Criptografía básica

(extracto de ponencia "Administración Electrónica")

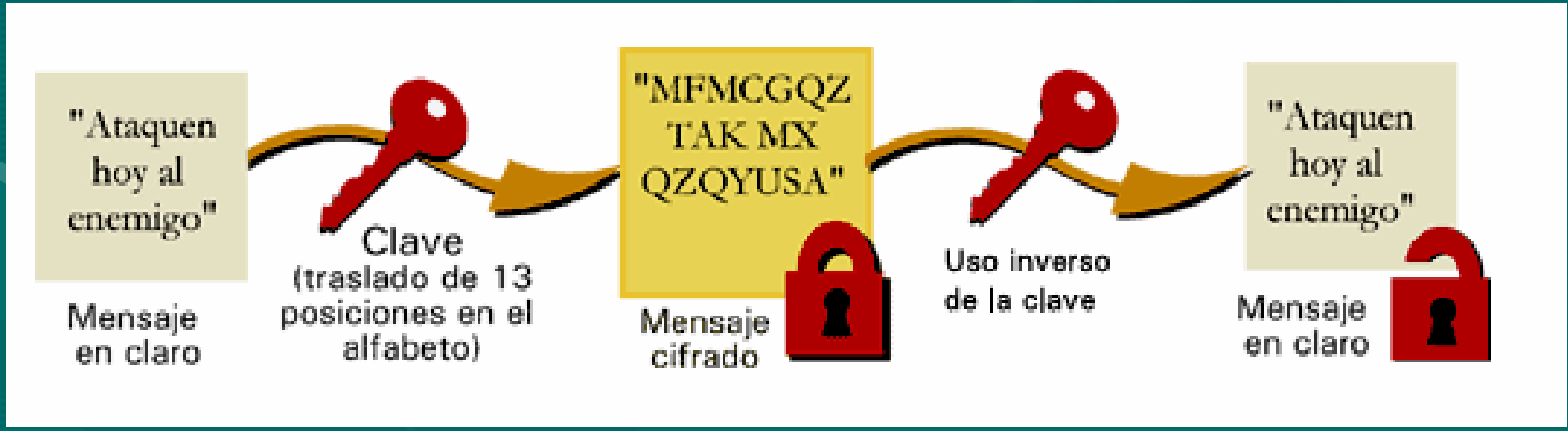
Alejandro Secades Gómez
EUITIO – Universidad de Oviedo

Criptografía básica

- La criptografía nació como la ciencia de ocultar mensajes,sea, cifrarlos para que sólo el receptor pueda acceder a ellos
- Su origen es militar (Julio César escribió sobre ello, en la II Guerra Mundial se usó ampliamente, etc.), para enviar mensajes y órdenes sin que el enemigo lo supiera aunque interceptara el mensaje (o al mensajero)
- En la última parte del s. XX, varios avances permitieron aplicar técnicas de cifrado para un nuevo propósito:
  - autenticar el origen de un mensaje, o lo que es lo mismo, *firmar* un mensaje, de modo que pudiéramos estar seguros de quién lo mandaba → concepto equivalente a la firma manuscrita

Criptografía básica

- Criptografía simétrica
  - La más sencilla, ya usada por Julio César
  - Existe una clave de cifrado y un algoritmo de cifrado (operaciones con el mensaje y la clave)
  - Aplicando el algoritmo de cifrado y la clave, convertimos el mensaje en algo ilegible
  - Aplicando el mismo algoritmo con la misma clave al mensaje cifrado, recuperamos el mensaje original
  - Veamos el ejemplo de Julio César:



Criptografía básica

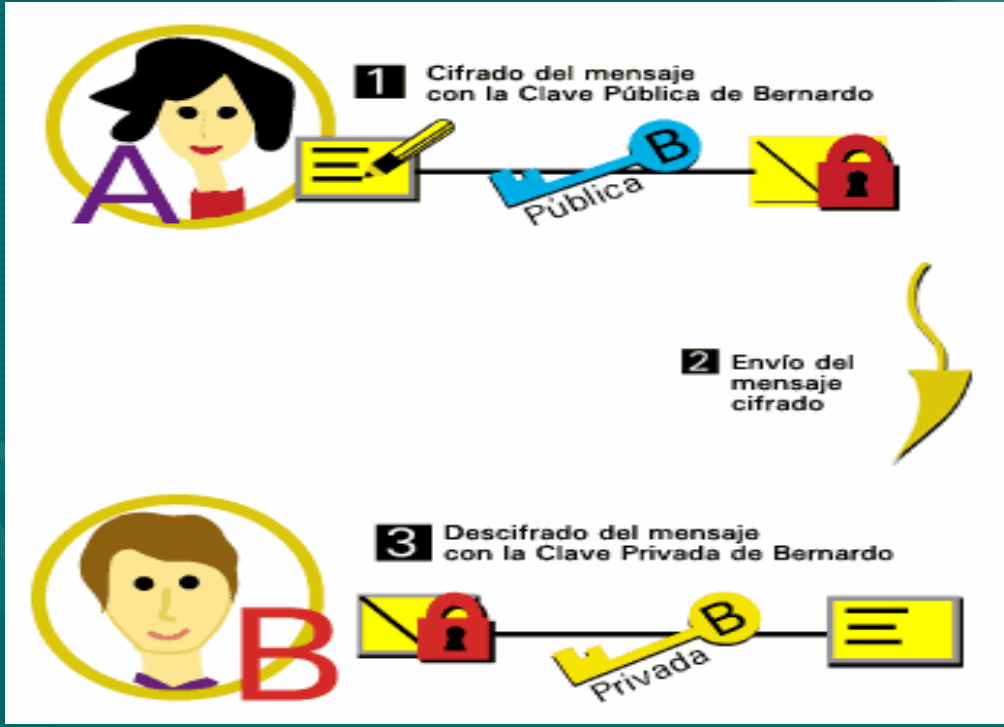
- Cifrado simétrico:
  - Resumen: Se cifra y descifra con la misma clave
  - Actualmente se usan algoritmos matemáticos mucho más complejos (DES, 3DES, AEDES, BlowFish…)
  - En un cifrado muy rápido de realizar para un ordenador (incluso hay hardware específico para ello)
  - El punto crítico es que para descifrar el mensaje se necesita conocer la clave:
    - ¿Cómo intercambiamos la clave de cifrado de forma segura por Internet? → En la II Guerra Mundial los alemanes tenían que llevar consigo la máquina de cifrado "enigma"
    - ¿Cómo gestionamos una clave única para cada ciudadano? → la clave privada no es una contraseña, sino una "ristra" enorme de números y letras…
    - El cifrado simétrico no es la solución para Internet y para múltiples usuarios (ciudadanos)
  - Aunque este cifrado es usado ampliamente en la Administración Electrónica, por sí solo no soluciona los problemas arriba indicados

Criptografía básica

- Criptografía asimétrica
  - Para solucionar el problema de tener que compartir la misma clave entre emisor y receptor
  - Desarrollada en los últimos 30 años (RSA)
  - Existen dos claves, denominadas clave pública y clave privada
    - Lo que se cifra con una se descifra solo con la otra, y viceversa → no es posible cifrar y descifrar con la misma clave (en la práctica con la pública se obtiene la privada)
    - Cada usuario conserva su clave privada y distribuye su clave pública abiertamente

Criptografía básica

- Cada participante tiene dos claves, la pública y la privada
- Para enviar un mensaje, lo cifro con la clave pública del receptor → sólo él con la clave privada lo podrá descifrar



Criptografía básica

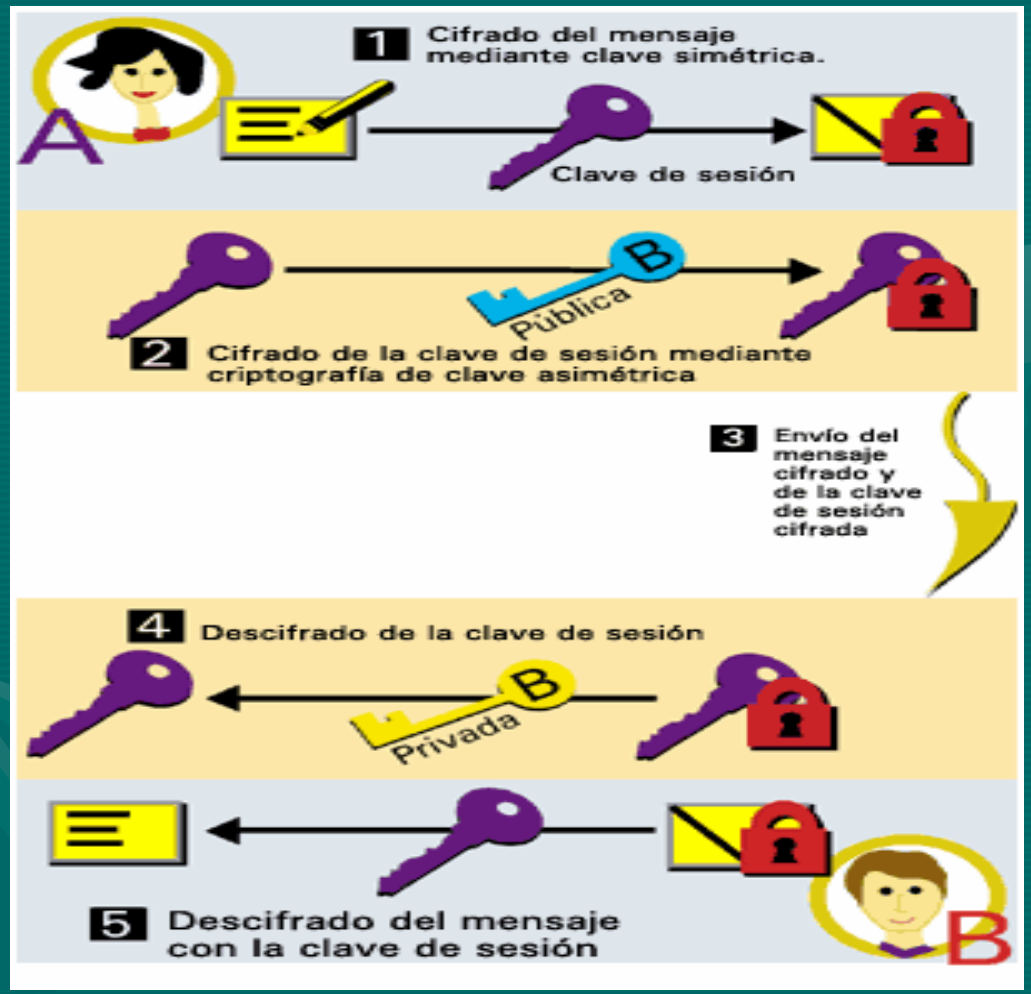
- Cifrado asimétrico:
  - Para enviar un mensaje a alguien, lo cifro con su clave pública
  - Sólo él, que tiene la clave privada, podrá descifrar dicho mensaje
  - No importa que la clave pública se distribuya a todo el mundo, no sirve para descifrar el mensaje
  - Computacionalmente el cifrado asimétrico es un proceso lento (p.e. RSA basado en números primos enormes cuyo producto es muy difícil de factorizar)
    - Problema: cifrar muchos datos en tiempo real sería muy lento y requeriría grandes ordenadores

Criptografía básica

- En la práctica se combina el cifrado simétrico y el asimétrico (sobre digital):
  - Se cifra con clave simétrica (rápido)
  - Se cifra la clave simétrica con cifrado asimétrico (usando la clave pública del receptor)
  - Se envía todo junto
  - El receptor descifra con su clave privada asimétrica la clave simétrica
  - El receptor ya puede descifrar el mensaje con la clave simétrica
  - Tiene la ventaja de la rapidez del cifrado simétrico para el mensaje (largo) y que la clave se distribuye de forma segura con cifrado asimétrico. En lo sucesivo se sobreentenderá que se usa éste método aunque solo se hable de cifrado asimétrico

Criptografía básica

- Sobre digital: combinación de cifrado simétrico y asimétrico para cifrar mensajes grandes de manera eficiente



Criptografía digital

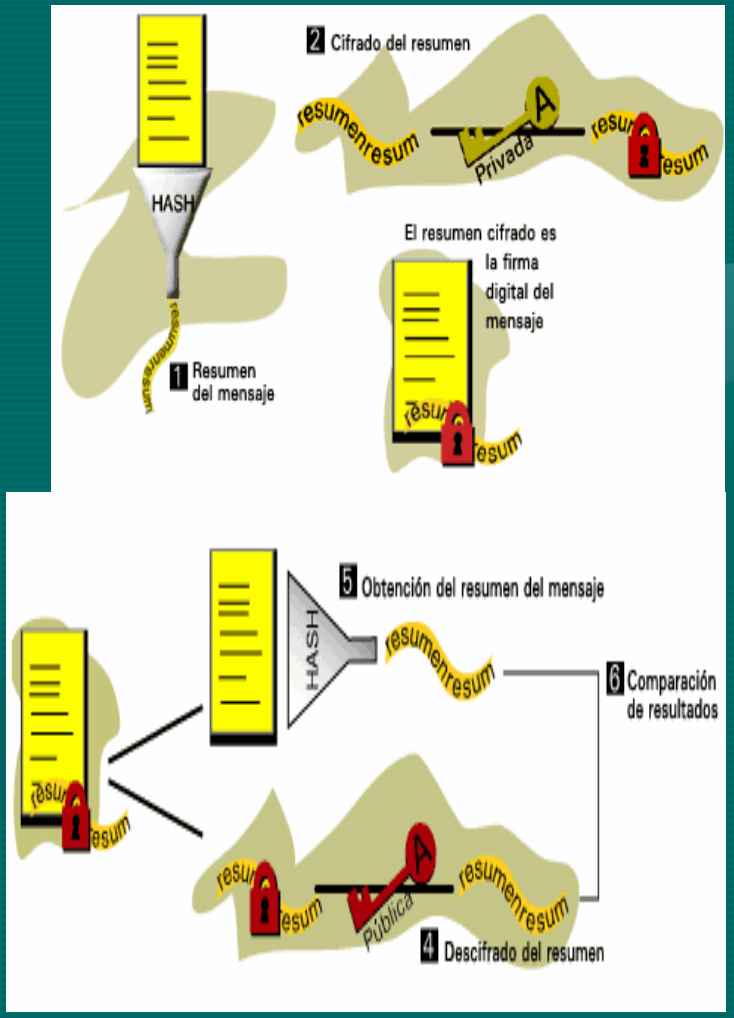
- Firma digital:
  - El emisor cifra el mensaje con clave **privada**
  - Lo envía cifrado y sin cifrar al receptor
  - El receptor descifra la parte cifrada con la clave **pública** del emisor
  - Si coincide con el mensaje, es que lo ha enviado el emisor y nadie lo ha alterado
    - Sólo el poseedor de la clave privada correspondiente a la clave pública usada para descifrar podría generar un mensaje cifrado que al descifrarse coincida con el original

Criptografía básica

- Firma digital (II):
  - En la práctica, no se cifra todo el mensaje, sino un hash o resumen de él
    - La firma digital busca identificar al emisor del mensaje, el cifrado del mensaje sería otro asunto
  - Hash: Un código de redundancia de tamaño fijo, como la letra del NIF o el código de comprobación de un número de cuenta (pero a lo grande)
    - Se envía firmado el hash del mensaje
    - Se descifra, se calcula el hash del mensaje recibido y se comparan
    - Cualquier cambio en el mensaje, por pequeño que sea, cambiará el hash, por lo que no coincidirán
  - La firma digital asegura que el poseedor de una clave privada ha generado un mensaje

Criptografía básica

- La firma digital consiste en adjuntar al documento electrónico un hash del mismo cifrado con la clave privada del emisor
  - Al recibirlo, si tenemos la clave pública del emisor podemos comprobar que el mensaje lo envió él



Criptografía básica

- Firma digital (III):
  - Problema: ¿Cómo saber que una clave pública es realmente de quien dice ser?
    - Podríamos enviar mensaje cifrados a la persona equivocada, o recibir claves públicas y no estar seguros de la identidad de su propietario
  - Solución: Autoridades de certificación y certificados digitales
    - **Certificado digital**: Una clave pública, los datos personales del dueño de la clave privada, y todo firmado por alguien de confianza (Autoridad de Certificación o AC)
    - El concepto es el equivalente al de un notario: si un notario firma un documento, nos fiamos de su autenticidad → en este caso el "notario" es la AC, que firma no un documento, sino el certificado de un usuario

Criptografía básica

- Certificados digitales:
  - Pueden ser un elemento de software instalado en el PC
    - No es fácil llevarlos a otro PC, que en cualquier caso debería ser de total confianza (no un cyber-café)
    - El PC puede ser usado por otra persona, el certificado copiado…
  - Pueden ir en chips criptográficos
    - DNI electrónico, tarjeta de la FNMT, llavero USB…
    - Son mucho más seguros: la clave privada no sale del chip, y requieren un PIN para su uso
  - Los certificados digitales tienen una fecha de caducidad, a partir de la cual no servirían
  - Los certificados digitales pueden ser revocados por la AC emisora
    - P.e.: el poseedor del certificado es cesado de su puesto, y por tanto ya no puede usar una determinada firma electrónica
    - Las AC mantienen listas públicas de certificados revocados, para poder comprobar en todo momento si un certificado sigue siendo válido o no

Criptografía básica

- Autoridad de certificación
  - Entidad que emite certificados digitales para otras personas
  - Todo el mundo tendría las claves públicas de las entidades de certificación → Podemos confirmar que un certificado digital está firmado por una de ellas → Podemos fiarnos de la validez del certificado
  - La autoridad de certificación tiene que comprobar que da cada certificado a la persona adecuada → hace de "notario", dando fe de que el certificado se entrega a la persona indicada… y nosotros nos fiamos de su firma
  - Autoridades de certificación: FNMT (certificados para la declaración de la renta), DNI electrónico…, y entidades privadas (Verisign, Thawte…)

Criptografiá básica

- Cadenas de certificación
  - Un certificado digital está firmado por una AC, el certificado de esa AC a su vez puede estar firmado por otra AC de mayor nivel…
    - Concepto similar al de la delegación de firma en las AA.PP
  - Al final, necesitamos fiarnos del certificado (firmado por ella misma) de una AC
    - La firma digital de una AC sería válida en sí misma, como la firma de un notario o de un presidente autonómico en el ámbito de sus competencias
    - Vienen preinstalados en los PCs, o pueden ser instalados manualmente
- Autoridades de certificación
  - ¿Deberían ser públicas o privadas? → En muchos paises no hay nada parecido al DNI español, por lo que no se entiende al Estado como emisor de certificados
  - ¿El DNI electrónico acabará con el resto de autoridades de certificación? → posiblemente no, se necesitarán certificados de tipo específico (p.e. de colegios profesionales)

Criptografía básica

- DNI electrónico:
  - Certificado digital en una tarjeta con chip criptográfico
  - La tarjeta es similar al DNI actual
  - Información en http://www.dnielectronico.es
  - La AC sería el Ministerio del Interior

Criptografía básica

- Resumen:
  - Sistemas de clave pública y privada → permiten cifrar y firmar digitalmente
  - Certificado digital: Clave pública con datos personales y firmada por una CA
  - Autoridad de certificación (CA): organismo que emite certificados digitales. Debe comprobar la identidad de los destinatarios de los mismos