Seguridad en Redes

- Clase práctica -

Teoría de las Comunicaciones

Departamento de Computación
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

11.11.2025

Agenda

Seguridad - ¿Dónde la vemos?

Protocolos y Capas

- La seguridad se implementa para resolver diferentes potenciales **problemas en diferentes capas** de la arquitectura de una red.

Seguridad - Principales conceptos

Seguridad - Principales conceptos

- **Confidencialidad.**
- **Integridad.**
- **Autenticación.**
- **No Repudio.**
- *Disponibilidad.*
- *Autorización (Control de acceso).*

Seguridad - Principales conceptos

Confidencialidad

Seguridad - Principales conceptos

Confidencialidad

Los mensajes sólo pueden ser entendidos por las partes “autorizadas” en la comunicación.

Seguridad - Principales conceptos

Confidencialidad

Los mensajes sólo pueden ser entendidos por las partes “autorizadas” en la comunicación.

Integridad

Seguridad - Principales conceptos

Confidencialidad

Los mensajes sólo pueden ser entendidos por las partes “autorizadas” en la comunicación.

Integridad

Los mensajes enviados no pueden ser modificados *(ni sustituidos por una copia artificial, ni demorados intencionalmente)* durante su transmisión.

Seguridad - Principales conceptos

Confidencialidad

Los mensajes sólo pueden ser entendidos por las partes “autorizadas” en la comunicación.

Integridad

Los mensajes enviados no pueden ser modificados *(ni sustituidos por una copia artificial, ni demorados intencionalmente)* durante su transmisión.

Autenticación

Seguridad - Principales conceptos

Confidencialidad

Los mensajes sólo pueden ser entendidos por las partes "autorizadas" en la comunicación.

Integridad

Los mensajes enviados no pueden ser modificados *(ni sustituidos por una copia artificial, ni demorados intencionalmente)* durante su transmisión.

Autenticación

Las partes "autorizadas" pueden verificar que el mensaje recibido es de quien dice ser el emisor. Podemos comprobar el origen de un mensaje.

Seguridad - Principales conceptos

Confidencialidad

Los mensajes sólo pueden ser entendidos por las partes "autorizadas" en la comunicación.

Integridad

Los mensajes enviados no pueden ser modificados *(ni sustituidos por una copia artificial, ni demorados intencionalmente)* durante su transmisión.

Autenticación

Las partes "autorizadas" pueden verificar que el mensaje recibido es de quien dice ser el emisor. Podemos comprobar el origen de un mensaje.

No repudio

Seguridad - Principales conceptos

Confidencialidad

Los mensajes sólo pueden ser entendidos por las partes "autorizadas" en la comunicación.

Integridad

Los mensajes enviados no pueden ser modificados *(ni sustituidos por una copia artificial, ni demorados intencionalmente)* durante su transmisión.

Autenticación

Las partes "autorizadas" pueden verificar que el mensaje recibido es de quien dice ser el emisor. Podemos comprobar el origen de un mensaje.

No repudio

Ninguna de las partes puede negar haber participado en una transacción.

Seguridad - Herramientas

Criptografía

La criptografía consiste en construir y analizar esquemas y protocolos para prevenir que terceros no deseados tengan acceso a mensajes privados.

Seguridad - Herramientas

Criptografía

La criptografía consiste en construir y analizar esquemas y protocolos para prevenir que terceros no deseados tengan acceso a mensajes privados.

Esquema de Firma Digital

Una esquema de firma digital es la versión electrónica de una firma manuscrita. Es un esquema criptográfico que garantiza la autenticidad, integridad y no repudio de un documento electrónico.

Seguridad - Herramientas

Criptografía

La criptografía consiste en construir y analizar esquemas y protocolos para prevenir que terceros no deseados tengan acceso a mensajes privados.

Esquema de Firma Digital

Una esquema de firma digital es la versión electrónica de una firma manuscrita. Es un esquema criptográfico que garantiza la autenticidad, integridad y no repudio de un documento electrónico.

Certificado Digital

Documento electrónico emitido por una Autoridad de Certificación (CA) que vincula la identidad de una persona, entidad o atributo a una clave pública.

Seguridad - ¿Mucha terminología confusa?

Glosario

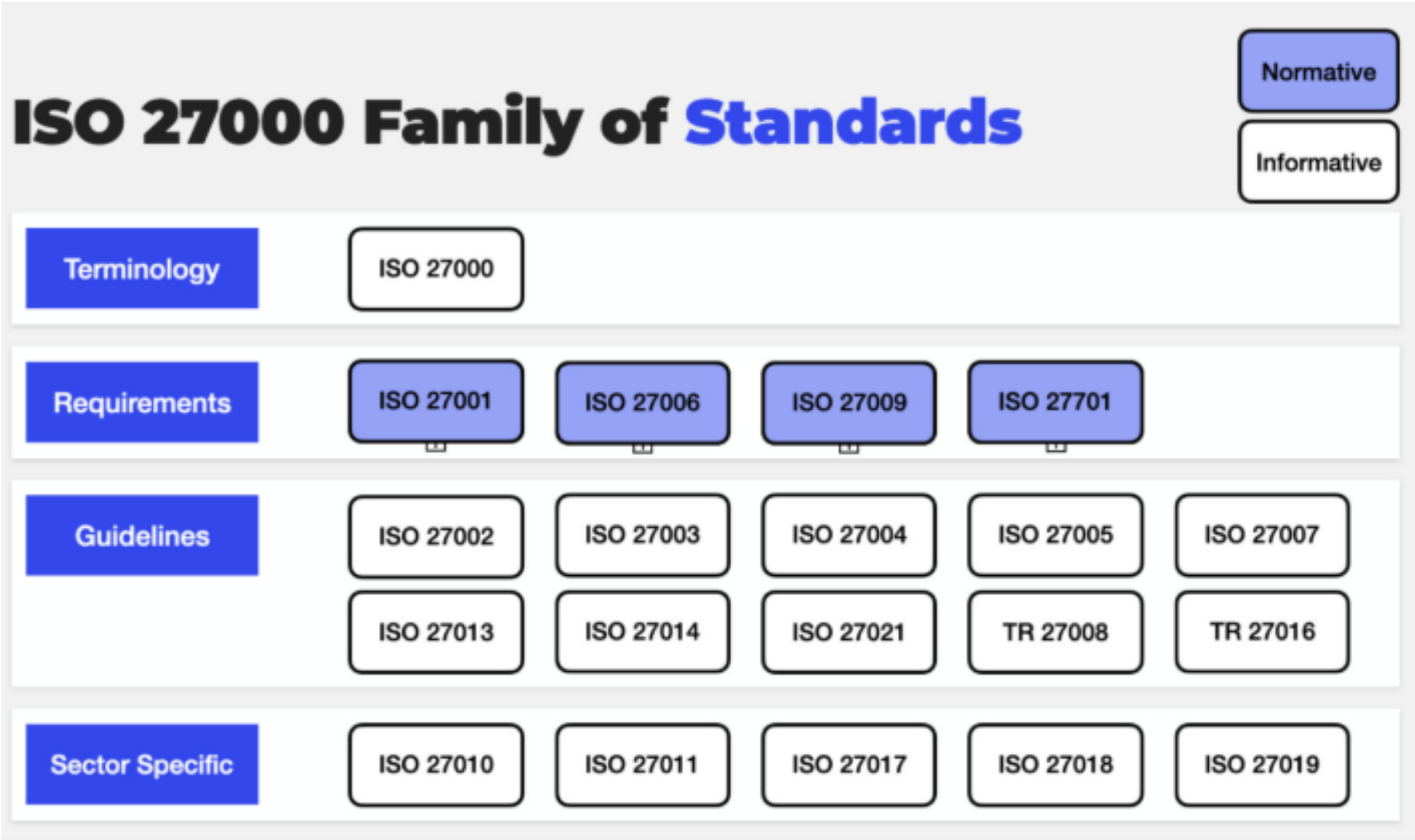
Esquema, protocolo, primitiva, control

Mucha terminología tiene definición borrosa. Generalmente,

- Un *esquema* es un conjunto de algoritmos que otorgan un determinado tipo de protección. Cada algoritmo corre en un particular sistema.
- Un *protocolo* es una descripción de operaciones entre múltiples partes, para otorgar comunicación segura. Varios esquemas pueden ser utilizados.
- Una *primitiva* es un esquema o sub-componente de un esquema que se lo ve como componente "atomica" de un sistema mas grande.
- Un *control* es un "componente" en un sistema "de seguridad": *e.g.*, cerraduras, matafuegos, sistemas de firma digital, antivirus, leyes de protección de datos.

Ante cada tecnología de Seguridad debemos preguntarnos:
¿Cual subconjunto de propiedades provee?

Seguridad - Definición



La familia de normas ISO2700 juegan el papel fundamental en la gestión de la **Seguridad de la Información** y la **Ciberseguridad**.

Seguridad - Herramientas y Conceptos

Añadir tabla!!!

Seguridad - Definición

La **seguridad** (RAE) es la **ausencia de peligro**, indestructibilidad, invulnerabilidad.

Pero, ¿podemos lograr redes 100 % seguras?

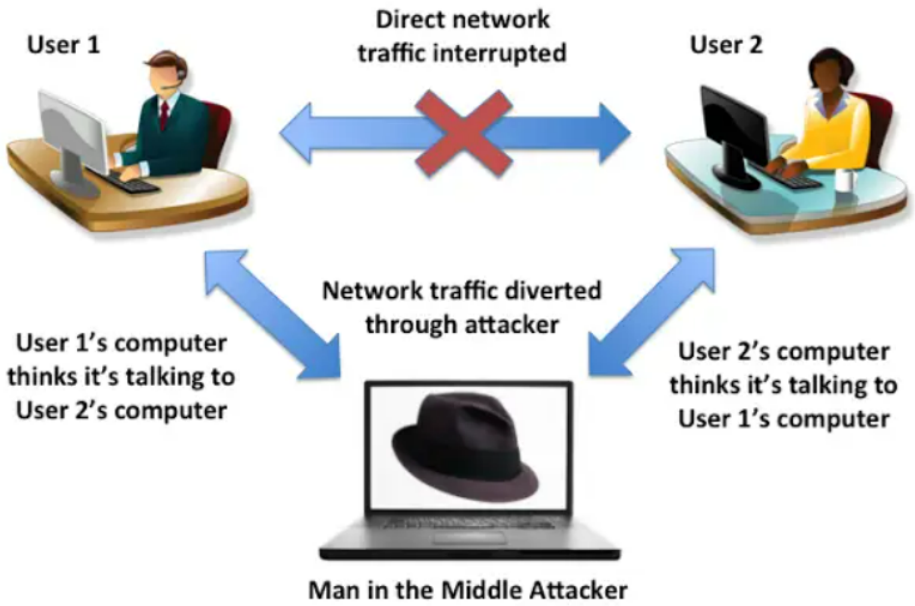
Criptografía Simétrica

Criptografía Simétrica

- Existe una **única** clave K
- K se utiliza para encriptar texto plano y desencriptar texto encriptado
- La clave es el secreto que comparten ambos extremos de la comunicación
- Garantiza **confidencialidad**
- El problema de distribución de claves siempre ha sido la parte más débil de este criptosistema
- Ejemplos: DES, 3DES, AES
- AES es lo mínimo que se usa hoy, es más rápido y seguro debido a su mayor tamaño de clave (128, 192, 256)

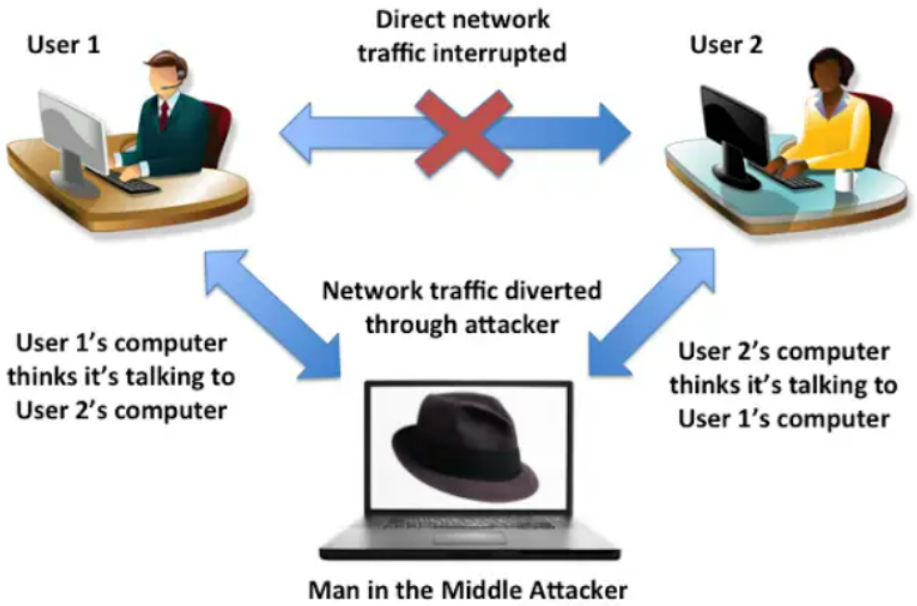
Criptografía Simétrica

¿Qué pasa si...?



Criptografía Simétrica

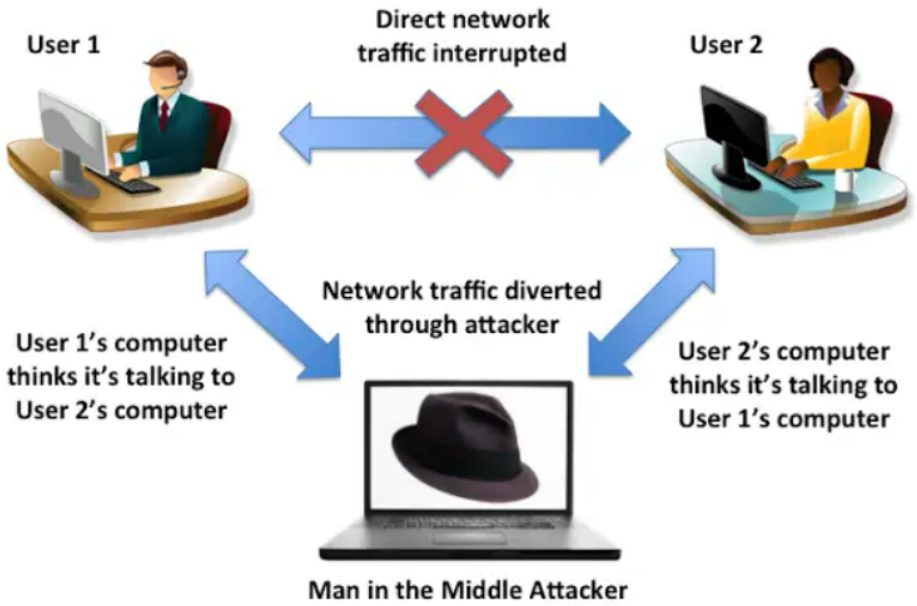
¿Qué pasa si...?



- Es posible modificar los mensajes, no hay manera de comprobar integridad. Aunque la clave no sea comprometida

Criptografía Simétrica

¿Qué pasa si...?



- Es posible modificar los mensajes, no hay manera de comprobar integridad. Aunque la clave no sea comprometida
- Tampoco podemos verificar autenticación. La clave es compartida

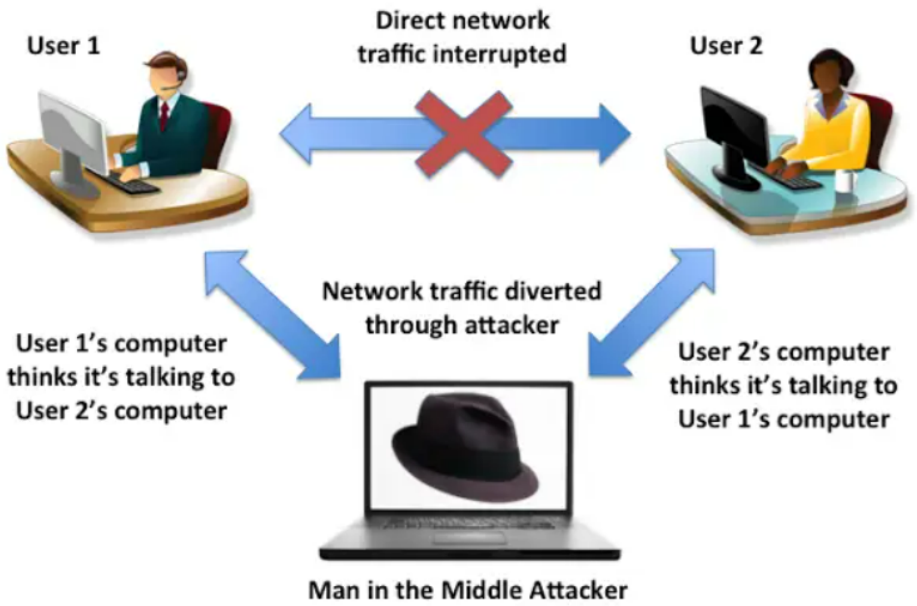
Criptografía Asimétrica

Criptografía Asimétrica

- **Diferentes** claves para cifrar y descifrar
- Una de las claves es (**pública**) y se comparte, la otra (**secreta**) es privada
- Puede garantizar tanto la **confidencialidad** como la **autenticación**, pero de manera diferente, dependiendo de cómo se utilicen las claves públicas y privadas.
- Desventaja: se puede vulnerar la relación entre las entidades y sus claves. ¿Tengo la clave pública correcta?
- Desventaja: Tiene un costo computacional mucho más elevado
- Ejemplo: RSA

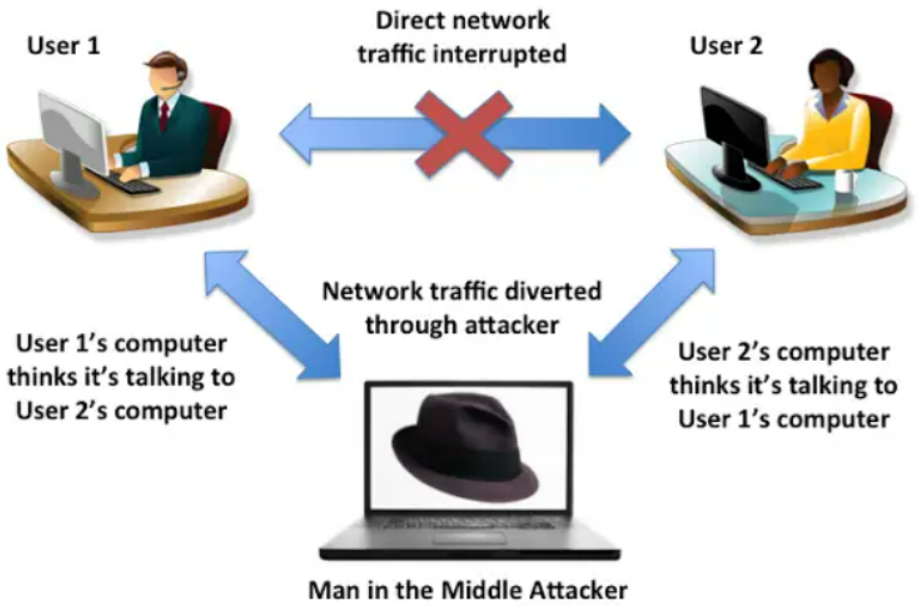
Criptografía Asimétrica

¿Qué pasa si...?



Criptografía Asimétrica

¿Qué pasa si...?



- Es posible modificar los mensajes, no hay manera de comprobar integridad.

Notación

Un **sistema criptográfico** es una tupla (M,K,C,E,D) tal que:

- M es el conjunto de los **mensajes válidos** en texto plano
- K el conjunto de **claves**
- C es el conjunto de los textos cifrados (**criptogramas**)
- E: $M \times K \rightarrow C$
- D: $C \times K \rightarrow M$

¿Cómo usar la Notación?

Mensaje: M

Criptograma: C

Digesto: D

Clave simétrica: K

Clave pública de A: K_A^+

Clave privada de A: K_A^-

Encriptar M utilizando la clave Q: $E_Q(M) = C$ con $Q \in \{K, K_A^+, K_A^-\}$

Desencriptar el C utilizando la clave Q: $D_Q(C) = M$ con $Q \in \{K, K_A^+, K_A^-\}$

Aplicar Función de Hash Criptográfico: $H(M) = D$

Aclaración: La notación permite combinar cada algoritmo con cada tipo de clave para obtener distintos resultados. No todo algoritmo permite toda clave. Deberá aclararse qué algoritmo es el utilizado.

Funciones de hash

Primitiva criptográfica que garantiza **integridad**

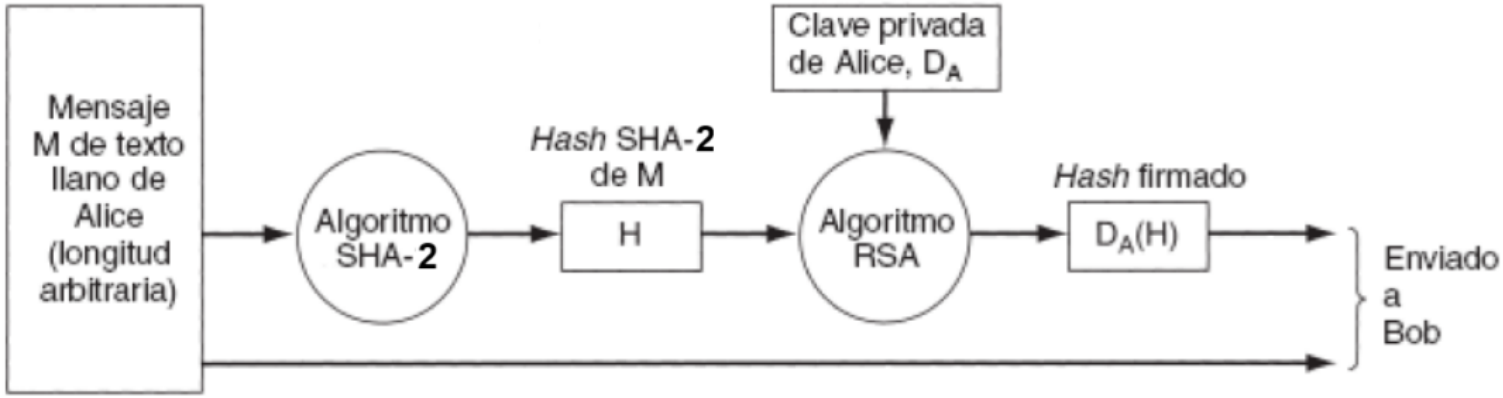
Funciones de hash

Primitiva criptográfica que garantiza **integridad**

- **Definición** $h : A \to B$
- **Mapea entradas de tamaño arbitrario a salidas de longitud fija**. Dado $x \in A$, $h(x)$ es fácil de computar
- Se dice que es "**no inversible**". $\forall\, y \in B$ es inviable encontrar $x \in A$ tq $h(x) = y$
- **Resistente a colisiones**. Es inviable computacionalmente encontrar $x, \hat{x} \in A$ tq $x <> \hat{x}$ y $h(x) = h(\hat{x})$
- Ejemplos: HAVAL, MD5, SHA-1, SHA-2, SHA-3, BLAKE2.
- SHA-2 (lo mismo que SHA-256) es lo mínimo que se usa hoy

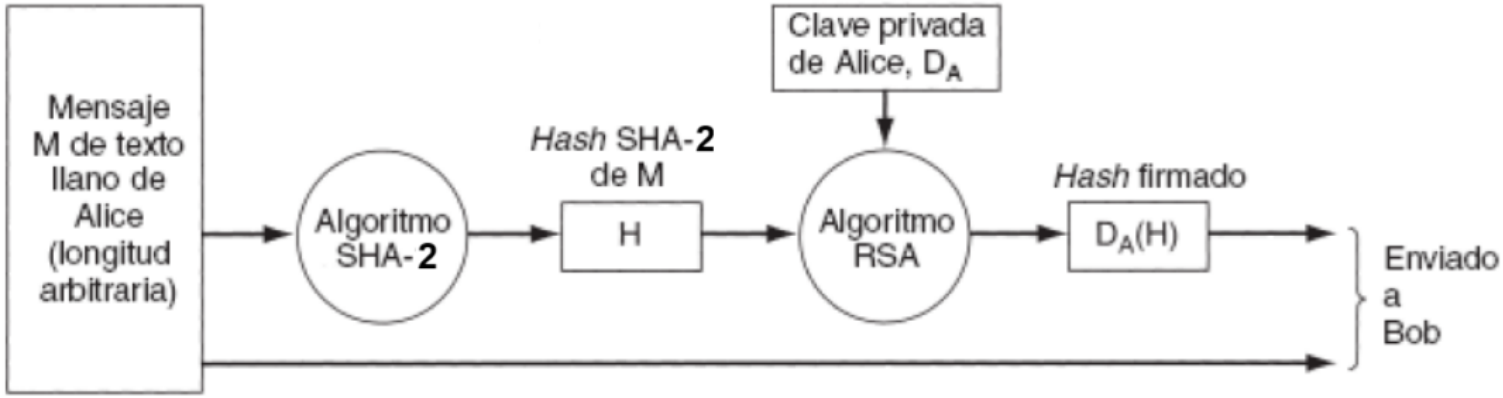
Firma digital

Firma digital



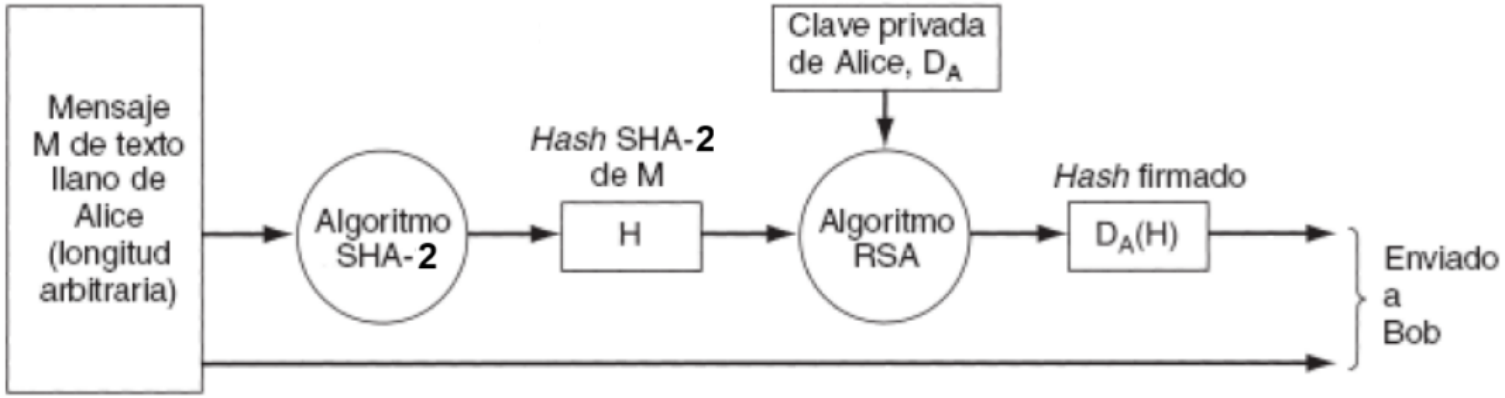
- El emisor **encripta con su llave privada** (firma) el hash del mensaje que desea enviar y lo manda junto con el mensaje al receptor

Firma digital



- El emisor **encripta con su llave privada** (firma) el hash del mensaje que desea enviar y lo manda junto con el mensaje al receptor
- Podemos verificar fácilmente la **integridad**

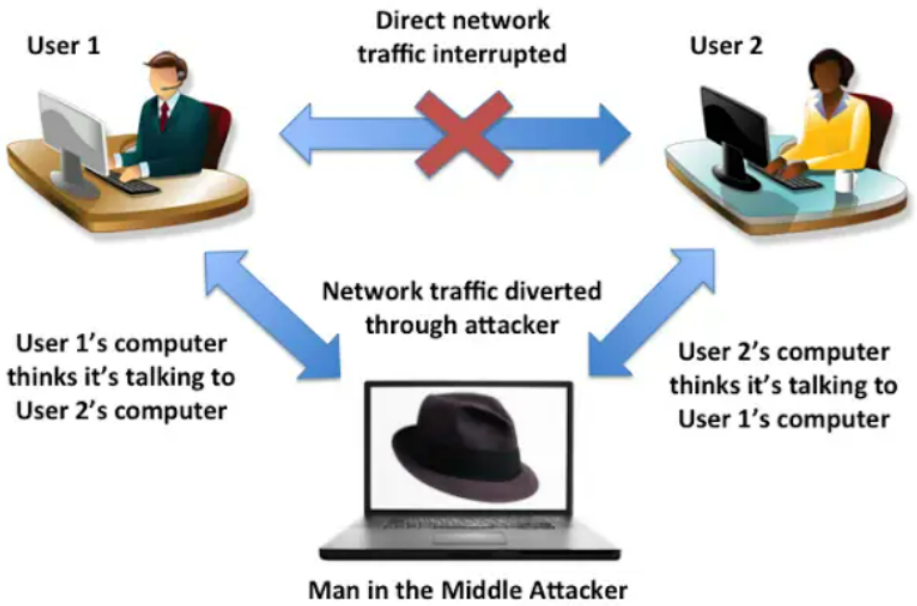
Firma digital



- El emisor **encripta con su llave privada** (firma) el hash del mensaje que desea enviar y lo manda junto con el mensaje al receptor
- Podemos verificar fácilmente la **integridad**
- ¿Por qué no se encripta directamente el mensaje?

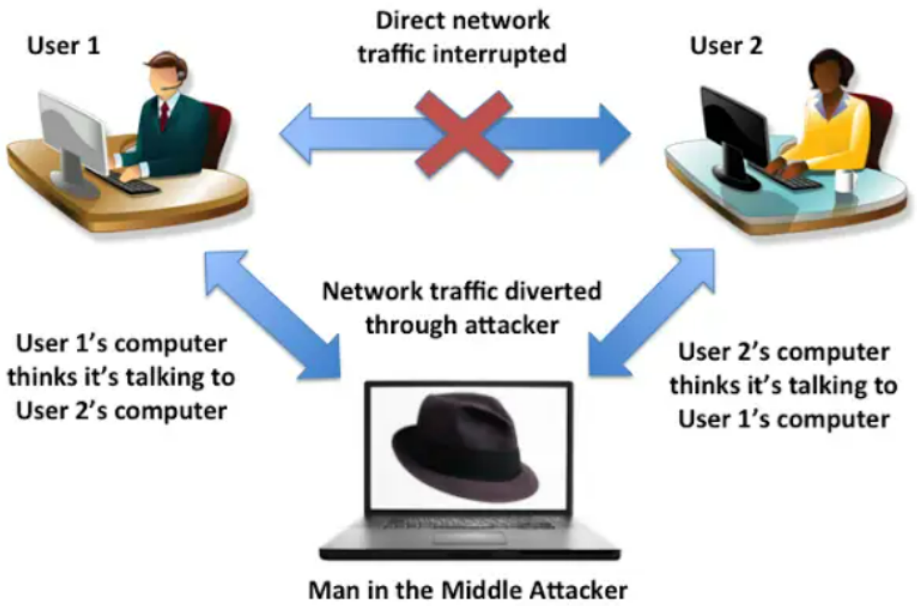
Firma digital

¿Qué pasa si...?



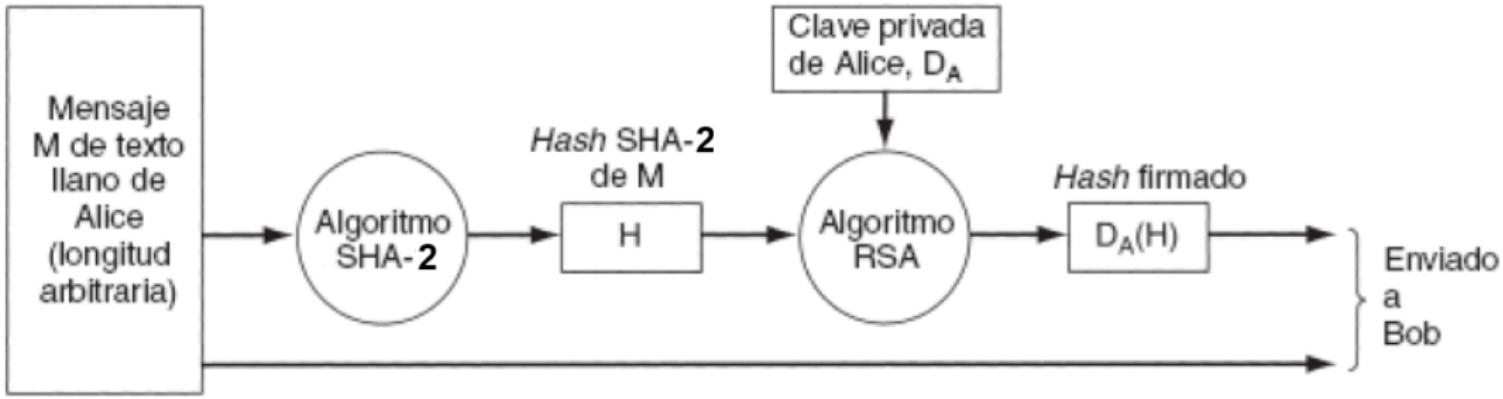
Firma digital

¿Qué pasa si...?



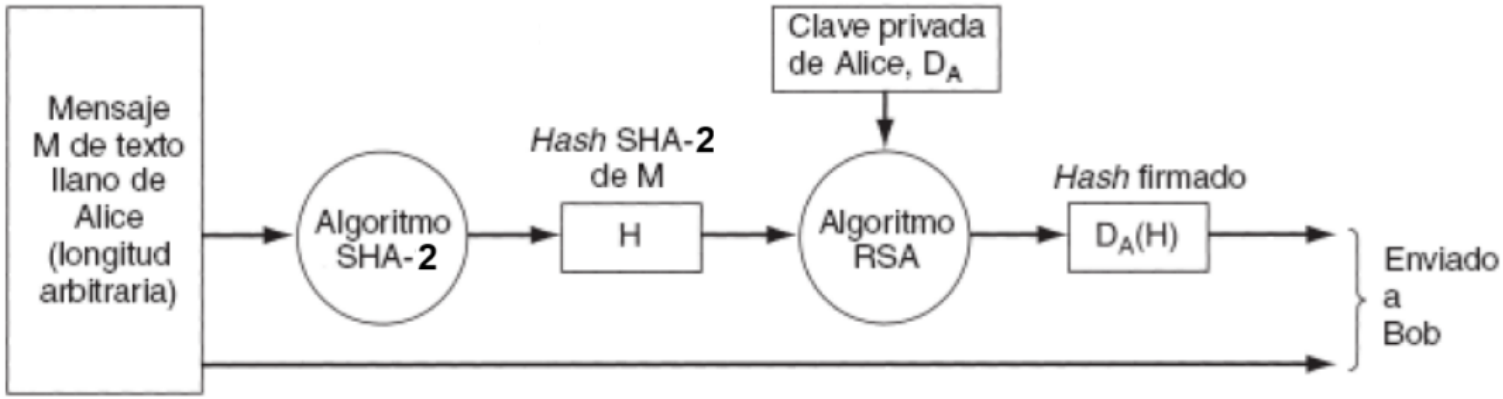
- Es posible modificar los mensajes, pero ahora tenemos una forma de comprobar la integridad

Firma digital



- También podemos verificar la **autenticidad** y **no repudio**

Firma digital

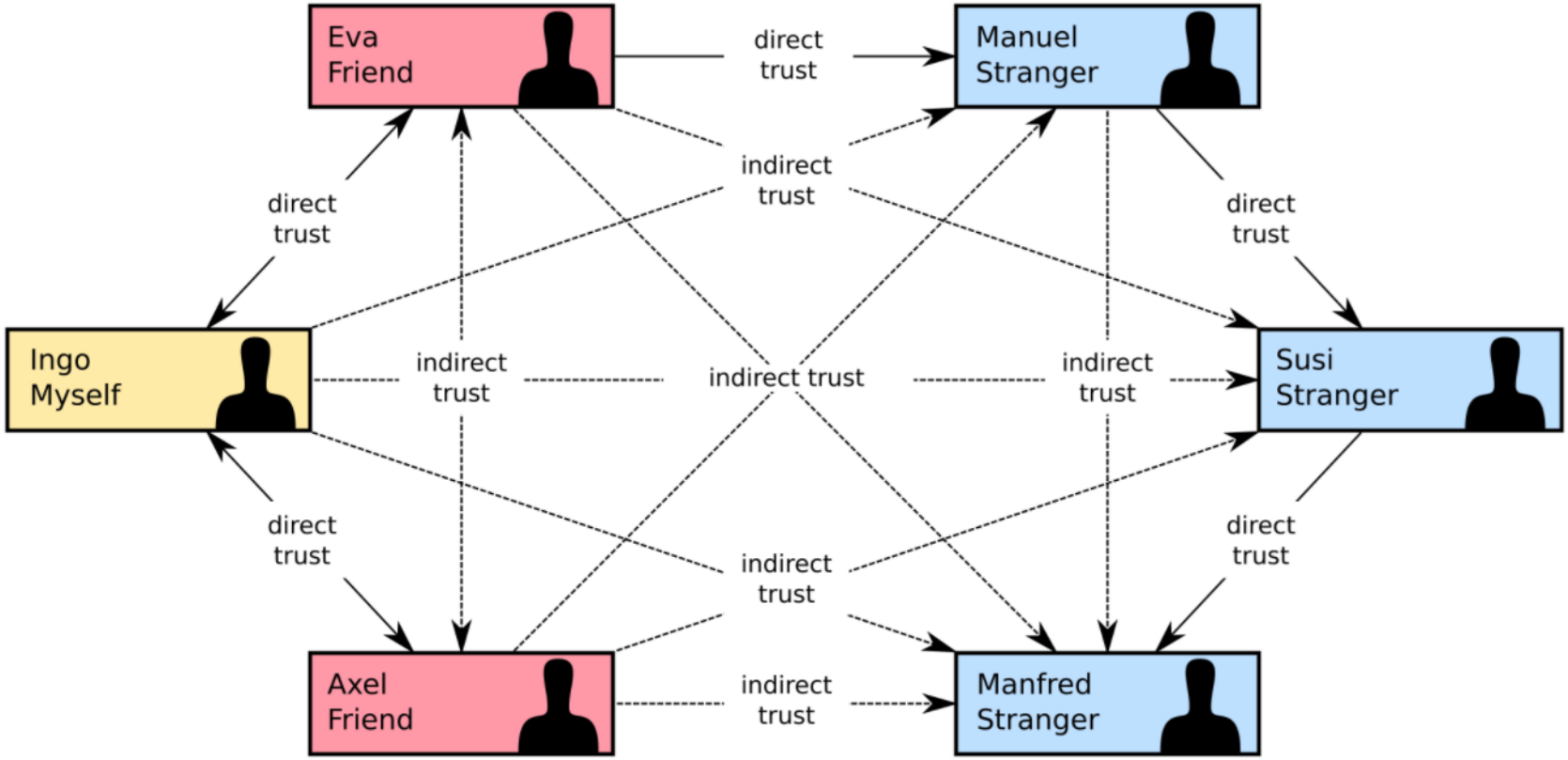


- También podemos verificar la **autenticidad** y **no repudio**
- Pero: ya habíamos visto que se puede vulnerar la relación entre las entidades y sus claves ¿Cómo obtiene cada uno la clave pública del otro para iniciar el proceso de comunicación?

¿Cómo lo podemos solucionar?

Web of Trust - PGP

Sistema descentralizado. Fiestas de firmado de claves.



Certificados digitales y PKI

Sistema centralizado.

Certificados digitales y PKI

Sistema centralizado.

- Los **certificados digitales** son relaciones válidas entre claves públicas y cierta entidad

Certificados digitales y PKI

Sistema centralizado.

- Los **certificados digitales** son relaciones válidas entre claves públicas y cierta entidad
- Para darle validez a estos certificados se confía en **autoridades certificantes** o **cadenas de confianza**, que conforman un esquema jerárquico denominado Infraestructura de Clave Pública (PKI)

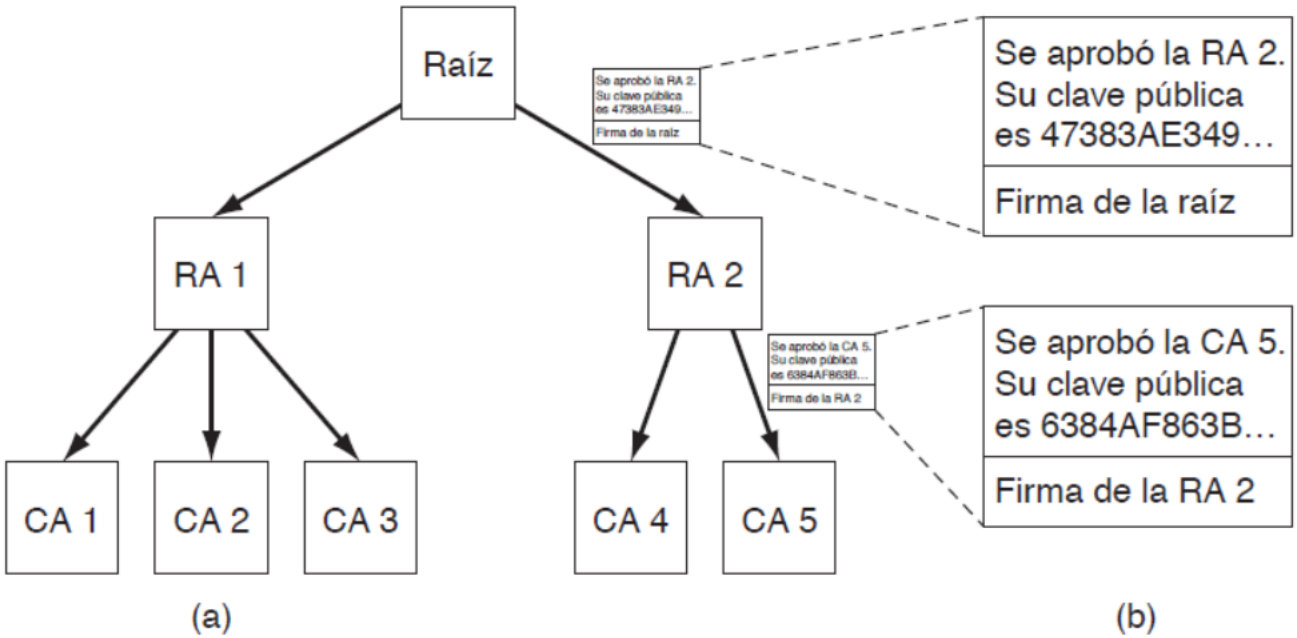


Figura 1-16. (a) Una PKI jerárquica. (b) Una cadena de certificados.

Certificados digitales y PKI

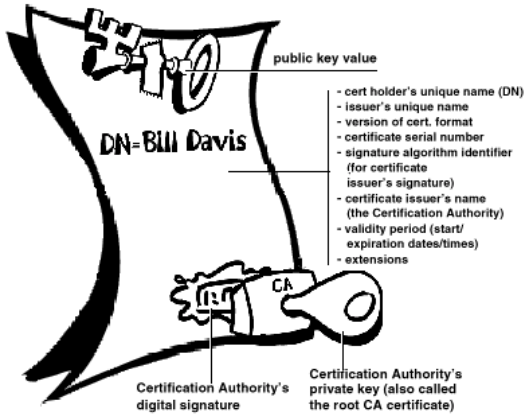
- **X.509v3** es el estándar de que define los formatos de certificados (RFC 6818 la última versión)

Certificados digitales y PKI

- **X.509v3** es el estándar de que define los formatos de certificados (RFC 6818 la última versión)

Certifico que la clave pública
19836A8B03030CF83737E3837837FC3s87092827262643FFA82710382828282A
pertenece a
Robert John Smith
12345 University Avenue
Berkeley, CA 94702
Cumpleaños: Julio 4, 1958
Correo electrónico: bob@superdupernet.com

Hash SHA-1 del certificado anterior firmado con la clave privada de la CA



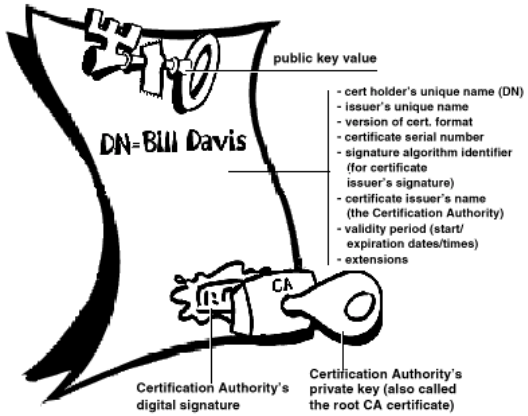
$$(C_i;\ K^+_{C_i};\ F_{CA,C_i}),\ \textbf{con}\ F_{CA,C_i} = E_{K^-_{CA}}(H(C_i + K^+_{C_i}))$$

Certificados digitales y PKI

- **X.509v3** es el estándar de que define los formatos de certificados (RFC 6818 la última versión)

Certifico que la clave pública
19836A8B03030CF83737E3837837FC3s87092827262643FFA82710382828282A
pertenece a
Robert John Smith
12345 University Avenue
Berkeley, CA 94702
Cumpleaños: Julio 4, 1958
Correo electrónico: bob@superdupernet.com

Hash SHA-1 del certificado anterior firmado con la clave privada de la CA



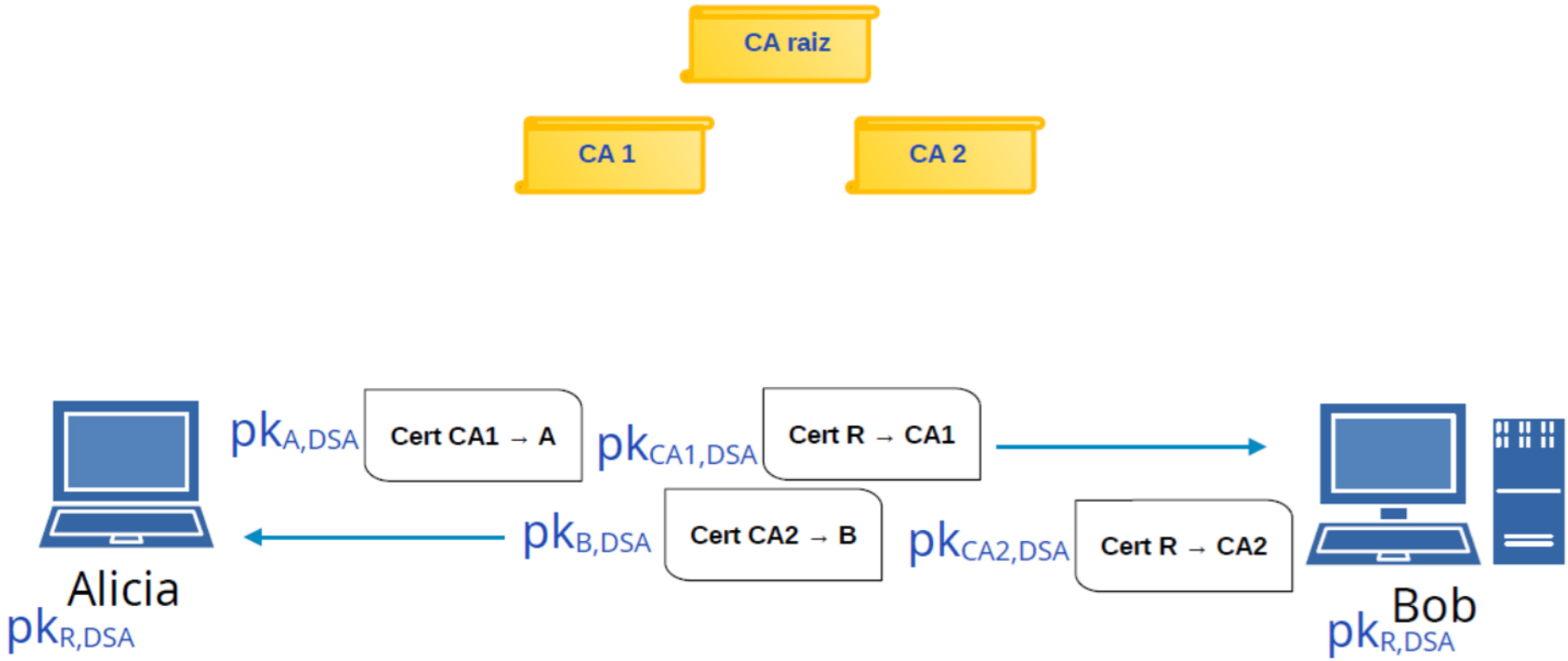
$$(C_i;\ K^+_{C_i};\ F_{CA,C_i}),\ \textbf{con}\ F_{CA,C_i} = E_{K^-_{CA}}(H(C_i + K^+_{C_i}))$$

¿Cómo podemos comprobar el certificado de un cliente C_i ?

Certificados digitales y PKI

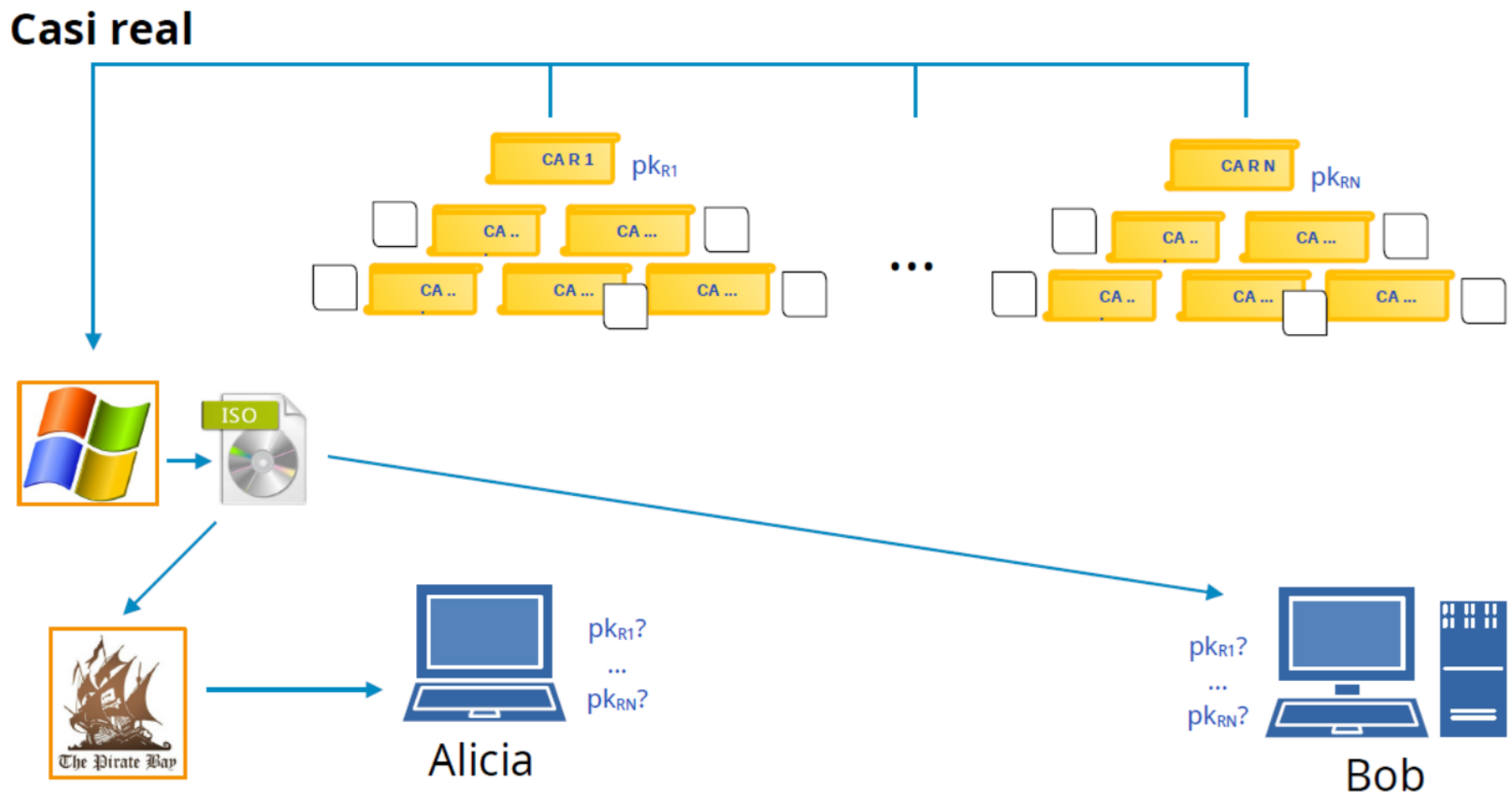
DEMO CERTIFICADOS

Certificados digitales y PKI



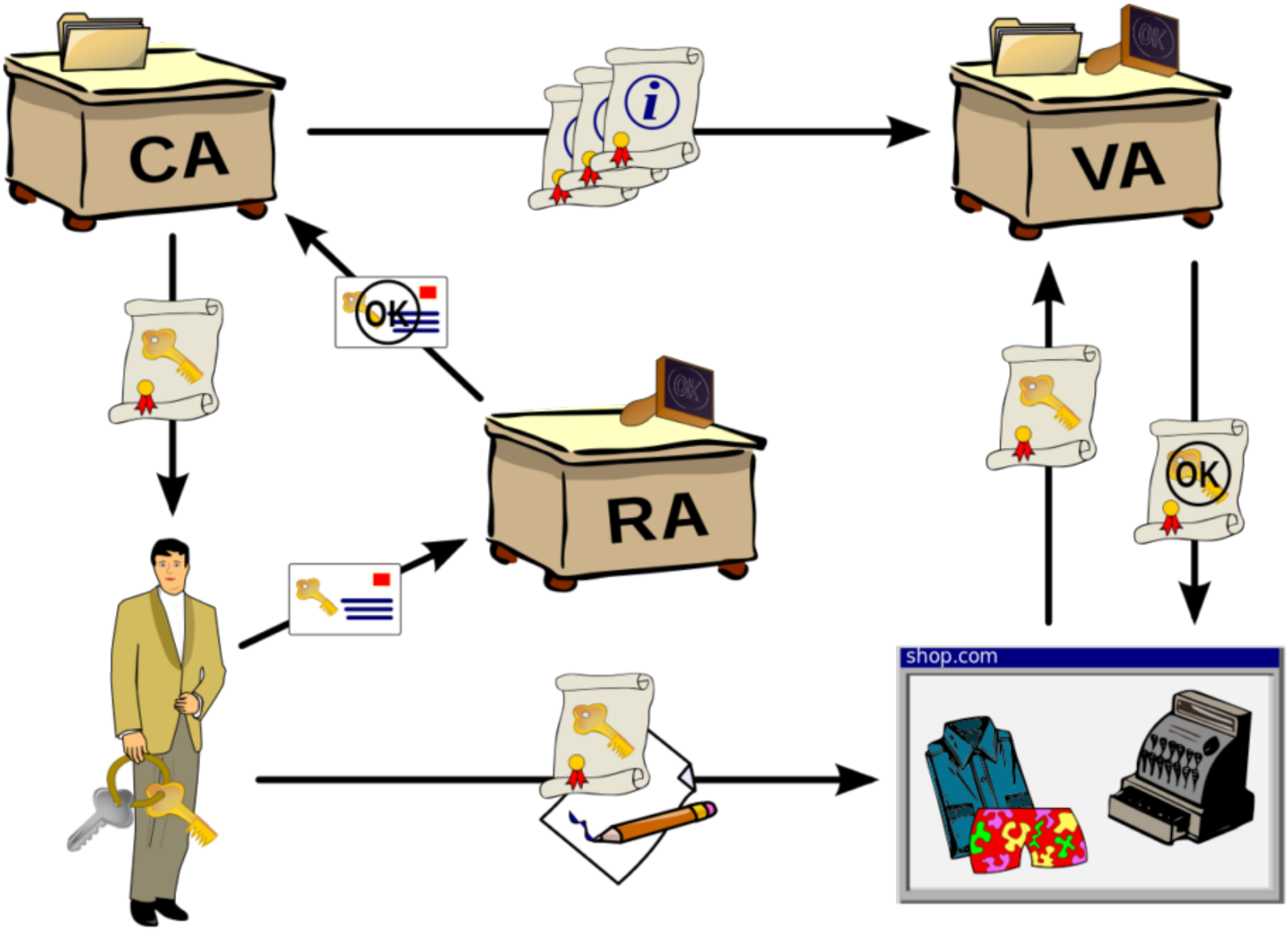
¿Qué pasa en este caso?

Certificados digitales y PKI



¿Qué pasa en este caso?

Certificado Digital y PKI

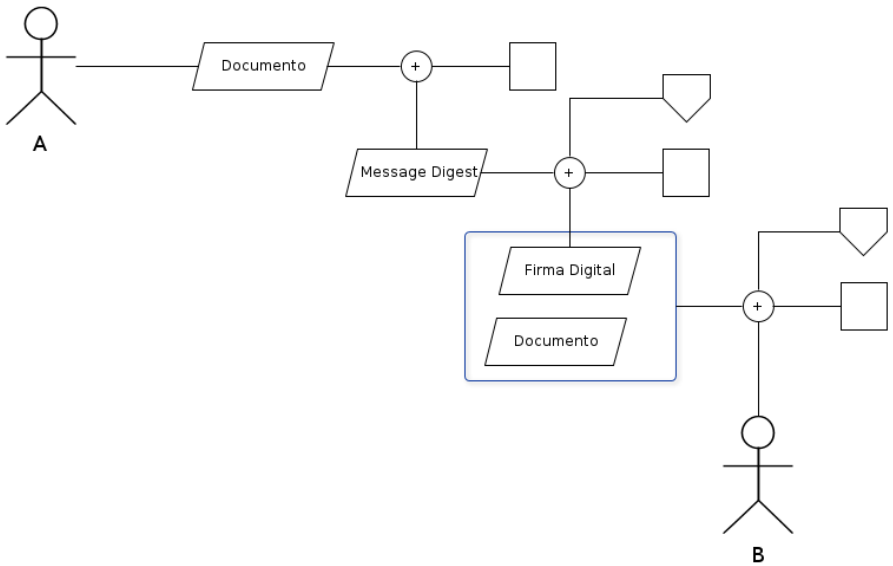


Ejercicio 1.

A desea enviarle un mensaje a B de carácter importante. A quiere asegurarse de que nadie excepto B pueda leerlo y que B pueda confiar en que A fue quién envió el mensaje.

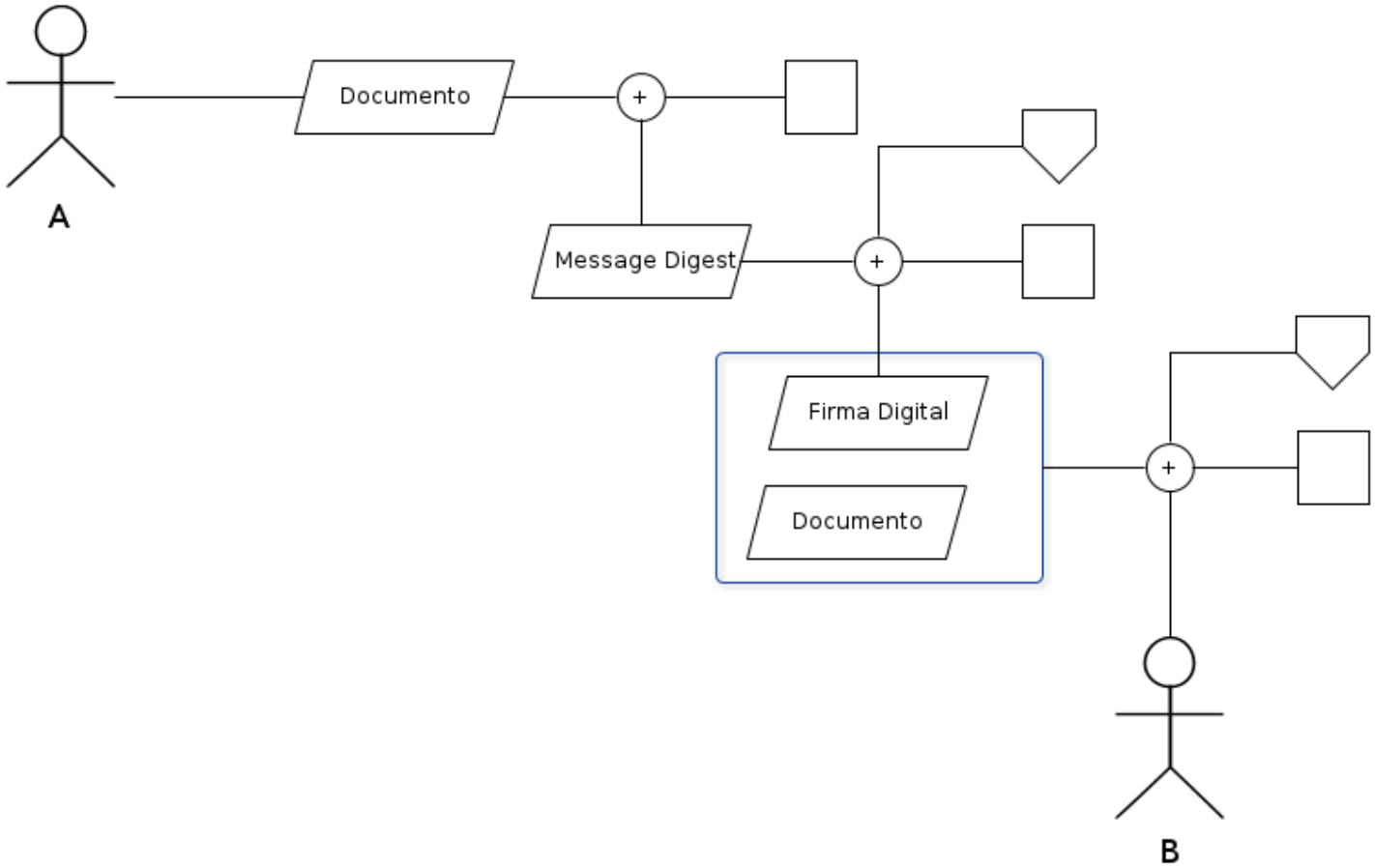
a. Basandose en el esquema a continuación, completando los cuadrados con algoritmos y las casitas con los parámetros adicionales que estos toman, explique cómo puede hacer A para construir el mensaje usando criptografía asimétrica, de manera de garantizar las propiedades de Confidencialidad y No repudio.

b. Explique qué debe hacer B para verificar que A fue quién envió el mensaje.



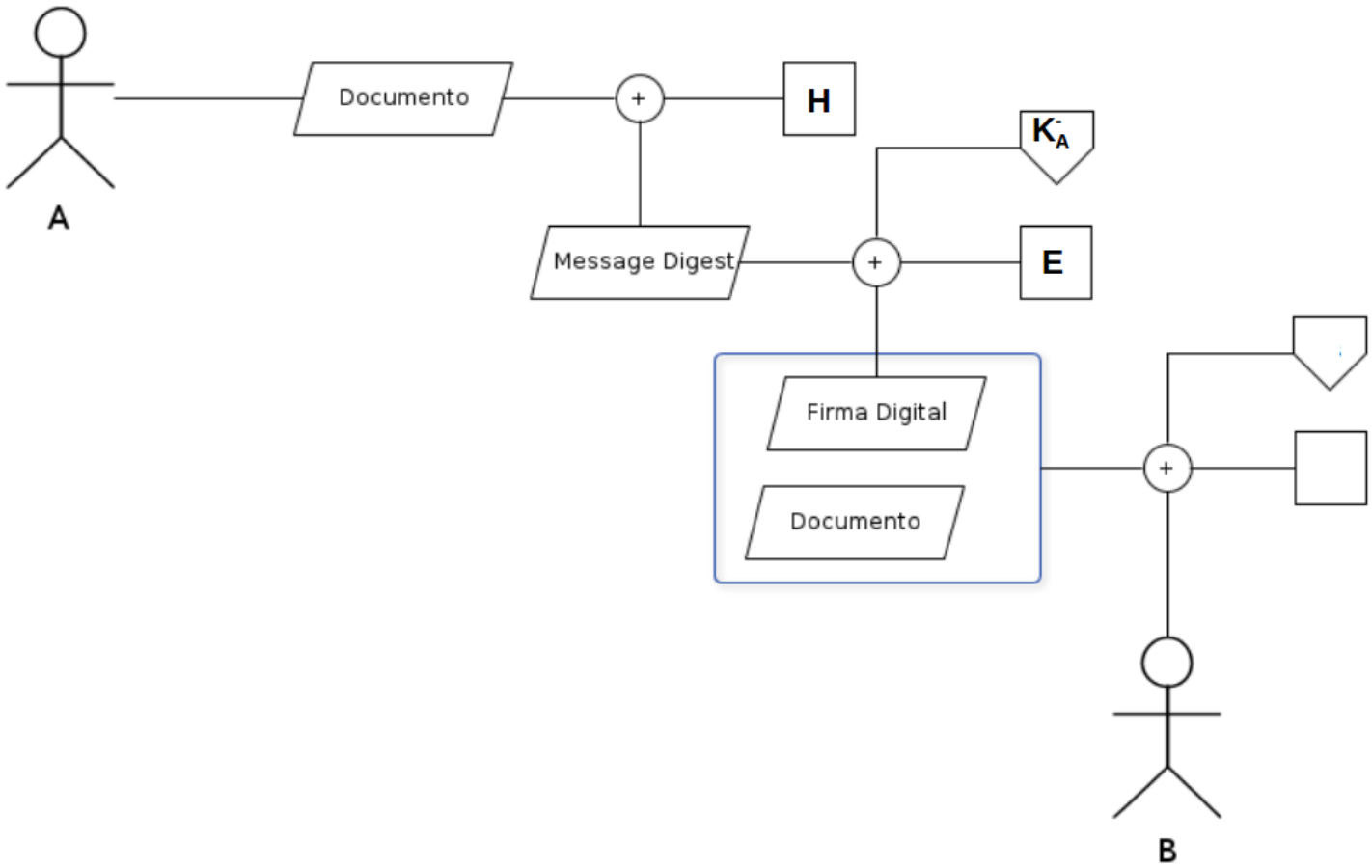
Ejercicio 1.

a. Ideas???



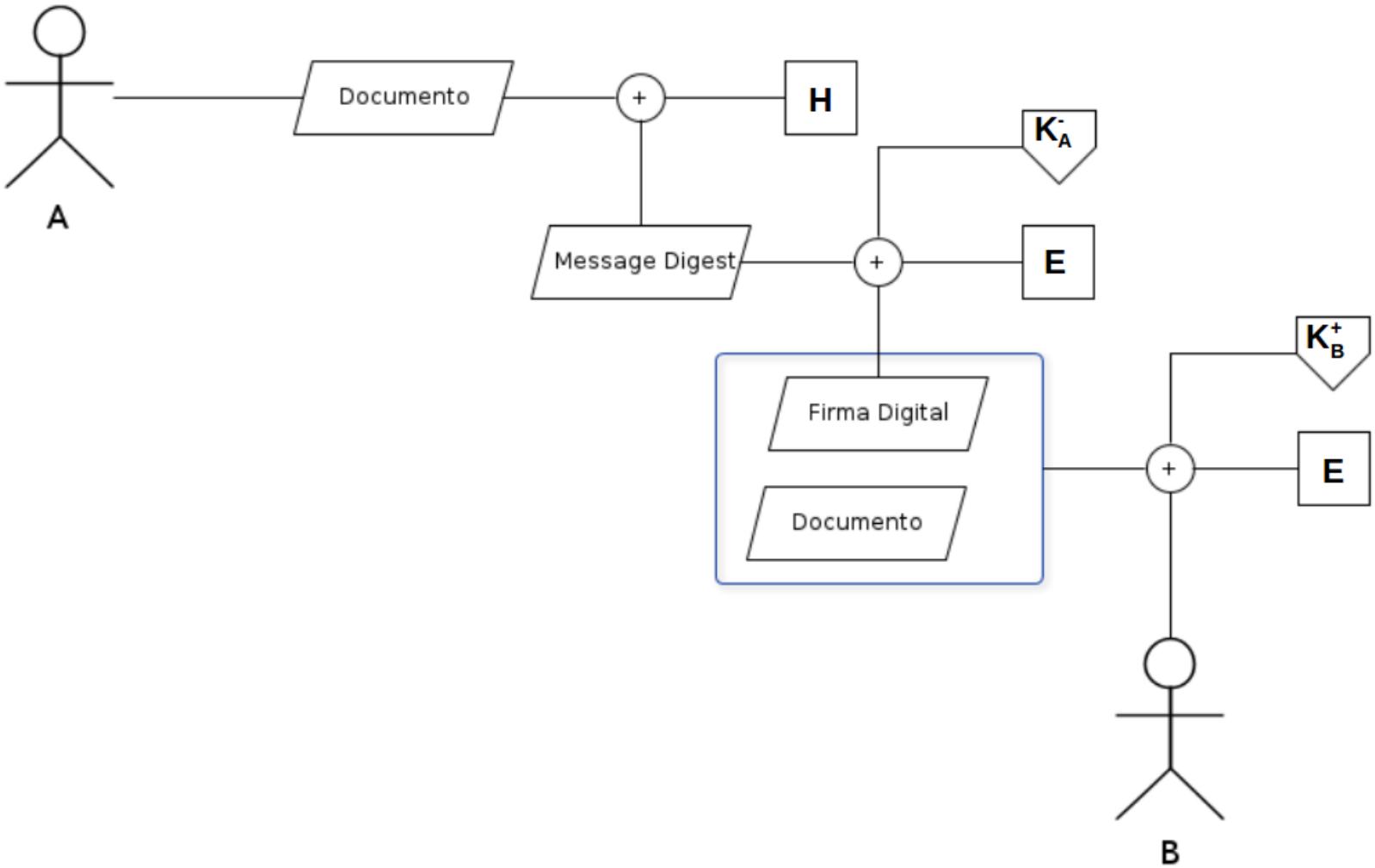
Ejercicio 1.

a. Sencillo de completar el hash del mensaje y la firma digital que nos garantiza **No repudio**!! Cómo podemos garantizar la **confidencialidad** del mensaje??



Ejercicio 1.

a.



Ejercicio 1.

b. Explique qué debe hacer B para verificar que A fue quién envió el mensaje.

Dado el criptograma C que recibe B, se **desencripta con su clave privada** K_B^-, obteniendo $D_{K_B^-}(C) = M + F$, dónde M es el documento original que envía A, y F, la firma digital. Como B es el único capaz de desencriptar el mensaje cifrado C con su clave privada, queda **garantizada la Confidencialidad**.

Ejercicio 1.

b. Explique qué debe hacer B para verificar que A fue quién envió el mensaje.

Dado el criptograma C que recibe B, se **desencripta con su clave privada** K_B^-, obteniendo $D_{K_B^-}(C) = M + F$, dónde M es el documento original que envía A, y F, la firma digital. Como B es el único capaz de desencriptar el mensaje cifrado C con su clave privada, queda **garantizada la Confidencialidad**.

Luego, para verificar la firma, B debe **desencriptar la firma usando la clave pública de A** (K_A^+) y comparar aplicando la misma función de Hash al documento: $D_{K_A^+}(F) == H(M)$, y así queda **garantizado el No repudio** de A sobre el mensaje enviado.

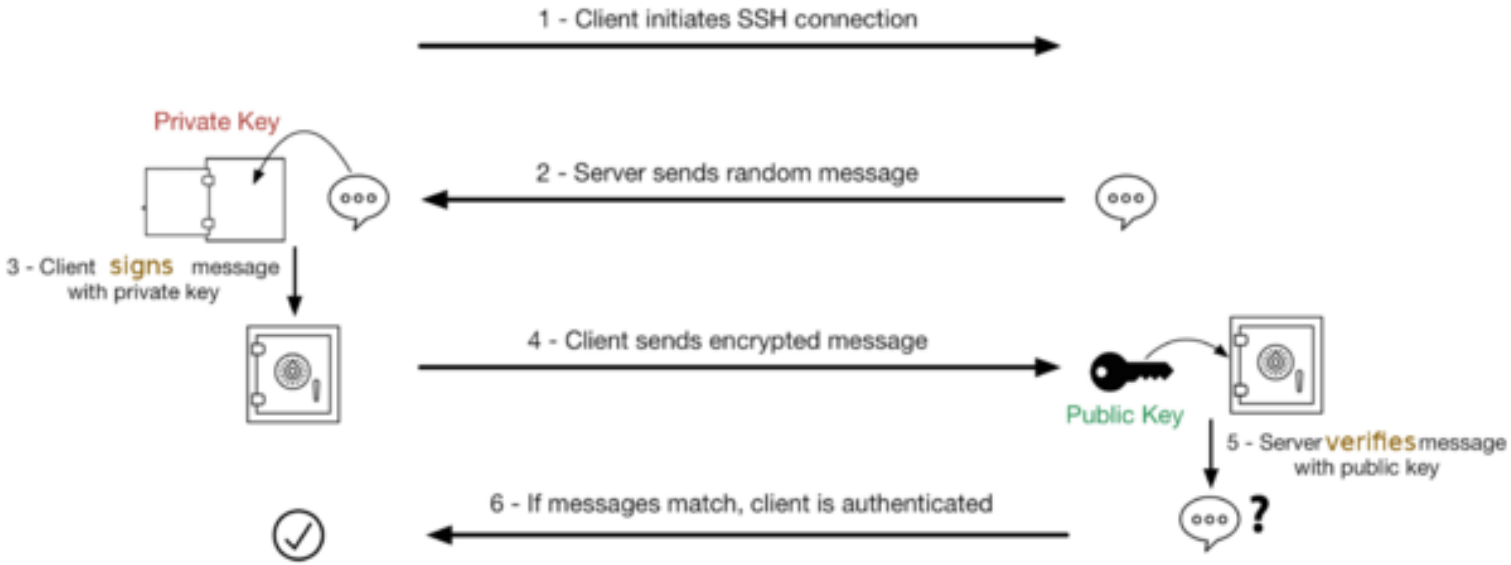
Ejercicio 2.

Suponga que una compañía necesita implementar un sistema que garantice la autenticidad de sus clientes usando un sólo servicio instalado en un servidor.

a. Se sabe que ssh admite autenticación por clave pública y privada mediante el método de challenge-response. Explique dónde y cuántas claves públicas y privadas deberían instalarse para que se pueda garantizar la autenticidad de los clientes usando ssh.
b. Suponga ahora que los clientes necesitan garantizar la autenticidad del servidor de la compañía, ¿Dónde deberían instalarse las claves públicas y privadas?

Ejercicio 2.

a. Ideas???



Ejercicio 2.

Respuestas

a. Para que se pueda garantizar la autenticidad de N clientes $(C_i, 1 \leq i \leq N)$, cada uno de ellos debe generar un par de claves pública y privada $(K_{C_i}^+, K_{C_i}^-)$. Luego, deben instalarse las N claves públicas $K_{C_i}^+$ en el servidor asociandose a cada uno de los clientes.

Ejercicio 2.

Respuestas

a. Para que se pueda garantizar la autenticidad de N clientes $(C_i, 1 \leq i \leq N)$, cada uno de ellos debe generar un par de claves pública y privada $(K^+_{C_i}, K^-_{C_i})$. Luego, deben instalarse las N claves públicas $K^+_{C_i}$ en el servidor asociandose a cada uno de los clientes.

b. Para garantizar la autenticidad del servidor, éste debe generar un par de claves pública y privada (K^+_S, K^-_S) y, luego, debe instalarse K^+_S en cada cliente.

Ejercicio 2.

DEMO SSH

Consideraciones

1. La máxima seguridad se logra de extremo a extremo. Hemos visto ejemplos que funcionan en la capa de aplicación
2. Sin embargo, podemos implementar mecanismos de seguridad en otras capas

Consideraciones

1. La máxima seguridad se logra de extremo a extremo. Hemos visto ejemplos que funcionan en la capa de aplicación
2. Sin embargo, podemos implementar mecanismos de seguridad en otras capas
3. Sobre la capa de transporte tenemos SSL/TLS o Seguridad de la Capa de Transporte
4. SSL fue el primer protocolo que se implementó.

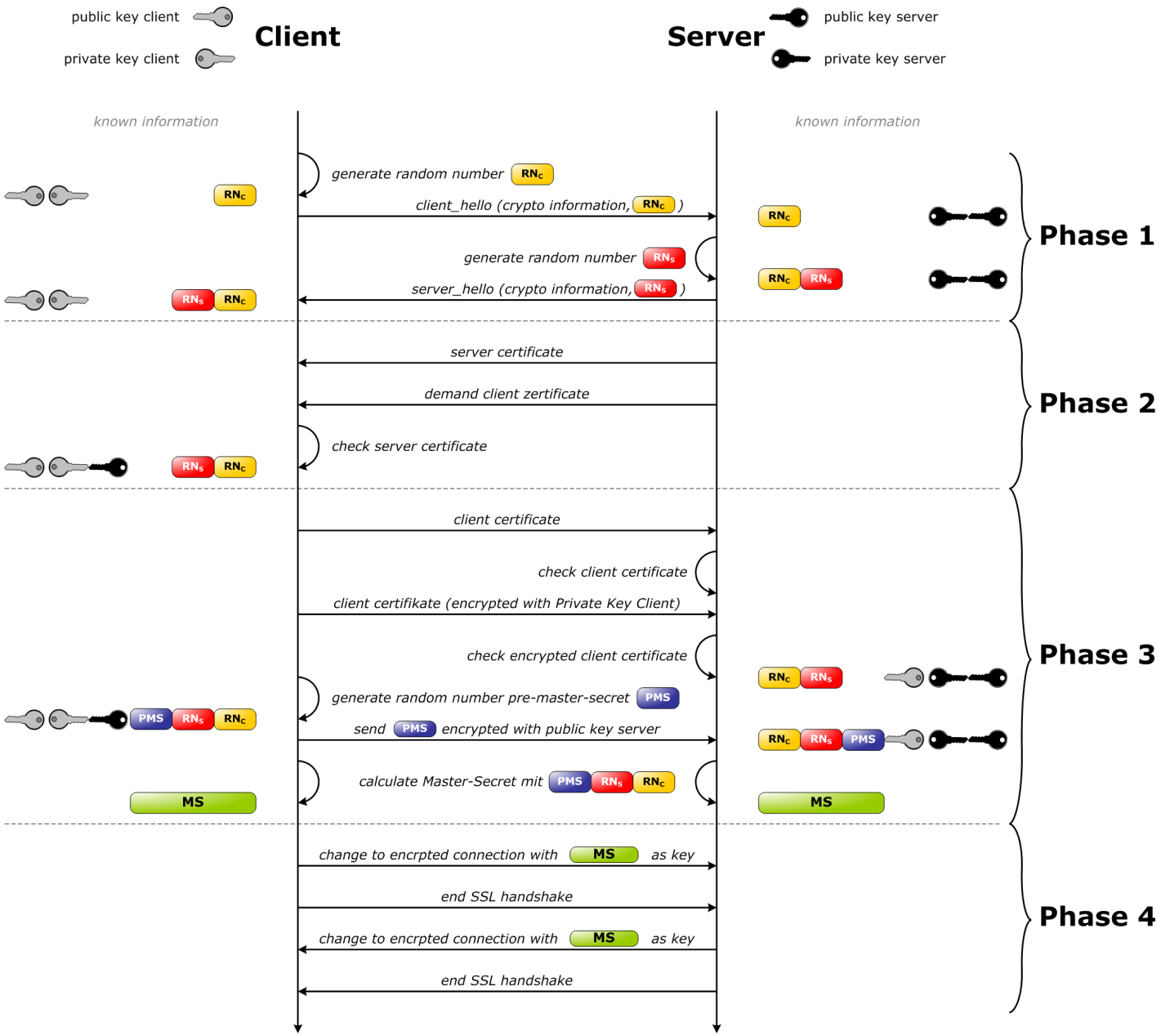
Consideraciones

1. La máxima seguridad se logra de extremo a extremo. Hemos visto ejemplos que funcionan en la capa de aplicación
2. Sin embargo, podemos implementar mecanismos de seguridad en otras capas
3. Sobre la capa de transporte tenemos SSL/TLS o Seguridad de la Capa de Transporte
4. SSL fue el primer protocolo que se implementó.
5. SSL está formado de dos subprotocolos, uno para establecer una conexión segura y otro para utilizarla
6. TLS fue el sucesor de SSL versión 1.3 , al que se le introdujeron mejoras, que de todas maneras no permiten la interoperación

Consideraciones

1. La máxima seguridad se logra de extremo a extremo. Hemos visto ejemplos que funcionan en la capa de aplicación
2. Sin embargo, podemos implementar mecanismos de seguridad en otras capas
3. Sobre la capa de transporte tenemos SSL/TLS o Seguridad de la Capa de Transporte
4. SSL fue el primer protocolo que se implementó.
5. SSL está formado de dos subprotocolos, uno para establecer una conexión segura y otro para utilizarla
6. TLS fue el sucesor de SSL versión 1.3 , al que se le introdujeron mejoras, que de todas maneras no permiten la interoperación
7. Debido a esta incompatibilidad, la mayoría de los navegadores implementan ambos protocolos, en donde TLS recurre a SSL durante la negociación si es necesario. A esto se le conoce como SSL/TLS

SSL handshake



Pasos

1. Se negocian los algoritmos a utilizar durante la conexión
2. Se **autentica** al servidor y/o cliente (opcional). Se utilizan **certificados digitales**

Pasos

1. Se negocian los algoritmos a utilizar durante la conexión
2. Se **autentica** al servidor y/o cliente (opcional). Se utilizan **certificados digitales**
3. El cliente genera pre-master key, que se envía al servidor **encriptada con la llave pública del servidor** (criptografía asimétrica - garantiza confidencialidad)
4. Se genera una clave maestra, de manera independiente en el cliente y el servidor, a partir de la pre-master key y los nonces intercambiados en la etapa inicial de negociación

Pasos

1. Se negocian los algoritmos a utilizar durante la conexión
2. Se **autentica** al servidor y/o cliente (opcional). Se utilizan **certificados digitales**
3. El cliente genera pre-master key, que se envía al servidor **encriptada con la llave pública del servidor** (criptografía asimétrica - garantiza confidencialidad)
4. Se genera una clave maestra, de manera independiente en el cliente y el servidor, a partir de la pre-master key y los nonces intercambiados en la etapa inicial de negociación
5. Una vez que termina el handshake SSL la comunicación se realiza encriptada generando **claves simétrica** para la sesión ¿Por qué?

Pasos

1. Se negocian los algoritmos a utilizar durante la conexión
2. Se **autentica** al servidor y/o cliente (opcional). Se utilizan **certificados digitales**
3. El cliente genera pre-master key, que se envía al servidor **encriptada con la llave pública del servidor** (criptografía asimétrica - garantiza confidencialidad)
4. Se genera una clave maestra, de manera independiente en el cliente y el servidor, a partir de la pre-master key y los nonces intercambiados en la etapa inicial de negociación
5. Una vez que termina el handshake SSL la comunicación se realiza encriptada generando **claves simétrica** para la sesión ¿Por qué?

Orientado a conexión

Ejercicio 2. SSL/TLS

Suponga que una compañía necesita implementar un sistema que garantice la autenticidad de sus clientes usando un sólo servicio instalado en un servidor.

c. También se puede garantizar autenticidad estableciendo una conexión SSL/TLS que usa un handshake seguro intercambiando certificados digitales. Explique cómo cambian la soluciones de los incisos **a.** y **b.**

Ejercicio de parcial

1. La Universidad dispone de un servidor Web que se expone a Internet para la consulta de sus estudiantes. Se necesita garantizar la autenticidad del servidor Web desde cualquier equipo que se intente conectar desde Internet. Para eso dispone de un certificado digital firmado por una Autoridad Certificante.
    a. Explique donde debería instalarse este certificado, en que momento y cómo se hace la validación del mismo.

Ejercicio de parcial

1. Una compañía desea implementar un sistema criptográfico de clave asimétrica para controlar el acceso de sus empleados mediante una aplicación móvil.
   a. Diseñe un sistema que verifique la autenticidad de los empleados, indicando dónde deben instalarse los certificados digitales.
   b. Suponga que la empresa dispone de un certificado digital firmado por una Autoridad Certificante. Describa cómo se validaría la autenticidad de los empleados en este caso y que certificados deben instalarse en este caso.

Ejercicio de parcial

1. Explique cómo se podría hacer para garantizar la integridad y autenticidad de las respuestas de un servidor DNS.