Seguridad y criptografía

Jorge Juan Chico <jjchico@dte.us.es>, Julián Viejo Cortés <julian@dte.us.es>. 2011-2020
Departamento de Tecnología Electrónica
Universidad de Sevilla

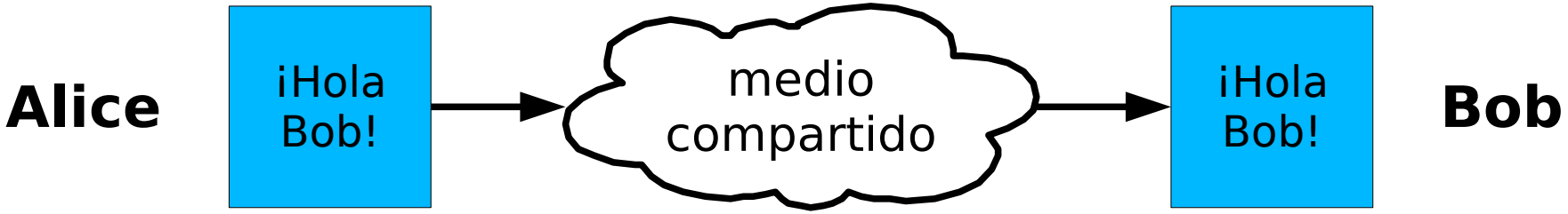
Objetivos

- Comprender los procedimientos básico que permiten establecer comunicaciones seguras entre usuarios y sistemas informáticos
- Conocer y saber utilizar diferentes elementos de seguridad: claves privadas y públicas, certificados digitales
- Conocer la situación legal de los sistemas de firma digital en nuestro entorno
- Valorar la importancia de los sistemas de comunicación segura en la sociedad actual

Contenidos

- Objetivos de la seguridad
- Cifrado simétrico
- Cifrado asimétrico y firma digital
- Algoritmos de hash
- Certificados digitales y gestión de claves

Objetivos de la seguridad en las comunicaciones informáticas



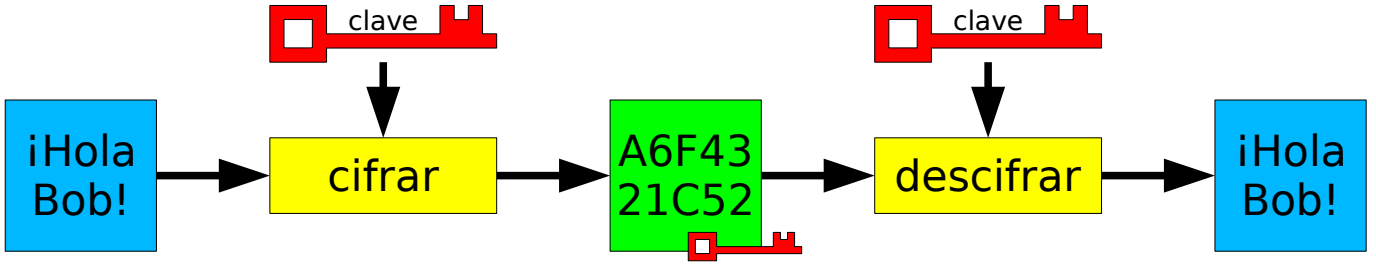
- Confidencialidad
  - Asegurar que sólo Bob recibe el mensaje
  - El mensaje resulta ininteligible para un espía que lo capture en tránsito
- Autenticidad
  - Asegurar a Bob que el mensaje recibido proviene de Alice
  - Un espía no puede falsificar un mensaje y hacer que parezca que viene de Alice
- Integridad
  - Asegurar que Bob recibe el mensaje íntegro y sin modificaciones
  - Un espía no puede alterar el mensaje en tránsito

Criptografía

Problemas a resolver

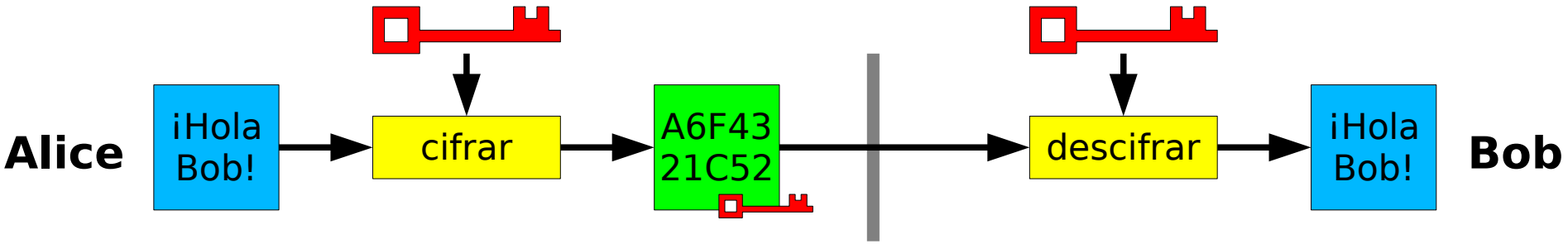
- Confidencialidad
- Integridad
- Autenticidad

Cifrado simétrico



- Cifrado
  - procedimiento que convierte un mensaje comprensible en otro incomprensible
  - el mensaje original puede recuperarse fácilmente si se conoce el algoritmo de cifrado y la “clave” empleada para su cifrado
- Propiedades
  - obtener el mensaje original a partir del mensaje cifrado es extremadamente difícil si no se conoce la clave, aunque se conozca el algoritmo de cifrado
  - las operaciones de cifrado y descifrado son muy eficientes
- Algoritmos: AES, Blowfish, DES, Triple DES, ...

Cifrado simétrico

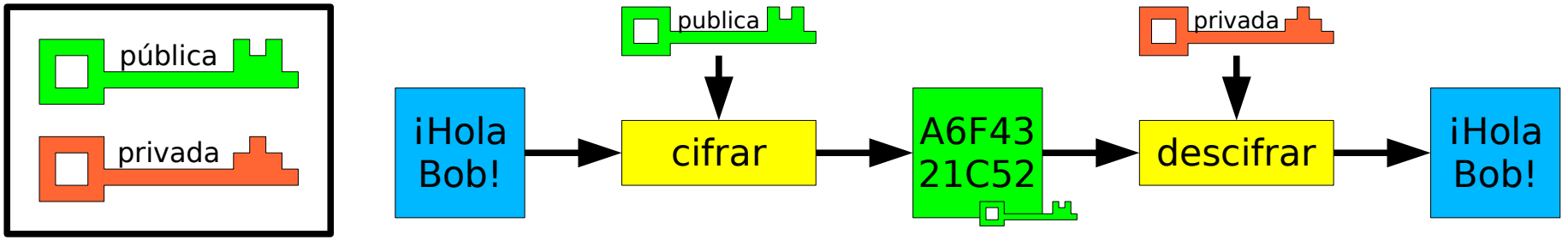


- Procedimiento
  - Alice cifra el mensaje con un algoritmo dado y una clave compartida con Bob (secreto compartido)
  - El mensaje cifrado es incomprensible para un posible espía
  - Bob descifra el mensaje fácilmente con el mismo algoritmo y la clave original
- Cualquier cambio en el mensaje cifrado produciría errores al descifrar y sería detectado (INTEGRIDAD)
- Bob sabe que el mensaje proviene de Alice sólo si únicamente Alice comparte la clave (AUTENTICIDAD)

Problemas pendientes

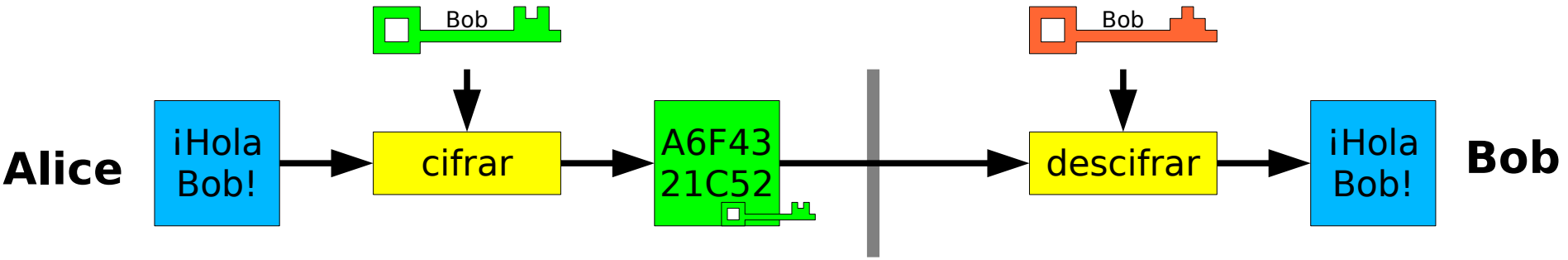
- ~~Confidencialidad~~
- ~~Integridad~~
  - depende del algoritmo
- ~~Autenticidad~~
- + Distribución de la clave
  - Es necesario la existencia de un canal seguro previo para compartir la clave. A veces esto es muy difícil o incluso imposible
  - Si un tercero averigua la clave, puede descifrar todos los mensajes enviados por Alice
  - Si varios actores usan la misma clave, Bob no puede saber de cual de ellos proviene el mensaje

Cifrado asimétrico



- Emplea una pareja de claves (pública y privada)
- Un mensaje cifrado con la clave pública se descifra fácilmente con la clave privada (y viceversa)
- Descifrar el mensaje sin la clave privada es extremadamente difícil
- La clave privada no puede deducirse de la clave pública

Cifrado asimétrico: confidencialidad

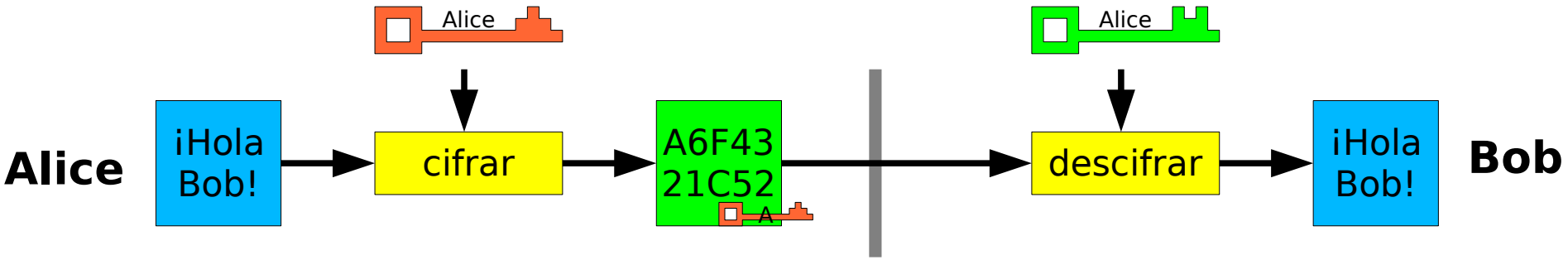


- Procedimiento
  - Bob genera una pareja de claves, hace accesible su clave pública y conserva en secreto su clave privada
  - Alice emplea la clave pública de Bop para cifrar el mensaje. Sólo la clave privada de Bob puede descifrar el mensaje cifrado (CONFIDENCIALIDAD)
  - Bob descifra el mensaje fácilmente con su clave privada
- Cualquier cambio en el mensaje cifrado produciría errores al descifrar y sería detectado (INTEGRIDAD)

Cifrado asimétrico: confidencialidad

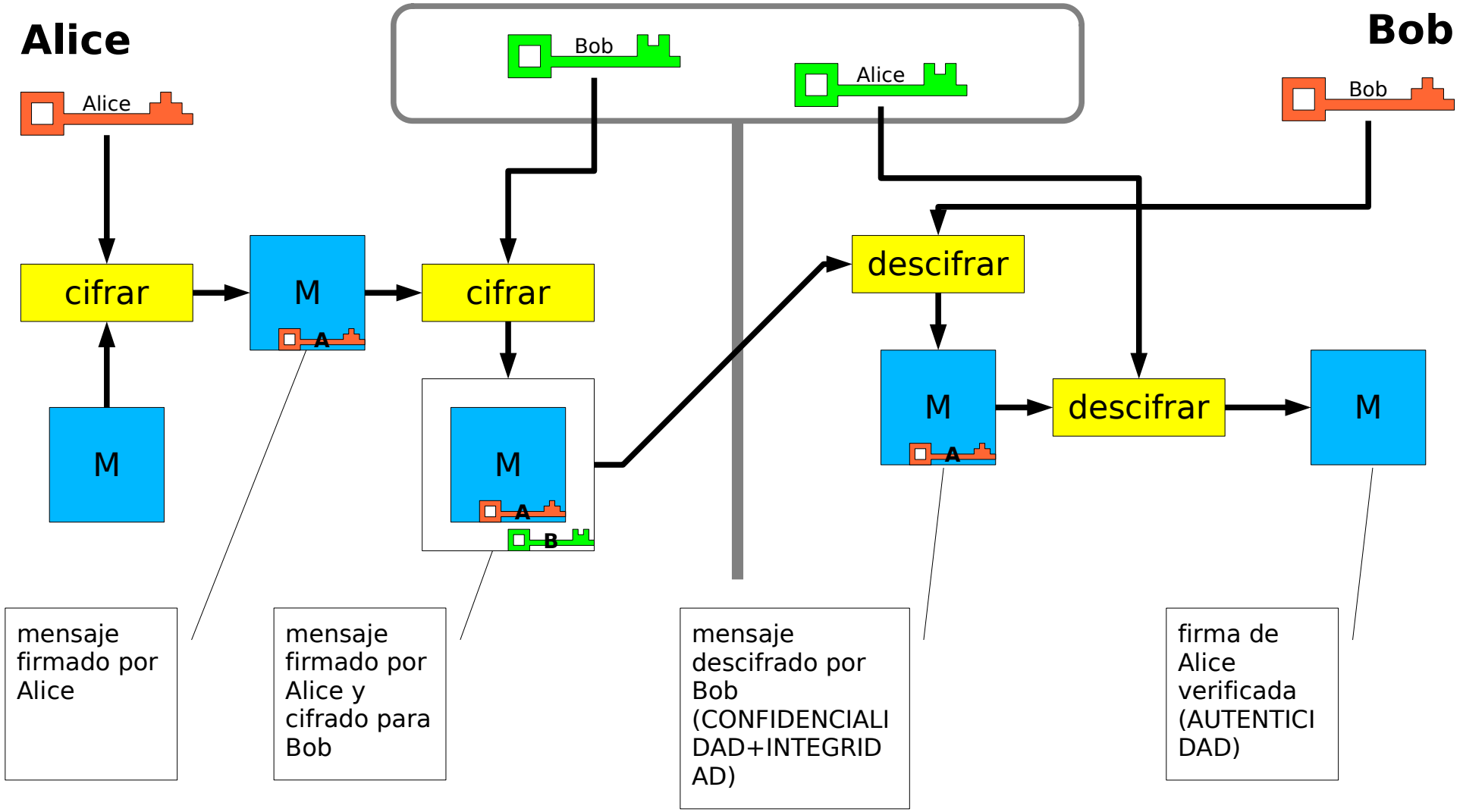
- Ventajas
  - Facilidad en la distribución de claves
    - no hay un “secreto compartido”
    - la clave pública puede distribuirse por un canal inseguro
  - Si un tercero averigua la clave privada de Bop, sólo los mensajes enviados a Bob se ven comprometidos
  - Proporciona un mecanismo de autenticación mejor que el derivado del uso de claves compartidas
    - Firma digital
- Algoritmos
  - RSA
  - DSA
  - ElGamal
  - ...

Cifrado asimétrico: autenticidad (Firma digital)



- Procedimiento
  - Alice emplea su clave privada para cifrar el mensaje
  - Cualquiera puede descifrar el mensaje empleando la clave pública de Alice:
    - Esto constituye una prueba de la autenticidad del emisor ya que sólo el poseedor de la clave privada (Alice) ha podido generar el mensaje
  - La firma digital NO proporciona CONFIDENCIALIDAD
- La firma digital puede (y suele) combinarse con el cifrado (con la clave pública del destinatario) para obtener CONFIDENCIALIDAD e INTEGRIDAD

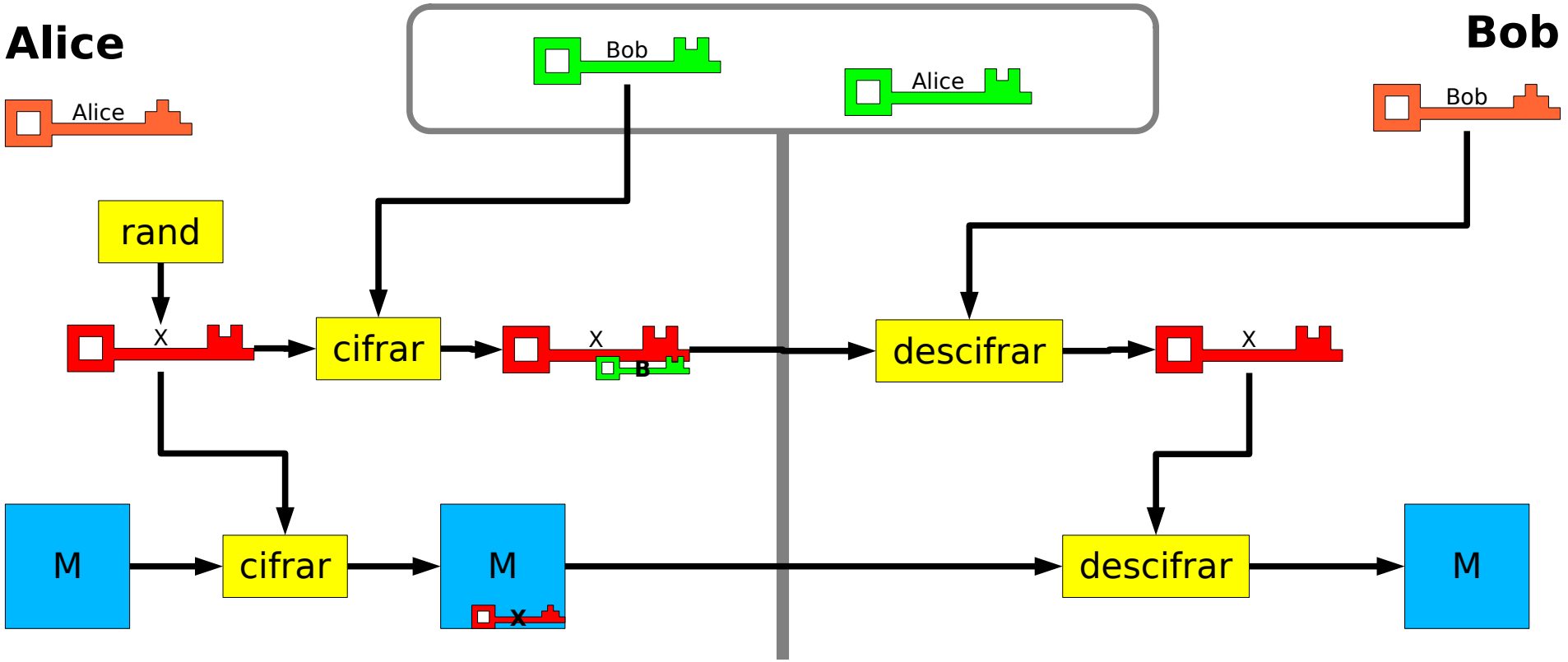
Cifrado asimétrico. Firma y cifrado



Problemas pendientes

- ~~Confidencialidad~~
- ~~Integridad~~
- ~~Autenticidad~~
- ~~Distribución de la clave~~
- + Coste computacional
  - Tiempo de cifrado/descifrado (x1000 respecto simétrico)
  - Tamaño del mensaje cifrado (x2 respecto mensaje original)
  - Cifrado para múltiples destinatarios
- + Gestión de claves
  - Autenticidad de claves públicas
  - Revocación de claves comprometidas

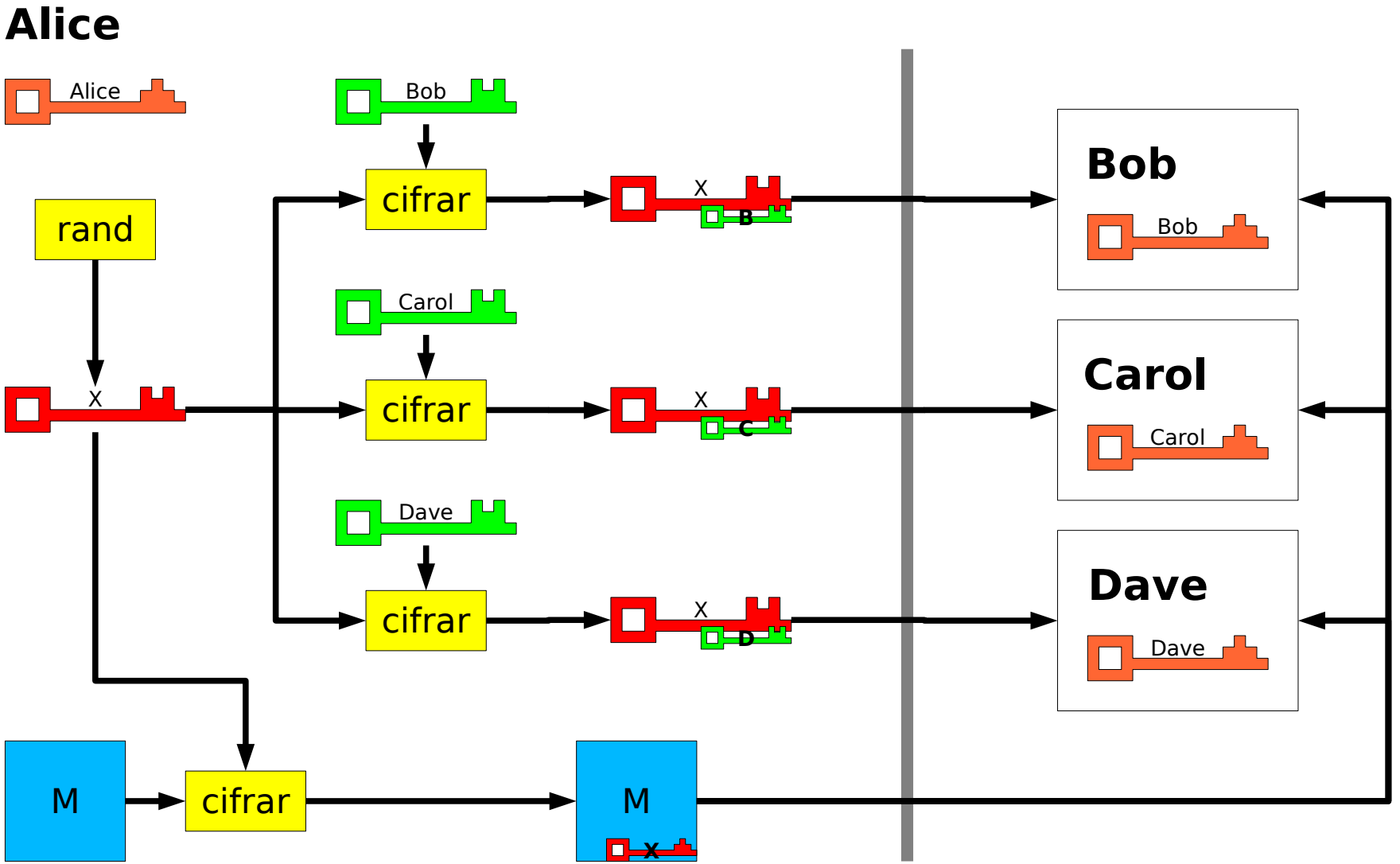
Cifrado híbrido



Cifrado híbrido

- Procedimiento
  - Alice genera una clave simétrica (X) para la sesión
  - Alice envía el mensaje cifrado con X, junto con X cifrado con la clave pública de Bob
  - Bob descifra la clave de sesión X y puede descifrar el mensaje
  - Sólo Bob puede descifrar el mensaje porque sólo Bob puede descifrar X
  - El algoritmo asimétrico se emplea únicamente para cifrar la clave X, que es mucho más pequeña que el mensaje completo
  - El mensaje se cifra con un algoritmo simétrico que es 1000 veces más rápido que el cifrado asimétrico, reduciendo el coste computacional
- Múltiples destinos
  - Se genera una clave de sesión cifrada para cada destino

Cifrado híbrido. Múltiples destinos



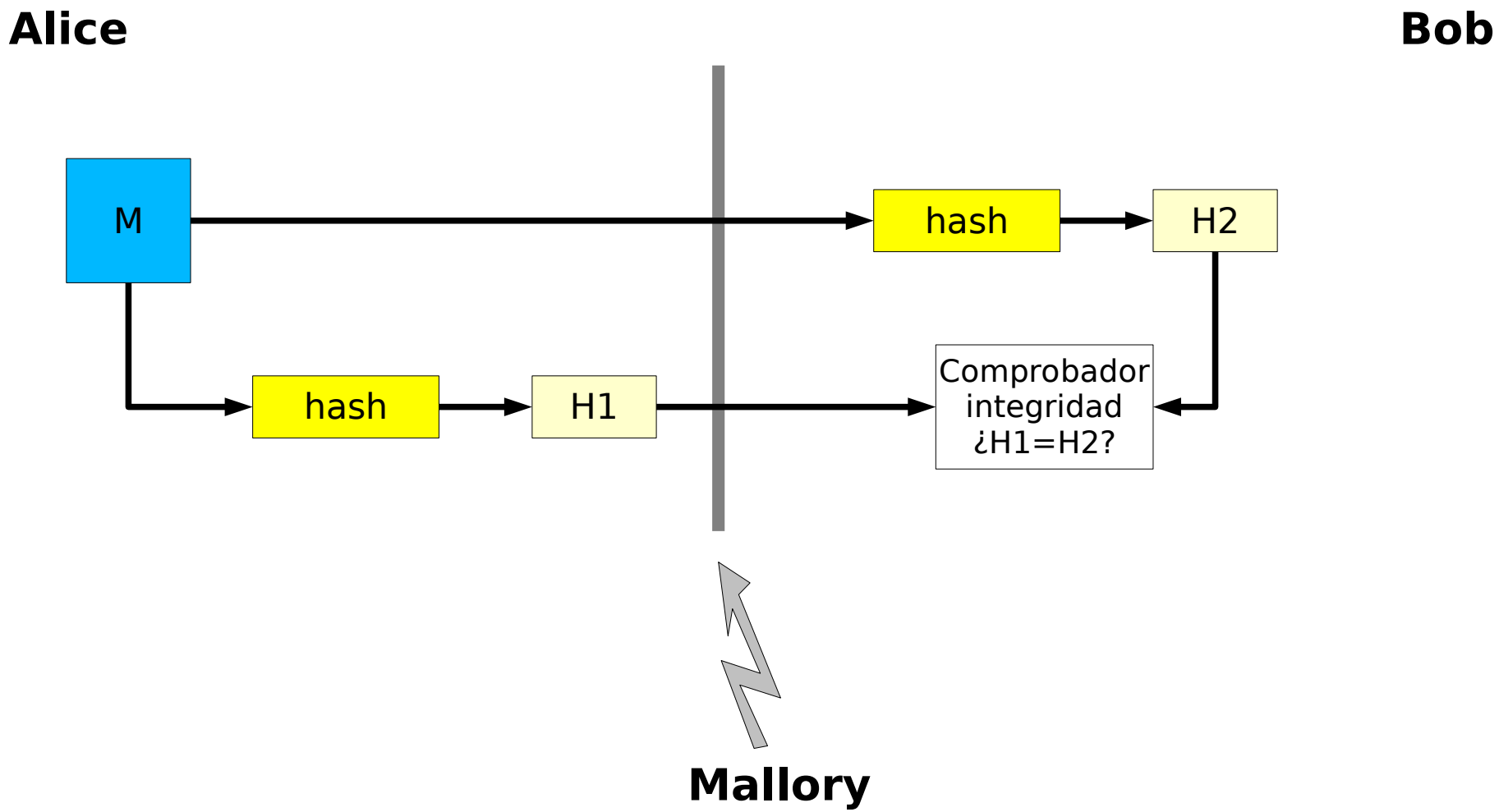
Problemas pendientes

- Hemos resuelto el problema de coste computacional para el cifrado de mensajes (confidencialidad)
- ¿Qué pasa con la firma digital (autenticidad)?
- ¿Cómo comprobamos la integridad del mensaje, incluso si no hacemos cifrado del mismo?
- Necesitamos más matemáticas...

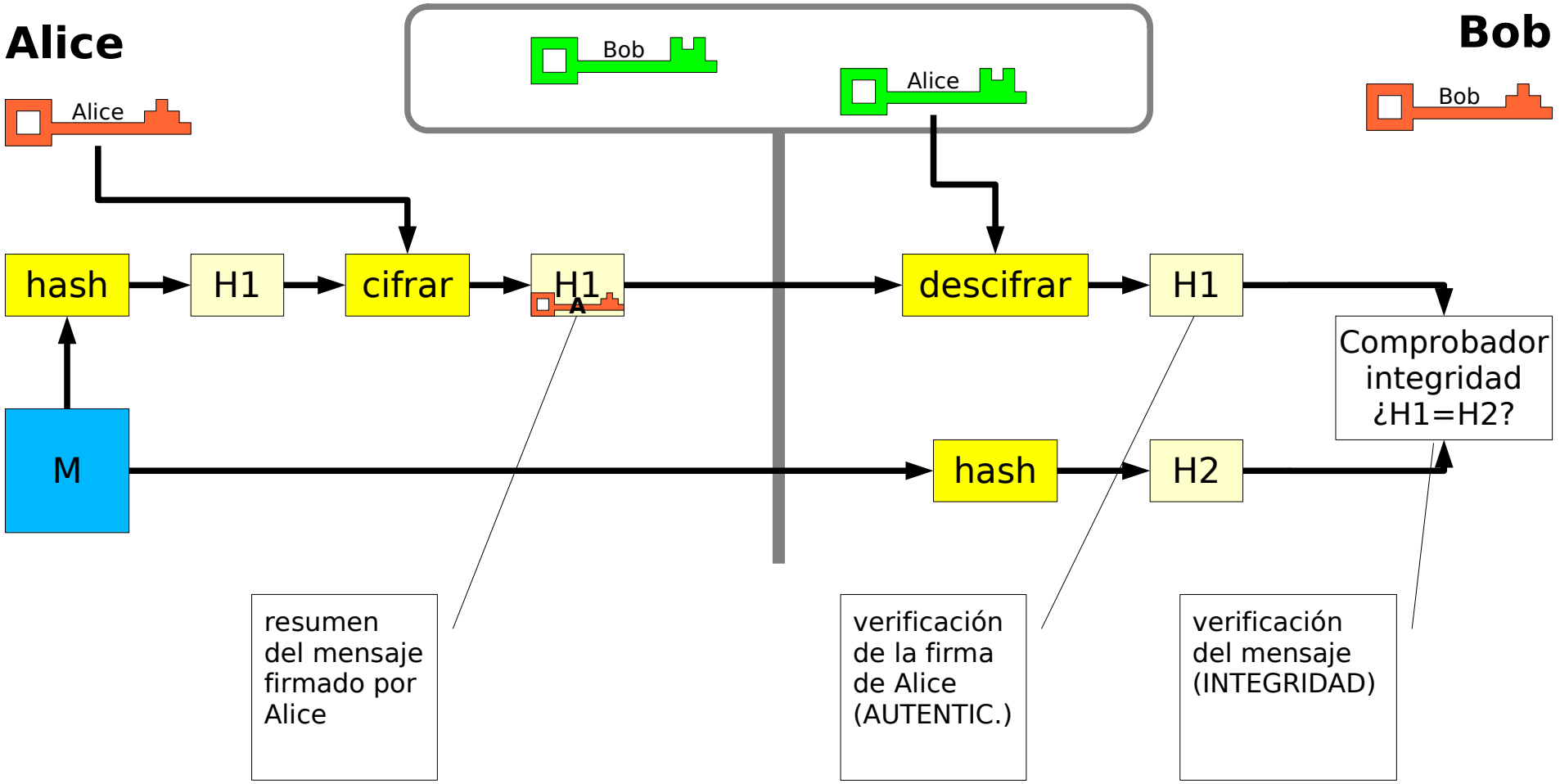
Algoritmos de resumen (*hash*)

- Algoritmo de *hash*
  - Procedimiento matemático por el que a partir de un mensaje dado se obtiene un código de tamaño fijo (resumen o *hash*) asociado a dicho mensaje
  - Ej: MD5, SHA1
- Propiedades
  - A partir del resumen es prácticamente imposible obtener datos sobre el contenido del mensaje
  - Es altamente improbable que dos mensajes diferentes generen el mismo resumen (es altamente probable que dos mensajes con el mismo resumen sean idénticos)
  - Cualquier cambio en el mensaje, por pequeño que sea, produce resúmenes completamente diferentes
- Aplicaciónes
  - Permiten verificar la integridad del mensaje sin tener que cifrarlo.
  - Permite comprobar la autenticidad del mensaje sin tener que aplicar la firma al mensaje completo.

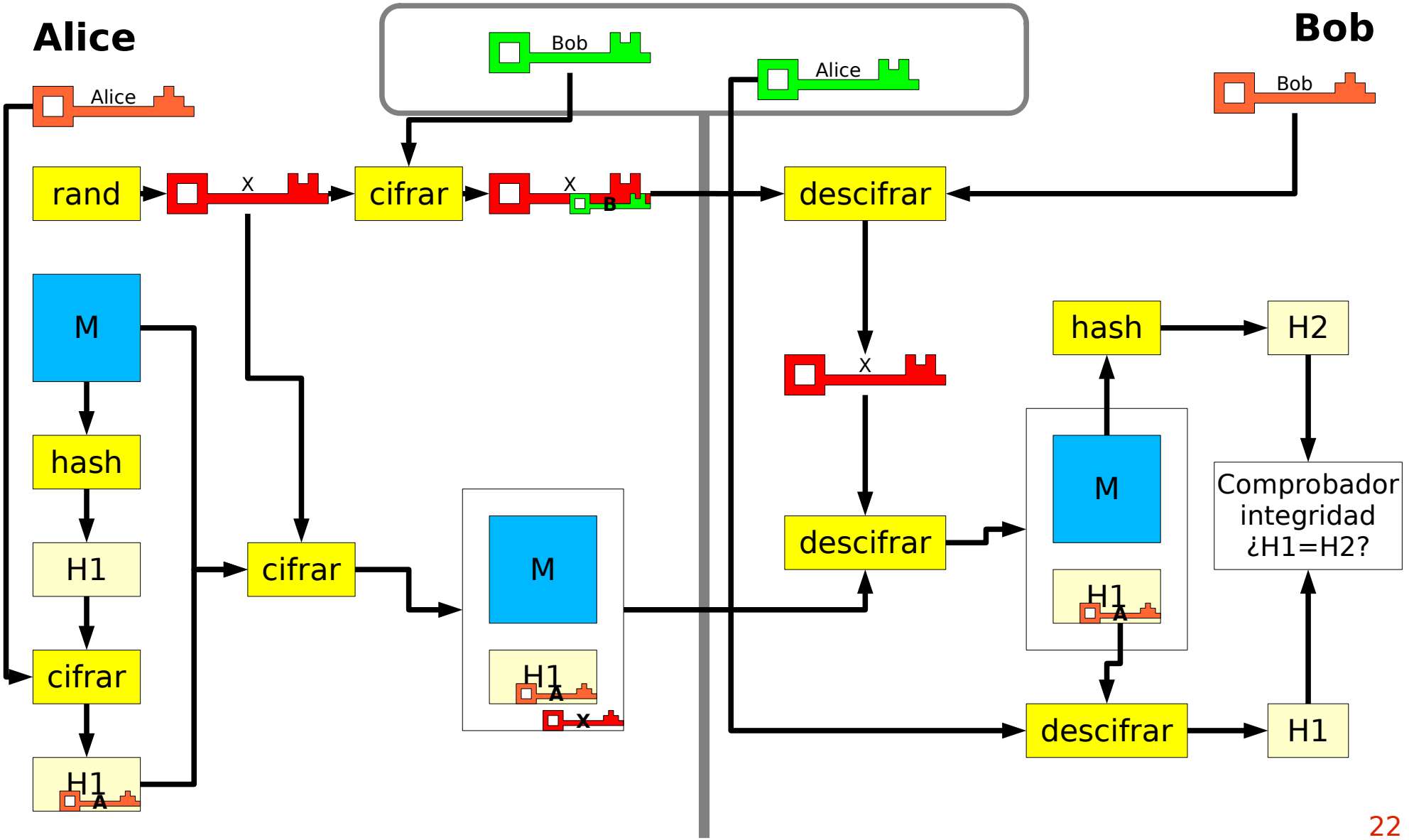
Algoritmos de *hash*. Integridad



Firma digital con *hash*



Cifrado híbrido y firma con hash



Problemas pendientes: gestión de claves

- ~~Confidencialidad~~
  - Clave simétrica de validez para una única sesión
- ~~Integridad~~
  - Generación de resumen (*hash*) y comprobación en el receptor
- ~~Autenticidad~~
  - Firma digital del resumen del mensaje
- ~~Distribución de la clave~~
  - Sólo hay que distribuir claves públicas no secretas
- ~~Coste computacional~~
  - Cifrado asimétrico solo para clave de sesión y resumen
- Gestión de claves
  - Autenticidad de claves públicas
  - Revocación de claves comprometidas

Gestión de claves
Distribución de claves públicas

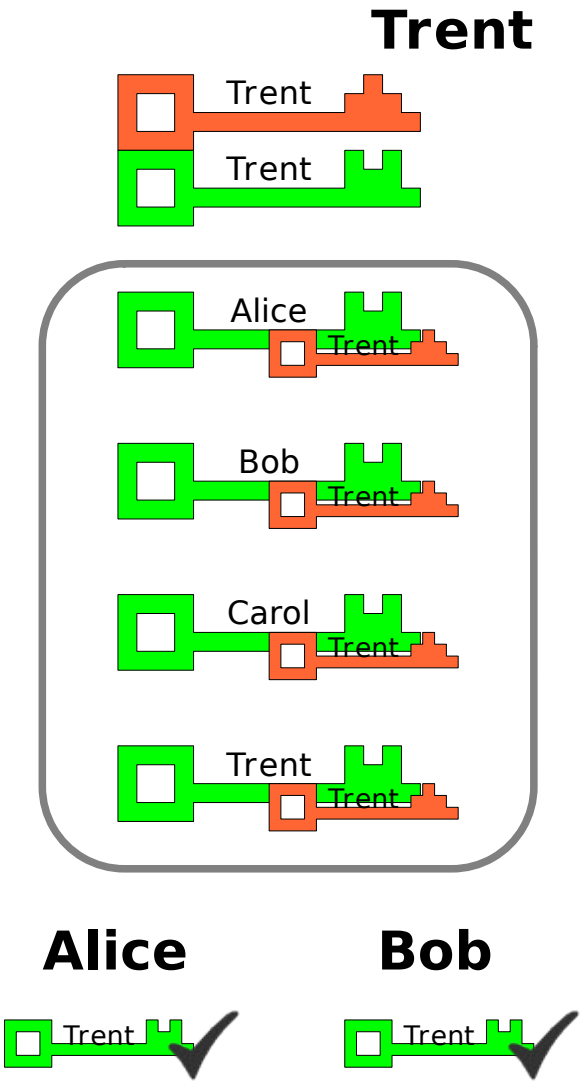
- No es un problema ya que puede usarse cualquier medio público
- Es necesario establecer mecanismos estandarizados para facilitar el uso de sistemas de cifrado
- Algunas opciones
  - Envío de la clave pública por cualquier canal, seguro o no
  - Publicación en la web
  - Publicación en servidores públicos de claves
  - Incluir clave pública con los mensajes
  - Etc.

Gestión de claves
Autenticidad de la clave pública

- Todo el sistema depende de que se pueda verificar que una clave pública pertenece a quien dice ser
- Opción 1: entrega personal de claves (poco adecuado, ineficiente)
- Opción 2: firma de claves públicas por un tercero de confianza
  - Alice y Bob conocen la clave pública de Trent y saben que es correcta
  - Alice y Bob confían en Trent para verificar la autenticidad de otras claves públicas
  - Trent firma digitalmente las claves públicas una vez que ha verificado la identidad del interlocutor
  - Alice y Bop aceptan como válida (auténtica) cualquier clave pública firmada por Trent

Firma de claves públicas

- Centralizado (jerárquico): autoridad de certificación (CA)
  - Permite confiar en todas las claves firmadas por un tercero
  - A menudo el tercero es quien expide las claves
  - Ej: estándar X.509
- Distribuido: red de confianza
  - Cada clave pública acumula la firma de terceros
  - Cualquiera puede firmar claves
  - El usuario establece la confianza en las claves y en los firmantes
  - Ej: OpenPGP



Certificados digitales

- Certificado digital
  - Unidad de información que contiene una pareja de claves pública y privada junto con la información necesaria para capacitar a su propietario (persona, equipo informático, etc.) a realizar operaciones de comunicación segura con otros interlocutores.
- Contenidos
  - Clave pública
  - Clave privada (sólo si es el propietario del certificado)
  - Datos del propietario: nombre, DNI, organización, ...
  - Datos sobre uso del certificado: algoritmos, funciones permitidas, ...
  - Periodo de validez: fecha inicial y final
  - Firmas de una o varias CA's o de

Certificados digitales
Almacenamiento

- Contenedor software: sistema informático que almacena la clave privada en un archivo informático convencional (disco duro, llave USB, etc.)
  - Habitualmente la clave se almacena cifrada y es necesaria una clave o frase de paso para descifrarla y poder usarla.
  - Si la clave cifrada es comprometida, su vulnerabilidad depende en gran medida de la frase de paso con que haya sido cifrada.
  - No se debe confiar en una clave comprometida, aunque estuviera cifrada.
- Tarjeta inteligente (smart-card): dispositivo *hardware* que contiene la clave privada y permite hacer operaciones de firma y descifrado con ella.
  - Las operaciones se hacen siempre dentro del dispositivo. La clave privada nunca se comunica al exterior.
  - La clave privada debe estar protegida con una frase de paso para mayor seguridad (robo de la tarjeta).

Revocación de certificados

- Si se descubre que una clave puede haber sido comprometida es necesario anularla
- Certificado de revocación: documento electrónico que informa de que una clave ha sido revocada. Contiene
  - Clave (pública) revocada
  - Firma del propietario de la clave
  - Firma de la autoridad certificadora (posiblemente)
  - Las autoridades de certificación suelen tener un servicio que informa sobre la lista de certificados revocados
- Periodo de validez
  - Toda clave tiene un periodo de validez tras el cual ya no puede ser utilizada
  - Evita que se utilicen claves antiguas cuya seguridad es dudosa

Problemas ~~pendientes~~

- ~~Confidencialidad~~
  - Clave simétrica de validez para una única sesión
- ~~Integridad~~
  - Generación de resumen (hash) y comprobación en el receptor
- ~~Autenticidad~~
  - Firma digital del resumen del mensaje
- ~~Coste computacional~~
  - Cifrado asimétrico solo para clave de sesión y resumen
- ~~Gestión de claves~~
  - Firma de claves públicas, listas de revocación y sistemas seguros de almacenamiento de claves

Seguridad y WWW

- La conexión segura se solicita usando el protocolo HTTPS, al puerto predeterminado 443.
- La comunicación segura se estable en base a un certificado digital instalado en el servidor, según estándar X.509.
- La autenticidad del servidor se establece mediante la firma de su certificado por una Autoridad de Certificación (CA).
- Los clientes (navegadores) incorporan certificados ya verificados de múltiples CA's, y pueden añadirse más.
- Los clientes (usuarios) pueden autenticarse mediante certificados personales instalados en el navegador.
  - Expedidos por alguna autoridad pública o privada.
  - Válidos en servidores que reconocen esta autoridad.
  - Ejemplos en España: certificados FNMT, DNI electrónico.

Seguridad y correo electrónico

- Se consigue mediante la firma/cifrado de extremo a extremo (en los MUA's de los usuarios).
- Existen varios estándares para el correo cifrado.
- S/MIME
  - Extensiones de correo incluyendo seguridad.
  - Emplea generalmente certificados X.509 (centralizado).
  - Soportado por la mayoría de clientes de correo.
  - Válido sólo en el ámbito de validez del certificado empleado.
- OpenPGP
  - Muchos clientes permiten el intercambio de correo seguro empleando el estándar OpenPGP (distribuido). Ej:
    - Thunderbird con extensión Enigmail (hasta la versión 68).
    - Thunderbird de forma nativa (desde la versión 78).
  - Válido globalmente, pero necesita mantenimiento de los certificados por parte de los usuarios.

Resumen

- Un certificado digital se compone de una pareja de claves
  - Clave privada: deber guardarse en secreto y protegerse
  - Clave pública: puede (y debe) publicarse y distribuirse
- Mediante certificados digitales se puede:
  - Firmar digitalmente mensajes y documentos
  - Enviar y recibir mensajes y documentos cifrados
  - Comprobar la autenticidad de un mensaje o documento
  - Acreditar la identidad propia ante un interlocutor
- Para enviar un mensaje cifrado a un destino necesito conocer su clave pública.
- La autenticidad de una clave pública se verifica si está firmada por alguien (ej: una autoridad de certificación) en quien confío.
- Los certificados que hayan podido ser comprometidos deben añadirse a una lista de revocación si no han caducado