

# Cifrado: introducción

Mikel Egaña Aranguren

[mikel-egana-aranguren.github.io](https://mikel-egana-aranguren.github.io)

[mikel.egana@ehu.eus](mailto:mikel.egana@ehu.eus)



# Cifrado: introducción

<https://doi.org/10.5281/zenodo.4302267>

<https://github.com/mikel-egana-aranguren/EHU-SGSSI-01>



# Introducción

Criptografía: cifrar la información

Mecanismo de seguridad muy antiguo

Asegura: **Confidencialidad, Integridad, Autenticidad**

# Introducción

Criptoanálisis: técnicas para descifrar mensajes encriptados

**Criptología: Criptografía + Criptoanálisis**

# Introducción

Criptoanálisis:

- Sin conocer la clave
- Obteniendo la clave a partir de uno o varios mensajes encriptados
- El algoritmo es público - [Principio de Kerckhoffs \(1883\)](#)

# Introducción

Principios Kerckhoffs:

- Si el sistema no es teóricamente irrompible, al menos debe serlo en la práctica
- **La efectividad del sistema no debe depender de que su diseño permanezca en secreto**
- La clave debe ser fácilmente memorizable de manera que no haya que recurrir a notas escritas

# Introducción

Principios Kerckhoffs:

- Los criptogramas deberán dar resultados alfanuméricos
- El sistema debe ser operable por una única persona
- El sistema debe ser fácil de utilizar

# Introducción

Criptosistema:  $D_K ( E_K ( M ) ) = M$

- M: Conjunto de todos los mensajes sin cifrar
- C: Conjunto de todos los mensajes encriptados (criptogramas)
- K: Conjunto de claves posibles
- E: algoritmo de encriptación
- D: algoritmo de desencriptación



# Introducción: Criptosistemas

**Simétricos o de clave privada:** Una clave para encriptar y desencriptar

**Asimétricos o de clave pública:** Una clave para encriptar y otra para desencriptar (Lo que una encripta, la otra lo desencripta)

# Introducción

Criptografía: **cifrar** la información

Algoritmos hash: **resumir** la información

Esteganografía: **ocultar** la información