4 FUNCIONES HASH CRIPOGRÁFICAS

Manual de clases

Objetivo

- Describir cómo se generan los códigos de autenticación de mensajes que permiten proporcionar mecanismos para asegurar la integridad de los mensajes.

Última modificación:
29 de junio de 2022

Tema 4 de:
SEGURIDAD EN REDES DE COMPUTADORAS

Edison Coimbra G.

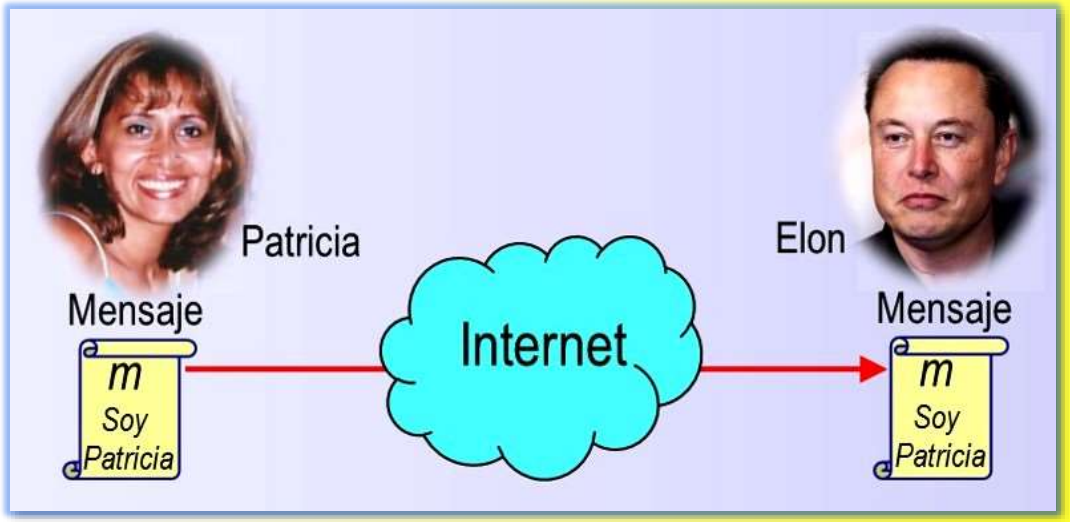
1.- EL PROBLEMA DE LA INTEGRIDAD DE LOS MENSAJES

FUNCIONES HASH CRIPTOGRÁFICAS

¿Cuál es el problema de la integridad de los mensajes?

(Kurose, 2017)

- **La integridad de los mensajes** es una de las cuatro propiedades deseables en una comunicación segura. Dos personas quieren estar seguras de que el contenido de sus comunicaciones no se ve alterado durante la transmisión, ni maliciosamente ni por accidente.
- **El cifrado criptográfico** se utiliza para proporcionar confidencialidad a dos entidades que desean comunicarse, pero también se lo utiliza para proporcionar integridad a los mensajes (técnica también conocida como autenticación de mensajes).
- **Para definir** el problema de la integridad de los mensajes, suponga que Elon recibe un mensaje de Patricia (que puede estar cifrado o en texto en claro) y que él cree que este mensaje fue enviado por Patricia. Para autenticar el mensaje, Elon tiene que verificar que:
  - ▶El origen del mensaje es efectivamente Patricia.
  - ▶El mensaje no ha sido alterado mientras viajaba hasta Elon.
- **Este problema** de integridad de los mensajes es una preocupación critica en prácticamente todos los protocolos de red seguros.



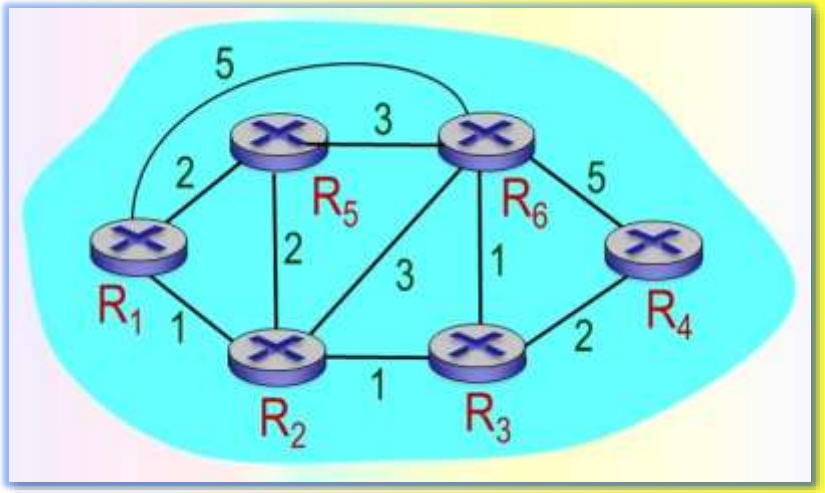
El problema de la integridad de los mensajes

El problema de la integridad de los mensajes

FUNCIONES HASH CRIPTOGRÁFICAS

La importancia de la integridad de los mensajes

- **Considere una red de computadoras** en la que se está empleando el algoritmo de routing de estado del enlace, OSPF, para determinar las rutas entre cada pareja de routers de la red. En este tipo de algoritmo, cada router necesita multidinfundir un mensaje de estado del enlace a todos los restantes routers de la red.

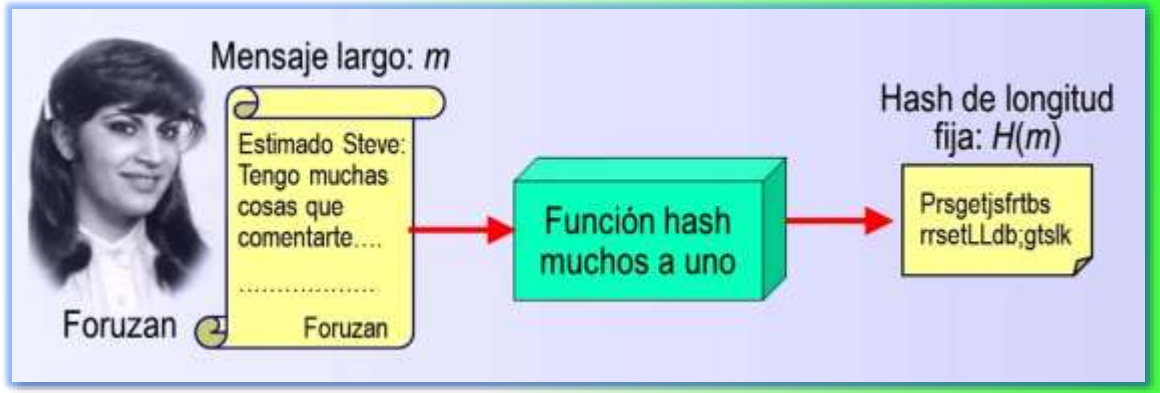


- **El mensaje de estado** del enlace de un router incluye una lista de sus vecinos directamente conectados, junto con los costos directos a esos vecinos. Una vez que un router recibe estos mensajes de todos los demás router, puede crear un mapa completo de la red (ver figura), ejecutar un algoritmo de routing de costo mínimo (el algoritmo de Dijkstra) y configurar su tabla de routing.
- **Un ataque** relativamente sencillo contra el algoritmo de routing consiste en que el atacante distribuya mensajes falsos de estado del enlace con información incorrecta acerca del estado de los enlaces.
- **Debido a la necesidad** de integridad de los mensajes, cuando el router B recibe un mensaje de estado del enlace procedente del router A, debe verificar que efectivamente el router A ha creado dicho mensaje y, además, que nadie lo ha alterado mientras que el mensaje se encontraba en tránsito.
- **Para proporcionar** integridad a los mensajes (técnica también conocida como autenticación de mensajes) se utilizan, mayormente, las funciones hash criptográficas.

Primeras funciones hash criptográficas

(Kurose, 2017)

- **Una función hash** toma una entrada, *m*, y calcula una cadena de tamaño fijo *H*(*m*) conocida con el nombre de hash.
- **Cumplen** con esta definición, las técnicas utilizadas para la detección de errores, es decir, para determinar si los bits contenidos en un mensaje enviado han sido alterados según se desplazaban desde el origen hasta el destino.
  - ✉ Los bits pueden sufrir alteraciones a causa de la existencia de ruido en los enlaces o mientras estaban almacenados en un router o por efecto de un ataque cibernético.



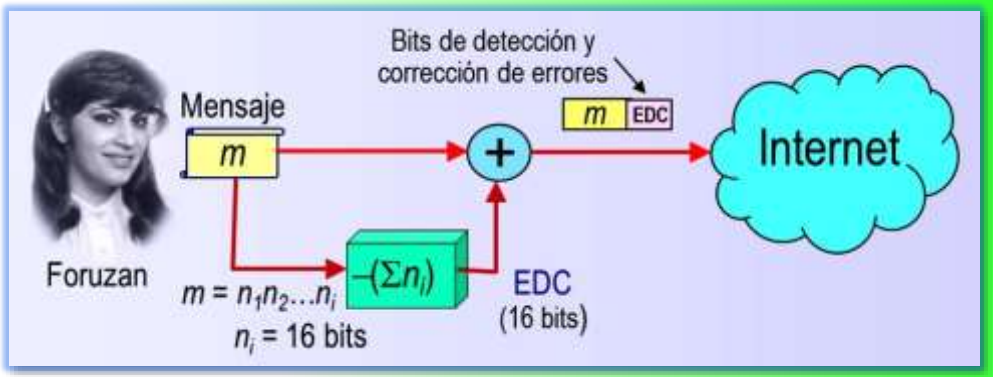
- **Las técnicas de detección** de errores permiten constatar la integridad de los mensajes, entre ellas:
  - ▶La suma de comprobación de Internet. En la capa de transporte, esta suma se calcula sobre todos los campos del segmento UDP o TDP, incluyendo la cabecera y la carga útil. Se implementa por software.
  - ▶El código de redundancia cíclica, CRC. En la capa de enlace se calcula el código CRC o código polinómico sobre todos los campos de la trama del enlace de datos, incluyendo la cabecera y la carga útil. Se implementa en un hardware dedicado dentro de las tarjetas NIC.
- **De entre estas primeras** funciones hash criptográficas solo se hablará de la suma de comprobación de Internet.

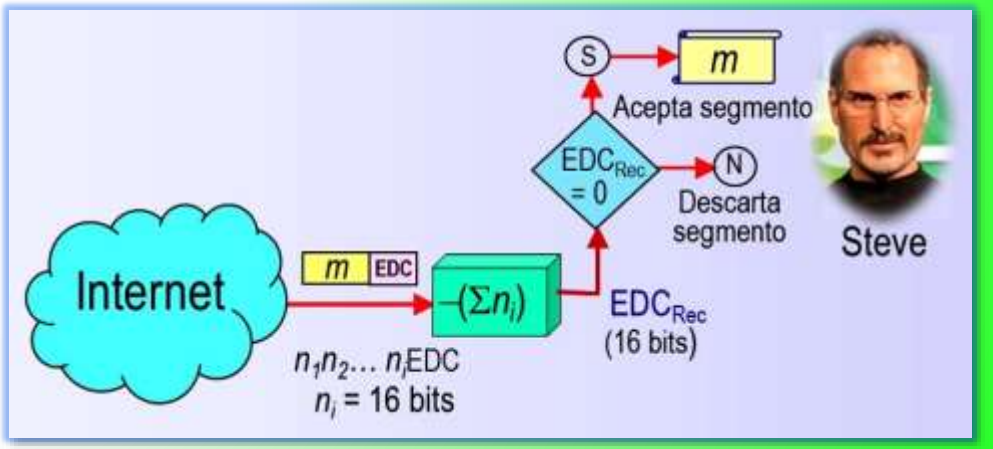
FUNCIONES HASH CRIPTOGRÁFICAS

Función hash: suma de comprobación de Internet

(Kurose, 2017)

- **¿Cómo funciona?** La idea es la siguiente: suponga que los datos son una lista de cinco números de 4 bits cada uno que se quieren enviar a destino: (7, 11, 12, 0, 6).
  - ▶El emisor calcula la suma de todos los datos y envía (7, 11, 12, 0 , 6, -36), donde -36 es el valor negativo de la suma de los números originales (el complemento).
  - ▶El receptor suma todos los números recibidos (incluyendo la suma de comprobación); si el resultado es 0, asume que no hay error, acepta los cinco números y descarta la suma.
- **Con base a este enfoque**, los bytes de datos se tratan como enteros de 16 bits y se suman. Después, se utiliza el complemento a 1 de esta suma para formar la suma de comprobación de Internet, que se denomina, por lo general, EDC (bits de detección y corrección de errores).
- **Los bits EDC** se incluye en la cabecera del segmento de transporte. Esta técnica requiere poca sobrecarga de paquete, solo utiliza 16 bits.



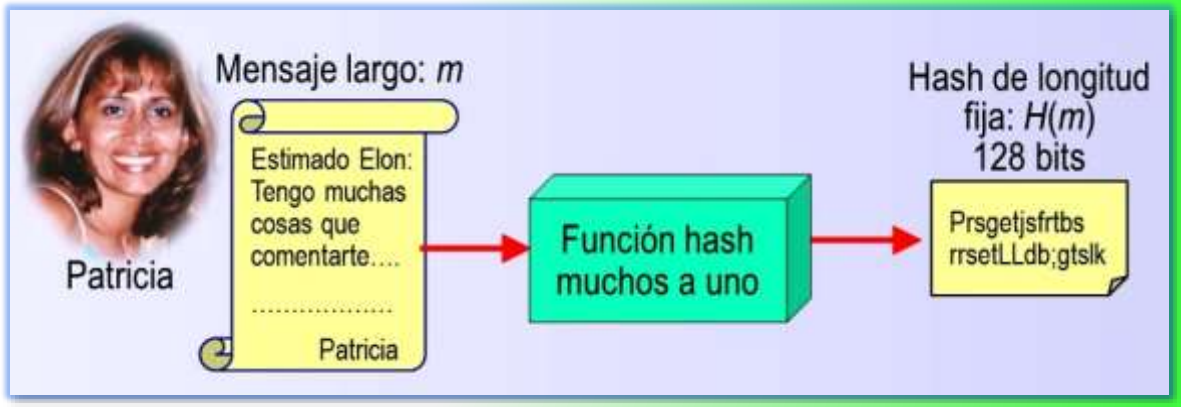


FUNCIONES HASH CRIPTOGRÁFICAS

¿Qué debe hacer una función hash criptográfica para ser potente?

(Kurose, 2017)

- **La suma de comprobación** de Internet proporcionaría una función hash criptográfica bastante poco segura, pues dados los datos originales, es muy sencillo encontrar otro conjunto de datos con la misma suma de comprobación.
- **Obviamente**, para propósitos de seguridad se necesita una función hash bastante mas potente que una mera suma de comprobación.
- **Una función hash** toma una entrada, *m*, y calcula una cadena de tamaño fijo *H*(*m*) conocida con el nombre de hash, de 128 bits.
- **Además**, una función hash criptográfica necesita exhibir la siguiente propiedad adicional:
  - ▶Es computacionalmente impracticable encontrar dos mensaje distintos *x* e *y* tales que *H*(*x*)= *H*(*y*).

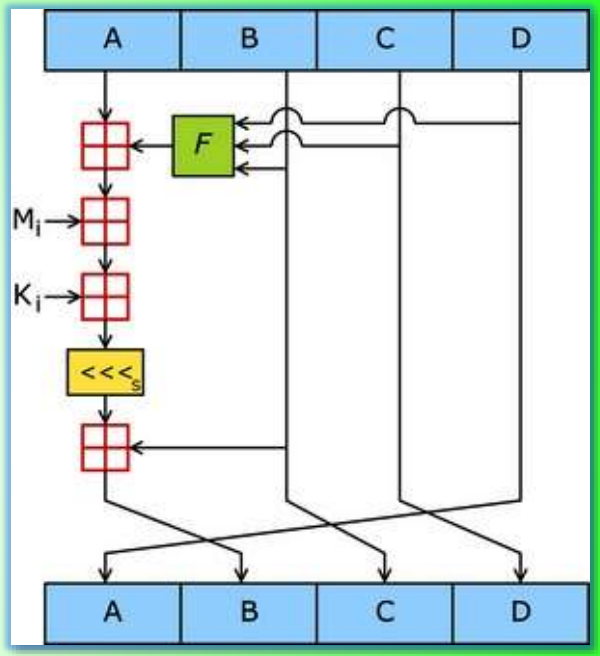


- **De manera informal**, se podría decir que esta propiedad significa que es computacionalmente impracticable que un intruso sustituya un mensaje protegido mediante la función hash por otro mensaje diferente.
- **Es decir**, si (*m, H*(*m*)) son el mensaje y el valor hash de dicho mensaje creado por el emisor, entonces un intruso no puede generar contenido de otro mensaje que tenga el mismo valor de hash que el mensaje original.
- **El hash criptográfico** se utiliza para proporcionar integridad a los mensajes (técnica también conocida como autenticación de mensajes), ya que no se puede generar el mismo hash con otro mensaje cambiado.

FUNCIONES HASH CRIPTOGRÁFICAS

Algoritmos hash

(Kurose, 2017)



- ▶**El algoritmo hash MD5** (Algoritmo de Resumen del Mensaje) de Ron Rivest (RFC 1321) se utiliza ampliamente hoy en día. Este algoritmo calcula un valor hash de 128 bits mediante un proceso en cuatro pasos que consiste en:
  - ▲**1.** Relleno. Se añade al mensaje un bit "1" seguido del número de "0"s suficiente como para que la longitud de mensaje satisfaga ciertas condiciones.
  - ▲**2.** Agregación. Una representación de 64 bits de la longitud del mensaje, antes de añadir los bits, se añade al resultado del paso anterior. Se usan los 64 bits de menor peso.
  - ▲**3.** Inicialización de un acumulador. Un búfer de cuatro palabras (A, B, C, D) se usa para calcular el resumen del mensaje. Aquí cada una de las letras A, B, C, D representa un registro de 32 bits. Estos registros se inicializan con ciertos valores hexadecimales, los bits de menor peso primero.
  - ▲**4.** Bucle final. En el que se procesan los bloques de 16 palabras del mensaje, en cuatro pasadas sucesivas .
- ▶**El algoritmo hash SHA-1** (Algoritmo Hash Seguro) (FIPS 1995) es el segundo algoritmo principal de hash que se utiliza hoy en día. Este algoritmo está basado en una serie de principios similares a los utilizados en el diseño de MD4, el predecesor de MD5. SHA-1 es un estándar federal del gobierno de Estados Unidos, es obligatorio siempre que se requiera un algoritmo hash criptográfico para aplicaciones gubernamentales. Produce un resumen de mensajes (message digest) de 160 bits. Esa mayor longitud de salida hace que SHA-1 sea más seguro.

3.- INTEGRIDAD DE LOS MENSAJES CON FUNCIONES HASH

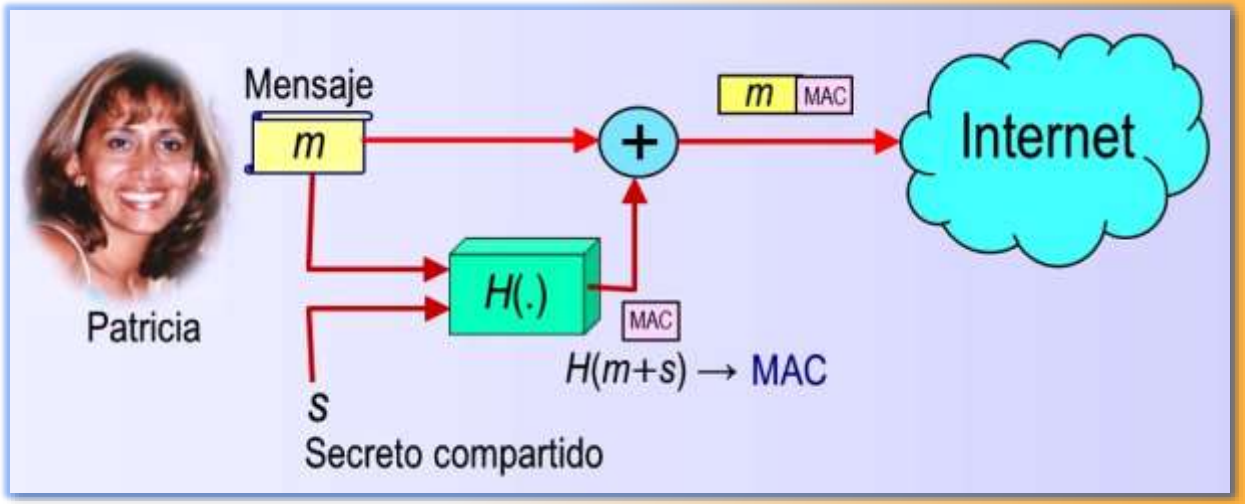
FUNCIONES HASH CRIPTOGRÁFICAS

¿Cómo se garantiza la integridad de los mensajes?

(Kurose, 2017)

- **Para garantizar** la integridad de los mensajes (o autenticarlos), además de utilizar funciones hash criptográficas Patricia y Elon necesitan un secreto compartido *s*. Este secreto compartido, que no es más que una cadena de bits, se denomina clave de autenticación. Utilizando este secreto compartido puede garantizarse de la forma siguiente la integridad de los mensajes:

- **En el emisor**
  - ▶**1.** Patricia crea el mensaje *m*.
  - ▶**2.** Concatena el secreto compartido *s* con el mensaje *m* para crear *m+s.*
  - ▶**3.** Calcula el valor hash *H*(*m+s*) (por ejemplo con el algoritmo SHA-1).
    - ✉ *H*(*m+s*) se denomina Código de Autenticación de Mensajes MAC.
  - ▶**4.** Patricia añade el código MAC al mensaje *m*, creando un mensaje ampliado (*m*, *MAC*), y lo envía a Elon**.**

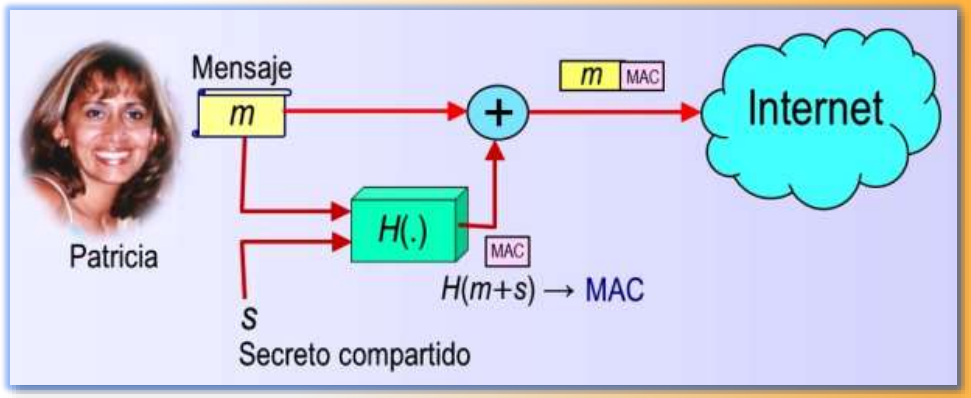


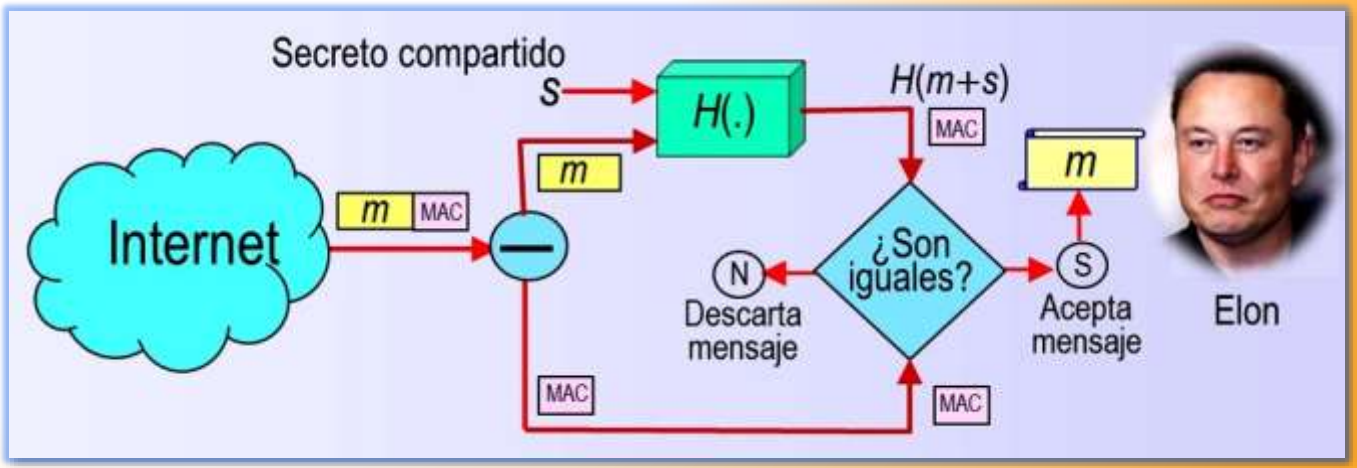
FUNCIONES HASH CRIPTOGRÁFICAS

¿Cómo se garantiza la integridad de los mensajes? (cont.)

(Kurose, 2017)

- **En el receptor**
  - ▶**1.** Elon recibe el mensaje ampliado (*m*,MAC) y lo separa.
  - ▶**2.** Concatena el secreto compartido *s* con el mensaje *m* para crear *m+s.*
  - ▶**3.** Calcula el valor hash *H*(*m+s*) (por ejemplo con el algoritmo SHA-1).
  - ▶**4.** Compara el valor *H*(*m+s*) creado, con el valor MAC enviado por Patricia.
  - ▶**5.** Si son iguales, Elon concluye que todo está correcto y acepta el mensaje**.**





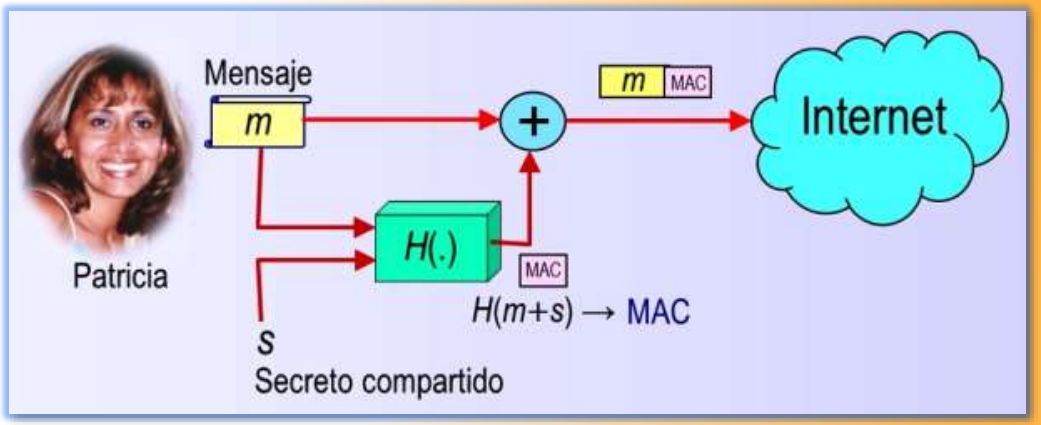
- **Es importante** fijarse en que las siglas MAC aquí (que corresponden a Código de Autenticación del Mensaje) no tienen nada que ver con las siglas MAC utilizadas en los protocolo de la capa de enlace (que corresponden a Control de Acceso al Medio).

FUNCIONES HASH CRIPTOGRÁFICAS

Características de los valores MAC

(Kurose, 2017)

- **Una característica** muy conveniente de los valores MAC (Código de Autenticación del Mensaje) es que no se necesita ningún algoritmo de cifrado.
- **De hecho**, en muchas aplicaciones, incluyendo el algoritmo de routing de estado del enlace, las entidades que se están comunicando solo se preocupan de la integridad de los mensajes mientras que la confidencialidad de los mismos no les importa.



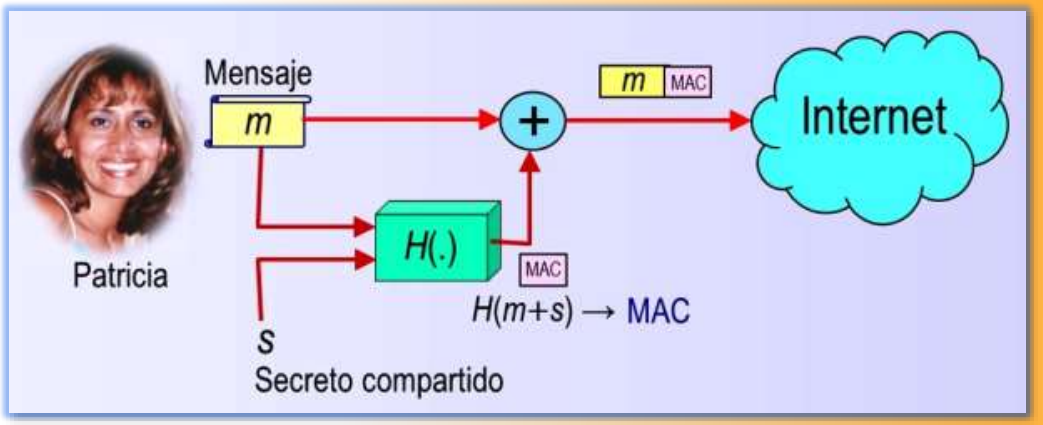
- **Utilizando un Codigo MAC**, las entidades pueden autenticar los mensajes que se intercambian sin tener que incluir complejos algoritmos de cifrado en el proceso de garantía de la integridad.
- **Como cabria esperar**, a lo largo de los años se han propuesto diversos estándares para los valores MAC. El estándar más popular hoy día es HMAC, que puede utilizarse con los algoritmos hash MD5 o SHA -1.
- **En la practica**, HMAC hace pasar los datos y la clave de autenticación a través de la función hash dos veces.

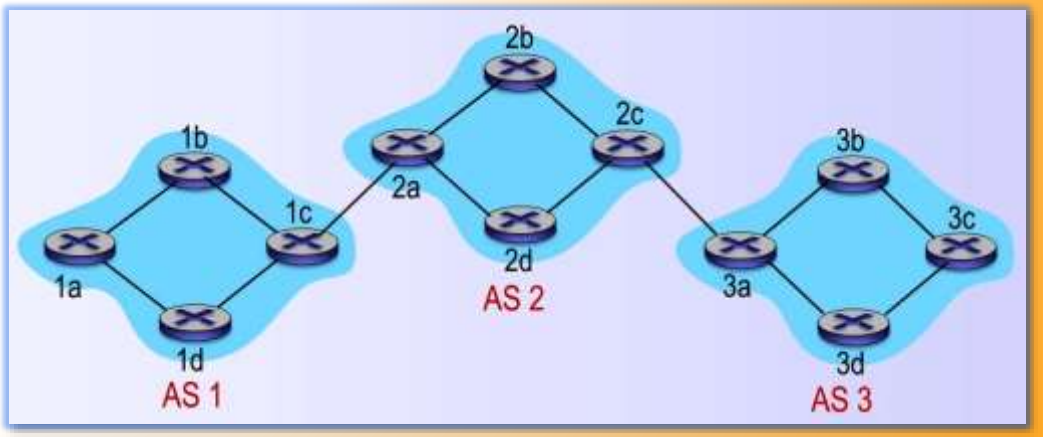
FUNCIONES HASH CRIPTOGRÁFICAS

¿Cómo se distribuye la clave secreta?

(Kurose, 2017)

- **Por ejemplo**, en el algoritmo de routing de estado del enlace se necesita distribuir la clave secreta *s* (secreto compartido) a cada uno de los router del sistema autónomo.
- **Observe** que todos los router puedan utilizar la misma clave secreta (denominada también clave de autenticación). Un administrador de red podría llevar a cabo esa distribución visitando físicamente cada uno de los routers.
- **O bien**, si el administrador de la red es demasiado flojo y si cada router tiene su propia clave pública, el administrador puede distribuir la clave de autenticación a cualquiera de los routers cifrándola con la clave púbica del router y luego enviando la clave cifrada hasta el router a través de la red.





FUNCIONES HASH CRIPTOGRÁFICAS

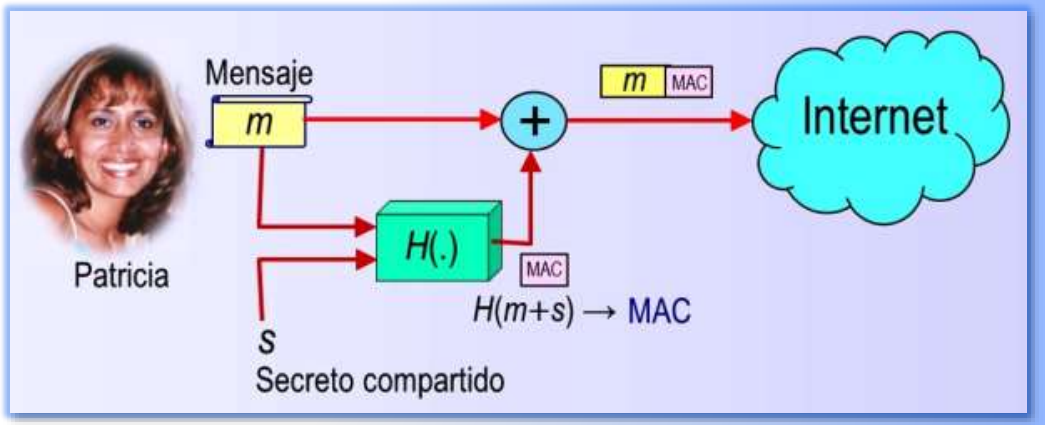
Resumen y preguntas de repaso

(Kurose, 2017)

- **Resumen**. En esta presentación, se ha examinado un método que permite proporcionar mecanismos para asegurar la integridad de los mensajes: la generación de los códigos de autenticación de mensajes (MAC) con base a las funciones hash criptográficas. Este método permite verificar el origen del mensaje, así como también la integridad del propio mensaje. Los códigos MAC no se basan en el cifrado.

- ▶**P1.** ¿De qué forma una función hash proporciona una mejor comprobación de la integridad de los mensajes que una suma de comprobación, tal como la suma de comprobación de Internet?

- ▶**P2.** ¿Se puede "descifrar" un valor hash de un mensaje para obtener el mensaje original? Explique su respuesta.



- ▶**P3**. Considere una variante del algoritmo MAC (ver figura), en la que el emisor envía (*m, H(m) + s*), siendo *H(m) + s* la concatenación de *H(m)* y *s.* ¿Tiene algún defecto esta variante? ¿Por qué?

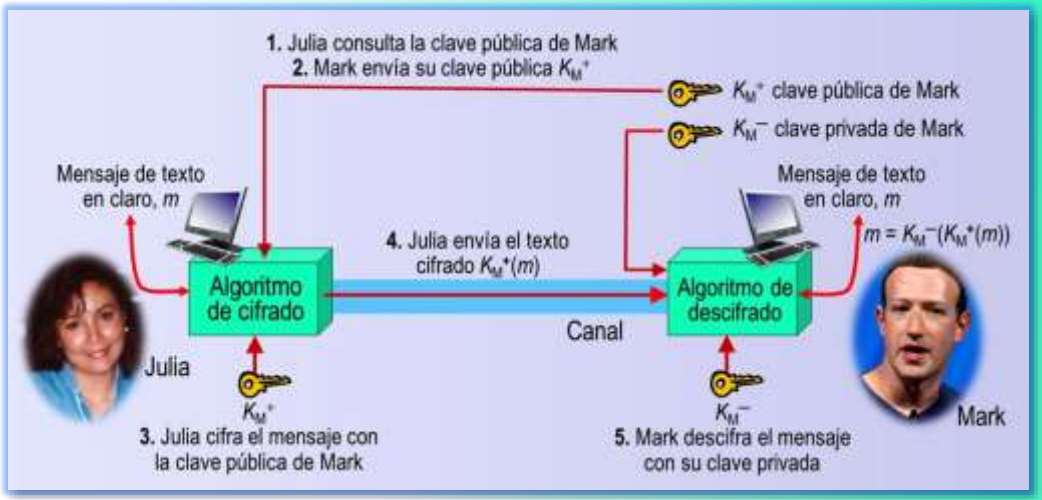
- ▶**P4.** Suponga que Patricia y Elon comparten dos claves secretas: una clave de autenticación S_1 y una clave simétrica de cifrado S_2. Amplíe la figura, de forma que se proporcionen tanto integridad como confidencialidad.

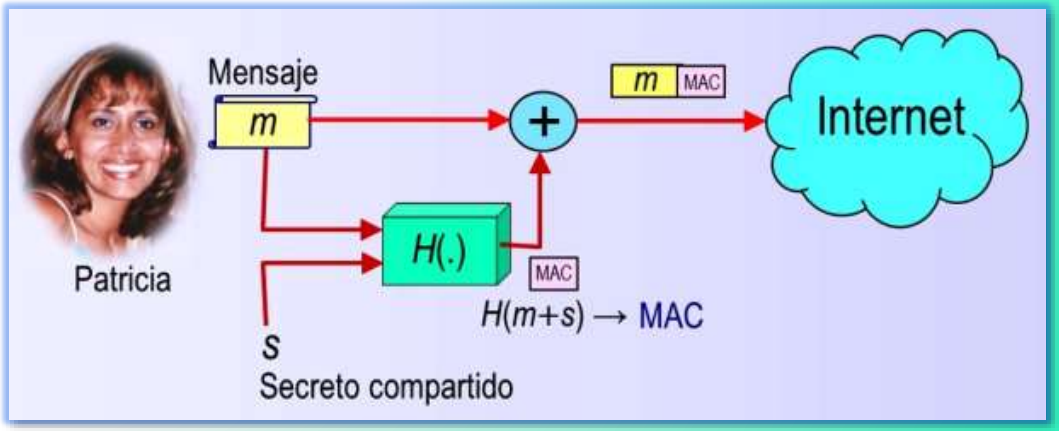
MAPA DE LOS SIGUIENTES TEMAS DE SEGURIDAD EN REDES

FUNCIONES HASH CRIPTOGRÁFICAS

¿Cómo se abordará la seguridad en redes?

- **Hasta aquí**, ya se han identificado las amenazas de seguridad en las redes modernas y se han identificado y definido las propiedades deseables en una comunicación segura.
- **Para una comunicación segura** es absolutamente necesario que los mensajes sean encriptados de alguna manera, para ello ya se han analizado los principios de criptografía y las funciones hash criptográfica para dotar de confiabilidad e integridad de los mensajes en las comunicaciones en la red.
- **En el siguiente tema** se analizará otro importante método para asegurar la integridad de los mensajes: la **firma digital**.
- **Luego**, se analizarán y seleccionarán los protocolos seguros en cada una de las cuatro capas superiores, comenzando por la capa de aplicación.
- **Por último**, se considerará la seguridad operacional, la cual se ocupa de la protección de las redes institucionales frente a los ataques. En particular, firewalls y los sistemas de detección de intrusos.





Referencias bibliográficas

- CISCO (2015). *CCNA Routing and Switching. Introduction to Networks*. CISCO.
- CISCO (2016). *Introducción a las redes.* Madrid: Pearson Education, S.A.
- Forouzan, B. A. (2020). *Transmisión de datos y redes de comunicaciones.* Madrid: McGraw-Hill.
- Huawei Technologies (2020). *Basics of data communication networks*. Huawei.
- Kurose, J. Keith, R. (2017). *Redes de computadoras: un enfoque descendente*. Madrid: Pearson Education, S.A.

FIN

Tema 4 de:

SEGURIDAD EN REDES DE COMPUTADORAS

Edison Coimbra G.