Seguridad en Sistemas Informáticos

Seguridad del canal de comunicaciones

Criptografía

Área de Ingeniería Telemática
Dpto. Automática y Computación
http://www.tlm.unavarra.es/

En clases anteriores...

- La cadena de seguridad
  - Seguridad perimetral
- Sistemas de defensa
  - Firewalls, IDSs, honeypots...

Hoy

- Asegurando el canal de comunicación
  - Un poco de criptografia

Criptografía

- En ocasiones tenemos que enviar datos sensibles a través de redes o enlaces que no son de confianza

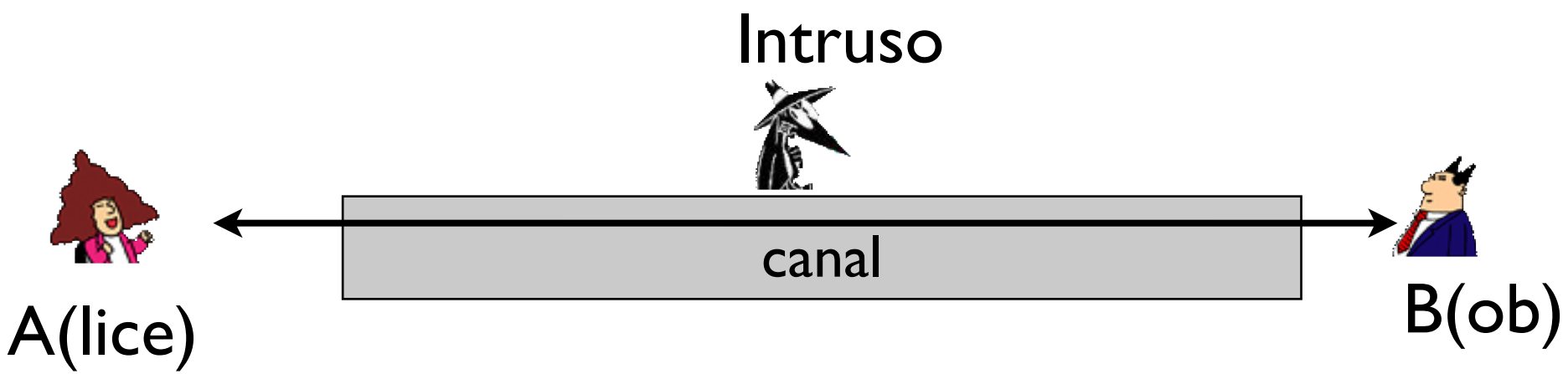
Propiedades a garantizar/problemas a resolver

- **Confidencialidad**
  - Solo emisor y receptor son capaces de entender el contenido del mensaje (encriptación)
- **Autentificación**
  - Ambos son capaces de confirmar la identidad del otro
- **Integridad y no repudio**
  - Verificar que el mensaje no se ha alterado
  - Probar que viene de quien dice
- **Disponibilidad y control de acceso**
  - Que la comunicación pueda tener lugar
  - Evitar accesos no autorizados y DoS

Criptografía: amigos y enemigos

- Usuarios A(Alice) y B(Bob)
  - Desean comunicarse de forma segura
  - Pueden ser
    - usuarios reales
    - navegador y servidor web
    - cliente y servidor de compras online
    - routers intercambiando información
    - servidores DNS
    - ...
- Intruso T(Trudy)
- ¿Qué puede hacer?
  - Ver mensajes
  - Insertar/modificar mensajes
  - Hacerse pasar por alguien
  - Evitar el uso del servicio

http://en.wikipedia.org/wiki/Alice_and_Bob



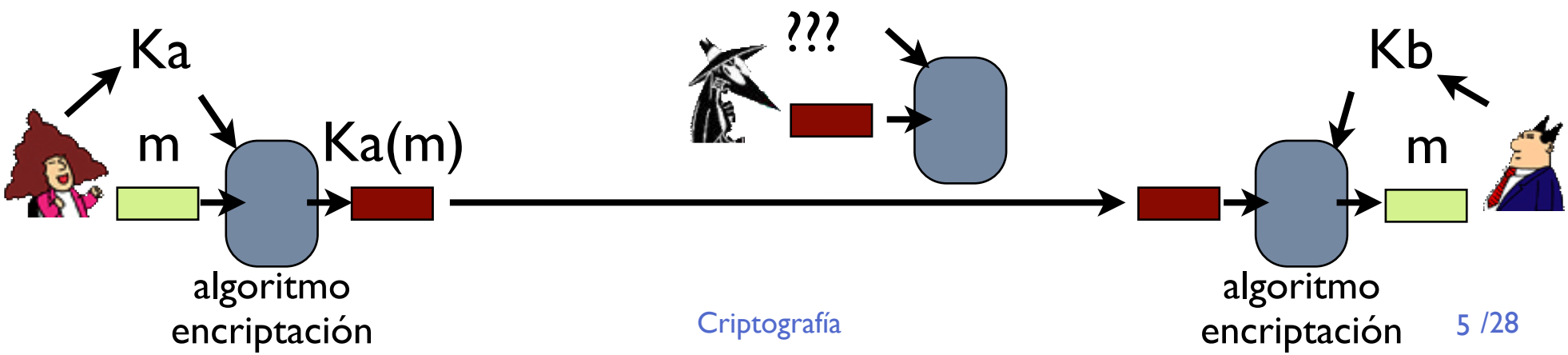
Criptografía: encriptación

- Algoritmos de encriptación

  Transforman un mensaje original m (plain text) en un nuevo mensaje cifrado. En el proceso se utiliza una clave.

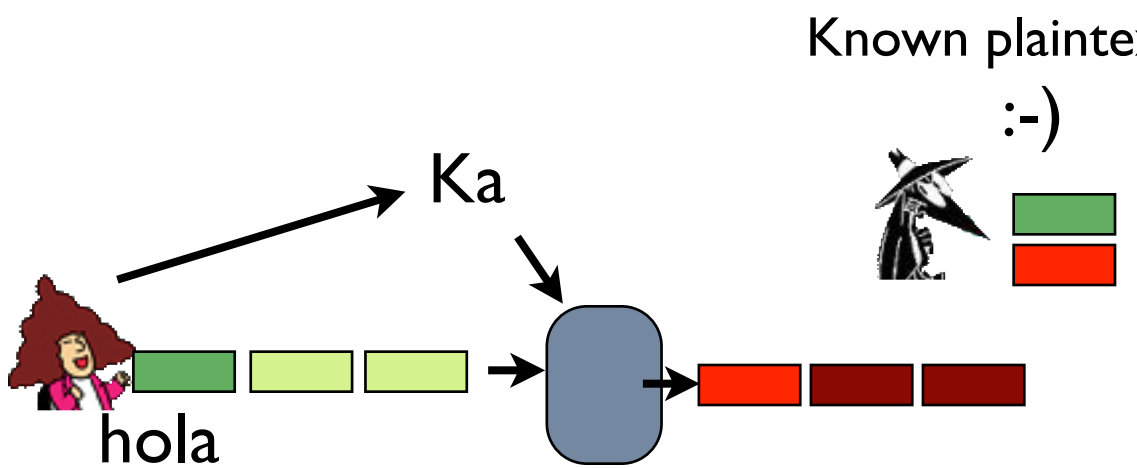
  - Utilizando un algoritmo asociado de desencriptación y la misma clave u otra asociada puedo reconstruir el texto original
  - El algoritmo de encriptación tiene que cumplir que el texto plano sea *dificil* de recuperar a partir del mensaje cifrado si no se conoce la clave

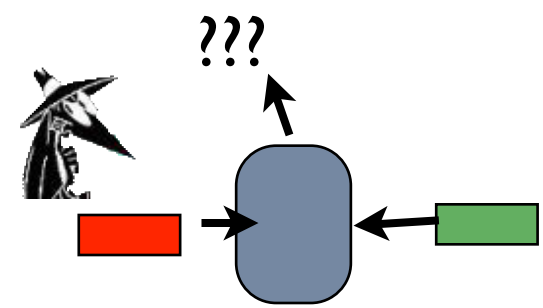
- Con esto podemos enviar el mensaje cifrado por el canal inseguro sin que sea descifrado por un observador que desconozca las claves



Criptografía: encriptación

- ¿Es suficiente con que sea dificil recuperar el texto a partir del texto cifrado?
- NO
- En criptografía moderna también debe cumplirse
  - Que sea difícil recuperar la clave aunque conozca el mensaje cifrado y sin cifrar (known plaintext attack)
  - Se supone que el atacante conoce el algoritmo de cifrado/descifrado
  - Se supone que el atacante conoce la existencia del mensaje
    - Ocultar la existencia de mensajes tiene sus propias técnicas (véase Steganography, steganografía?)





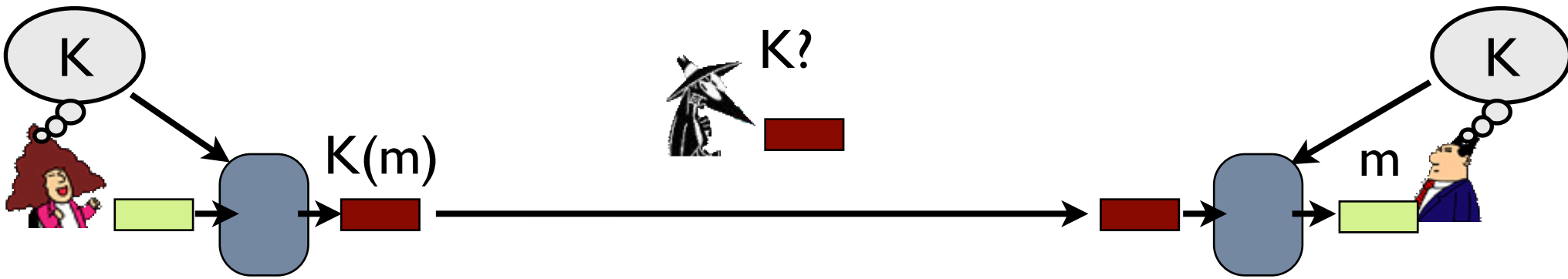
Si con eso puedo sacar la clave podria descifrar los siguientes

Criptografía: herramientas

- Algoritmos de encriptación/desencriptación
  - Encriptación de clave privada (encriptación simétrica)
  - Encriptación de clave pública (encriptación asimétrica)
- Algoritmos de hash (resumen de mensaje o message digest)
  - Como un cifrador sin clave
  - Generan un resumen del mensaje de un tamaño limitado.
  - Cumplen que es muy difícil de invertir. Obtener un mensaje original que al aplicarle el algoritmo de hash de un valor determinado

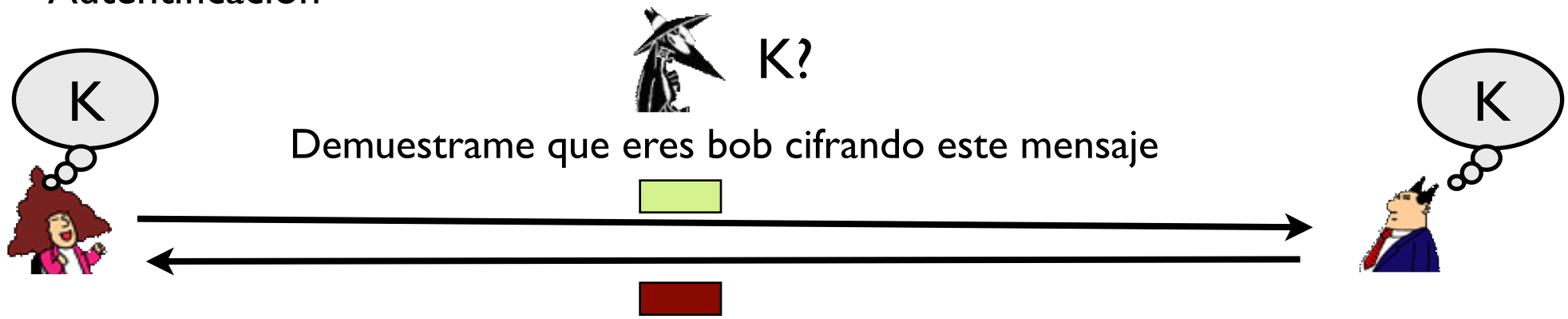
Criptografía de clave privada/secreta

- Alice y Bob comparten una clave secreta K
- La misma clave que se usó para encriptar el mensaje debe usarse para desencriptarlo
- Algunas propiedades
  - La confidencialidad viene de que el atacante no conozca la clave secreta
  - El conocimiento de la clave secreta se puede usar también como prueba de identidad (autentificación)
  - Los algoritmos de este tipo suelen ser más sencillos de implementar (y rápidos)



Criptografía de clave privada/secreta

- Autentificación



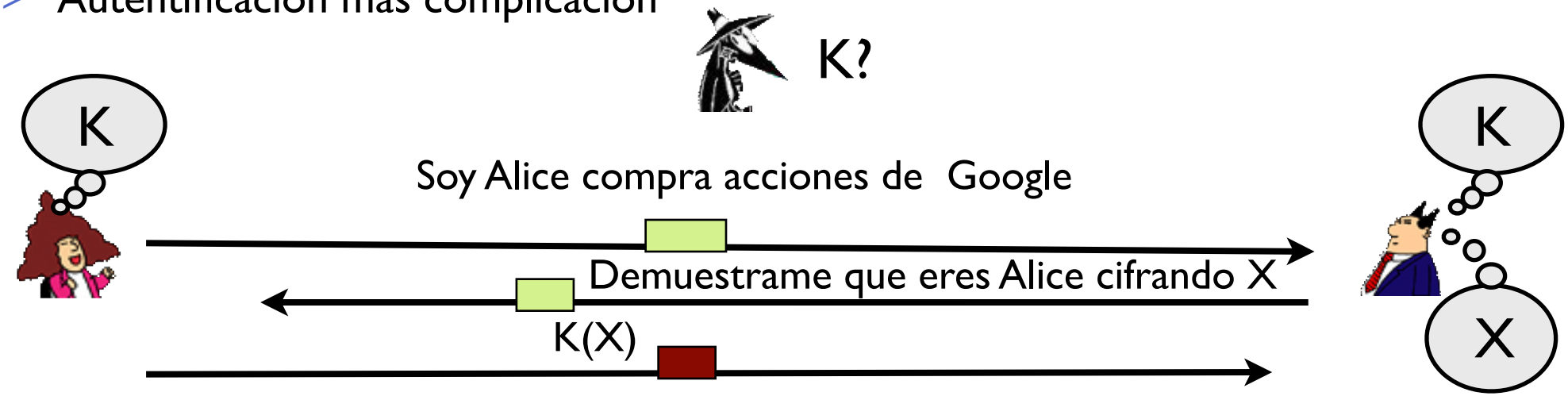
- **El mensaje cifrado funciona como firma del mensaje**

Puedo imitar el mensaje pero no la firma

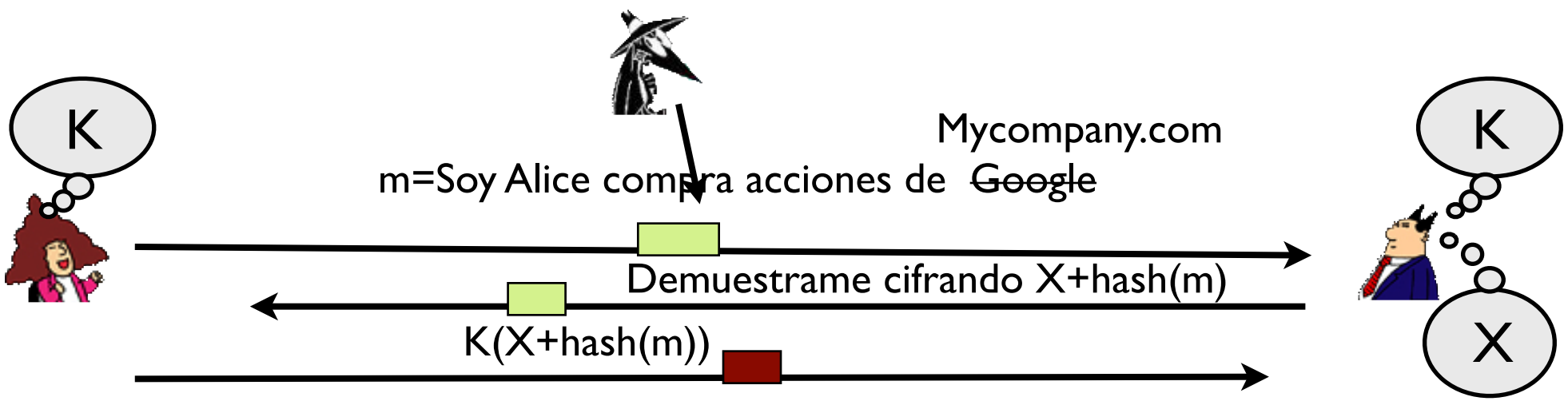
Pero si que puedo repetir mensajes válidos :-)

Criptografía de clave privada/secreta

- Autentificación mas complicacion

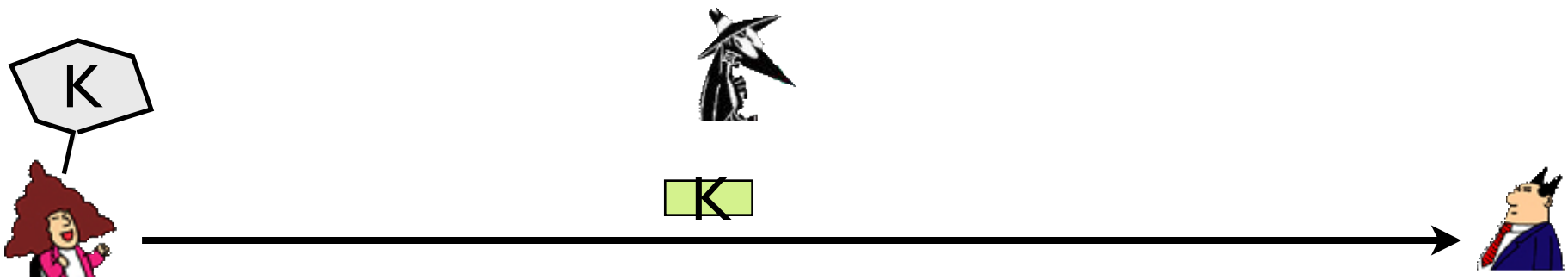


- Y si el intruso puede modificar el mensaje inicial?



Criptografía de clave privada/secreta

- Y si no compartimos una clave? Podemos comunicarnosla de alguna manera?
  - Si pudieramos hacer eso no necesitaríamos la clave



- ¿Hay alguna manera de generar una clave entre dos partes si el canal está siendo observado?

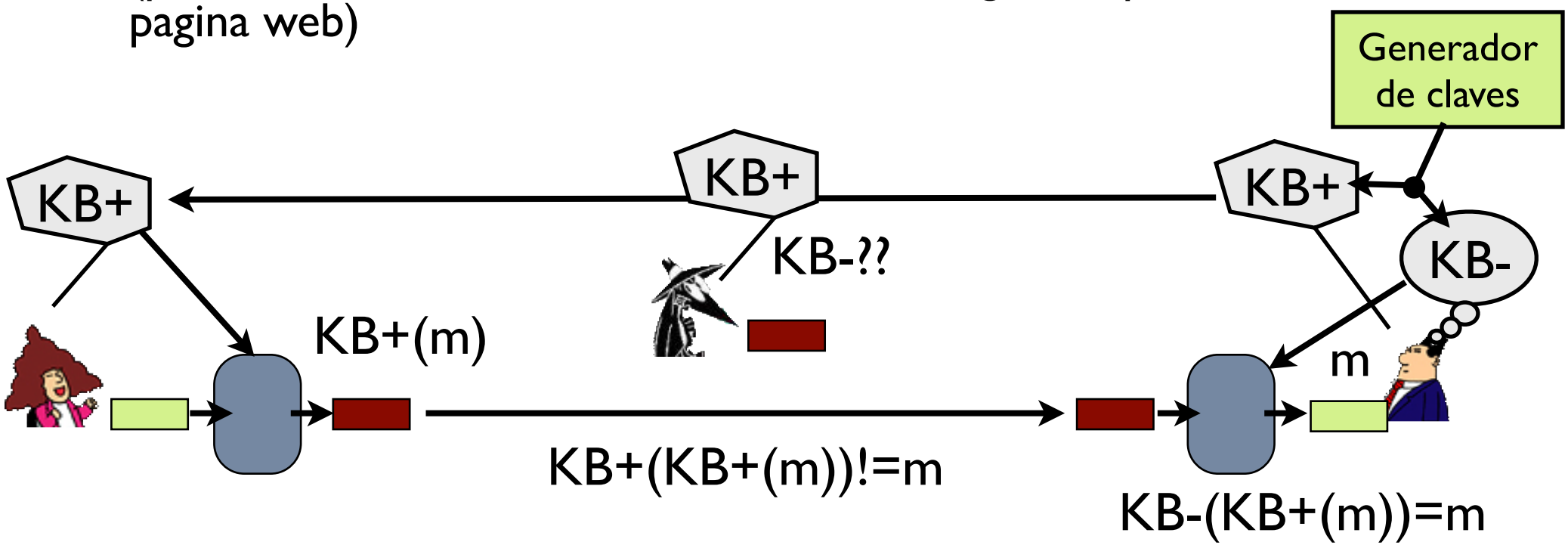
- **En resumen**
  - Se pueden hacer muchas cosas con criptografía simetrica
  - Hay que tener cuidado con el protocolo no todo son los algoritmos de cifrado
  - Pero tiene sus límites (compartición inicial de claves)

Criptografía de clave pública (asimétrica)

- Algoritmos con clave diferente para cifrar y descifrar
- Bob genera dos claves K_B^+ (publica) y K_B^- (privada)
  - Lo que cifra una lo descifra la otra

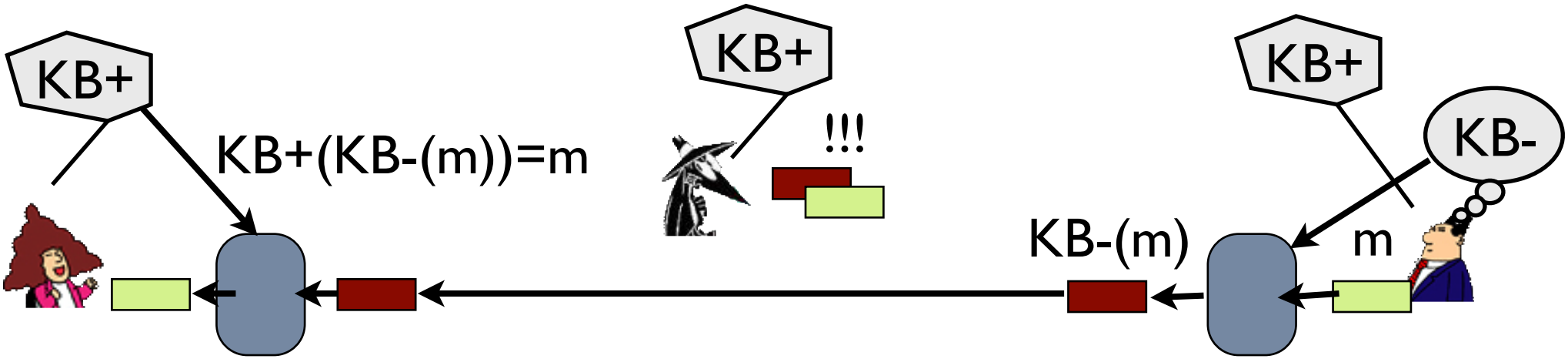
    $K_B^-(K_B^+(m))=m$ (O mejor $K_B^-(K_B^+(m))= K_B^+(K_B^-(m)) =m$)
  - Bob puede hacer publica su clave K_B^+

    (puede enviarla a Alice sobre el canal o inseguro o ponerla en su pagina web)

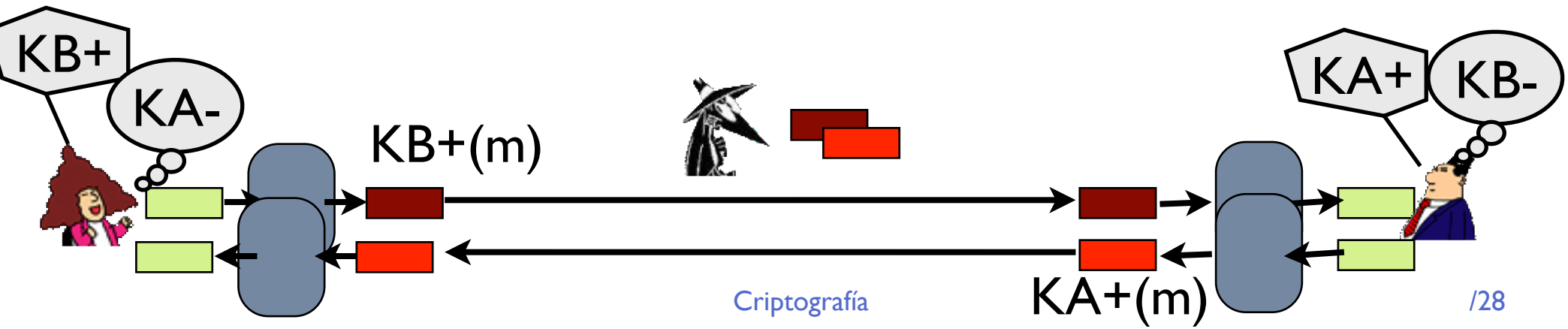


Criptografía de clave pública (asimétrica)

- Y esto para que vale?
  - Cifrado unidireccional a costa de que una clave no sea secreta



- Cifrando con KB- cualquiera puede descifrar y no vale para mucho
- Para bidireccional Alice y Bob deben generar cada uno una pareja de claves



Criptografía de clave pública (asimétrica)

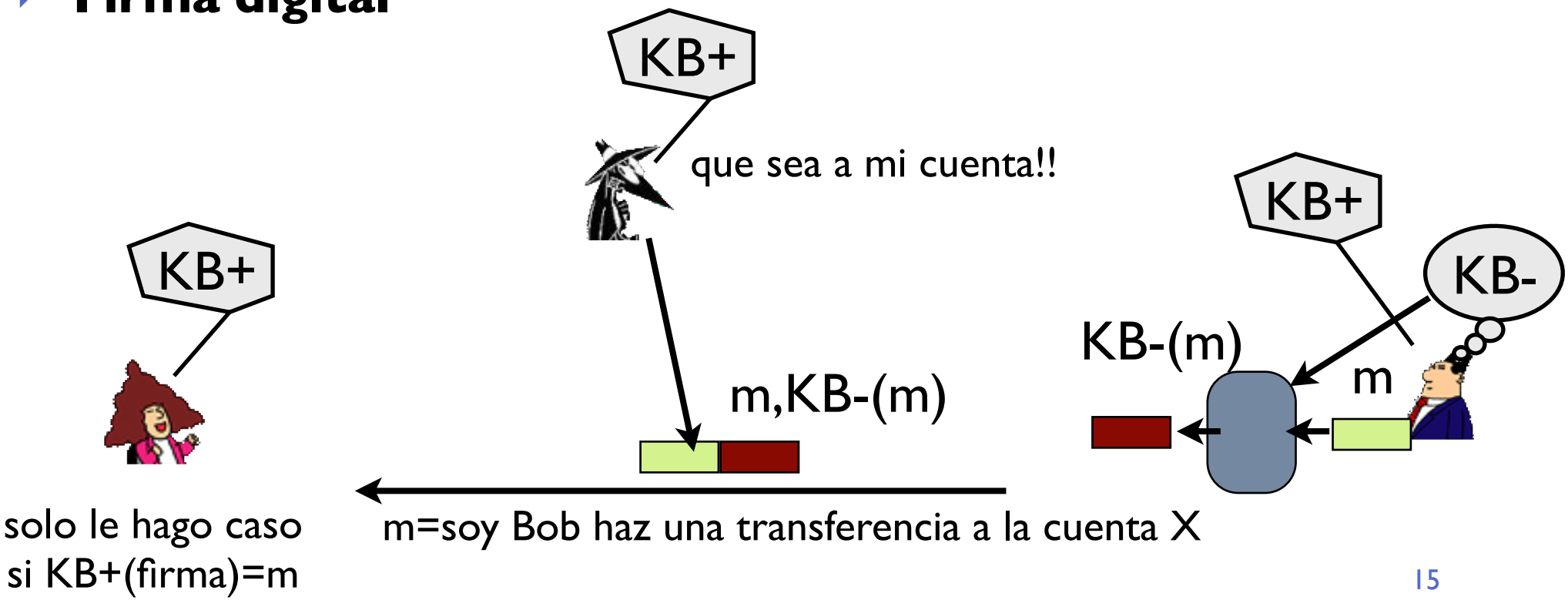
- **Cifrado bidireccional entre dos partes que no se conocen previamente !!!**

- ¿Ha resuelto esto el problema del intercambio de claves?
- Hay algo que pueda hacer nuestro intruso?

.... La respuesta despues de la publicidad....

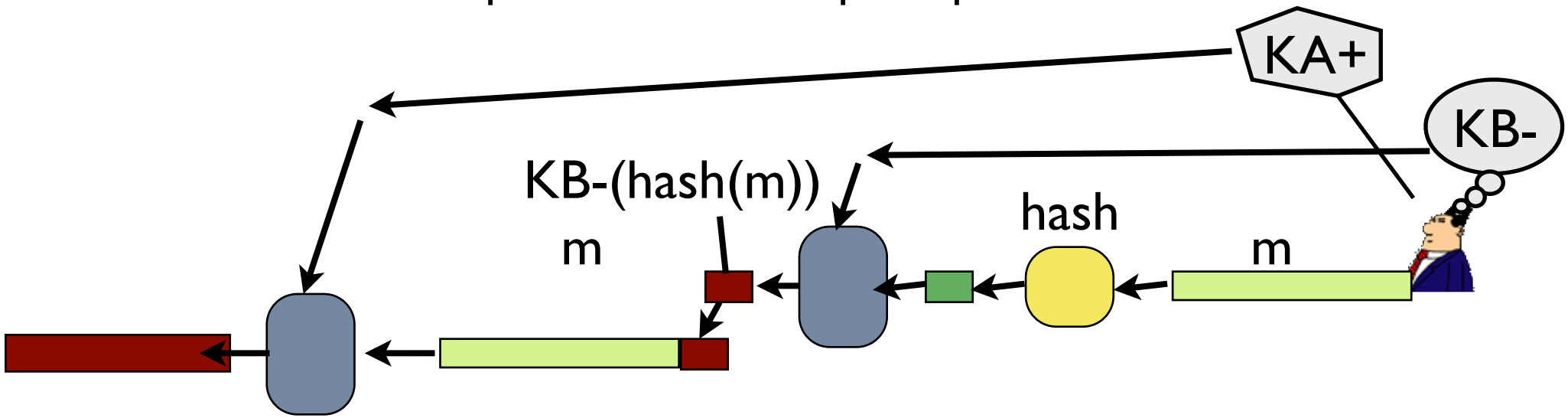
Criptografía de clave pública (asimétrica)

- Otra utilidad
  - > Ahora la capacidad de cifrar un mensaje no prueba la identidad
    Todo el mundo tiene KB+ y puede cifrar para Bob
  - > La capacidad de cifrar Si prueba la identidad
- **Firma digital**



Criptografía de clave pública (asimétrica)

- **Firma digital**
  - Ahora la firma puede ser verificada por cualquiera porque KB+ es publica
  - Normalmente no se cifra el mensaje completo para firmar sino algo que dependa de todo el mensaje para que no pueda ser modificado nada
  - Una vez firmado podemos cifrarlo para que solo lo lea Alice



Alice necesita KA- para descifrar el mensaje y KB+ para verificar la firma

Algoritmos

- **Estas son las herramientas criptograficas**

  Cifradores simetricos, asimetricos y hashes
- **Cifradores simétricos**
  - **DES** (Data Encryption Standard),

    AES (Advanced Encryption Standard),

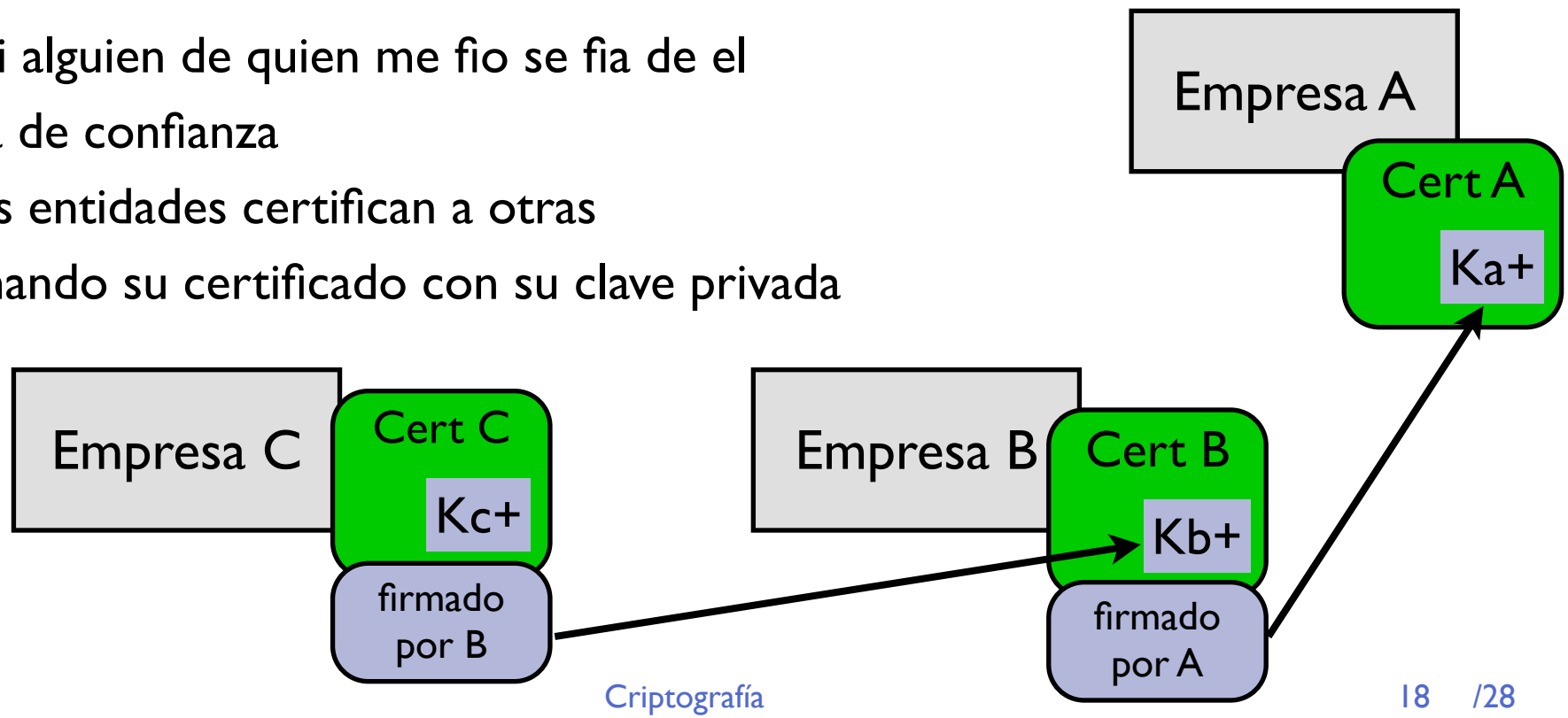
    Blowfish, **IDEA**...
  - Combinaciones y encadenamientos de cifradores para utilizar claves mas largas
- **Cifradores asimétricos (de clave pública)**
  - **Diffie-Hellman**
  - **RSA**

    Basados en general en la dificultad de descomponer un numero muy grande en sus factores primos
  - Son más costosos de calcular que los simetricos

    (= cifran a menos velocidad)
  - Se puede usar un intercambio de claves basado en clave publica para decidir entre dos partes una clave secreta y luego usar un cifrador simétrico

Certificados

- Estantar X.509
- **Certificado**
  - Declaración de datos de una entidad incluyendo una clave pública
  - Puede bajarse de una web o enviarse al principio del protocolo
  - Y como decido si me fio de un certificado?
    - Si lo he obtenido de una fuente fiable
    - Si alguien de quien me fio se fia de el
- Cadena de confianza
  - Unas entidades certifican a otras
  - Firmando su certificado con su clave privada



Certificados

- Autoridades de certificacion
  - Dan certificados a otras autoridades de mas bajo nivel y a servidores web
  - Se supone que me fio de los certificados de las empresas de arriba de la jerarquia (i.e. Verisign)
  - Si el certificado esta firmado con una clave que esta firmada por una clave que esta firmada por una clave que esta firmada...

    ... que esta firmada por alguno de los top level CAs (Certification authority)

- Los navegadores se fian automaticamente de los certificados de la lista de CAs que tienen
- Y aparte yo puedo fiarme individualmente de los que quiera

- Pero esencialmente fiarme o no del certificado es lo mismo que fiarme o no de una clave publica que tengo

Aplicaciones

Encriptando el canal a nivel de transporte/aplicación

- SSL: secure socket layer

  Librerias de sockets con encriptación para establecer sesiones utilizando intercambio de claves basado en claves publicas y cifrado con claves de sesión (por ejemplo usando certificados X.509)

  Aplicaciones que usan SSL para asegurar sus comunicaciones

  - HTTPS: HTTP seguro sobre SSL
  - SSH: Secure shell, acceso remoto y transferencia de ficheros sobre SSL
  - ...
- PGP: pretty good privacy, correo seguro utilizando clave pública
- Muchas otras aplicaciones más o menos estándares...

Nivel de red y enlace

- VPN virtual private networks y túneles...

Ejemplos

- SSH: Protocolo de sesion remota

  El servidor me envia una clave publica, la primera vez me pregunta si me fio y posteriormente se fija si envia la misma

  Mediante esa clave puedo generar una clave de sesion y cifrar con criptografia simetrica

  Tambien puedo verificar la contraseña sin enviarla

  O autentificar al cliente con otra clave publica

- HTTPS: Web sobre SSL

  El servidor envia un certificado que puede verificarse segun la cadena de confianza X.509 o preguntar al usuario.

  A partir de ahi se generan claves de sesion y se cifra todo

- Pero...

Problemas

- Recordemos... el intruso podia hacer algo aqui?

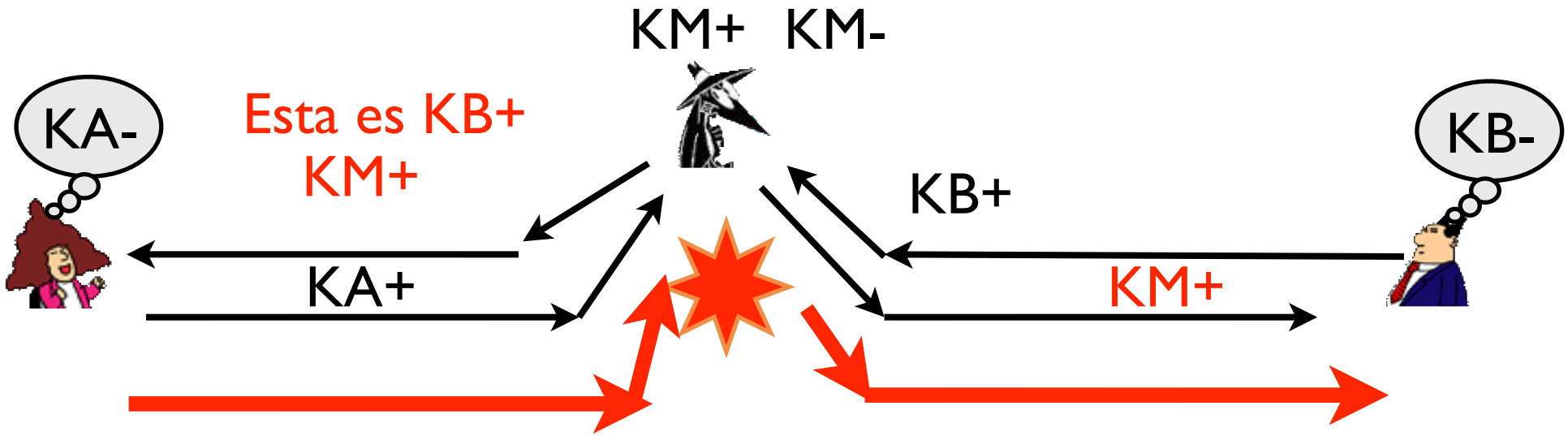
- SI !!!

  Man in the middle

  Una vez que los extremos tienen las claves no puede hacer nada... pero puede hacer man in the middle en el intercambio inicial

Problemas

- Si el intruso puede modificar el flujo de mensajes...



A y B creen que son seguras
pero cada uno envia cifrado para M
que las descifra y reenvia al destino

- El man in the middle tiene que ser hecho al principio en el intercambio de claves pero se puede

Soluciones

- Cuidado en el intercambio de claves

  Verificar que es un certificado firmado por alguien de confianza

  Verificar el fingerprint: huella del certificado (un hash) obtenido de la fuente de confianza (reduce el problema de verificar la clave publica a verifiacar una informacion reducida)

- En HTTPS, SSH asegurarse que la primera vez no hubo man in the middle
- El peligro de decir que se fie de un certificado que no conzco

¿Podemos confiar en la criptografía?

- Los algoritmos criptograficós usados se basan en propiedades matemáticas.

  En algunos está probada la dificultad de romperse por ser equivalente a resolver un problema matemático conocido
- Pero en el peor caso todo se reduce a la longitud de la clave

  Con un plain-text attack hay un ataque que siempre va a tener éxito: probar todas las claves posibles = brute-force attack
- Al final es una cuestión de recursos a emplear rompiendo la clave y tiempo para romperla, conforme hay mejores maquinas, habrá que ir aumentando la longitud de las claves

- De hecho existe el sistema criptográfico perfecto !!!

  Sólo hace falta que la clave sea de un solo uso e igual de larga que el mensaje (vease cifrador de Vernan, 1917)

¿Podemos confiar en la criptografía?

- A efectos prácticos se puede confiar en la criptografía

  Es decir es una herramienta suficientemente buena para que no merezca la pena atacar por ahi... hay otros caminos más fáciles
- La criptografía no puede protegerte de:
  - Mensajes que no se cifran
  - Robo de claves almacenadas en un ordenador
  - Extorsión o engaño a los usuarios para que revelen la clave
  - **Protocolos mal diseñados (por ejemplo que admitan el reenvio de un mensaje cifrado anteriormente con el mismo significado)...**
- En resumen, es una buena herramienta, lo suficiente para no ser el eslabón más debil.

Para saber más sobre criptografía...

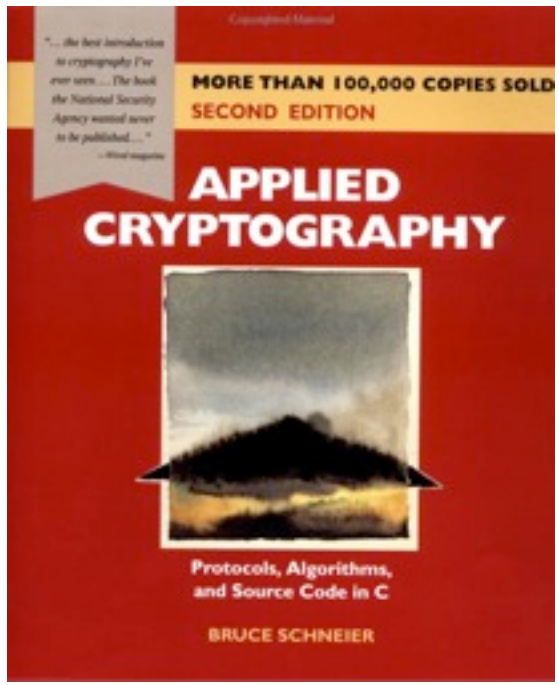
- **La biblia de la criptografia :-)**

  Bruce Schneier

  Applied Criptography. Protocolos, Algorithms and Source Code in C

  John Wiley & Sons, 1996 (segunda edicion)

- De como encriptar comunicaciones
- O jugar al poker, o tirar un dado en Internet, de forma que dos partes que no se conocen previamente estén de acuerdo en que la tirada ha sido justa
- Y otras aplicaciones tipicas:
  - dinero electronico
  - votación electronica
  - lanzamiento conjunto de misiles nucleares
  - ...



Conclusiones

- Herramientas para proteger el canal de comunicaciones
  - Criptografía Simétrica (clave secreta)
  - Criptografía Asimétrica (clave pública)

- Próximas clases
  - VPNs
  - Seguridad en WiFi