William Stallings
Comunicaciones y Redes de Computadores

Capítulo 18

Seguridad en redes

Requisitos para la seguridad

- Secreto.
- Integridad.
- Disponibilidad.

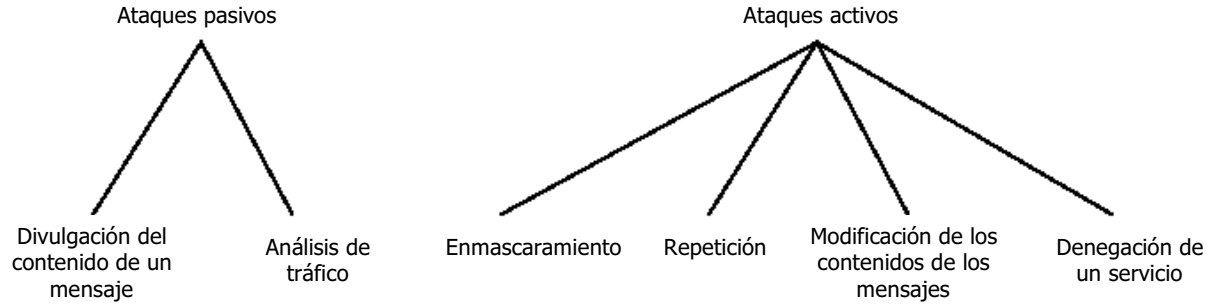
Ataques pasivos

- Escuchas de las transmisiones.
- Para obtener información.
- Divulgación del contenido del mensaje:
  - El intruso se entera del contenido de la transmisión.
- Análisis del tráfico:
  - Controlando la frecuencia y la longitud de los mensajes, incluso los cifrados, se puede adivinar la naturaleza de la conexión.
- Difíciles de detectar.
- Se pueden prevenir.

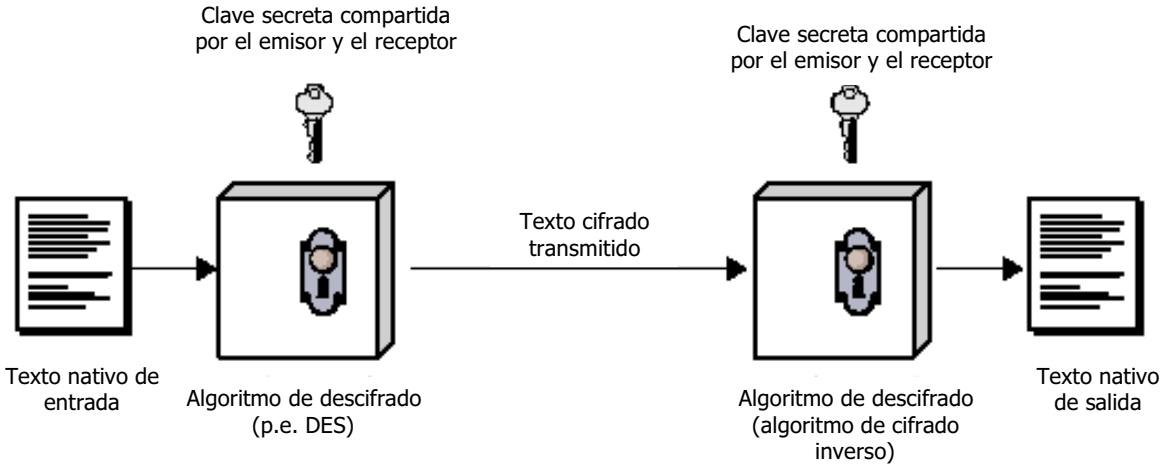
Ataques activos

- Enmascaramiento:
  - Una entidad pretende ser otra entidad diferente.
- Repetición.
- Modificación de mensajes.
- Denegación de un servicio.
- Fácil de detectar:
  - La detección tiene un efecto disuasivo.
- Difícil de prevenir.

Agresiones a la seguridad de red



Cifrado convencional



Ingredientes

- Texto nativo.
- Algoritmo de cifrado.
- Clave secreta.
- Texto cifrado.
- Algoritmo de descifrado.

Requisitos para la seguridad

- Algoritmo de cifrado robusto:
  - Incluso si conoce el algoritmo, no debería ser capaz de descifrar el texto o describir la clave.
  - Incluso si posee un determinado número de textos cifrados junto con los textos nativos que produce cada texto.
- El emisor y el receptor deben haber obtenido las copias de la clave secreta de una forma segura.
- Una vez que se conoce la clave, todas las comunicaciones que utilicen esta clave pueden ser leídas.

Ataque al sistema de cifrado convencional

- Criptoanálisis:
  - Se basa en la naturaleza del algoritmo más algún conocimiento de las características generales del texto nativo.
  - Intento de deducir un texto nativo o la clave.
- Fuerza bruta:
  - Intentar cada clave posible hasta que se obtenga una traducción inteligible del texto nativo.

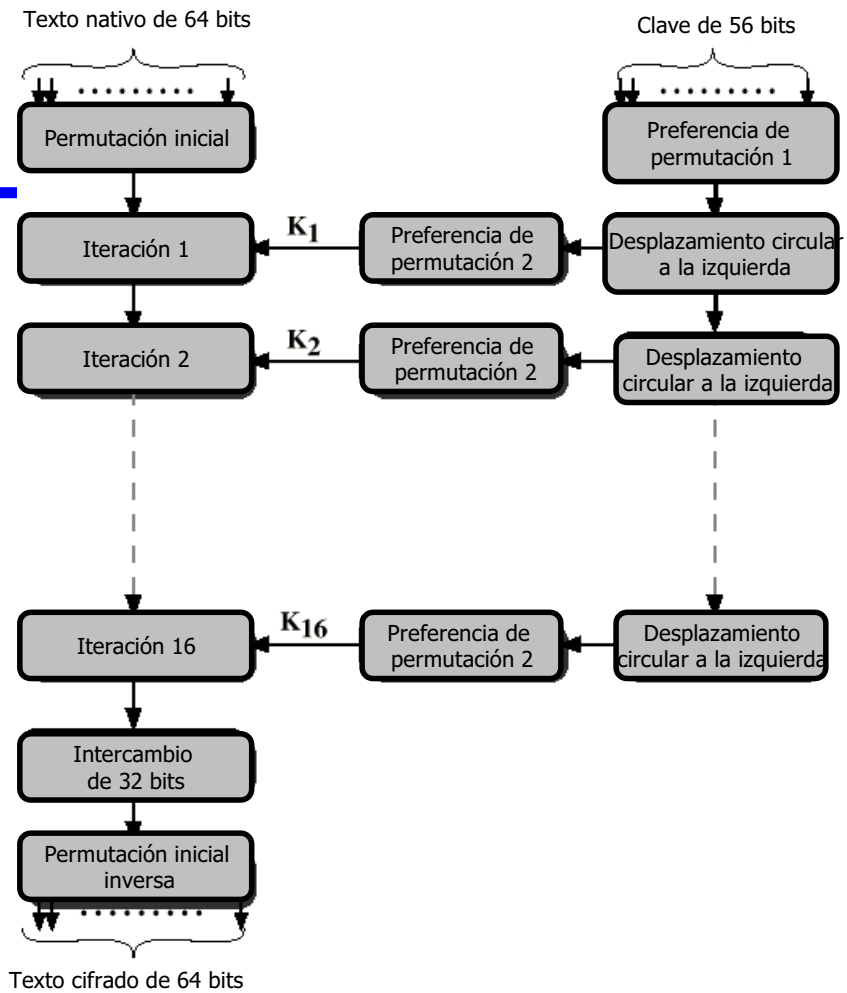
Algoritmos

- Cifradores de bloque:
  - Procesan una entrada de texto nativo en bloques de tamaño fijo, y produce un bloque de texto cifrado de igual tamaño.
  - Estándar de cifrado de datos (DES).
  - DEA Triple (TDEA).

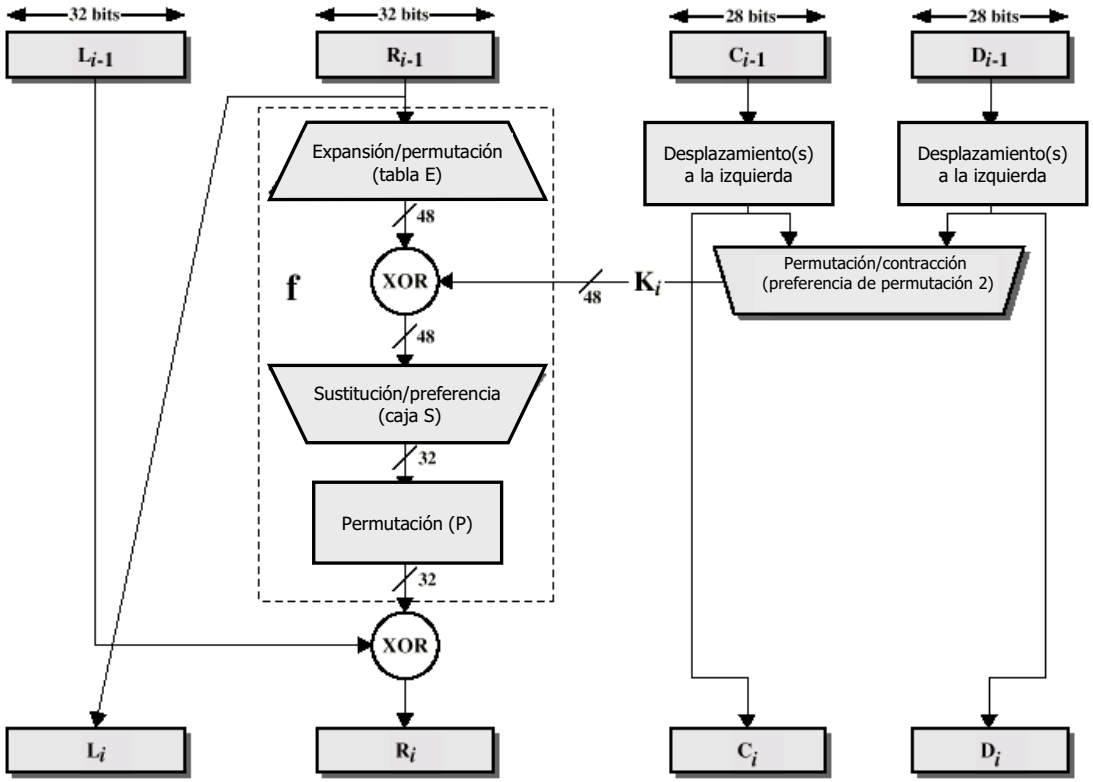
Estándar de cifrado de datos

- Estándar en EE.UU.
- Bloques de texto nativo de 64 bits.
- Clave de 56 bits.

Algoritmo de cifrado DES



Interación simple del algoritmo DES



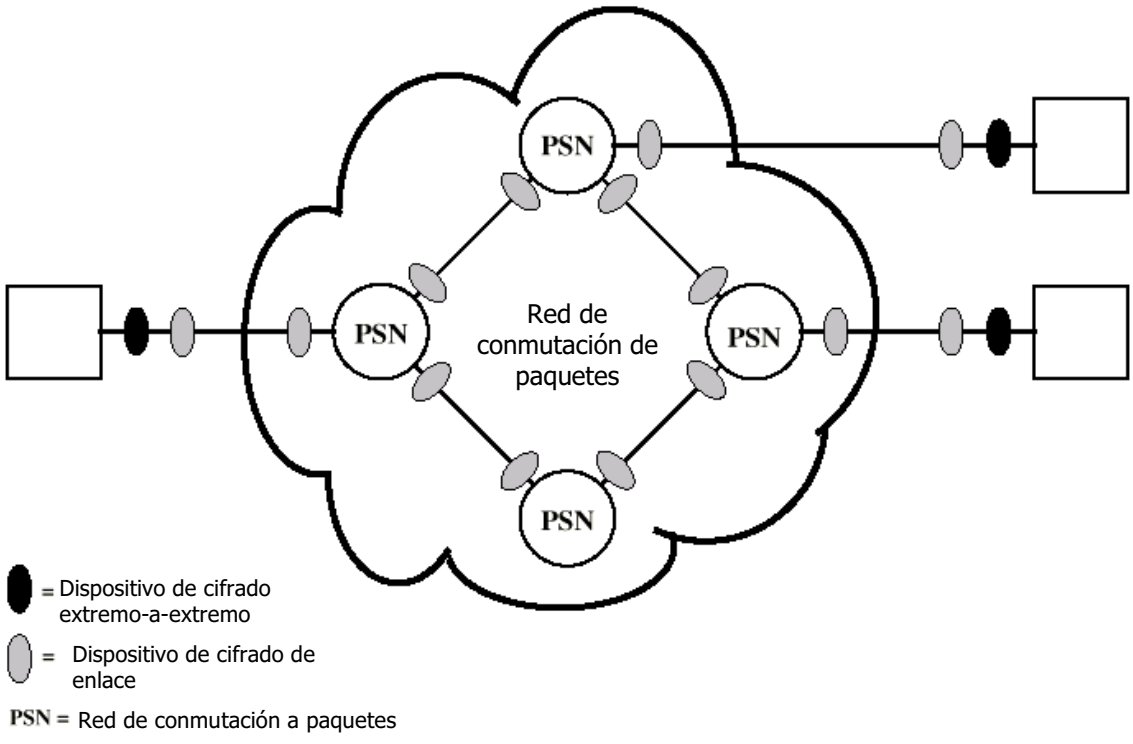
La potencia de DES

- Declarada insegura en 1998.
- Fundación las Fronteras Electrónicas (EFF, Electronic Frontier Foundation).
- Máquina saboteadora de DES.
- Actualmente, DES no tiene ningún valor.
- Entre las alternativas está el DEA Triple.

DEA Triple

- ANSI X9.17 de 1985.
- Incorporado como una parte del Estándar de Cifrado de Datos en 1999.
- Utiliza tres claves y tres ejecuciones del algoritmo DES.
- Longitud de clave efectiva de 168 bits.

Localización de los dispositivos de cifrado



Cifrado de enlace

- Cada enlace de comunicación tiene un dispositivo de cifrado a ambos lados.
- Todo el tráfico se protege.
- Alto grado de seguridad.
- Requiere muchos dispositivos de cifrado.
- El mensaje debe ser descifrado en cada conmutador para leer la dirección (número de circuito virtual).
- El mensaje es vulnerable en cada nodo:
  - Especialmente si la red es de conmutación de paquetes pública.

Cifrado extremo-a-extremo

- El cifrado se hace en los dos sistemas finales.
- Los datos cifrados se transmiten sin alteraciones a través de la red.
- El destino comparte una clave con el origen para descifrar los datos.
- El computador sólo puede descifrar los datos del usuario:
  - Si no, los nodos de conmutación no podrían leer la cabecera o paquete de encaminamiento.
- Modelo de tráfico no seguro.
- Uso de cifrado de enlace y extremo-a-extremo.

Distribución de claves

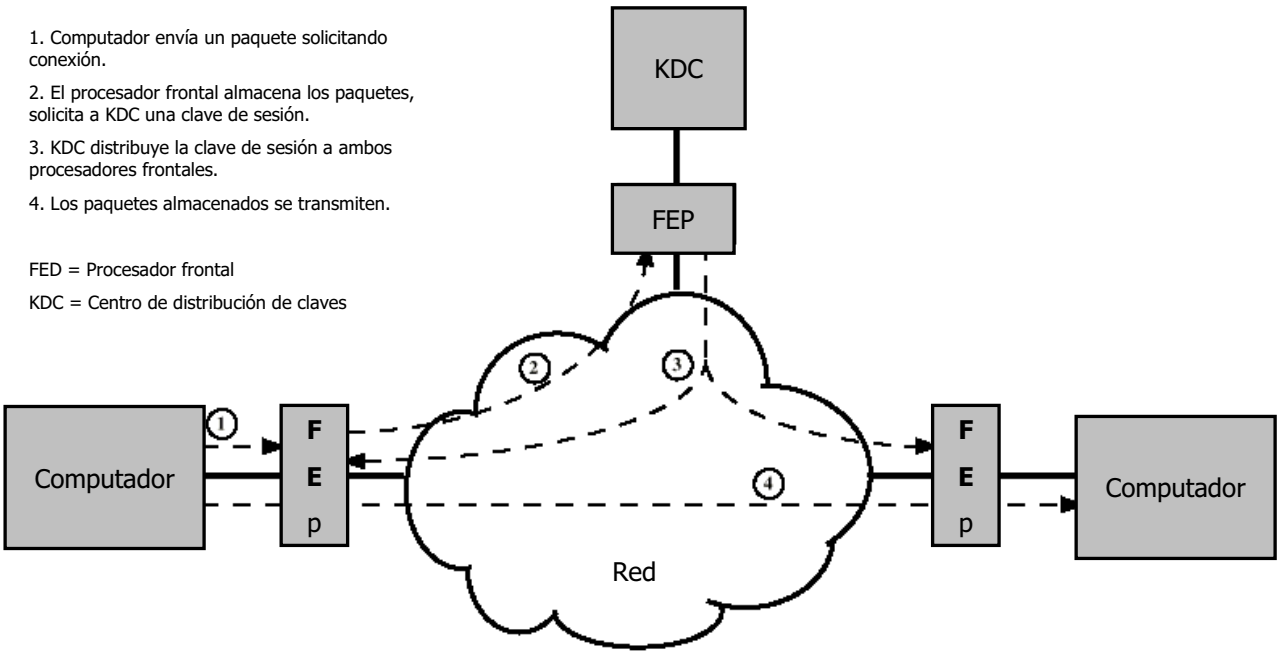
- A selecciona la clave y la entrega a B.
- Una tercera parte selecciona la clave y la entrega a A y a B.
- Se utiliza la clave previa para cifrar y transmitir una nueva clave de A a B.
- Se usa la clave antigua para transmitir la clave nueva de la tercera parte a A y a B.

Distribución de claves automática

1. Computador envía un paquete solicitando conexión.
2. El procesador frontal almacena los paquetes, solicita a KDC una clave de sesión.
3. KDC distribuye la clave de sesión a ambos procesadores frontales.
4. Los paquetes almacenados se transmiten.

FED = Procesador frontal

KDC = Centro de distribución de claves



Distribución de claves automática

- Clave de sesión:
  - Se usa durante el tiempo de una conexión lógica.
  - Se destruye al final de la sesión.
  - Se utiliza para los datos del usuario.
- Clave permanente:
  - Empleada para la distribución de claves.
- Centro de distribución de claves:
  - Determina qué sistemas pueden comunicarse.
  - Proporciona una clave de sesión de un solo uso a esa conexión.
- Procesador frontal:
  - Lleva a cabo el cifrado extremo-a-extremo.
  - Obtiene las claves de sesión en representación de su computador.

Relleno de tráfico

- Produce salida de texto cifrado continuamente.
- Cuando no hay disponible texto nativo, los datos aleatorios se cifran y transmiten.
- Resulta imposible deducir la cantidad de tráfico.

Autentificación de mensajes

- Protección frente a las agresiones activas:
  - Falsificación de datos.
  - Escuchas.
- Un mensaje está autentificado cuando es genuino y viene del origen pretendido.
- La autentificación permite al receptor verificar que el mensaje recibido es auténtico:
  - No se ha alterado el mensaje.
  - El origen del mensaje es auténtico.
  - Los datos son oportunos.

Autentificación utilizando cifrado

- Supone que el emisor y el receptor son los únicos que conocen la clave.
- El mensaje incluye:
  - Un código de detección de errores.
  - Un número de secuencia.
  - Una marca de tiempo.

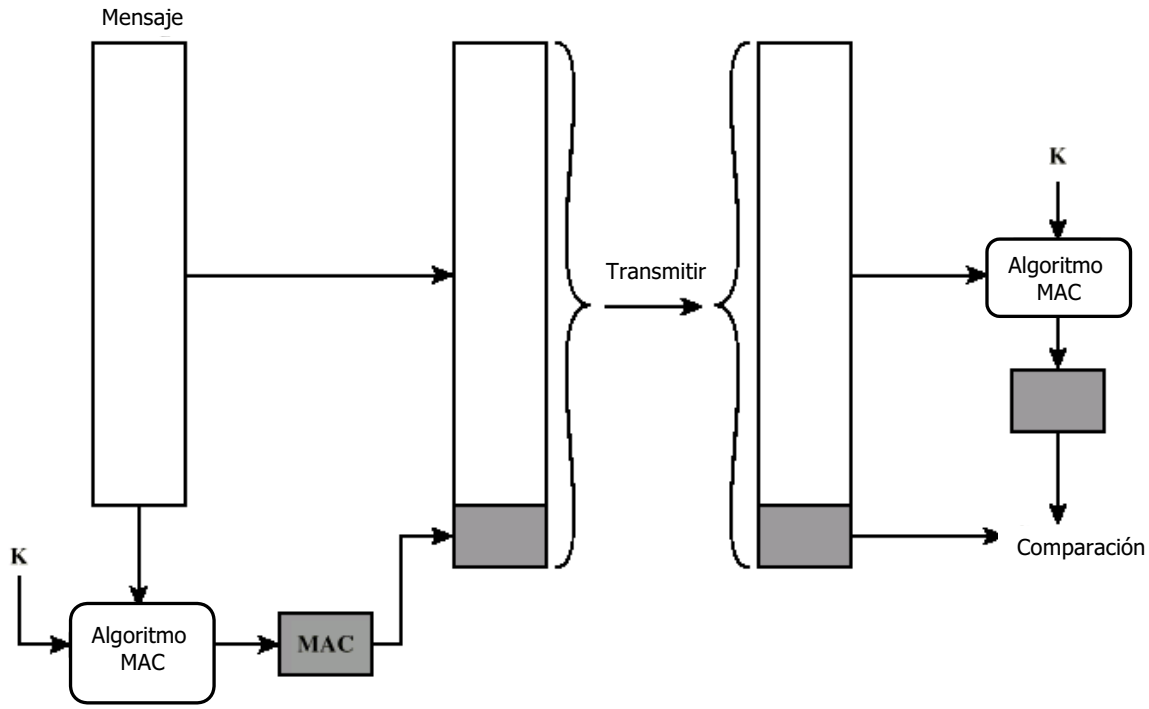
Autentificación sin cifrado

- Se genera e incorpora a cada mensaje una etiqueta de autentificación.
- Mensaje no cifrado.
- Útil para:
  - Mensajes enviados a varios destinos:
    - Sólo existe un destino responsable de la autentificación.
  - Casos en los que una de las partes tiene una carga muy elevada:
    - El cifrado supone una gran carga de trabajo.
    - Puede autentificar mensajes elegidos de forma aleatoria.
  - Programas autentificados sin cifrado. Se pueden ejecutar sin descifrarlos.

Código de autentificación de mensajes

- Genera un código de autentificación basándose en la clave compartida y en el mensaje.
- Clave secreta compartida entre A y B.
- Si sólo el emisor y el receptor conocen la clave y el código coincide:
  - El receptor está seguro de que el mensaje no ha sido alterado.
  - El receptor está seguro de que el mensaje es del emisor pretendido.
  - Si el mensaje incluye un número de secuencia, el receptor está seguro de la secuencia adecuada.

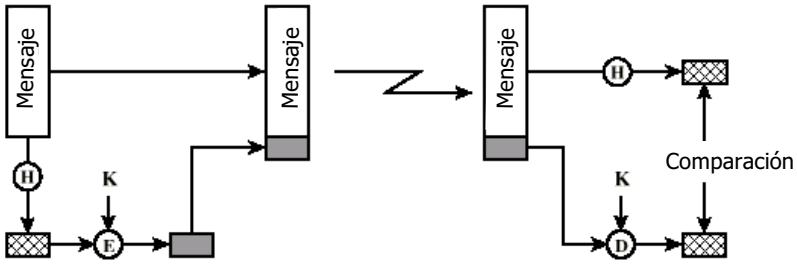
Autentificación de mensajes utilizando un código de autentificación de mensaje



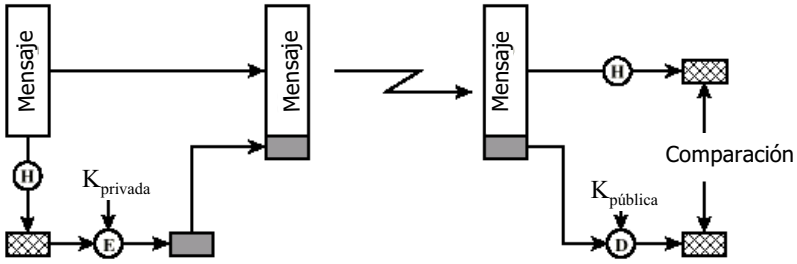
Función de dispersión de un solo sentido

- Acepta mensajes de longitud variable y produce una etiqueta de tamaño fijo (resumen del mensaje).
- Ventajas de la autentificación sin cifrado:
  - El cifrado es lento.
  - El hardware de cifrado es caro.
  - El hardware de cifrado está optimizado para tamaños de datos grandes.
  - Algoritmos protegidos por patentes.
  - Algoritmos sujetos a controles de exportación (desde EE.UU.).

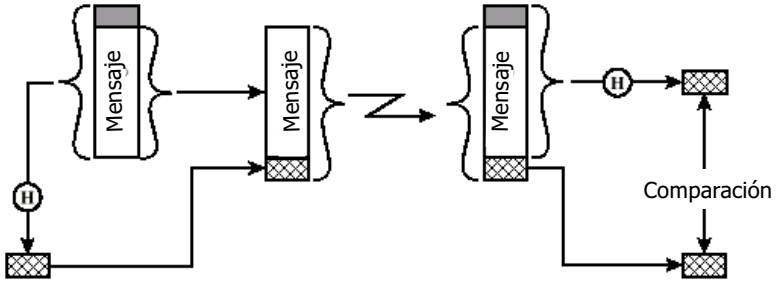
Uso de función de dispersión de un solo sentido



(a) Utilizando cifrado convencional



(b) Utilizando cifrado de clave pública



(c) Utilizando un valor secreto

Funciones de dispersión seguras

- Una función de dispersión H debe tener las siguientes propiedades:
  - Se puede aplicar a bloques de datos de cualquier tamaño.
  - Produce una salida de longitud fija.
  - Fácil de calcular.
  - No es posible invertirla.
  - No es posible encontrar dos mensajes que produzcan el mismo valor.

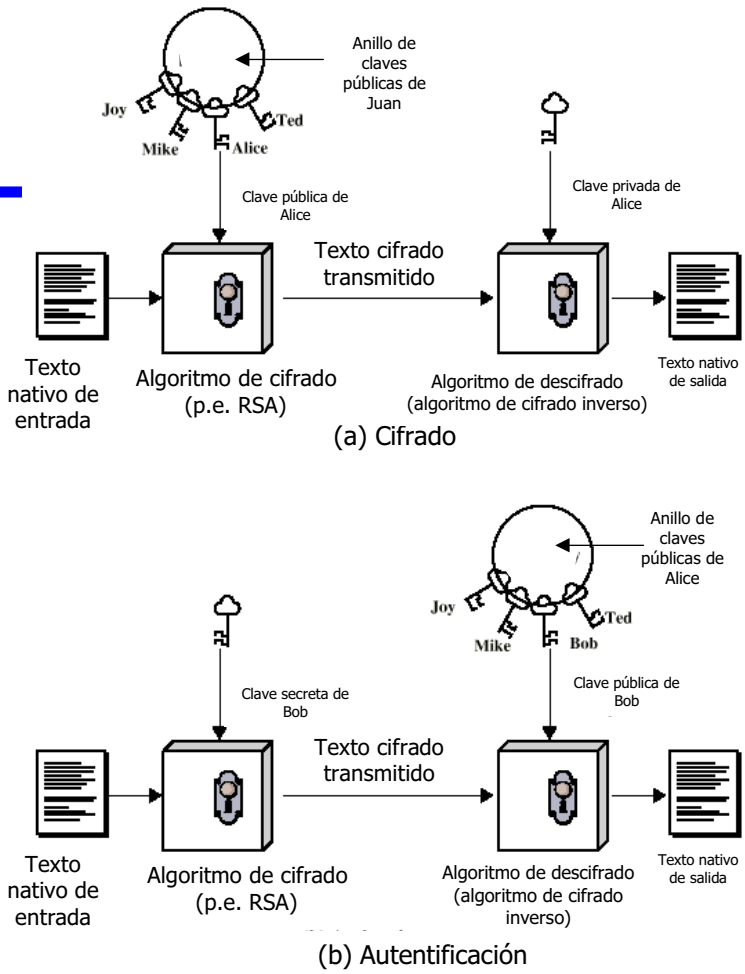
SHA-1

- Algoritmo seguro de dispersión 1.
- Mensaje de entrada con longitud máxima de 2^{64} bits:
  - Procesado en bloques de 512 bits.
- Produce un resumen del mensaje de 160 bits.

Cifrado de clave pública

- Se basa en funciones matemáticas.
- Asimétrica:
  - Usa dos claves independientes.
- Ingredientes:
  - Texto nativo.
  - Algoritmo de cifrado.
  - Clave pública y privada.
  - Texto cifrado.
  - Algoritmo de descifrado.

Cifrado de clave pública



Técnica de cifrado de clave pública

- Una clave se hace pública:
  - Se usa para el cifrado.
- Otra clave se mantiene privada:
  - Se usa para el descifrado.
- No es factible determinar la clave de descifrado dadas la clave de cifrado y el algoritmo.
- Cualquiera de las claves se puede usar para cifrar, la otra para descifrar.

Pasos

- Cada usuario genera un par de claves.
- Cada usuario publica una de las dos claves.
- Para enviar un mensaje al usuario, se cifra el mensaje utilizando la clave pública.
- El usuario descifra el mensaje utilizando su clave privada.

Firma digital

- El emisor cifra el mensaje con su clave privada.
- El receptor puede descifrar el mensaje utilizando la clave pública del emisor.
- Esto autentifica al emisor, que es la única persona que tiene la clave que coincide.
- No proporciona privacidad a los datos:
  - La clave de descifrado es pública.

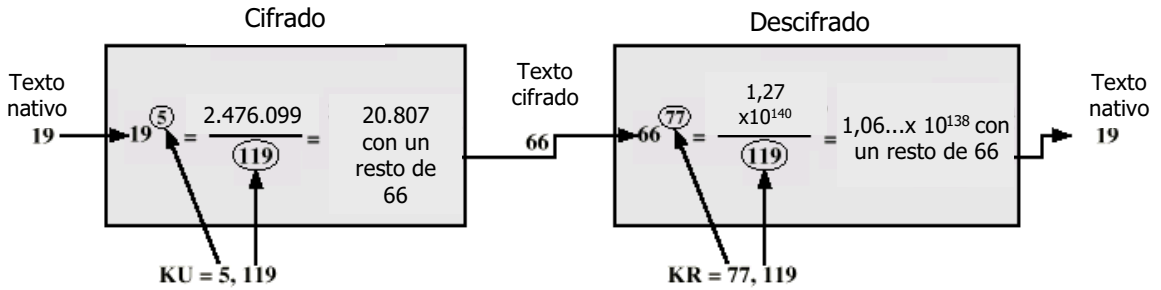
El algoritmo RSA

Generación de clave	
Seleccionar p, q	p y q ambos primos
Calcular n= p x q	
Calcular $\phi(n) = (p-1)(q-1)$	
Seleccionar entero e	$\gcd(\phi(n), e = 1; 1 < e < \phi(n)$
Calcular d	$d = e^{-1} \bmod \phi(n)$
Clave pública	KU = {e, n}
Clave privada	KR = {d, n}

Cifrado	
Texto nativo:	$M < n$
Texto cifrado:	$C = M^e \pmod n$

Descifrado	
Texto nativo:	C
Texto cifrado:	$M = C^d \pmod n$

Ejemplo del algoritmo RSA



Seguridad con IPv4 e IPv6

- IPSec.
- Conectividad segura entre oficinas sucursales a través de Internet.
- Acceso remoto seguro a través de Internet.
- Conectividad intranet y extranet con asociados.
- Mejora de la seguridad en el comercio electrónico.

Ámbito de IPSec

- Cabecera de Autentificación.
- Encapsulado de seguridad de la carga útil.
- Intercambio de claves.
- RFC$_s$ 2401,2402,2406,2408.

Asociaciones de seguridad

- Relación en un solo sentido entre el emisor y el receptor.
- En el caso de intercambio en dos sentidos, se necesitan dos asociaciones de seguridad.
- Tres parámetros que identifican una asociación de seguridad:
  - Índice de parámetros de seguridad.
  - Dirección IP destino.
  - Identificador del protocolo de seguridad.

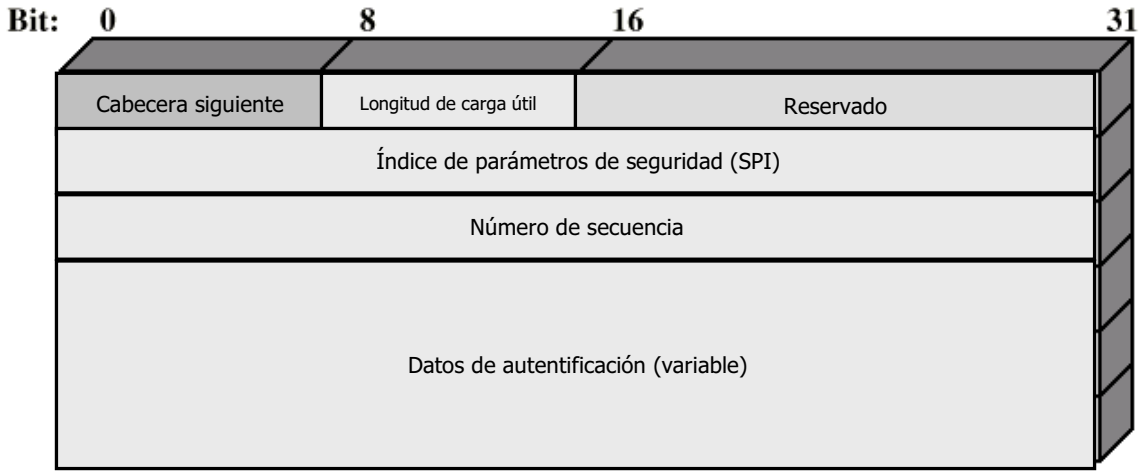
Parámetros asociados con cada SA

- Contador de número de secuencia.
- Desbordamiento del contador de secuencia.
- Ventana anti-repeticiones.
- Información AH.
- Información ESP.
- Tiempo de vida de la asociación de seguridad.
- Modo de protocolo IPSec:
  - Túnel, transporte o marca de ambos.
- MTU del camino.

Modos de transporte y modos túnel

- Modo transporte ESP:
  - Protección a los protocolos de las capas superiores.
  - Se extiende a la carga útil de un paquete IP.
  - Extremo-a-extremo entre dos computadores.
- Modo túnel ESP:
  - Protección al paquete IP.
  - El paquete entero se trata como la carga útil de un paquete IP exterior.
  - Ningún dispositivo de encaminamiento examina el paquete interior.
  - Puede tener direcciones de origen y destino totalmente diferentes.
  - Se puede aplicar en el cortafuegos.

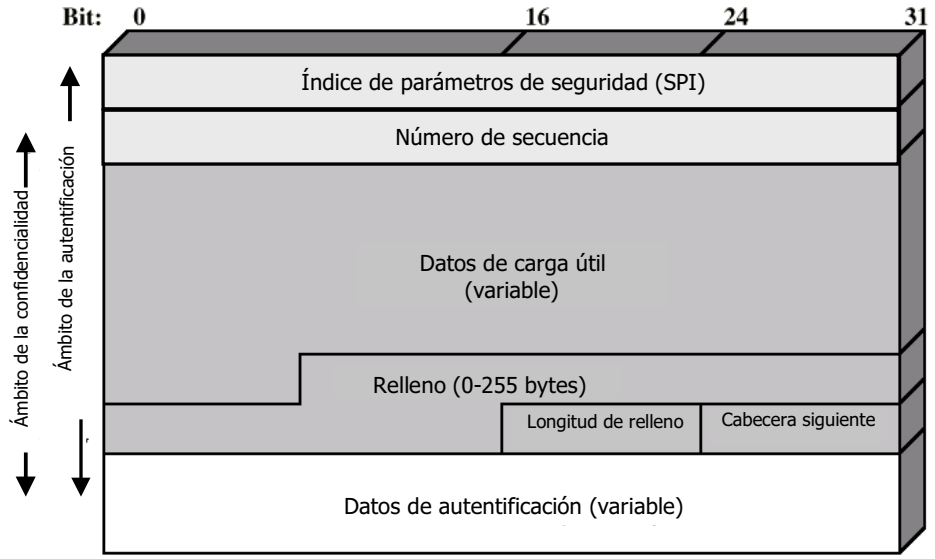
Cabecera de autentificación



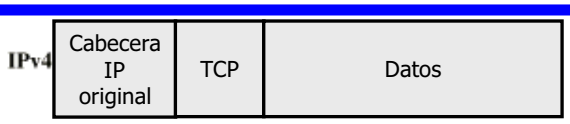
Encapsulado de seguridad de la carga útil

- ESP
- Servicios de privacidad.

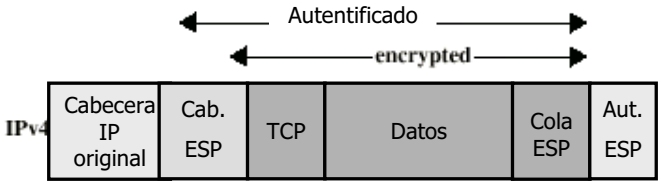
Formato ESP



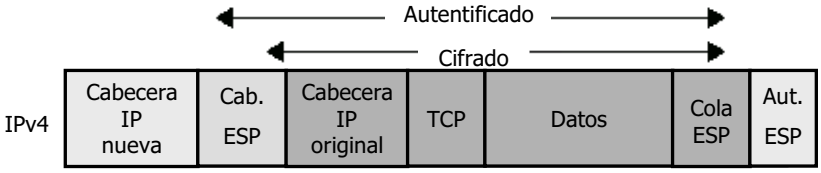
Ámbito de ESP



(a) Paquete IP original



(b) Modo transporte



(c) Modo túnel

Gestión de claves

- Manual.
- Automática:
  - ISAKMP/Oakley:
    - Protocolo de intercambio de claves Oakley.
    - Asociación de Seguridad de Internet y protocolo de Gestión de claves.

Lecturas recomendadas

- Stallings, W. *Comunicaciones y Redes de Computadores*, sexta edición. Madrid: Prentice Hall, 2000: Capítulo 18.