Introducción a la Criptografía

Seguridad criptográfica

eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea
KISA

Seguridad criptográfica

El **objetivo de la Criptografía** en la actualidad es garantizar la seguridad de un sistema de comunicaciones.

- La *seguridad absoluta* no existe.
- Siempre es relativa a la capacidad de ataque de posibles adversarios.

Tenemos que:

- Explorar qué aspectos pueden protegerse.
- De qué herramientas se dispone.
- Analizar el grado de protección alcanzado. Estudiar técnicas de ataque.

Servicios de seguridad

La Criptografía pretende proporcionar los siguientes servicios:

- **Confidencialidad**: garantizar la privacidad.
  Se consigue con el *cifrado*.
- **Autenticación**: garantizar la autenticidad de origen (la información proviene de la entidad de quien dice provenir).
  Se consigue mediante la *firma digital*.
- **Integridad**: garantizar la autenticidad de contenido.
  Se consigue con:
  funciones resumen ("hash functions"),
  MACs (*Message Authentication Codes*).
- **Disponibilidad**: garantizar el acceso a la información.
  Se consigue con la *gestión de claves*.

Tipos de seguridad criptográfica

- La seguridad se considera violada cuando se obtiene la clave secreta del sistema.
- En ocasiones es posible obtener el mensaje en claro sin encontrar la clave de cifrado.

1. **Seguridad de los criptosistemas**:

   Según el grado de seguridad de un criptosistema, puede ser:

   1.1 Seguridad *incondicional*.
   1.2 Seguridad *computacional*.
   1.3 Seguridad *probable*.
   1.4 Seguridad *condicional*.

2. **Seguridad de los protocolos**.
   Difícil de analizar.

1. Seguridad de los criptosistemas:

1.1 Seguridad *incondicional*. Proporcionada por métodos de cifrado para los que el conocimiento del texto cifrado no aporta ninguna información sobre el texto en claro, cualquiera que sea la fortaleza del adversario.

Es decir, el conocimiento del cifrado no ayuda a conocer el texto en claro de forma más sencilla que en el caso de que dicho cifrado no se conozca.

Ejemplo: Sólo se conoce un cifrado incondicional, el Cifrado de *Vernam*.

1.2 Seguridad *computacional*. Proporcionada por métodos de cifrado para los que no existe capacidad de cálculo suficiente para obtener la clave secreta.

Ejemplos: RSA y la mayoría de cifrados de clave pública.

1.3 Seguridad *probable*. Proporcionada por métodos de cifrado que no han podido ser violados pese a los continuos esfuerzos para conseguirlo.

Ejemplos: DES y cifrados en bloque simétricos.

1.4 Seguridad *condicional*. Proporcionada por métodos de cifrado diseñados con fines específicos para los que la dificultad de violación es siempre muy superior a la supuesta capacidad de análisis de un eventual atacante.

2. Seguridad de los protocolos: la seguridad de un protocolo es difícil de definir, ya que depende de su diseño.

Cualquier protocolo puede ser vulnerable si no está bien diseñado.

En ocasiones se puede violar un protocolo sin necesidad de encontrar la clave secreta.

Ataques a la seguridad criptográfica

Por su naturaleza, podemos clasificar los ataques a los criptosistemas en dos tipos:

- *Ataques pasivos:* el atacante sólo puede monitorizar el canal de comunicación.
  - Observación del mensaje.
  - Análisis de tráfico.
- *Ataques activos:* el atacante pretende no sólo obtener información, sino también modificarla.
  - *Intercepción*. No confidencialidad.
  - *Interrupción*. No disponibilidad.
  - *Modificación*. No integridad.
  - *Inserción*. No autenticidad de origen.

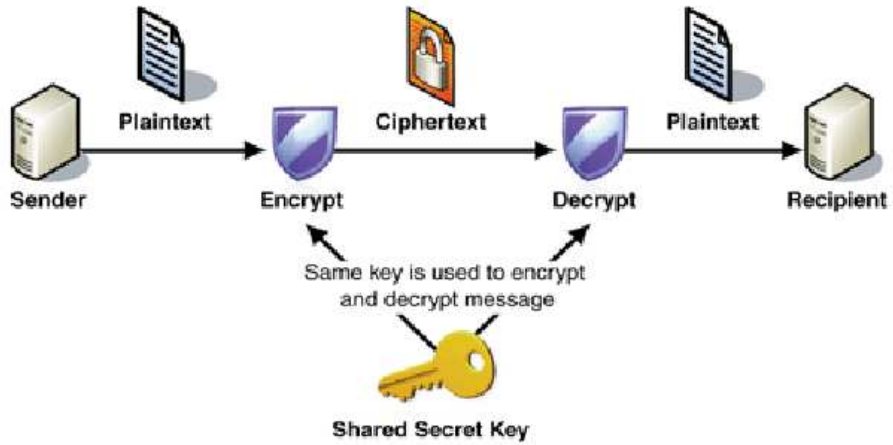
Por el modo de proceder, podemos clasificar los ataques en:

- **Ataques a los criptosistemas**: pueden realizarse:
  - Por *fuerza bruta*. Se pretende encontrar la clave probando con cada clave del espacio de claves.
  - *A partir del cifrado*. El atacante sólo tiene acceso al cifrado y a partir de él trata de encontrar la clave secreta.
    Ejemplo: análisis de frecuencias.
  - *A partir del texto en claro*. El atacante tiene acceso al texto en claro y su correspondiente cifrado.
  - *A partir del texto en claro elegido*. El atacante puede obtener el cifrado de cualquier texto que él elija, entendiéndose que él no sabe cifrarlo, sino que lo obtiene ya cifrado.
  - *A partir del texto cifrado elegido*. El atacante puede obtener el texto en claro correspondiente a determinados textos cifrados de su elección.

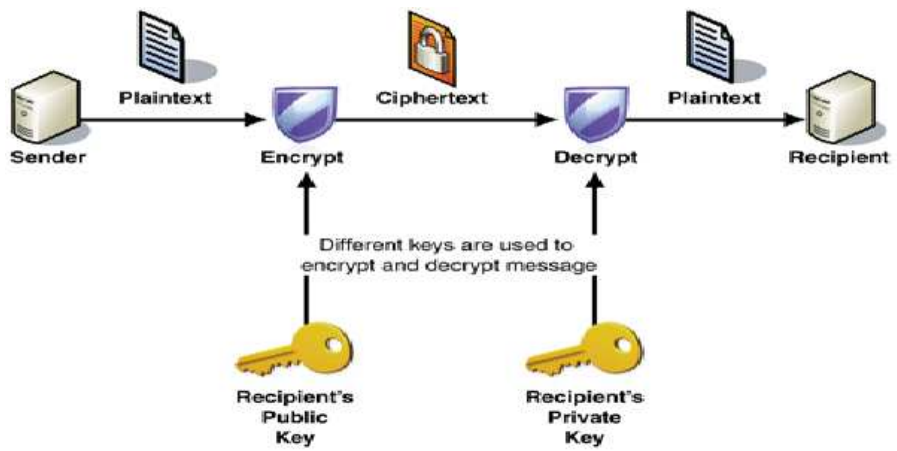
- **Ataques a los protocolos**:
  - *Con clave conocida*.
    El atacante obtiene algunas claves utilizadas en cifrados previos e intenta determinar nuevas claves.
  - *Reutilización del protocolo*.
    El atacante registra una de las comunicaciones o parte de ella e intenta insertarla en una comunicación posterior.
  - *Suplantación de personalidad*.
    El atacante asume la identidad de uno de los comunicantes.
  - *Compilación de un diccionario*.
    El atacante colecciona una lista de posibles claves y las prueba hasta encontrar una útil.
  - *Búsqueda exhaustiva*.
    Búsqueda con todas las claves.
  - *Ataque de intermediario (man-in-the-middle)*.
    El atacante se introduce en la línea entre dos usuarios, pudiendo comunicarse con ambos.

Tipos de cifrado

1. **Cifrado simétrico o de clave secreta.**



2. **Cifrado asimétrico o de clave pública.**



Fuente: Internet, "draw+of+public+key+cryptography"

1. Cifrado simétrico o de clave secreta.

- Ambos comunicantes comparten la clave.
- La clave para cifrar y descifrar es la misma, o al menos es posible deducir la clave de descifrado a partir de la de cifrado.
- Son altamente eficientes y resistentes a ataques.

1.1 **Cifrado en flujo**: el cifrado se efectúa bit a bit.
Ejemplo: Cifrado de Vernam.

1.2 **Cifrado en bloque**: se cifran bloques de bits.
Ejemplos: DES, 3-DES, Blowfish, CAST, IDEA, RC2, RC4, RC5, SAFER, AES.

2. Cifrado asimétrico o de clave pública.

- Cifrado en bloque.
- Cada usuario posee una pareja de claves:
  una pública compartida (para cifrar),
  y una secreta privada (para descifrar).
- Claves de mayor tamaño que en cifrados en bloque simétrico.
- Tasa de cifrado inferior al cifrado simétrico.

Ejemplos: RSA, El Gamal, criptosistema de Rabin, ECC.
Basados en problemas matemáticos de difícil solución.

Fin de la sección