seguridad
 - Internet es bidireccional
 - La web se emplea cada vez más como herramienta de negocios
 - La ilusión de simplicidad del software aumenta su complejidad interna
 - Un servidor web puede convertirse en un punto de acceso a la infraestructura computacional de una empresa
 - Los usuarios suelen ignorar los riesgos de seguridad

Amenazas a la seguridad web



- Las amenazas pueden agruparse en ataques pasivos y ataques activos
 - Los ataques pasivos incluyen escuchas del tráfico de red entre navegador y servidor, y obtener información restringida
 - Los ataques activos incluyen suplantar a otro usuario, alterar mensajes en tránsito y modificar un sitio web
- Otra forma de clasificar las amenazas es de acuerdo a su ubicación
 - Por ejemplo, servidor web, navegador web y tráfico de red entre navegador y servidor
 - Nos centraremos en la seguridad del tráfico

SSL



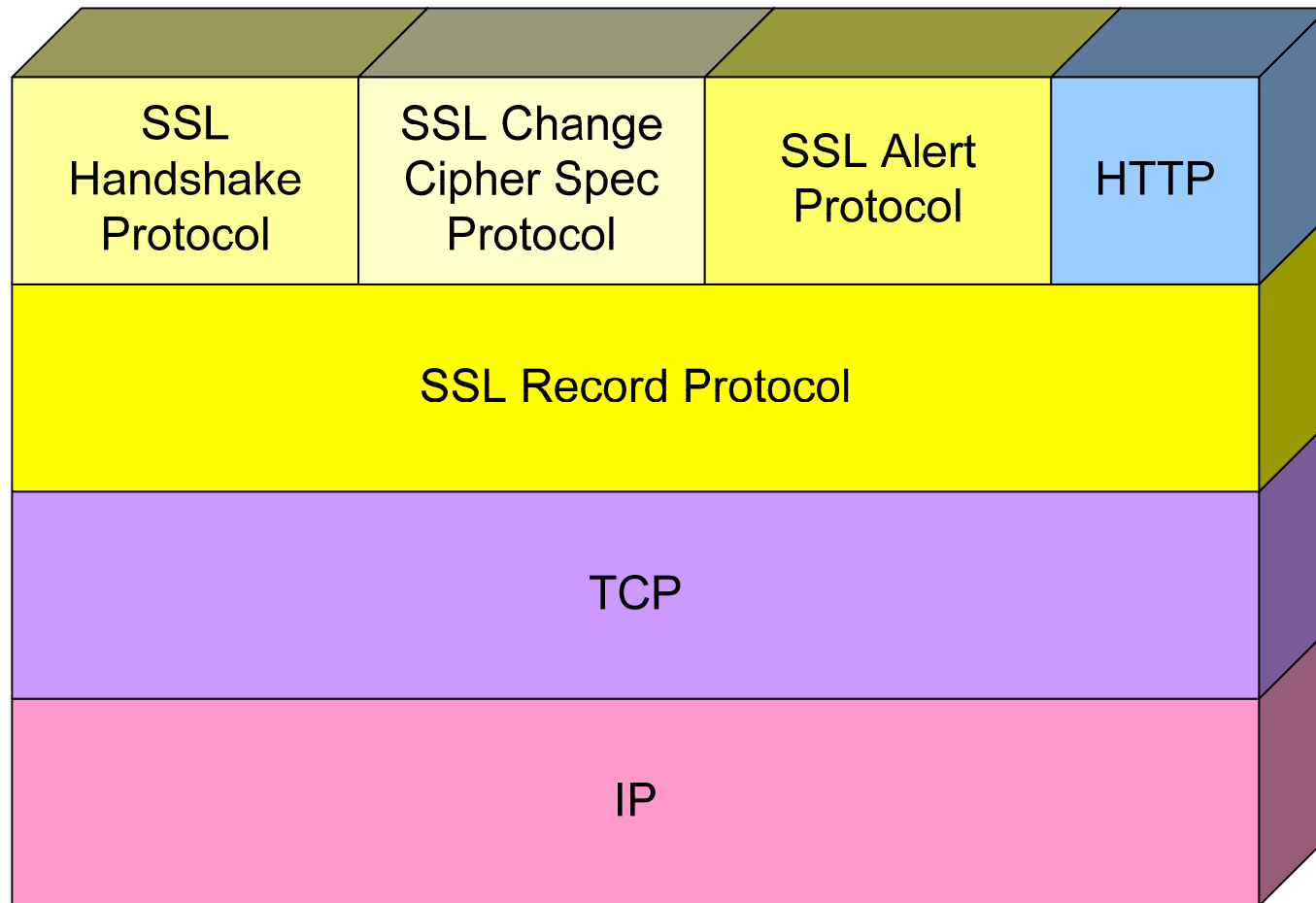
- Es el estándar precursor de TLS (IETF)
- SSLv3.1 sería el equivalente de TLSv1.0
- Utiliza TCP para proporcionar un servicio fiable
- Proporciona las siguientes funciones y servicios:
 - Fragmentación
 - Compresión
 - Autenticación
 - Integridad
 - Confidencialidad

SSL



- El funcionamiento general es el siguiente
 - Establece una sesión
 - Autentifica
 - Negocia los parámetros
 - Comparte los valores secretos
 - Inicia la transferencia de datos
 - Proporcionando integridad y confidencialidad
- No es un protocolo simple. Tiene dos niveles:
 - El protocolo Record en un nivel, proporciona servicios de seguridad básicos a protocolos de nivel superior (como HTTP)
 - Handshake Protocol, Change Cipher Spec Protocol y Alert Protocol, que se hallan en el nivel superior

SSL



SSL



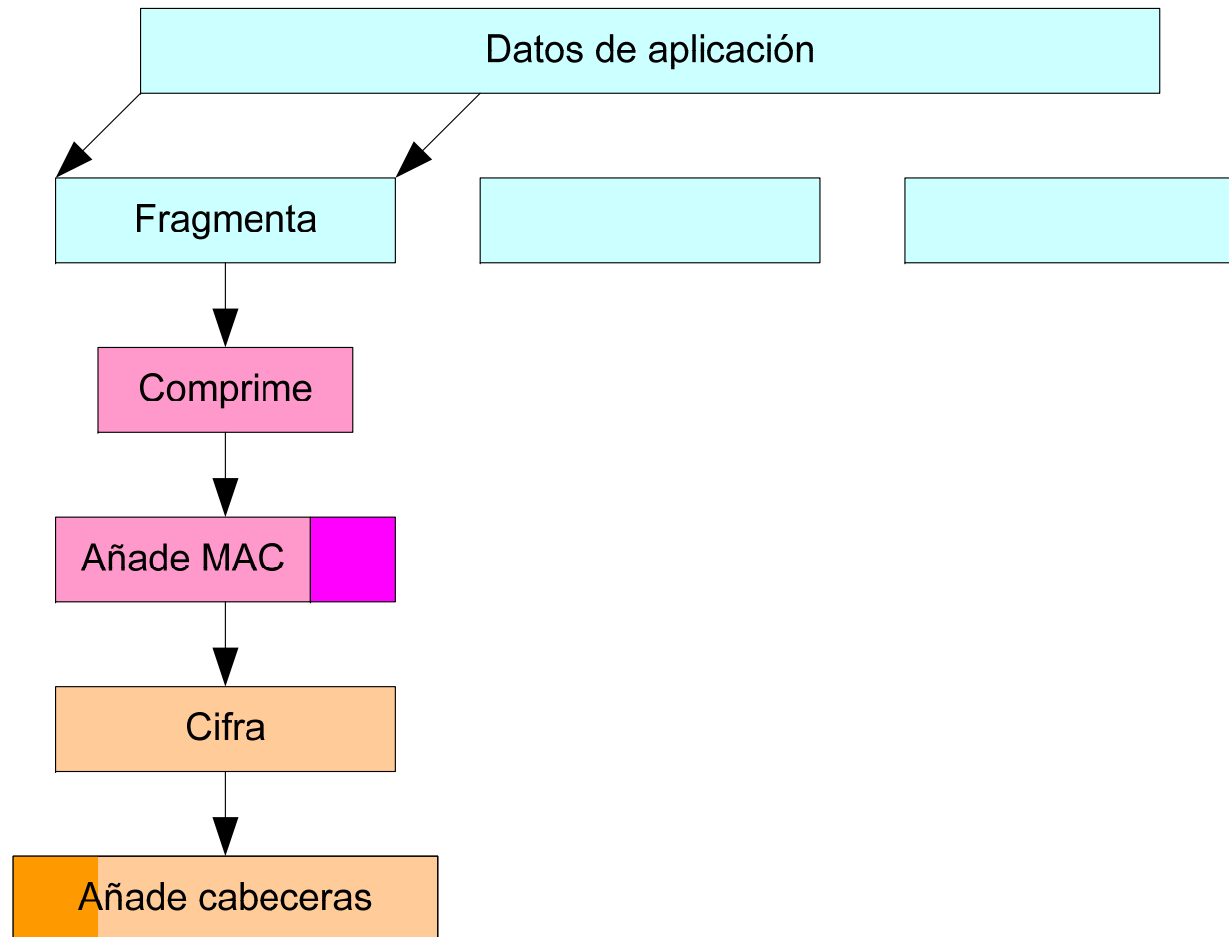
- El protocolo SSL se comporta como una MEF
 - durante una transmisión siempre hay distintos estados
 - estado de escritura activo
 - estado de escritura pendiente
 - estado de lectura activo
 - estado de lectura pendiente
 - Para cambiar de un estado pendiente a otro activo se utiliza el subprotocolo **Change Cypher Spec**
- Dos conceptos importantes de SSL son
 - Sesión SSL
 - Conexión SSL

Protocolo Record de SSL

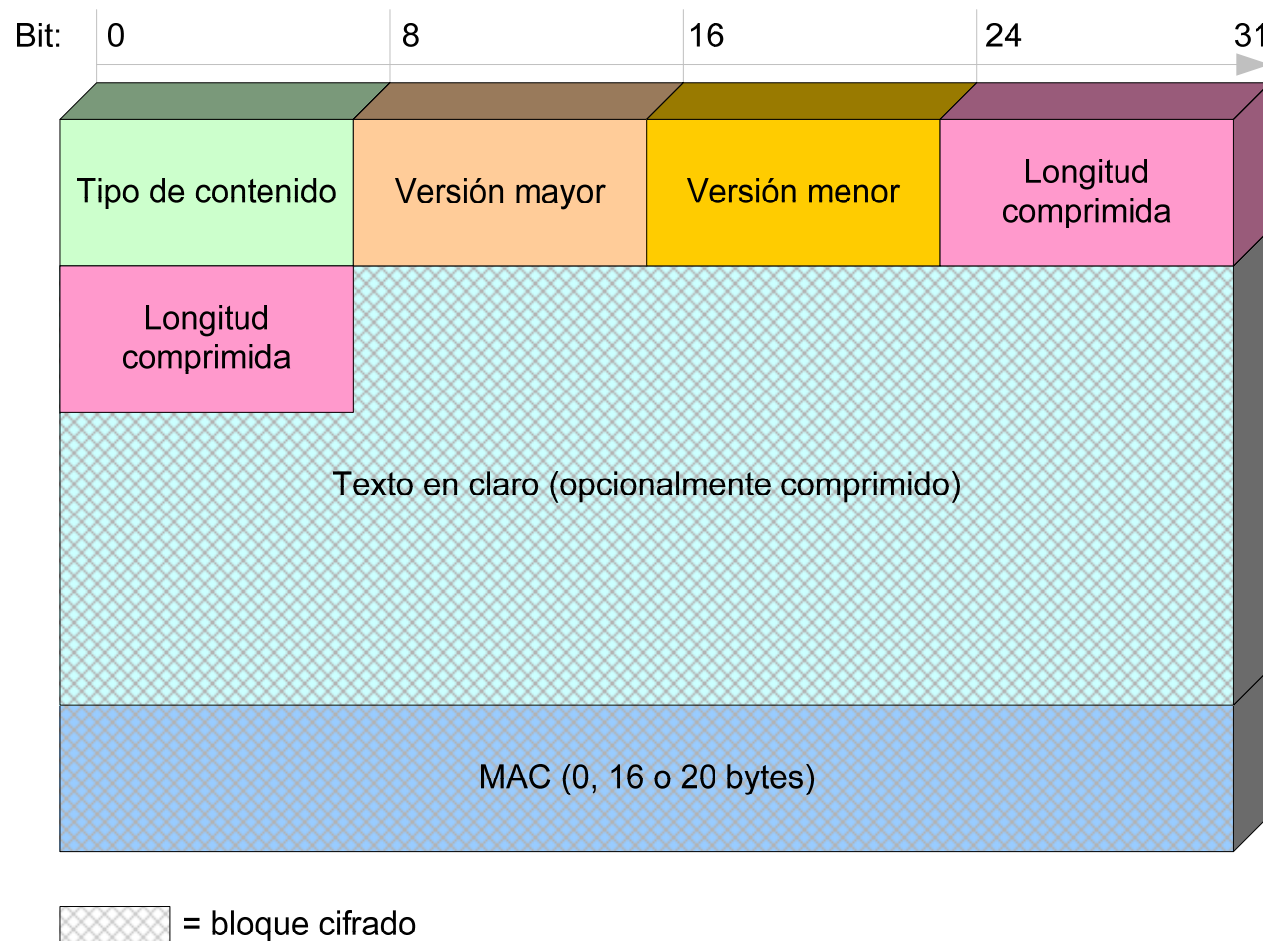


- Proporciona dos servicios a las conexiones SSL
 - Confidencialidad
 - Integridad de mensajes
- Realiza las siguientes funciones en su operación:
 - Fragmenta los datos de aplicación
 - Comprime los datos
 - Autentifica los datos comprimidos
 - Cifra los datos comprimidos y autenticados
 - Añade las cabeceras SSL correspondientes

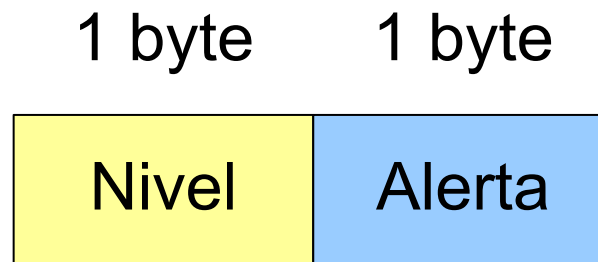
Protocolo Record de SSL



Protocolo Record de SSL Header



Protocolo Alert



- Transmite alertas vinculadas con SSL a la entidad par
- Cada mensaje está formado por dos bytes
 - El primer byte toma el valor de aviso (1) o fatal (2)
 - El segundo contiene un código que indica la alerta específica
 - Alertas fatales:
 - Alertas de aviso

Protocolo Handshake



- Es la parte más compleja de SSL
- Permite autenticación mutua entre cliente y servidor y negociar algoritmos de MAC y las claves criptográficas
- Se utiliza antes de transmitir los datos de aplicación

Protocolo Handshake

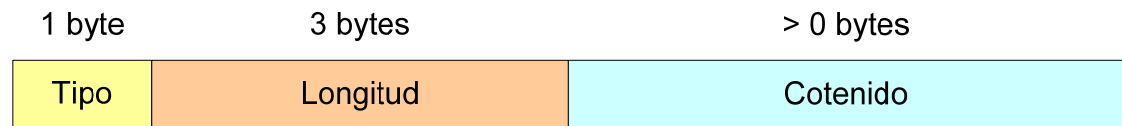
- Los mensajes tienen los siguientes campos

- Tipo

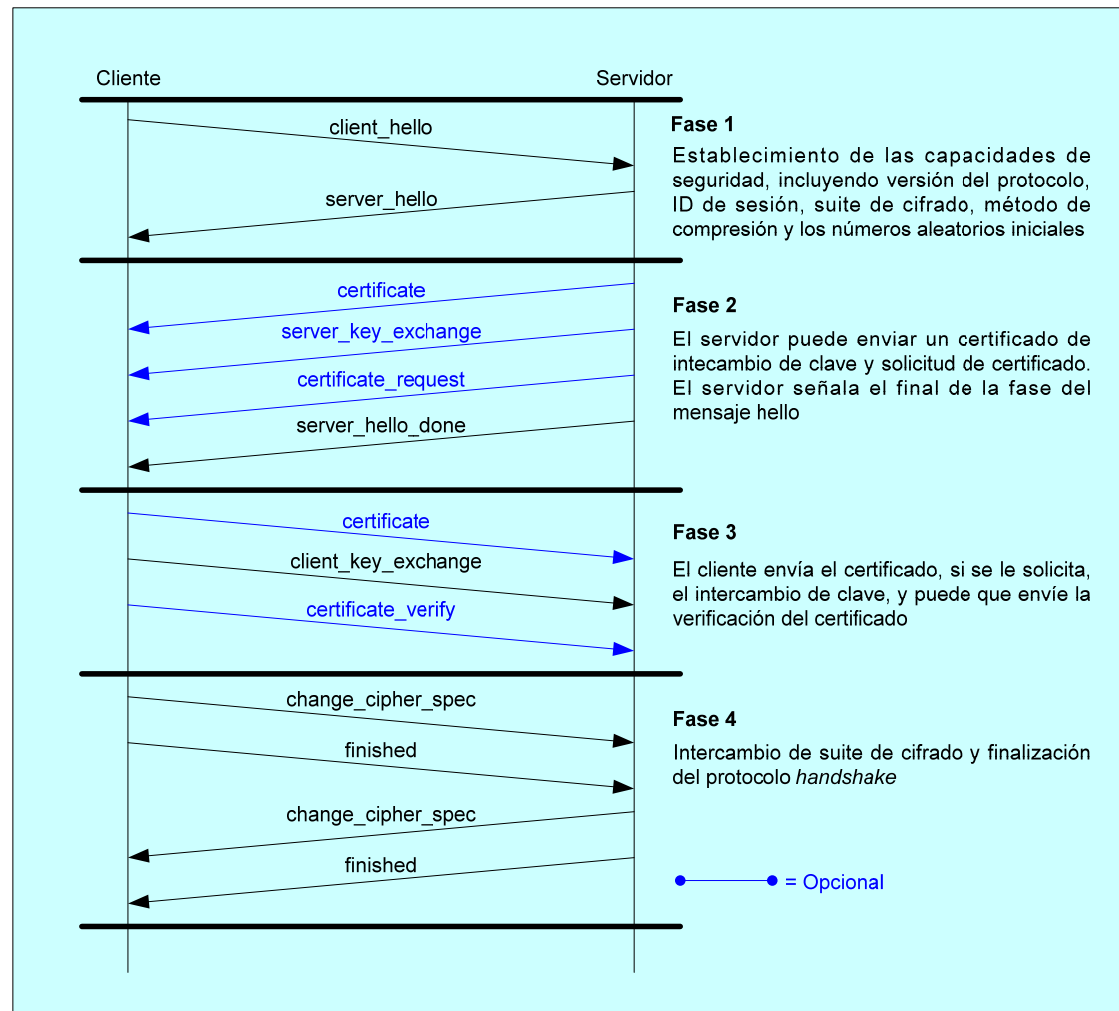
- hello_request
 - client_hello
 - server_hello
 - Certificate
 - Server_key_exchange
 - Certificate_request
 - Server_done
 - Certificate_verify
 - Client_key_exchange
 - Finished

- Longitud

- Contenido



Protocolo Handshake



Aplicaciones de SSL



- HTTPS
- S/MIME
- Telnet, FTP
- Muchas aplicaciones más
 - <http://www.openssl.org/related/apps.html>