# Kerckhoffs y Shannon

*José Galaviz*

## Auguste Kerckhoffs

- Jean Guillaume Auguste Victor François Hubert Kerckhoffs (1835 - 1903). Holandés.
- Profesor de lingüística en École des Hautes Études Commerciales en París.
- En 1883 escribió dos ensayos publicados en *le Journal des Sciences Militaires.*
- *La Cryptographie Militaire.*

## Kerckhoffs (1 - 3)

1. El sistema debe ser prácticamente, si no matemáticamente, indescifrable.
2. El sistema no debe requerir de que su diseño sea secreto para ser seguro.
3. La clave debe ser fácil de comunicar y de recordar sin el auxilio de notas escritas. Debe poder modificarse por acuerdo de las partes.

## Kerckhoffs (4 - 6)

4. Debe poder ser utilizado en comunicaciones telegráficas.
5. Debe ser portátil y no requerir de más de una persona para operarlo.
6. Dadas las circunstancias en las que será usado, el sistema debe ser fácil de usar y no requerir de gran esfuerzo mental ni de recordar una larga serie de reglas de uso.

## El principio de Kerckhoffs

Con frecuencia se sintetiza todo en un único principio:

Un sistema criptográfico debe permanecer seguro a pesar de que todo en él sea de dominio público, salvo **la clave**.

## Corolarios...

El principio 1 señala indirectamente:

- Que la comunicación criptográfica no necesariamente es indescifrable, pero sí que para cuando el criptoanálisis rinda frutos al adversario, ya no sirva de nada.
- Una consecuencia indirecta es que **no se debe subestimar al enemigo**.

El principio 6:

- La seguridad del sistema debe considerar errores u omisiones en su uso.

El 2, 5 y 6:

- Las complicaciones en el método pueden ser puramente ilusorias.
- La seguridad del sistema debe ser juzgada por el criptoanalista y no por el criptógrafo.

El 2:

- El peor mecanismo de seguridad es por obscuridad.

Paráfrasis de Shanon del principio 2:

El enemigo conoce el método de cifrado.

## Claude Elwood Shannon

- Norteamericano, 1916 - 2001.
- Funciones de conmutación y redes de relevadores (1937), Teoría de la información (1948).
- Communication theory of secrecy systems, 1949.

## Dos principios

- Confusión. No hay relación evidente entre el criptograma y el texto claro. El vínculo entre ellos es tan complejo como es posible.
- Difusión. Cada elemento simple del texto claro propaga su influencia a la mayor parte de los elementos del criptograma. Un pequeño cambio en el texto claro acarrea una gran cantidad de cambios en el criptograma. Disipa la estructura estadística del texto claro.

## Dos tipos de operaciones

Dos operaciones criptográficas primitivas:

- Confusión. Por substitución de elementos. Realizada por una *S-box*.
- Difusión. Por permutación, transposición. Realizada por una *P-box*.

Shannon propone el concepto de una red S-P o de substitución-permutación.

## Ataque de criptotexto conocido.

Se poseen uno o varios criptogramas solamente. El objetivo es descifrar los criptogramas y eventualmente obtener la clave.

## Ataque de texto claro conocido

Se posee un criptograma y un fragmento del texto claro que le corresponde. El objetivo es terminar de descifrar y conocer la clave.

## Ataque de texto claro elegido

El criptoanalista puede elegir un texto claro para cifrar y conocer el criptograma resultante. El objetivo es determinar la clave.

## Ataque de texto claro elegido adaptable

El criptoanalista puede escoger el texto a cifrar y luego continuar eligiendo conociendo los criptogramas. El objetivo es conocer la clave.

## Ataque de texto cifrado elegido

Surge en el contexto teórico de la criptografía de llave pública. El criptoanalista elige el texto a descifrar. El objetivo es conocer la influencia de la clave.

## Ataque de clave elegida

El criptoanalista pretende encontrar relaciones entre claves viendo los efectos de estas en el criptotexto.

## Ataque por garrote

El enemigo tortura, chantajea, soborna, amenaza, engaña o seduce a alguien para obtener la clave.