Introducción a la Criptografía

M.I. GONZÁLEZ VASCO / A. PÉREZ DEL POZO
GRADO EN INGENIERÍA DE LA CIBERSEGURIDAD
UNIVERSIDAD REY JUAN CARLOS

Índice

1. Algunas definiciones básicas.
2. Un poco de historia.
3. ¿Para qué sirve la Criptografía?
4. Primitivas criptográficas.
5. Criptoanálisis. Tipos de ataques.
6. Principios de la Criptografía moderna.

1. Algunas nociones básicas.

Introducción.

- **Criptografía:** ciencia que se ocupa de la búsqueda y mejora de técnicas para la transmisión segura de la información.
- **Criptoanálisis:** estudio crítico de los sistemas criptográficos.
- **Criptología: Criptografía + Criptoanálisis.**

Dos tipos de criptología: **clásica o de clave secreta**.

- Máximo nivel de seguridad y rapidez.
- Exige que exista un intercambio previo de información entre usuarios.
- Usada fundamentalmente a nivel militar.

Dos tipos de criptología: **moderna o de clave pública**.

- Surge en 1976.
- Seguridad es, a menudo, heurística.
- No exige intercambio previo de información.
- De uso civil.

Esteganografía.

- Técnicas de transmisión segura de la información por medio de ocultación (¡¡distinto de la criptografía!!).

2. Un poco de historia.

Criptología.

- 3000 a.C. Jeroglíficos egipcios, ¿primer intento de limitar el acceso a la información?
- 50 a.C. Criptosistema del César.
- 1500 Criptosistema de Vigenère.
- 1917 Criptosistema de Vernam (one-time pad).

Criptología.

- 1944 Máquinas de cifrado: Enigma, Colossus.
- 1949 Teorema de Shannon: secretos perfectos.
- 1976 Nacimiento de la Criptografía de Clave Pública (Diffie-Hellmann).

3. ¿Para qué sirve la Criptografía?

Para obtener:

- Privacidad: la información sólo debe ser accesible a aquellos autorizados a obtenerla.
- Integridad: la información sólo debe ser alterada por aquellos autorizados a hacerlo.

Para obtener:

- Autentificación: las partes que intercambian información deben ser capaces de identificarse de manera irrefutable.
- No repudio: no se deben poder negar acciones o afirmaciones previas.

4. Primitivas criptográficas.

Algunas de ellas:

- Funciones Hash.
- Funciones one way.
- Generadores pseudoaleatorios.
- Esquemas de cifrado.
- Esquemas de firma.

Ejemplo: esquema de cifrado de clave secreta.

- Consta de 3 algoritmos (Gen, Enc, Dec).
- Gen (genera la clave secreta).
- $Enc_k(m)$ (cifra el texto en claro).
- $Dec_k(c)$ (descifra el texto cifrado).
- Corrección: $m= Dec_k(Enc_k(m))$

5. Criptoanálisis. Tipos de ataques.

Principio de Kerckhoff (s. XIX)

- Se asumirá que un adversario potencial conoce toda la información acerca de la herramienta criptográfica que pretende atacar, con la excepción de las claves secretas.

¿Por qué?

- El algoritmo es difícil de mantener oculto.
- El algoritmo es más costoso de reemplazar si es descubierto.
- Permite comunicación dos a dos en un grupo sólo utilizando claves distintas.

Es más, actualmente, se prefiere hacerlo público:

- Da confianza en la seguridad del esquema.
- Fallos se detectan públicamente, permite corregir o desechar.
- Evita que alguien que llega al mismo esquema pueda romperlo.
- Permite establecer estándares.

Ataques a un sistema de cifrado (**pasivos**).

- Ciphertext-only (**eav**): el adversario sólo tiene acceso a (uno o varios) textos cifrados.
- Known-plaintext (**kpa**): el adversario tiene acceso a (uno o varios) pares

  texto en claro / texto cifrado

Ataques a un sistema de cifrado (**activos**).

- Chosen-plaintext (**cpa**): el adversario puede ver el cifrado correspondiente a textos en claro de su elección.
- Chosen-chipertext (**cca**): el adversario puede ver el descifrado de textos cifrados de su elección.
- Estos ataques pueden ser adaptativos.

6. Principios de la Criptografía moderna.

1. Definiciones exactas.

- ¿Qué es seguridad?
- ¿Qué tipo de adversarios permito?
- ¿Qué facilidades supongo que pueden tener esos adversarios?
- ¿Cuándo considero que el adversario ha “roto” el sistema?

2. Hipótesis computacionales.

- La mayoría de los esquemas no pueden ser demostrados incondicionalmente seguros.
- La seguridad se basa en que ciertos problemas son computacionalmente difíciles de resolver.

3. Pruebas de seguridad rigurosas.

- Enfoque reduccionista: un sistema criptográfico se demuestra (matemáticamente) seguro:
- Para cierta definición de seguridad (principio 1).
- Asumiendo que cierto problema computacional es difícil (principio 2).

Bibliografía.

- N. Smart. “Cryptography, an Introduction”
- J. Katz, Y. Lindell. “Introduction to Modern Criptography”. Chapman & Hall /CRC