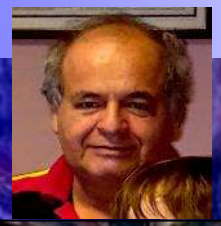
5 FIRMAS DIGITALES



Manual de clases

Objetivo

- Describir la infraestructura de clave pública que requieren las firmas digitales que permiten verificar el origen y la integridad de los mensajes.

Última modificación:
1 de julio de 2022

Tema 5 de:
SEGURIDAD EN REDES DE CMPUTADORAS

Edison Coimbra G.

FIRMAS DIGITALES

Consideraciones para diseñar una firma digital

(Kurose, 2017)

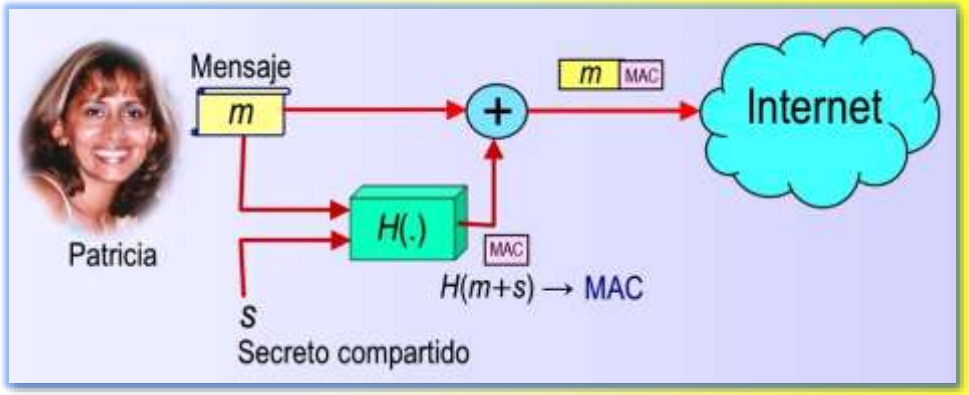
- **Piense** en el número de veces que ha estampado su firma en un papel durante el último año. Todas las personas están acostumbradas a firmar cheques, recibos de tarjetas de crédito, documentos legales y cartas. La firma atestigua el hecho de que una persona ha aceptado y/o acordado el contenido de un documento.
- **En un mundo digital** a menudo surge la necesidad de indicar quién es el propietario o creador de un documento o de explicitar el acuerdo con el contenido de un documento. Una firma digital es una técnica criptográfica que permite conseguir estos objetivos en el mundo digital.
- **Al igual que ocurre** con las firmas manuscritas, las firmas digitales deben realizarse de forma que sean verificables y no falsificables. Es decir debe ser posible demostrar que un documento firmado por una persona ha sido, de hecho, firmado por esa persona (la firma tiene que ser verificable) y que solo una persona podría haber firmado el documento (la firma no puede ser falsificada).
- **¿Cómo se podría diseñar un esquema de firma digital?** Se van a considerar tres técnicas:
  - **1.** Diseño con MAC
  - **2.** Diseño con criptografía de clave pública
  - **3.** Diseño con funciones hash

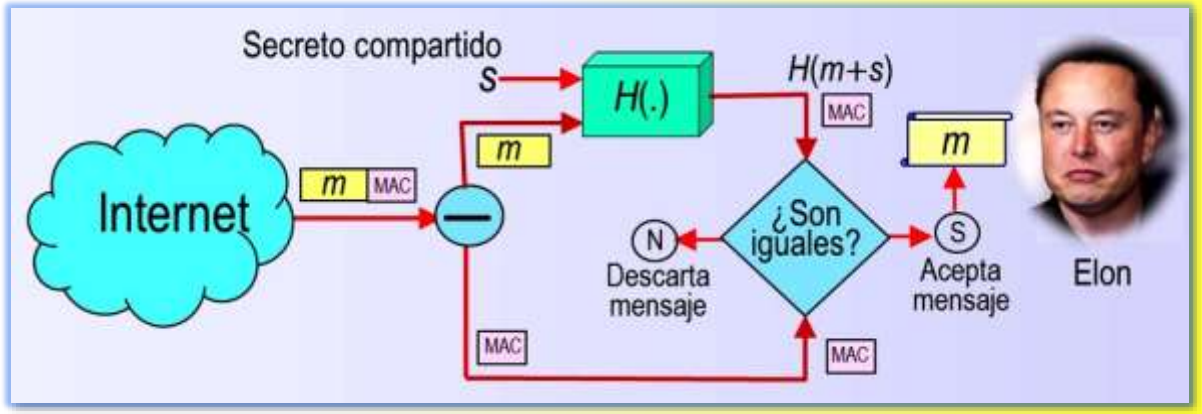
FIRMAS DIGITALES

Diseño de firma digital con con MAC

(Kurose, 2017)

- **En el emisor**
  - ▶**1.** Cuando Patricia firma un mensaje debe poner algo en el mensaje que sea distintivo de ella; podría pensar en asociar un valor MAC (Código de Autenticación del Mensaje) para la firma.
  - ▶**2.** Patricia, por tanto, crearía el valor MAC añadiendo una clave secreta *s* o su clave (que le distingue del resto de las personas) al mensaje *m* y luego aplicando la función hash obtiene *H*(*m*+*s*) que es el valor MAC, y lo envía a Elon.
- **En el receptor**
  - ▶**1.** Para que Elon pueda verificar esa firma, también debería disponer de una copia de la clave *s*, en cuyo caso la clave dejaría de ser distintiva de Patricia.
- **Por tanto**, los códigos MAC no permiten conseguir el objetivo en este caso.



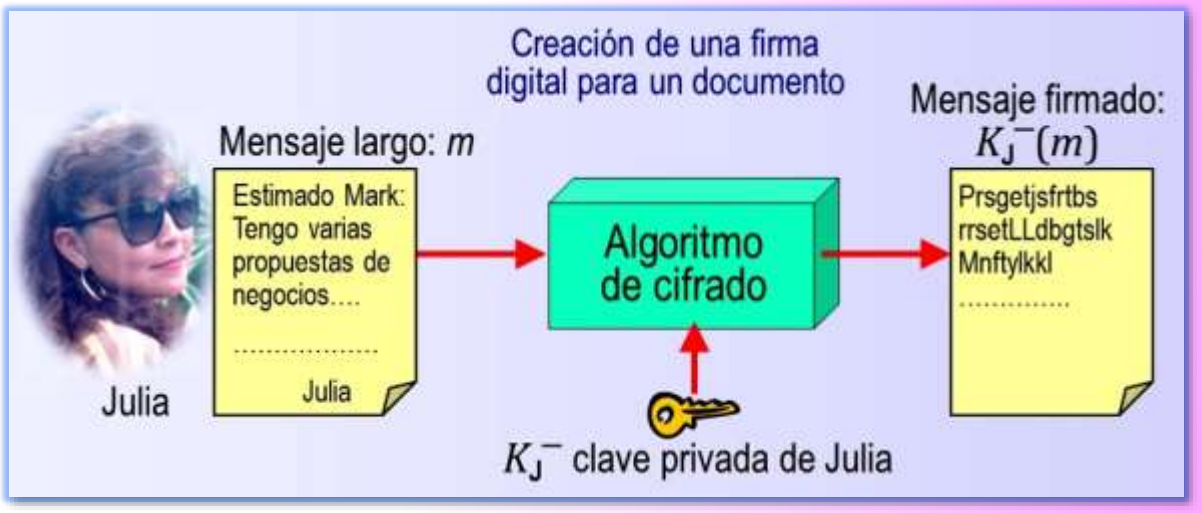


FIRMAS DIGITALES

Diseño con criptografía de clave pública

(Kurose, 2017)

- **En esta técnica**, Julia dispone de sendas claves pública y privada, las cuales se convierten en las claves distintiva de Julia. Por tanto, la criptografía de clave pública es un candidato excelente para poder proporcionar un mecanismo de firma digital. Para estructurar dicho mecanismo, considere lo siguiente:
- **En el emisor**
  - ▶**1.** Julia desea firmar digitalmente un documento, m. Se puede pensar en el documento como si fuera un archivo o un mensaje que Julia va firmar y enviar.
  - ▶**2.** Para firmar este documento Julia utiliza solamente su clave privada K_J^- para cifrar el mensaje y calcular $K_J^-(m)$.
  - ▶**3.** Puede parecer extraño que Julia utilice su clave privada para cifrar un mensaje, ya que, por lo general, se la utiliza para descifrarlo. Pero recuerde que el cifrado y el descifrado no son otra cosa que operaciones matemáticas que permiten intercambiar el papel de la clave publica y la clave privada.

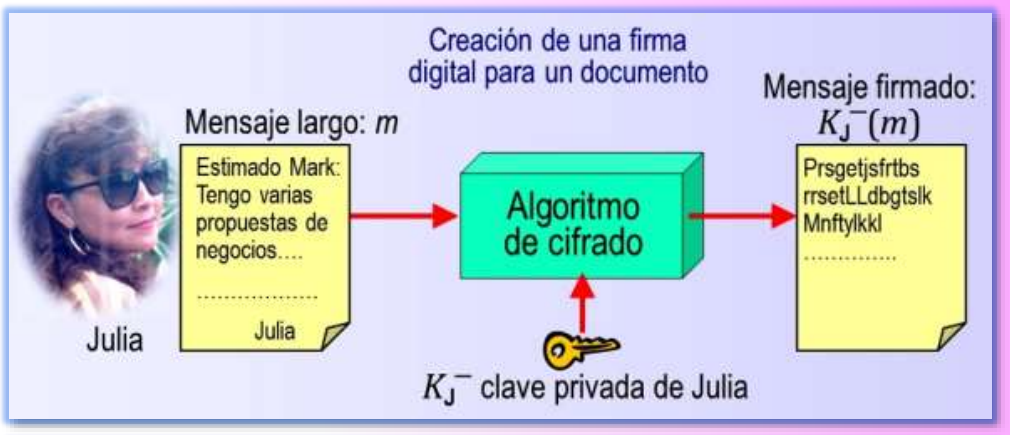


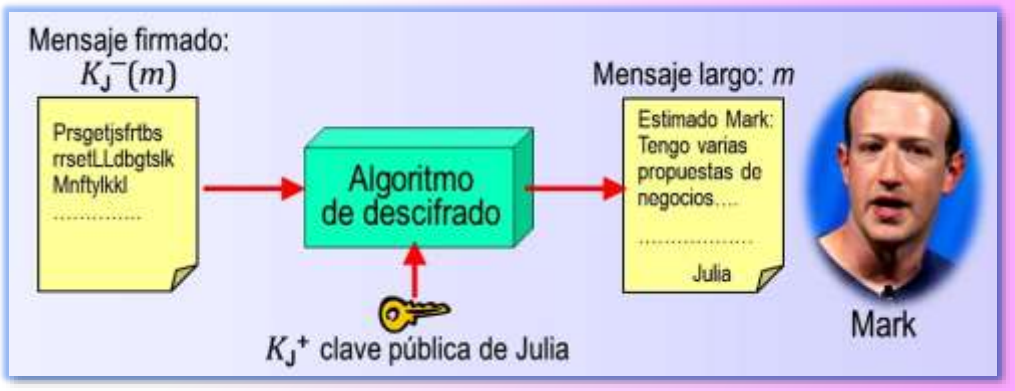
  - ▶**4.** Recuerde que el objetivo de Julia no es cifrar u ocultar el contenido del documento, sino solo firmarlo de una manera que sea verificable y no falsificable. La firma digital del documento realizada por Julia es, por lo tanto, $K_J^-(m)$.

FIRMAS DIGITALES

Diseño con criptografía de clave pública (cont.)

(Kurose, 2017)





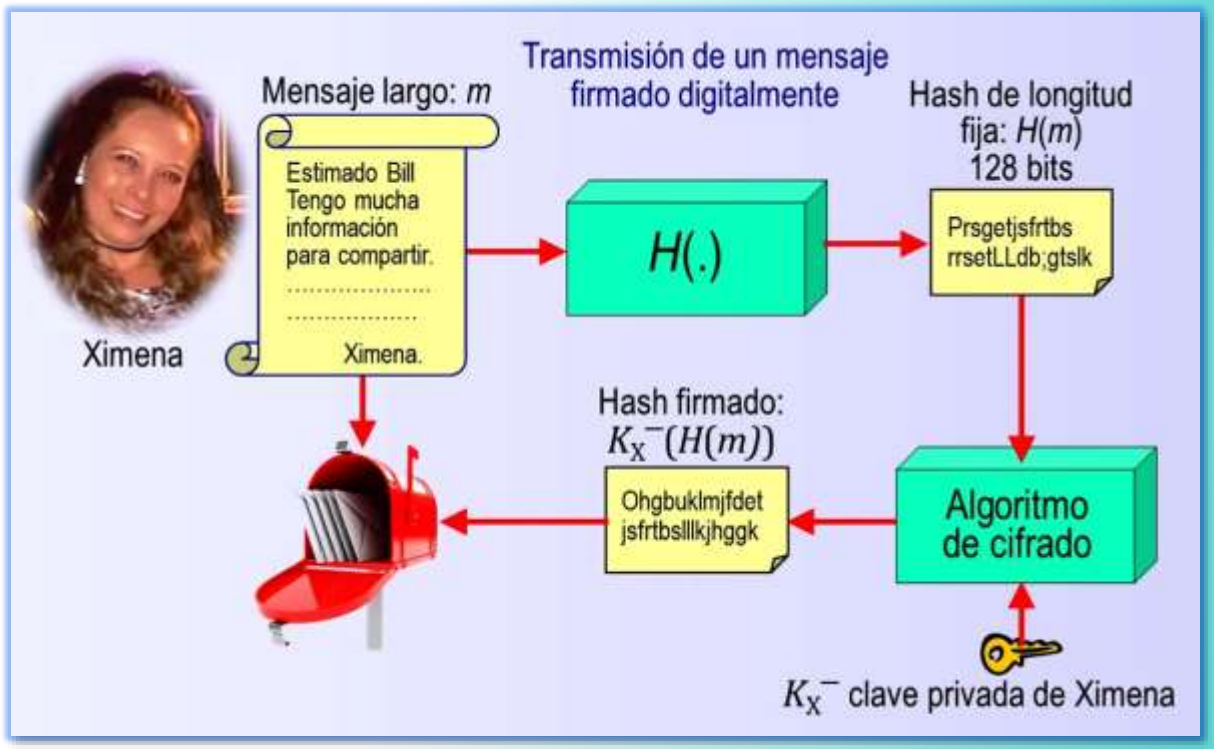
- **En el receptor**
  - ▶**1.** Mark recibe el mensaje m y la firma digital $K_J^-(m)$. Él quiere verificar que Julia es quien firmó el documento. Para ello, toma la clave pública de Julia K_J^+, y se la aplica a la firma digital $K_J^-(m)$ asociada con el documento m. Es decir, calcula $K_J^+(K_J^-(m))$ y obtiene m, que se corresponde exactamente con el documento original, los compara.
  - ▶**2.** Mark argumenta a continuación, que solo Julia podría haber firmado el documento, es decir la firma digital es verificable y no falsificable.
- **Por tanto**, se puede concluir que las firmas digitales creadas con criptografía de clave pública, proporcionan un mecanismo de integridad de los mensajes, permitiendo al receptor verificar que el mensaje no ha sido alterado, además de verificar el origen del mismo.
- **Sin embargo**, uno de los problemas con la firma de datos mediante mecanismo de cifrado es que el cifrado y el descifrado son computacionalmente muy caros. Dada la cantidad adicional de procesamiento que el cifrado y el descifrado exigen, el firmar los datos vía cifrándolos/descifrándolos completamente puede ser como matar moscas a cañonazos.

3. DISEÑO DE FIRMA DIGITAL CON FUNCIONES HASH

Diseño con funciones hash

(Kurose, 2017)

- **En el contexto** del envío de un mensaje a Bill por parte de Ximena, la figura proporciona un resumen del procedimiento operativo requerido para crear una firma digital.
- **En el emisor**
  - ▶**1.** Ximena hace pasar su mensaje original *m*, de gran longitud, a través de una función hash, la cual calcula una especie de "huella digital" de longitud fija (128 bits) para el mensaje, y que se designa mediante $H(m)$.
  - ▶**2.** A continuación, Ximena firma digitalmente el valor hash resultante utilizando para ello su clave privada, es decir, Ximena calcula $K_X^-(H(m))$. Puesto que $H(m)$ es, generalmente, mucho mas pequeño que el mensaje original *m*, la capacidad de proceso necesario para generar la firma digital se reduce sustancialmente.



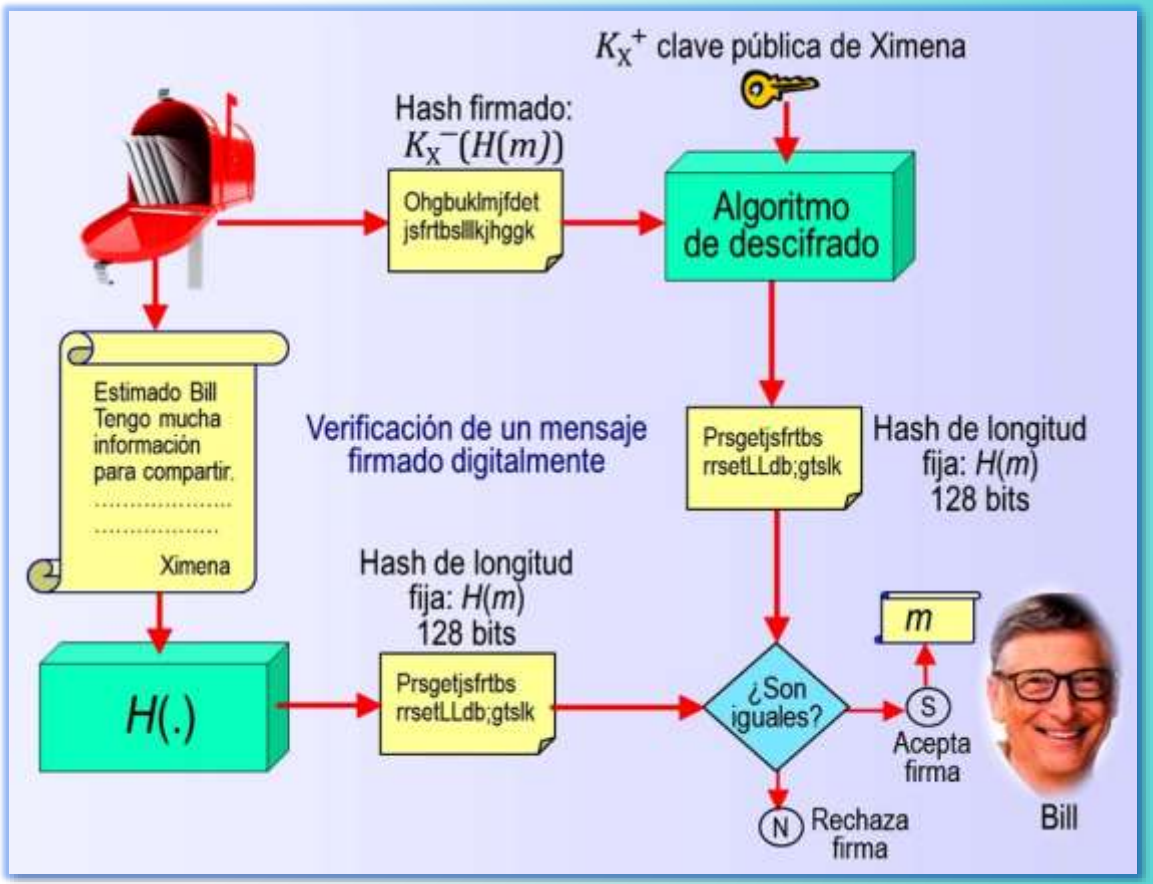
- ▶**3.** Después, Ximena la envía a Bill el mensaje original *m* (como texto en claro) junto con el mensaje digitalmente firmado $K_X^-(H(m))$, al que se denomina **firma digital**.

FIRMAS DIGITALES

Diseño con funciones hash (cont.)

(Kurose, 2017)

- **En el receptor**
  - ▶**1.** Bill recibe el mensaje original *m* (como texto en claro) junto con el mensaje digitalmente firmado $K_X^-(H(m))$, al que se denomina **firma digital**.
  - ▶**2.** Bill aplica la clave pública de Ximena a la firma digital para obtener un valor hash: $K_X^+(K_X^-(H(m)) = H(m)$.
  - ▶**3.** Asimismo, aplica la función hash al mensaje recibido *m* como texto en claro, para obtener un segundo valor hash $H(m)$.
  - ▶**4.** Bill compara los dos valores hash $H(m)$. Si son iguales, entonces Bill puede estar seguro acerca de la integridad y del autor del mensaje.
- **En conclusión**, para crear una firma digital, primero se calcula el valor hash del mensaje $H(m)$ y luego se lo cifra con la clave privada $K_X^-(H(m))$, utilizando criptografía de clave pública.



- **Por tanto**, la firma digital es una técnica "pesada", dado que requiere una insfraestructura de clave publica PKI subyacente, en las que existan autoridades de certificación como las que se describirán.

FIRMAS DIGITALES

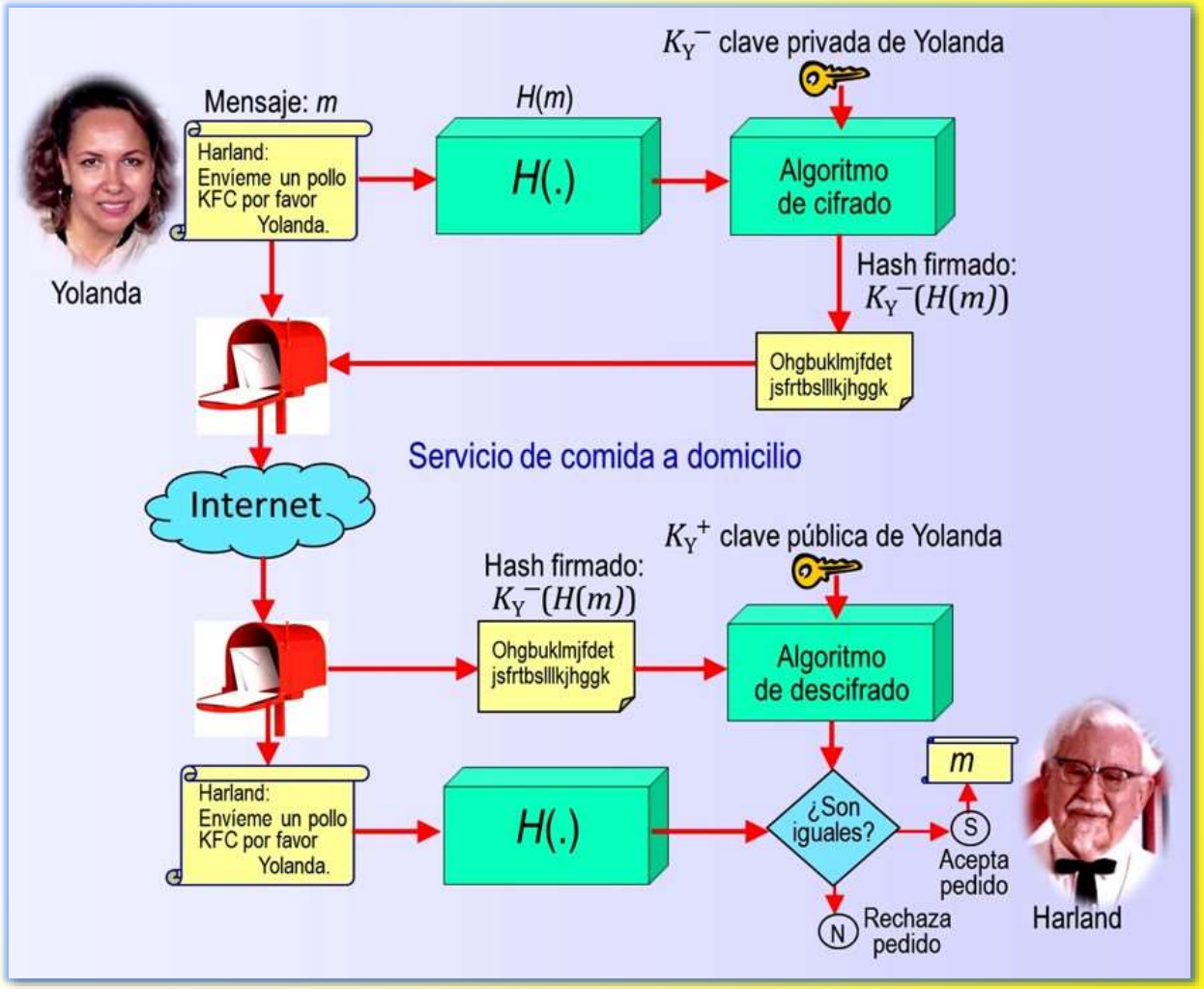
¿Qué es y por qué es importante la certificación de clave pública?

(Kurose, 2017)

- **Una importante aplicación** de las firmas digitales es la certificación de clave publica, es decir, certificar que una clave publica pertenece a una entidad especifica.
- **Las técnicas de certificación** de clave publica se utilizan en muchos protocolos populares de seguridad para las comunicaciones de red, incluyendo IPsec y SSL.
- **Para comprender el problema**, se va a considerar una versión de comercio electrónico por Internet del clásico servicio de pizza o pollo frito a domicilio.

En el emisor

- ▶**1.** Harland trabaja en el sector de la venta de pollo a domicilio y acepta pedidos a través de Internet. Yolanda envía a Harland un mensaje de texto en claro, *m*, que incluye su dirección particular y el tipo de pollo que desea.
- ▶**2.** En ese mensaje, Yolanda también incluye una firma digital (es decir, un valor hash firmado del mensaje en claro original), $K_Y^-(H(m))$, para demostrar a Harland que ella es el verdadero origen del mensaje.

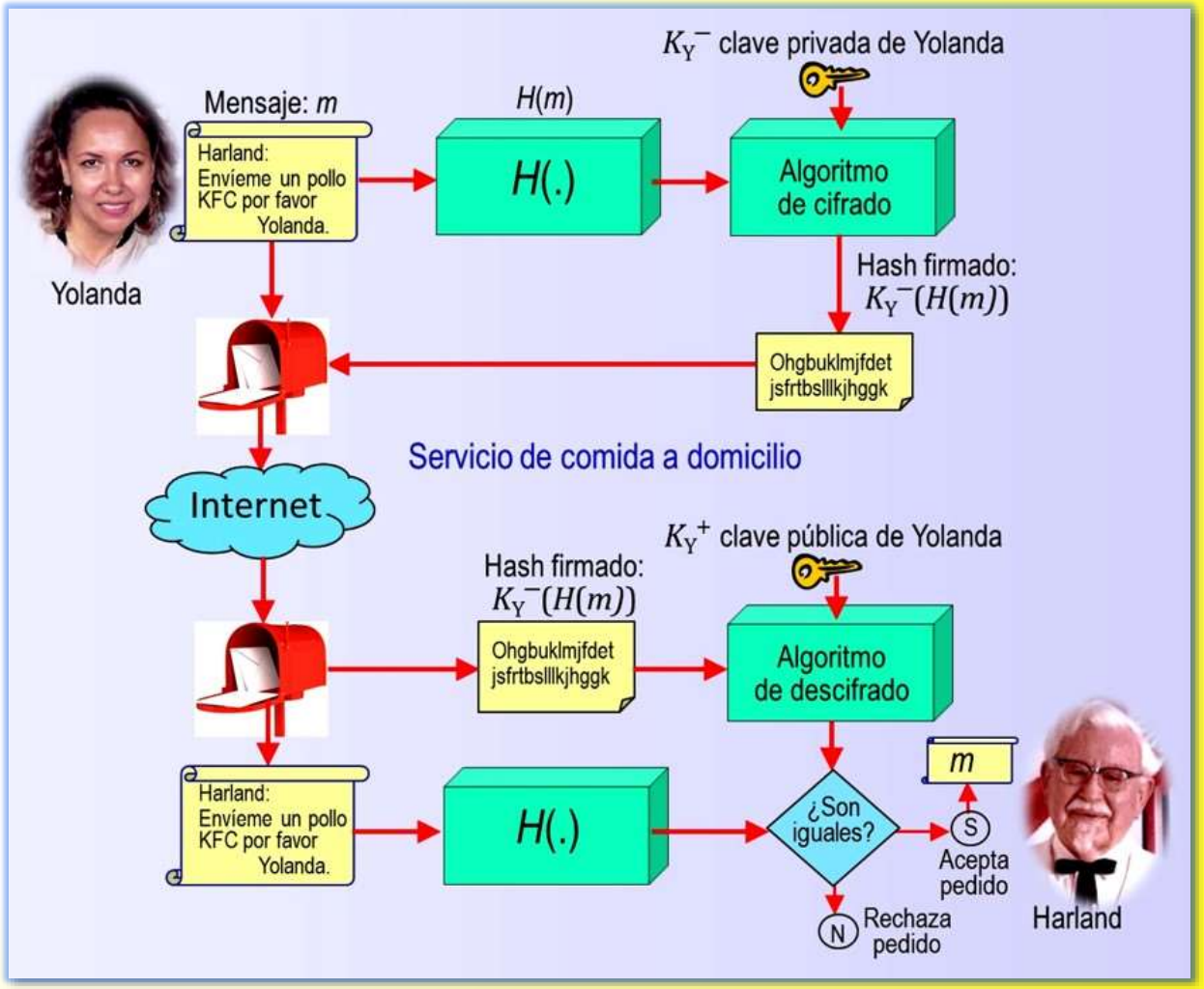


FIRMAS DIGITALES

¿Qué es y por qué es importante la certificación de clave pública? (cont.)

(Kurose, 2017)

- **En el receptor**
  - ▶**1.** Para verificar la firma, Harland obtiene la clave publica K_Y^+ de Yolanda, (quizá acudiendo a un servidor de clave publica o a partir del propio mensaje de correo electrónico), y comprueba la firma digital, de esta forma se asegura de que Yolanda, y no algún intruso haya realizado el pedido.
  - ▶**2.** Este procedimiento parece correcto, hasta que una **intrusa entra en escena**. La intrusa puede enviar un mensaje a Harland en el que dice que es Yolanda, proporciona la dirección particular de Yolanda y pide 10 pollos. En este mensaje, la intrusa incluye también su clave pública.
  - ▶**3.** Después de recibir el mensaje, Harland aplica la clave publica de la **intrusa** (pensando que es la de Yolanda) a la firma digital y concluye que el mensaje de texto en claro ha sido creado por Yolanda, quién se quedará muy sorprendida cuando el repartidor le lleve a su casa 10 pollos fritos.

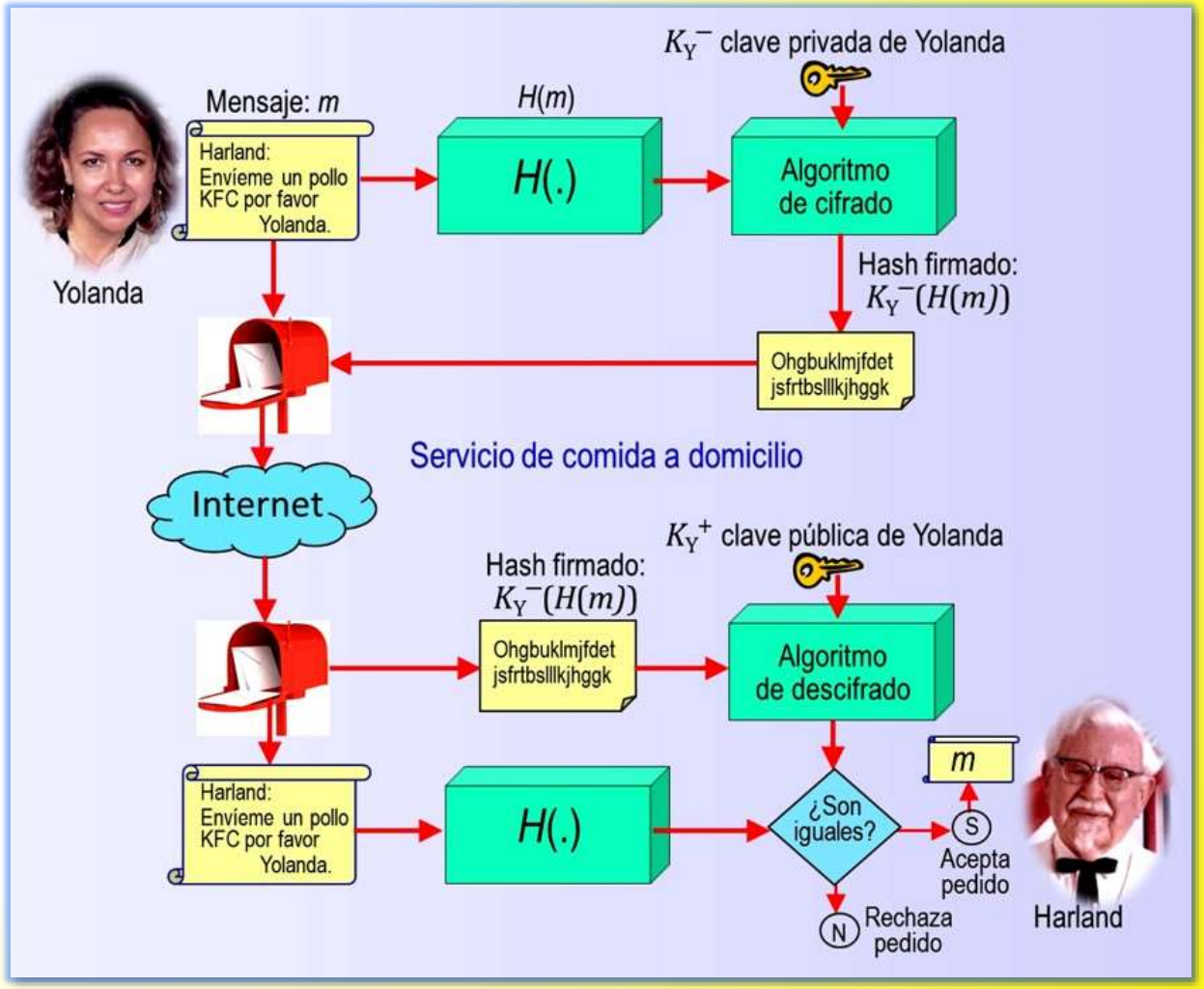


FIRMAS DIGITALES

¿Qué es y por qué es importante la certificación de clave pública? (cont.)

(Kurose, 2017)

- **Se puede ver**, a partir de este ejemplo, que para que la criptografía de clave pública resulte útil se necesita poder verificar que se dispone de la verdadera clave pública de la entidad (persona, router, navegador, etc.) con la que se quiere comunicar.
- **Por ejemplo**, cuando Harland quiere comunicarse con Yolanda empleando criptografía de clave pública necesita verificar que la clave pública que se supone que pertenece a Yolanda es verdaderamente de Yolanda.
- **La asociación** entre una clave pública y una entidad concreta normalmente la realiza una **Autoridad de Certificación (CA)**, cuyo trabajo consiste en validar las identidades y emitir los certificados.



FIRMAS DIGITALES

Funciones de la Autoridad de Certificación (CA)

(Kurose, 2017)

- **1. Una Autoridad de Certificación (CA)** verifica que una entidad (una persona, un router etc.) es quien dice ser. No hay procedimiento establecido para la forma en que se lleva a cabo esa certificación. A la hora de tratar con una CA, se debe confiar en que esa CA ha realizado una verificación de identidad adecuadamente rigurosa.
- **2. Una vez que la CA** verifica la identidad de la entidad, genera un certificado que asocia con esa entidad su correspondiente clave publica.
- **3. El certificado** contiene la clave pública y la información de identificación globalmente distintiva acerca del propietario de la clave pública (por ejemplo, el nombre de una persona o de una dirección IP).

- **4. El certificado** es firmado digitalmente por la autoridad de certificación. (Estos pasos se muestran en la figura).

- **Surge la pregunta**: ¿Cómo pueden utilizarse los certificados para combatir a los bromistas de los pollos como a la intrusa?. Cuando Yolanda hace su pedido, también envía su certificado firmado por la CA. Harland utiliza una clave publica de la CA para comprobar la validez del certificado de Yolanda y extraer la clave publica de Yolanda.

FIRMAS DIGITALES

Campos de un certificado de clave pública

(Kurose, 2017)

- **Tanto** la Union Internacional de Telecomunicaciones (ITU) como el IETF han desarrollado estándares para las CA.
- **La tabla** describe alguno de los campos mas importantes de un certificado.
  - ▶ITU X.509 especifica un servicio de autenticación, así como una sintaxis específica para los certificados.
  - ▶RFC 1422 describe un mecanismo de administración de claves basado en CA para su utilización con el correo electrónico seguro a través de Internet.
    - ✉Es compatible con X.509, pero va mas allá de dicho estándar al establecer procedimientos y convenios para una arquitectura de gestión de claves.

Campos seleccionados en una clave pública X.509 y RFC 1422	
Nombre del campo	**Descripción**
Versión	Número de versión de la especificación X.509
Número de serie	Identificador único para un certificado emitido por una CA.
Firma	Especifica el algoritmo utilizado por la CA para firmar este certificado.
Nombre del emisor	Identidad de la CA que emite este certificado, en formato de nombre distintivo (DN) [RFC 4514].
Periodo de validez	Inicio y final del periodo de validez del certificado.
Nombre del sujeto	Identidad de la entidad cuya clave pública está asociada con este certificado, en formato DN.
Clave pública del sujeto	La clave pública del sujeto, así como una indicación del algoritmo de clave pública (y de los parámetros del algoritmo) con el que hay que usar esta clave.

FIRMAS DIGITALES

Resumen y preguntas de repaso

(Kurose, 2017)

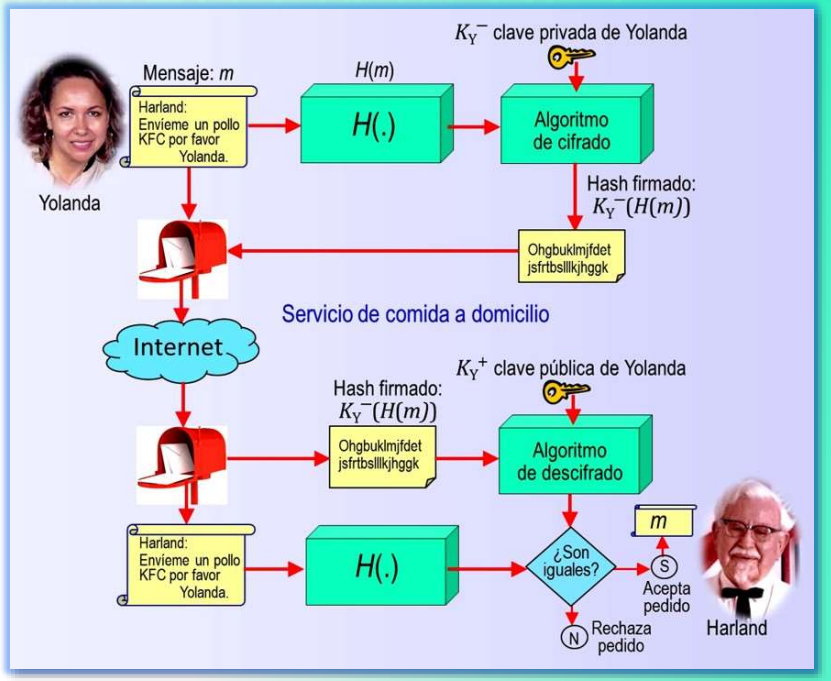
- **Resumen**. En las dos últimas presentaciones se han examinado dos métodos que permiten proporcionar mecanismos para asegurar la integridad de los mensajes: los códigos de autenticación de mensajes (MAC) y las firmas digitales. Los dos métodos presentan una serie de paralelismos. Ambos utilizan funciones hash criptográficas y ambas técnicas permiten verificar el origen del mensaje, así como la integridad del propio mensaje. Una diferencia importante es que los códigos MAC no se basan en el cifrado, mientras que las firmas digitales requieren una infraestructura de clave pública. Ambas técnicas se usan ampliamente en la práctica. Además, las firmas digitales se utilizan para crear certificados digitales, los cuales son importantes para verificar la validez de las claves públicas.
  - ▶**P1.** ¿Qué quiere decir que un documento firmado sea verificable y no falsificable?
  - ▶**P2.** ¿En qué sentido es mejor utilizar como firma digital la versión cifrada mediante clave pública del valor hash de un mensaje, en lugar de usar la versión cifrada mediante clave pública del mensaje completo?.
  - ▶**P3**. Suponga que *certificador.com* crea un certificado para *eddy.com*. Normalmente, el certificado completo será cifrado con la clave pública de *certificador.com*. ¿Verdadero o falso?
  - ▶**P4.** Suponga que Shaquira tiene un mensaje que está dispuesta a enviar a cualquiera que se lo solicite. Miles de personas desean obtener el mensaje de Shaquira, pero cada una de ellas desea estar segura de la integridad del mensaje. En este contexto, ¿qué piensa que es más adecuado: un esquema de integridad basado en MAC o uno basado en firma digital? ¿Por qué?.
  - ▶**P5.** El protocolo de routing OSPF utiliza un valor MAC en lugar de firmas digitales para garantizar la integridad de los mensajes. ¿Por qué cree que se eligió un valor MAC en lugar de firmas digitales?

MAPA DE LOS SIGUIENTES TEMAS DE SEGURIDAD EN REDES

FIRMAS DIGITALES

¿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, las funciones hash criptográfica y las firmas digitales, para dotar de confiabilidad e integridad de los mensajes en las comunicaciones en la red.
- **En el siguiente tema** se analizará la **autenticación del punto terminal**, que es el proceso de demostrar a alguien la propia identidad a través de una red de computadoras.
- **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.



FIRMAS DIGITALES

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 5 de:

SEGURIDAD EN REDES DE COMPUTADORAS

Edison Coimbra G.