Principios de criptografía

Jacobo Tarrío Barreiro
<jtarrio@alfa21.com>

Antes de empezar

- En castellano se dice:
  - Criptografía
  - Criptográfico
  - Cifrar
  - Descifrar
- "Encriptar" es meter en una cripta

Para qué sirve la criptografía

- Transmisión de mensajes secretos por canales abiertos
- Validación de mensajes
- Ocultación de información

¿Quién necesita criptografía?

- Gobiernos
- Delincuentes
- El común de los mortales
  - Banca/comercio online
  - Mensajes privados
  - Datos sensibles
  - ...

Transmisión de secretos

- Criptografía de clave secreta
  - Sustitución
  - Permutación
- Criptografía de clave pública

Clave secreta

- Se cifra y se descifra con la misma clave
- Sustitución
  - El ejemplo típico es el "césar"
  - Por ejemplo: EL GATO -> GN ICVQ
  - Otro ejemplo: EL GATO -> 31 6470
- Sustitución polialfabética
  - Ejemplo: EL GATO -> FN HCUQ

Clave secreta

- Permutación
  - Por ejemplo: EL GATO -> LEG TA O
- Diversas combinaciones
  - 136 74 0

Clave secreta

- Métodos modernos
  - Rotores (ENIGMA)
  - Bit a bit (Lorenz)
  - Ordenadores (DES, IDEA, AES, ...)

Clave pública

- Se cifra con una clave, se descifra con otra
- Ventaja: no hay que ponerse de acuerdo previamente
- Intercambio de clave: Diffie-Hellman
- Cifrado/descifrado: RSA, DSA...

Validación de mensajes

- Verificar si un mensaje se ha transmitido correctamente
- Verificar si un mensaje ha sido modificado
- Verificar la procedencia de un mensaje

Verificar transmisión correcta

- Función hash: a partir de un texto calcula un n úmero
- Hashes: MD5 (128 bits), SHA (160 bits)
- Con el texto del mensaje se transmite el hash
- Si el hash no coincide, el mensaje está corrompido

Verificar mensaje modificado

- Se crea el mensaje y se calcula su hash
- El hash se almacena en un lugar seguro
- Después de leer el mensaje, se calcula su hash
- Si no coincide con el hash guardado, el mensaje ha sido modificado

Verificar procedencia de un mensaje

- Se crea el mensaje y se calcula su hash
- El remitente cifra el hash con su clave privada (firma)
- Después de leer el mensaje, se calcula su hash
- Con la clave pública del remitente se descifra el hash original
- Si no coinciden, el mensaje no ha sido escrito por el remitente

Validez de las claves

- Problema: ¿la clave es de quién dice ser?
- Se puede solucionar haciendo que usuarios de confianza certifiquen las claves firmándolas
- Dos aproximaciones: autoridades certificadoras (X.509) y redes de confianza (PGP)

Ocultación de información

- Ocultar la propia existencia de un mensaje
- Útil cuando la presencia de un mensaje cifrado es sospechosa de por sí

- Métodos clásicos
  - Dobles fondos
  - Letras en una carta pinchadas
  - Hilos con marcas
- Métodos modernos
  - En una imagen
  - Varias formas de codificar algo
  - ...