8 CORREO ELECTRÓNICO SEGURO

Objetivo

- Describir cómo se pueden utilizar los principios criptográficos para crear un sistema de correo electrónico seguro.

Manual de clases

Última modificación:
21 de septiembre de 2022

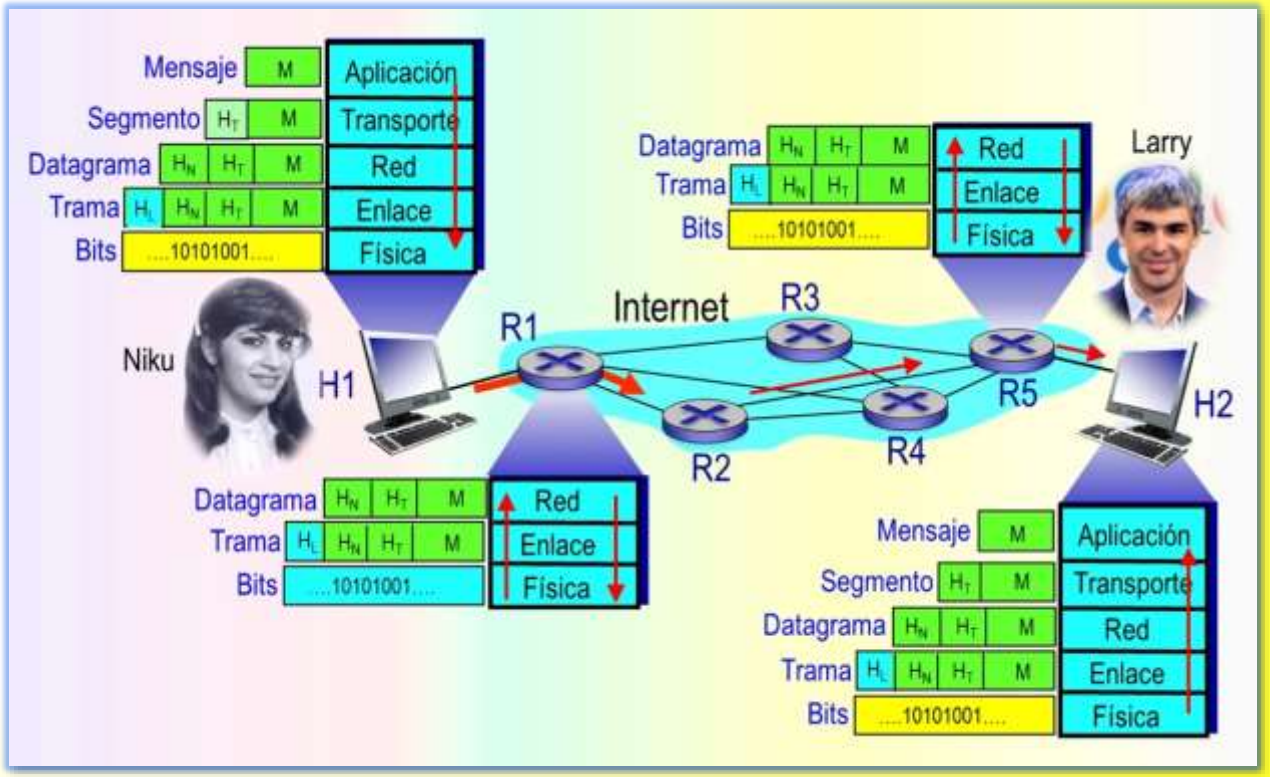
Tema 8 de:
SEGURIDAD EN REDES
Edison Coimbra G.

CORREO ELECTRÓNICO SEGURO

Seguridad en las capas de protocolos

(Kurose, 2017)

- **En los temas anteriores** se han examinado una serie de problemas fundamentales en el campo de la seguridad de red, incluyendo las técnicas de criptografía de clave simétrica y de clave pública, las de autenticación de punto terminal, los mecanismos de distribución de claves, el problema de la integridad de los mensajes y las técnicas de firma digital. Ahora se va a examinar cómo se utilizan hoy en día dichas herramientas para proporcionar seguridad en Internet.
- **Es interesante observar** que es posible proporcionar servicios de seguridad en cualquiera de las cuatro capas superiores de la pila de protocolo de Internet.
- **En la capa de aplicación**, el enfoque va a consistir en utilizar una aplicación específica como el correo electrónico, como caso de estudio de las técnicas de seguridad de la capa de aplicación.
- **Cuando se proporciona** seguridad, como por ejemplo el cifrado PGP, para un protocolo específico de la capa de aplicación, la aplicación que utiliza ese protocolo disfrutará de uno o más servicios de seguridad, como los de confidencialidad, autenticación o integridad.

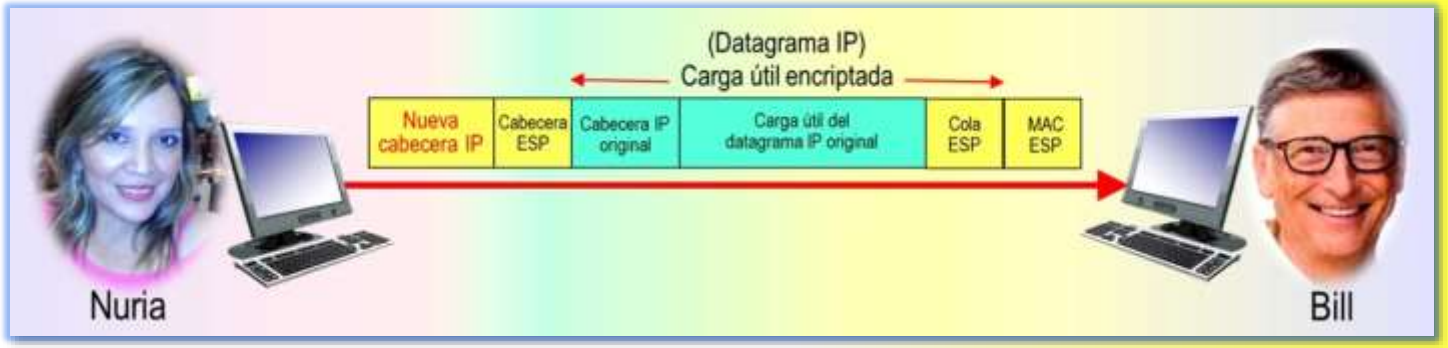


CORREO ELECTRÓNICO SEGURO

¿Por qué la seguridad en las capas superiores?

(Kurose, 2017)

- ▶**Respuesta 1.** La seguridad en la capa de red puede proporcionar la funcionalidad básica de cifrado de todos los datos contenidos en los datagramas y de autenticar todas direcciones IP de origen, lo que no puede es ofrecer seguridad de nivel de usuario.



  - ✉ Por ejemplo, un sitio web de correo electrónico (Bill) no puede confiar en la seguridad de la capa IP para autenticar a un cliente (Nuria) que esté comprando bienes o servicios en ese sitio. Por tanto, existe una necesidad de incorporar funcionalidades básicas en la capas superiores.
- ▶**Respuesta 2.** Es más fácil generalmente implantar servicios Internet nuevos, incluyendo los servicios de seguridad, en las capas superiores de la pila de protocolos. Mientras se espera a que un nuevo mecanismo de seguridad se implante de forma generalizada en la capa de red, lo que puede llegar a tardar años.
  - ✉ Un ejemplo clásico es el cifrado PGP (*Pretty Good Privacy)*, que proporciona correo electrónico seguro. Requiere únicamente código de aplicación de cliente y de servidor. PGP fue una de las primeras tecnologías de seguridad y se utilizó ampliamente en Internet.

Seguridad en internet

CORREO ELECTRÓNICO SEGURO

Protocolos seguros

(Kurose, 2017)

- **La tabla muestra** un resumen de los protocolos seguros desarrollados para dar seguridad a Internet y los dispositivos que protegen la infraestructura de redes.
- **En este y en los** siguientes temas se examinaran varios protocolos de red seguros que disfrutan de un amplio uso en la práctica. Se verá que:
  - ▶La criptografía de clave simétrica se encuentra en el núcleo de PGP, SSL, IPsec y la seguridad inalámbrica.
  - ▶La criptografía de clave pública es crucial tanto para PGP como para SSL.
  - ▶PGP utiliza firmas digitales para proporcionar la integridad de los mensajes.
  - ▶SSL e IPsec utilizan códigos MAC.

Propiedades de una comunicación segura			
1. Confidencialidad	**2. Integridad de los mensajes**	**3. Autenticación del punto terminal**	**4. Seguridad operacional**
Cifrado PGP para correo	Cifrado PGP para correo	Cifrado PGP para correo	Firewalls (Filtros de paquetes. Filtros con memoria del estado. Gateways de aplicación)
Protocolo TCP-SSL	Protocolo TCP-SSL	Protocolos de autenticación (Contraseñas y números distintivos)	Sistemas de Detección y de Prevención de Intrusiones
Protocolo IPsec (ESP)	Protocolo IPsec (AH, ESP)	Protocolo TCP-SSL Protocolo IPsec (AH, ESP)	Zonas de seguridad y zonas desmilitarizadas

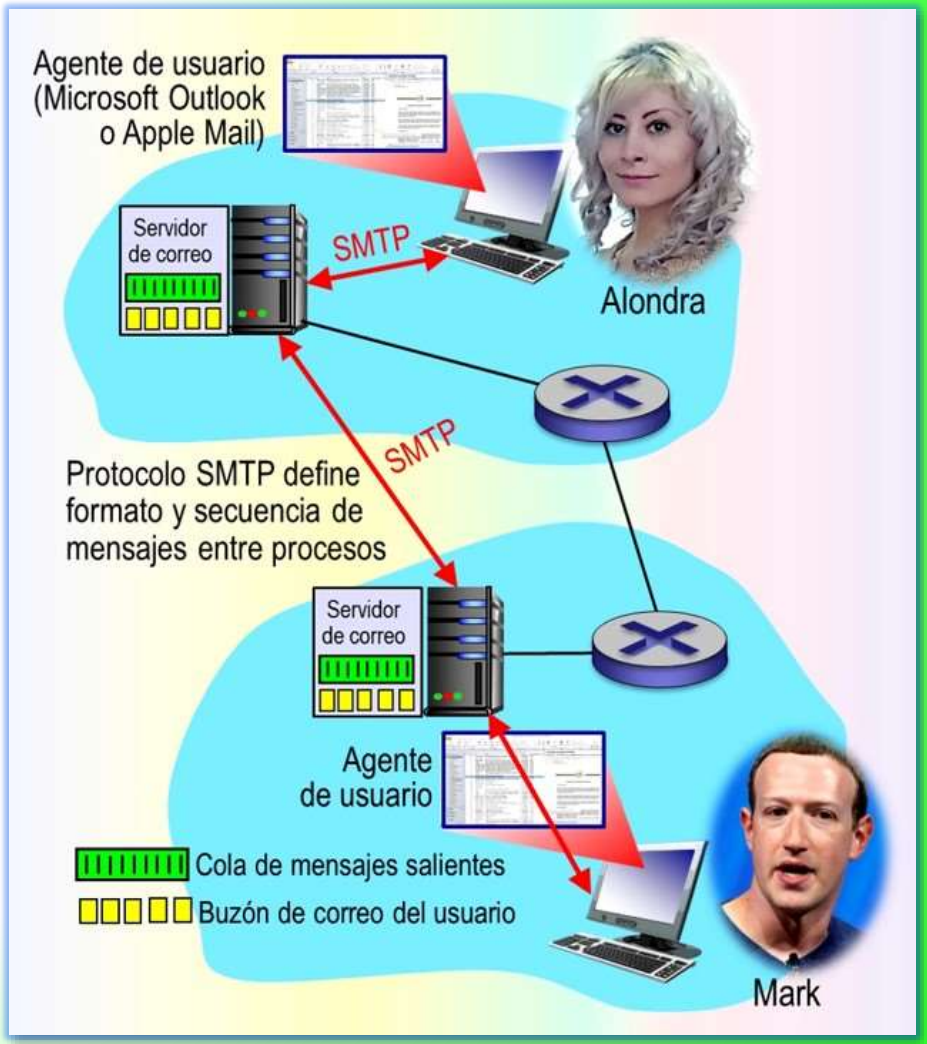
2.- DISEÑO DE UN CORREO ELECTRÓNICO SEGURO

CORREO ELECTRÓNICO SEGURO

El correo electrónico Internet

(Kurose, 2017)

- **Esta aplicación** está constituida por muchos componentes, entre los que se incluyen:
  - ▶**Los servidores de correo** que albergan los buzones de los usuarios.
  - ▶**Los agentes de usuario**, como Microsoft Outlook o Apple Mail, que permiten a los usuarios leer y crear mensajes; es un estándar para definir la estructura de los mensajes de correo electrónico.
  - ▶**Los protocolos** de la capa de aplicación que definen cómo se pasan los mensajes entre los servidores, cómo se pasan los mensajes entre los servidores y los clientes de correo y cómo se interpretan los contenidos de las cabeceras de los mensajes.
    - ✉ El principal protocolo de la capa de aplicación para el correo electrónico es el protocolo simple de transferencia de correo SMTP (RFC 5321).
- **Por tanto**, el protocolo principal de la capa de aplicación para correo electrónico, SMTP, sólo es un componente (aunque importante) de la aplicación de correo electrónico.



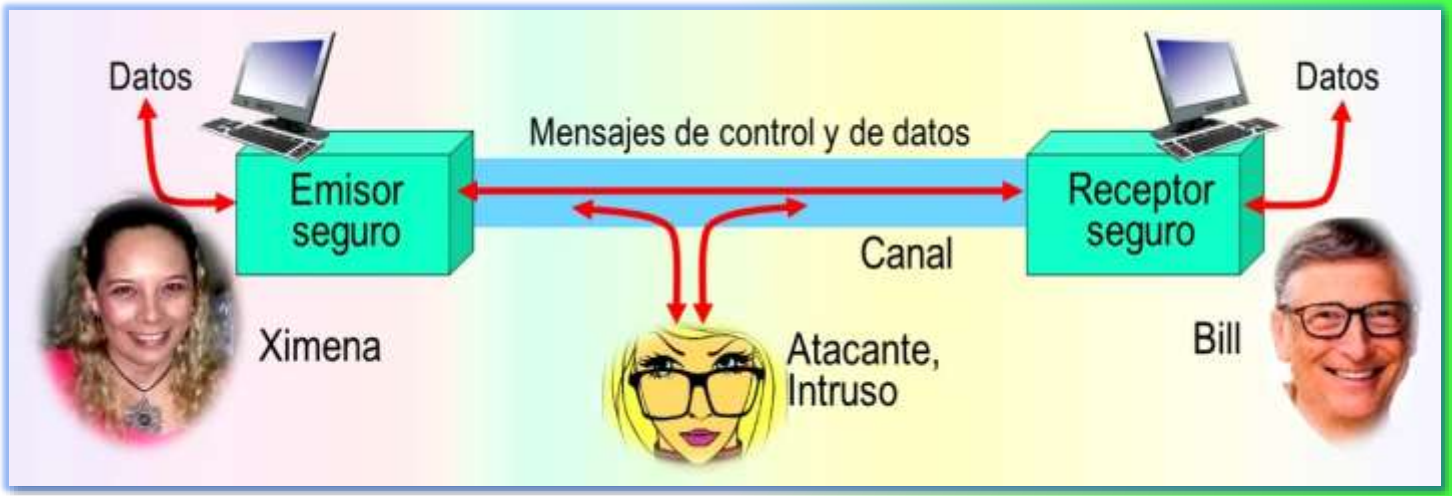
Diseño de un correo electrónico seguro

Criterios para el diseño de un correo electrónico seguro

(Kurose, 2017)

- **Se va a utilizar** la criptografía para crear un sistema de correo electrónico seguro. Este diseño de alto nivel se creará de una forma incremental, introduciendo en cada paso nuevos servicios de seguridad.

- **Para diseñar** un sistema de correo electrónico seguro se va suponer una relación de amistad entre Ximena y Bill. Imagine que Ximena quiere enviar un mensaje de correo electrónico a Bill y que una intrusa pretende inmiscuirse en la conversación.

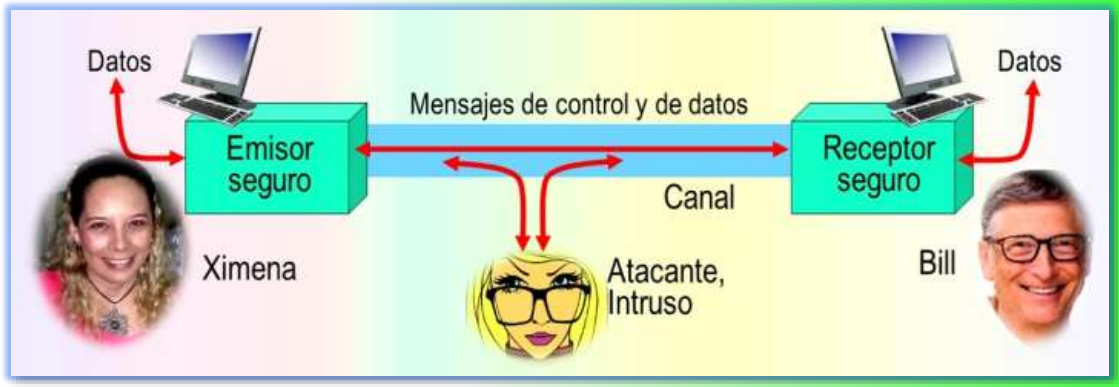


  - **Antes de seguir** adelante y diseñar un sistema de correo electrónico seguro para Ximena y Bill, se tiene que considerar qué características de seguridad serian más deseables para ellos.

CORREO ELECTRÓNICO SEGURO

Características de seguridad deseables

- ▶**1. Confidencialidad**. La primera y principal es la confidencialidad. Pues ni Ximena ni Bill quieren que la intrusa lea el correo electrónico de Ximena.
- ▶**2. Autenticación del emisor.** La segunda característica es que Ximena y Bill deseen para su sistema de correo electrónico seguro es la de autenticación del emisor**.** En particular, cuando Bill recibe el mensaje ”*necesito hablarte*, *quiero proponerte un negocio que te puede interesar*, *Ximena*” naturalmente le gustaría estar seguro que el mensaje procede de Ximena y no de la intrusa.



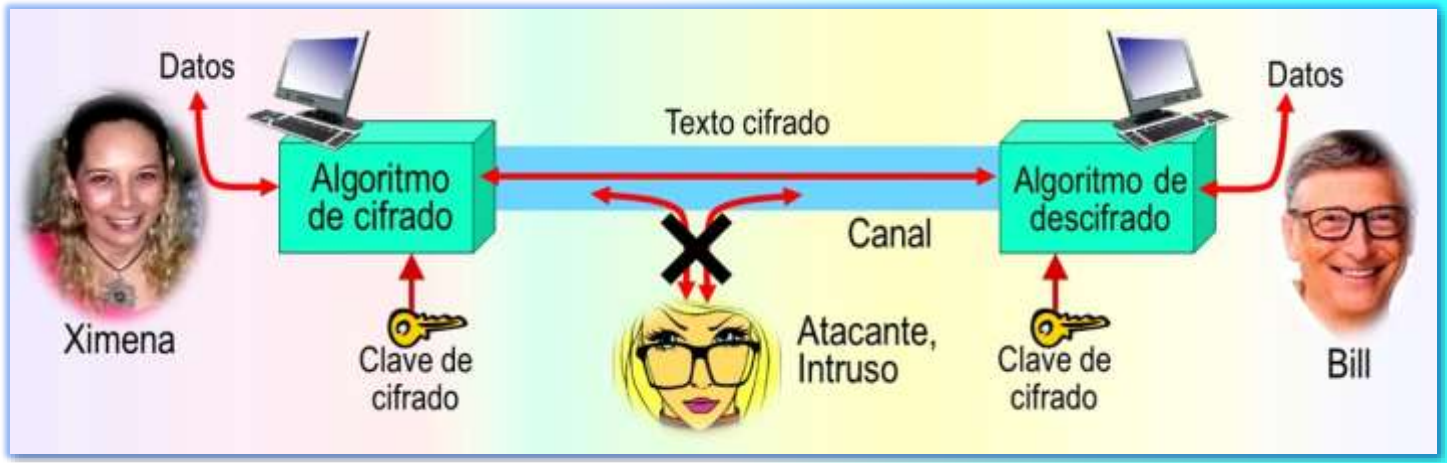
- ▶**3. Integridad de los mensajes**. Otra característica que los dos amigos apreciarían seria la de integridad de los mensajes, es decir, una garantía de que los mensajes que Ximena envíe no sean modificados a lo largo del camino hasta llegar a Bill.
- ▶**4. Autenticación del receptor**. Por último, el sistema de correo electrónico debe proporcionar una autenticación del receptor, es decir, Ximena querrá asegurarse de que está enviando su mensaje a Bill y no a alguna otra persona (por ejemplo a la intrusa) que esté haciéndose pasar por Bill.

CORREO ELECTRÓNICO SEGURO

Opción 1. Confidencialidad con criptografía de clave simétrica

(Kurose, 2017)

- **Se comenzará** analizando el primero de los objetivos, la confidencialidad.
- ▶**1.** La forma mas directa de proporcionar confidencialidad es que Ximena cifre el mensaje con una tecnología de clave simétrica (como DES o AES) y que Bill descifre el mensaje al recibirlo.
- ▶**2.** Si la clave simétrica es lo suficientemente larga y si únicamente Ximena y Bill tienen la clave, entonces es extremadamente difícil que ninguna otra persona (incluyendo la intrusa) lea el mensaje.



- **Aunque esta técnica** es muy sencilla, presenta la dificultad fundamental de distribuir la clave simétrica, de modo que solo Ximena y Bill tengan copia de la misma.
- **Por tanto**, se va a considerar una solución alternativa: la criptografía de clave pública (utilizando por ejemplo RSA).

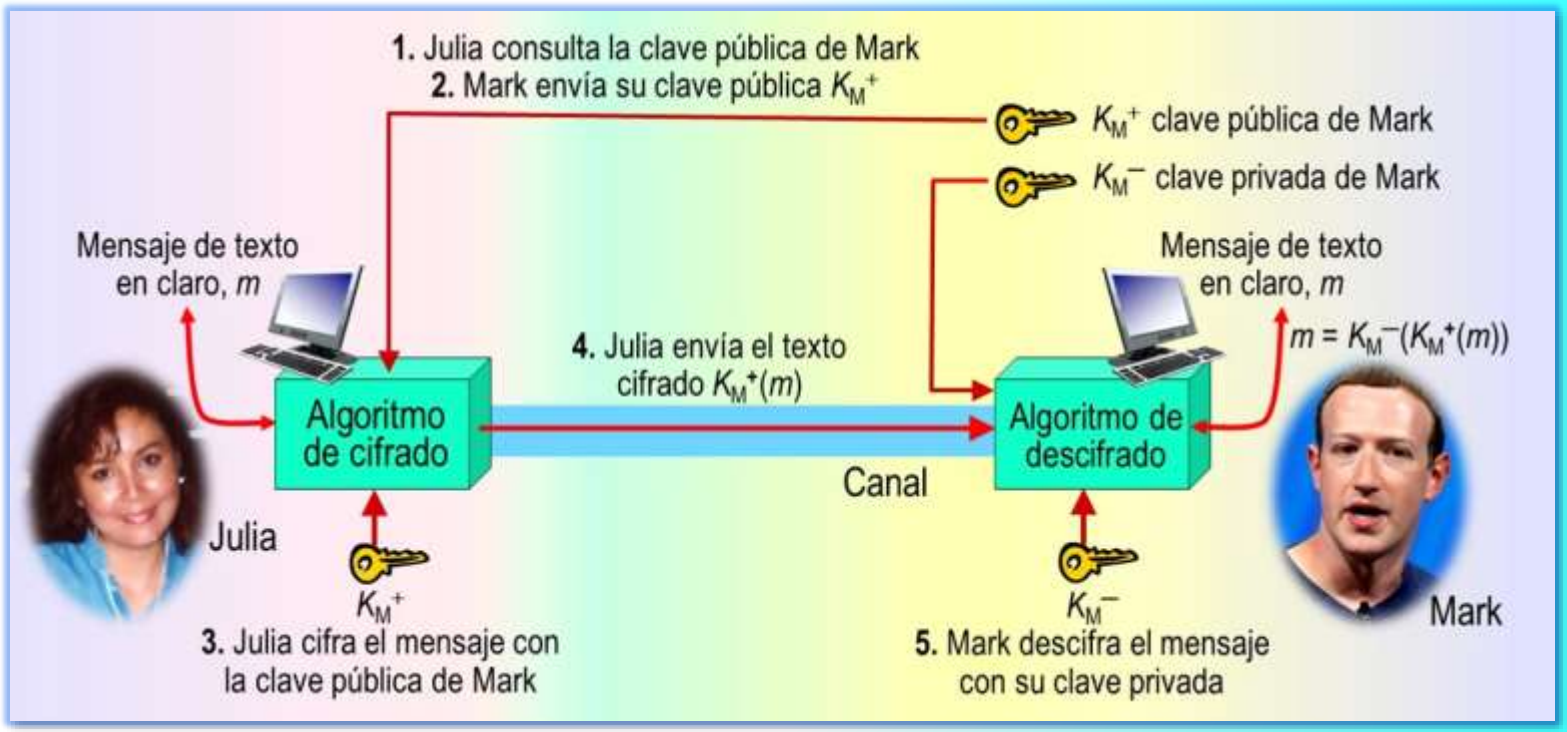
Confidencialidad en un correo electrónico seguro

CORREO ELECTRÓNICO SEGURO

Opción 2. Confidencialidad con criptografía de clave pública

(Kurose, 2017)

- ▶**1.** En la técnica de clave pública. Mark pone a disposición de todo el mundo su clave pública K_M^+ (por ejemplo, en un servidor de claves públicas o en su página web personal).
- ▶**2.** Julia obtiene la clave pública de Mark, K_M^+, y con ella cifra su mensaje y lo envía a la dirección de correo electrónico de Mark.
- ▶**3.** Cuando Mark recibe el mensaje, simplemente lo descifra con su clave privada K_M^-.



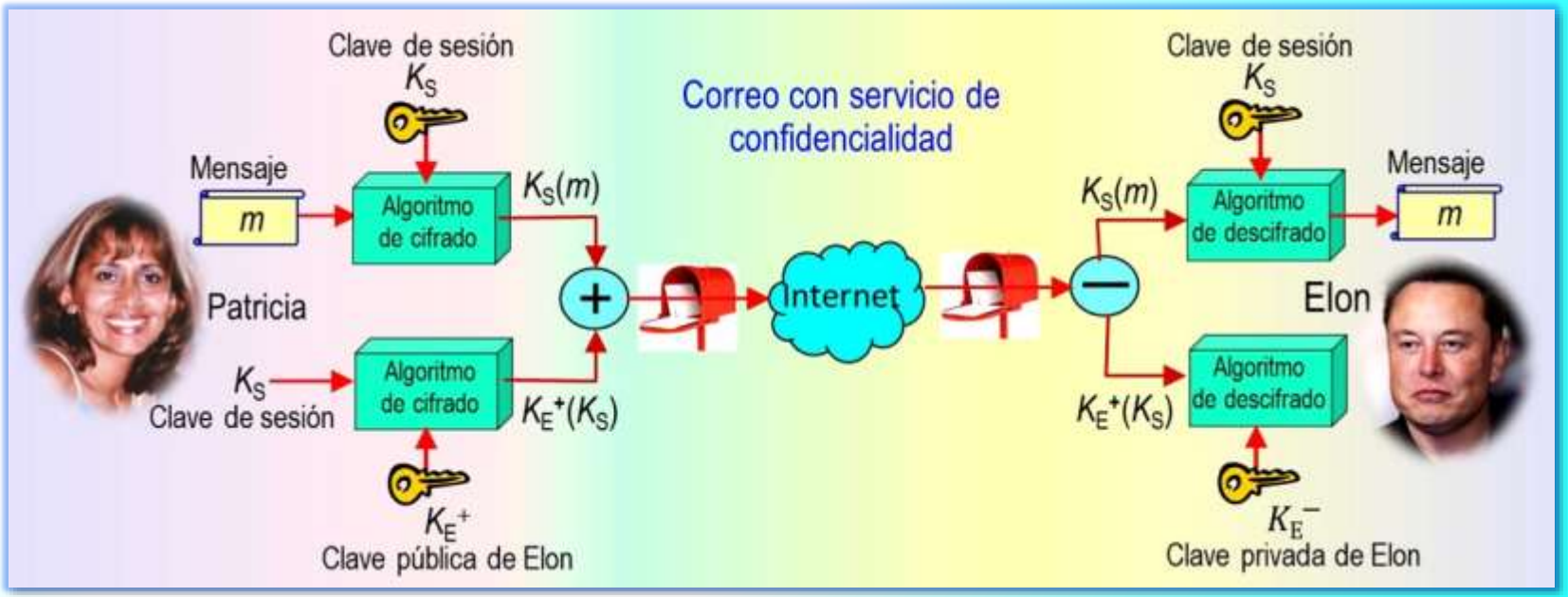
- ▶**4.** Suponiendo que Julia esté segura de que la clave pública utilizada es la de Mark, ésta técnica constituye un método excelente para proporcionar la confidencialidad deseada.
- **Sin embargo**, un problema es que el cifrado de clave pública es relativamente poco eficiente, particularmente para mensajes de gran longitud.

CORREO ELECTRÓNICO SEGURO

Opción 3. Confidencialidad con clave de sesión

(Kurose, 2017)

- **Para solventar** el problema de eficiencia del cifrado de clave pública, se va a hacer uso de una clave de sesión K_S. El algoritmo de cifrado RSA utiliza una clave simétrica en una combinación con algún otro mecanismo criptográfico; a esta clave simétrica se la conoce como clave de sesión K_S. En particular:
  - **Patricia envía un paquete:**
    - ▶**1.** Selecciona una clave de sesión simétrica aleatoria, K_S.
    - ▶**2.** Cifra su mensaje, m, con la clave de sesión K_S.
    - ▶**3.** Cifra la clave de sesión K_S con la clave pública de Elon K_E^+.
    - ▶**4.** Concatena el mensaje cifrado y la clave simétrica cifrada para formar un paquete: $K_S(m) + K_E^+(K_S)$
    - ▶**5.** Envía este paquete a la dirección de correo electrónico de Elon.



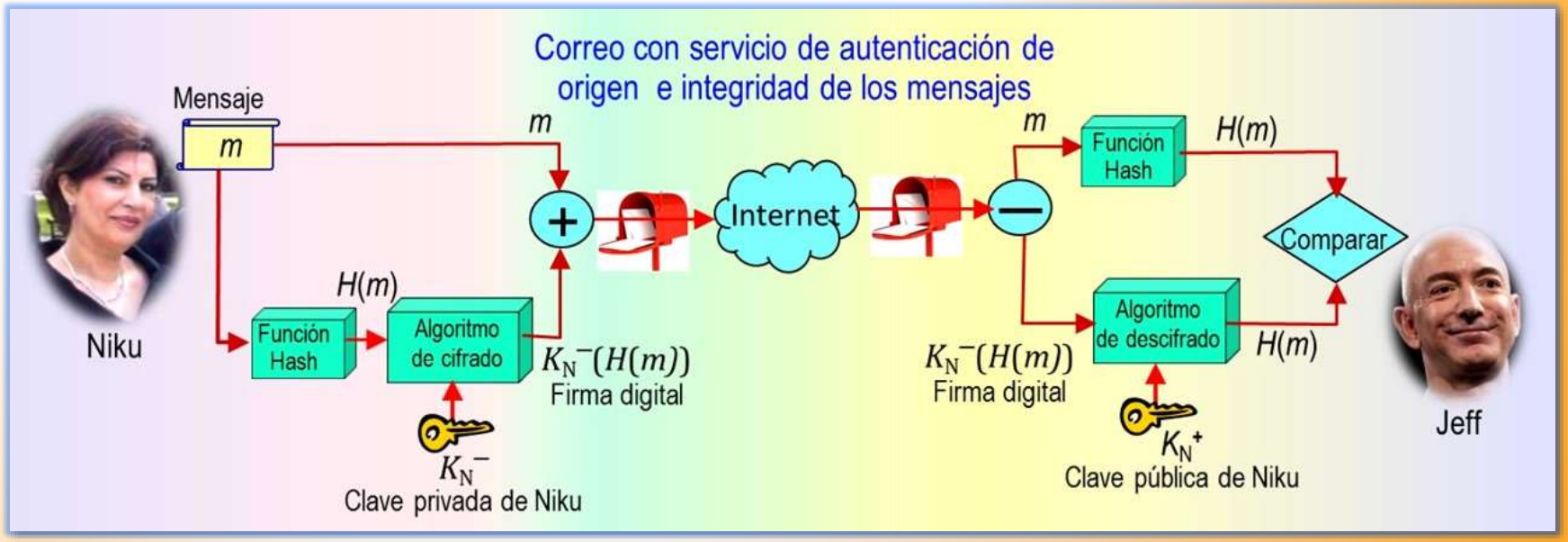
- **Cuando Elon recibe el paquete.**
  - ▶**1.** Utiliza su clave privada K_E^- para obtener la clave de sesión K_S, simétrica.
  - ▶**2.** Utiliza la clave sesión K_S para descifrar el mensaje m.

CORREO ELECTRÓNICO SEGURO

Autenticación de origen e integridad de los mensajes

(Kurose, 2017)

- **Habiendo diseñado** un sistema de correo electrónico seguro que proporciona confidencialidad, se va diseñar ahora otro sistema que proporcione tanto autenticación del emisor como integridad de los mensajes.
- **Se va suponer** que a Niku y a Jeff nos les preocupa la confidencialidad (quieren compartir sus códigos con todo el mundo) y que solo les preocupa la autenticación del emisor y la integridad de los mensajes.
- **Para llevar a c**abo esta tarea, se utilizan firmas digitales y resúmenes de mensajes (Hash).
- **Niku envía un paquete:**
  - ▶**1.** Aplica una función hash (por ejemplo MD5)a su mensaje, m, para obtener un resumen del mensaje, $H(m)$.
  - ▶**2.** Firma el resultado de la función hash con su clave privada K_N^-, para crear una firma digital, $K_N^-(H(m))$.

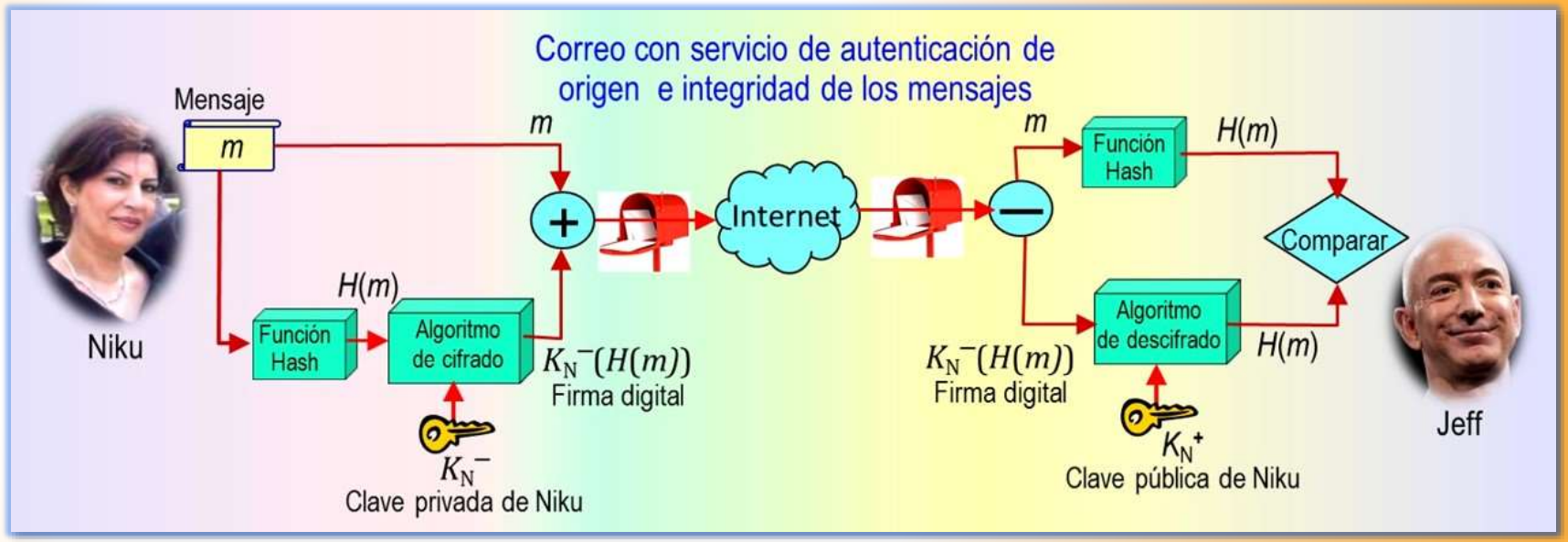


CORREO ELECTRÓNICO SEGURO

Autenticación de origen e integridad de los mensajes (cont.)

(Kurose, 2017)

- ▶**3.** Niku concatena el mensaje original (no cifrado) con la firma digital para crear un paquete: $m + K_N^-(H(m))$.
- ▶**4.** Niku envía el paquete a la dirección del correo electrónico de Jeff.



- **Jeff recibe el paquete:**
- ▶**1.** Separa el mensaje original (no cifrado), m, y la firma digital, $K_N^-(H(m))$.
- ▶**2.** Aplica la clave pública de Niku K_N^+ al resumen del mensaje firmado para obtener el valor Hash $H(m)$.
- ▶**3.** Compara el resultado de esta operación con su propio valor hash, $H(m)$, del mensaje. Si los dos resultados coinciden, Bill puede estar seguro de que el mensaje procede de Niku y no ha sido alterado.

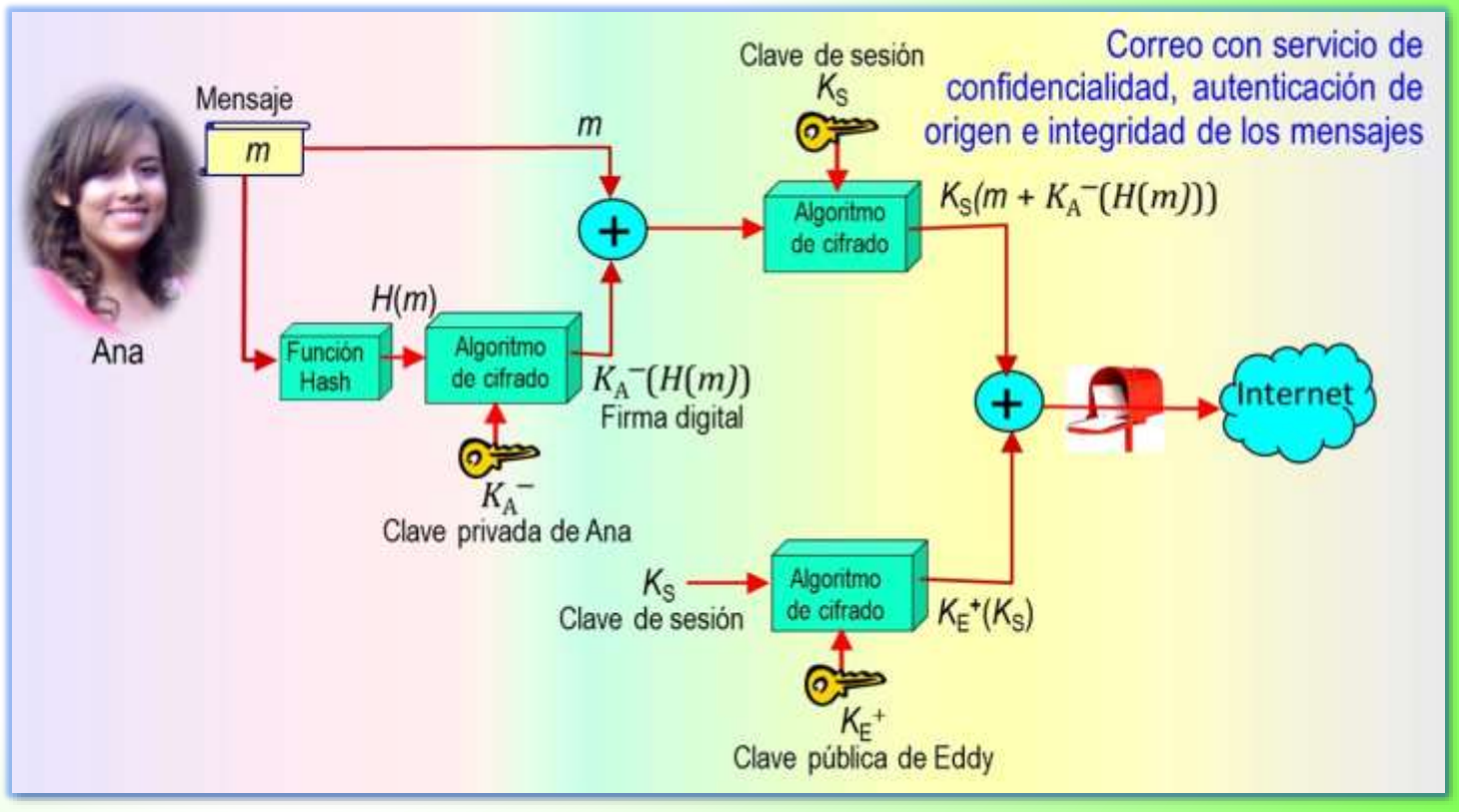
CORREO ELECTRÓNICO SEGURO

Todas las propiedades

(Kurose, 2017)

- **Se va a considerar** ahora el diseño de un sistema de correo electrónico que proporcione confidencialidad, autenticación del emisor e integridad de los mensajes. Esto puede hacerse combinando los procedimientos anteriormente descritos.

- **Ana envía un paquete:**
- ▶**1.** Crea primero un paquete preliminar, que está compuesto por su mensaje original y un valor Hash del mensaje firmado digitalmente: $m + K_A^-(H(m))$.
- ▶**2.** Trata este paquete preliminar como un mensaje en si mismo y envía este nuevo mensaje utilizando una clave de sesión K_S, creando un nuevo paquete que es enviado al correo electrónico de Eddy.
- **Eddy recibe el paquete:**
- ▶**1.** Aplica lo que corresponde, primero obtiene la clave de sesión K_S con la cual podrá descifrar el paquete que contiene el mensaje m y la función $H(m)$, lo cual le permitirá hacer la comparación para estar seguro de la procedencia y de la integridad del mensaje m.

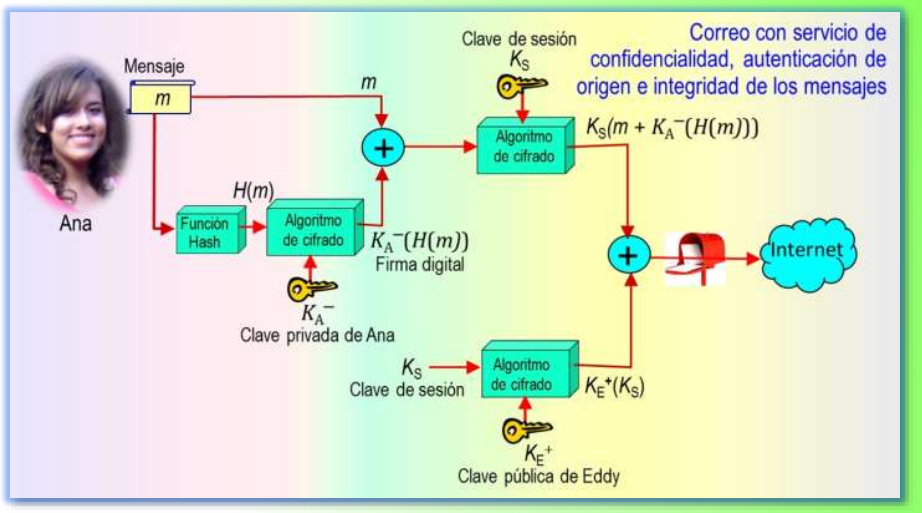


CORREO ELECTRÓNICO SEGURO

Todas las propiedades (cont.)

(Kurose, 2017)

- **Observe** que, con este esquema, Ana utiliza la criptografía de clave pública dos veces: una vez con su propia clave privada K_A^- y otra con la clave pública de Eddy K_E^+.
- **De forma similar**, Eddy también emplea la criptografía de clave pública dos veces: una con su clave privada K_E^- y otra con la clave publica de Ana K_A^+.
- **Este diseño** de correo electrónico seguro probablemente proporciona una seguridad satisfactoria para la mayoría de los usuarios de correo electrónico, en la mayoría de las ocasiones, pero aun tiene un problema importante por resolver.
- **Este diseño** requiere que Ana obtenga la clave publica de Eddy K_E^+. La distribución de estas claves publicas no es un problema trivial. Por ejemplo, una intrusa podría hacerse pasar por Eddy y darle a Ana su propia clave pública, mientras que le hace creer que se trata de la clave publica de Eddy, lo que permitiría a la intrusa recibir el mensaje destinado a Eddy.
- **Una técnica** muy popular para distribuir de forma segura las claves publicas consiste en certificar esas claves publicas utilizando una autoridad de certificación (CA).

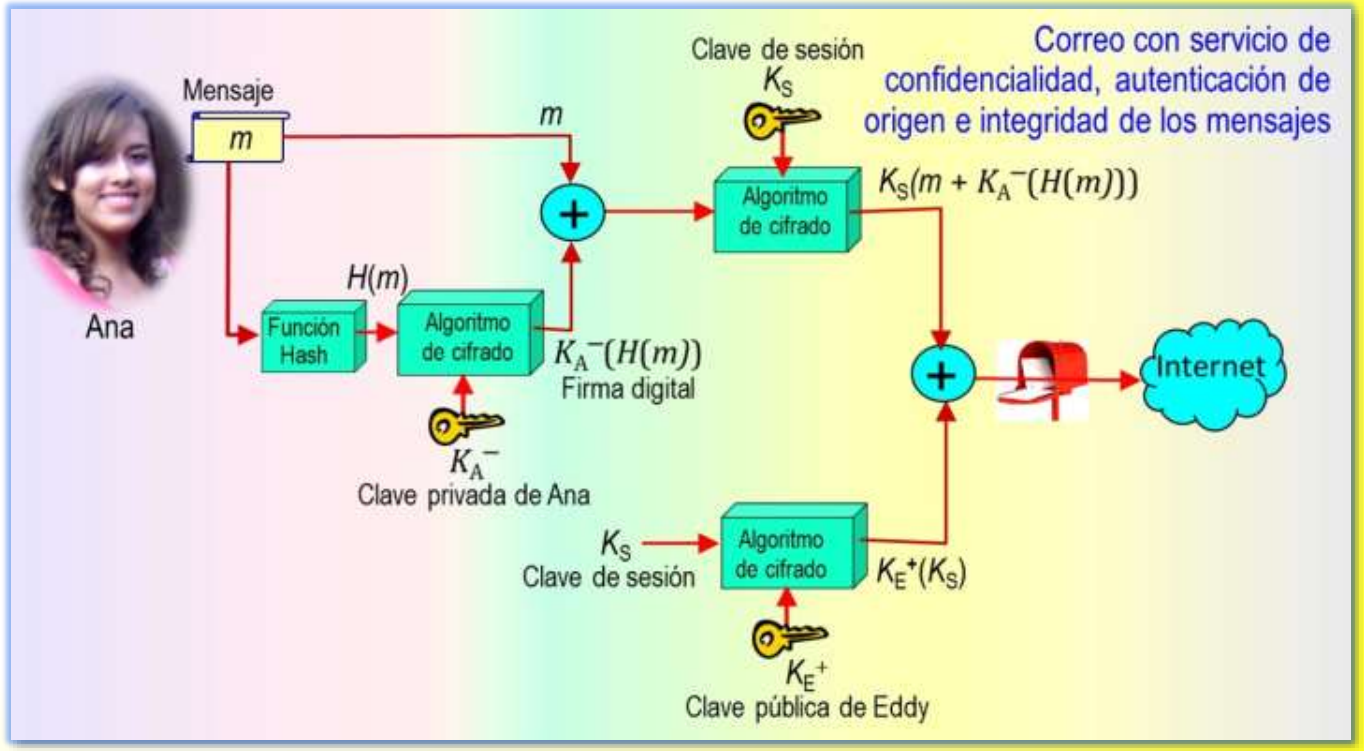


CORREO ELECTRÓNICO SEGURO

El cifrado *Pretty Good Privacy* (PGP)

(Kurose, 2017)

- **Escrito por** Phil Zimmermann en 1991. PGP es un buen ejemplo de esquema de cifrado de correo electrónico. Hay versiones de PGP disponibles en el dominio público, por ejemplo, se puede encontrar el software PGP para cualquier plataforma, así como una gran cantidad de artículos interesantes, en la página web internacional de PGP (PGP 2016).
- **Básicamente**, el diseño PGP es igual al mostrado en la figura. Dependiendo de la versión, el software PGP utiliza:
  - MD5 o SHA para calcular el resumen del mensaje (hash).
  - CAST, 3DES o IDEA para el Cifrado de clave simétrica.
  - RSA para el cifrado de la clave pública.



CORREO ELECTRÓNICO SEGURO

Mensajes firmados mediante PGP

(Kurose, 2017)

- ▶**1.** Cuando se instala PGP, el software crea una pareja de clave pública y clave privada para el usuario.
- ▶**2.** La clave pública puede darse a conocer a todo el mundo a través del sitio web del usuario o puede almacenarse en un servidor de clave pública.
- ▶**3.** La clave privada está protegida mediante el uso de una contraseña. La contraseña debe introducirse cada vez que el usuario accede a la clave privada.
- ▶**4.** PGP le da al usuario la opción de firmar digitalmente el mensaje, de cifrar el mensaje o de realizar tanto la operación de firmas como la de cifrado.
- **La figura** muestra un mensaje firmado de PGP. Los datos codificados en el mensaje son iguales a $K_A^-(H(m))$, es decir, son un resumen firmado digitalmente del mensaje.
- **Para que Eddy** verifique la integridad del mensaje necesitará tener acceso a la clave pública de Ana.

Mensaje firmado mediante PGP

```
--------BEGIN PGP SIGNED MESSAGE---------
Hash: SHA1
Bill:
¿Puedo verte esta tarde?
Te extraño mucho, Ximena
-----------BEGIN PGP SIGNATURE -----------------
Version: PGP for Personal Privacy 5.0
Charset: noconv
yhHJRHhgg /12EpJ+lo8gE4vB3mqJHFEvZP9t6n7G6m%GW2
----------------------END PGP SIGNATURE --------------------
```

CORREO ELECTRÓNICO SEGURO

Mensajes PGP secretos

(Kurose, 2017)

- **La figura** muestra un mensaje PGP secreto.
- ▶**1.** Por supuesto, el mensaje de texto en claro no está incluido en el mensaje secreto de correo electrónico. Cuando un emisor (como Ana) quiere tanto confidencialidad como integridad, PGP contiene un mensaje dentro del mensaje firmado.
- ▶**2.** PGP proporciona un mecanismo para certificación de clave pública, el cual es bastante distinto del sistema más convencional basado en autoridades de certificación.

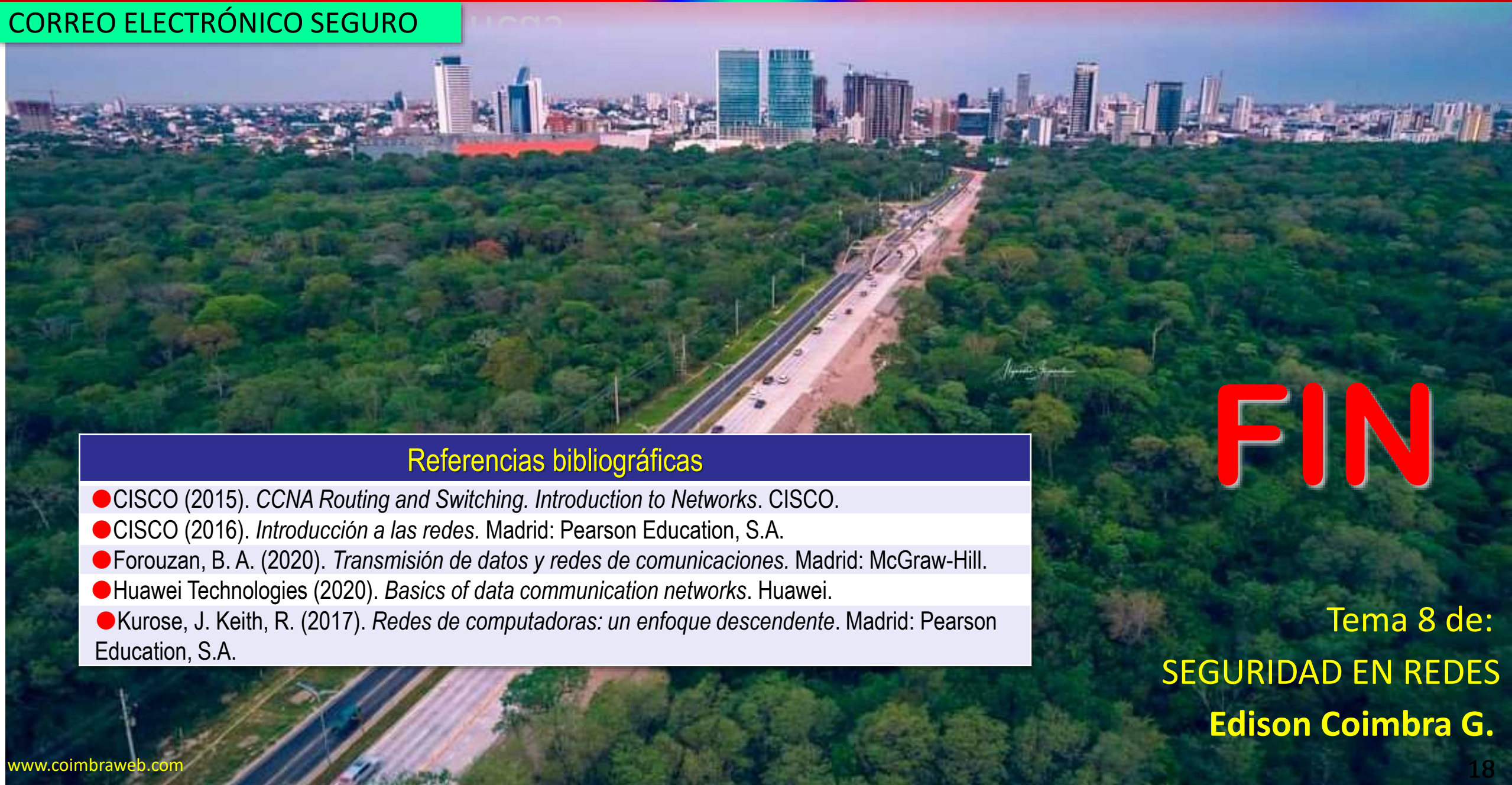
Mensaje PGP secreto

```
----------------------BEGIN PGP MESSAGE ----------------------
Version: PGP for Personal Privacy 5.0
u2R4d+/jKmn8BC5+hgDsqAewsDfrGdszX68liKm5F6Gc4sDfcX
RfdS10JuHgbcfDssWe7/K=1KhnMiKLoo+1/BvcX4t=Ujk9PbcD4
Thdf2awQfgHbmnKloK8iY6gThlp
----------------------END PGP MESSAGE ----------
```

- ▶**3.** Las claves públicas PGP están codificadas por una red de confianza. La propia Ana puede certificar cualquier pareja de clave/nombre de usuario cuando crea que esa pareja es realmente correcta. Además, PGP permite que Ana diga que confía en algún otro usuario a la hora de certificar la autenticidad de otras claves.
- ▶**4.** Algunos otros usuarios PGP firman mutuamente sus claves manteniendo reuniones específicas de firma de claves. Los usuarios se reúnen físicamente, intercambian sus claves públicas y certifican las claves unos con otros firmándolas con sus claves privadas.

Referencias bibliográficas

CORREO ELECTRÓNICO SEGURO



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 8 de:

SEGURIDAD EN REDES

Edison Coimbra G.