

# Zifraketa

Mikel Egaña Aranguren

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

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



# Zifraketa

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

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



# Sarrera

Kriptografia: informazioa zifratu

Segurtasun mekanismo oso zaharra (Aintzinekoa)

**Konfidentzialtasuna, Osotasuna, Kautotzea bermatzen ditu**

# Sarrera

Kriptoanalisia: mezu zifratuak deszifratzeko teknikak

**Kriptologia: Kriptografia + Kriptoanalisia**

# Sarrera

Kriptoanalisia:

- Gakoa ezagutu gabe
- Gakoa mezu zifratu(eta)tik lortuz
- Algoritmoa publikoa da - [Kerckhoffs-en printzipoa \(1883\)](#)

# Sarrera

Kerckhoffs-en printzipoak:

- Sistemak apurtezina izan behar du, teorikoki apurtezina izatea posiblea ez bada, gutxienez praktikan
- **Sistemaren segurtasunak ez du diseinua isilpean gordetzearen mende egon behar. Etsaiaren eskuetara iritsiko balitz, horrek ez luke kriptosistema arriskuan jarri beharko**

# Sarrera

Kerckhoffs-en printzipoak:

- Kriptogramak telegrafo bidez transmititzeko modukoa izan behar du, karaktere alfanumerikoetan idazteko modukoa
- Sistemak (tresnak) eramangarria izan behar du, eta pertsona bakar batek erabiltzeko modukoa
- Sistemak erabilerraza izan behar du; erabiltzaileak jarraitu beharreko agindu-sorta luzerik edota gaitasun intelektual berezirik ez du eskatu behar

# Sarrera

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

- M: zifratu gabeko mezuak
- C: zifratutako mezuak (kriptogramak)
- K: gako posibleak
- E: enkriptazio algoritmoa
- D: desenkriptazio algoritmoa



# Sarrera: Kriptosistemak

**Simetrikoak edo gako pribatukoak:** Gako bakarra enkriptatu eta desenkriptatzeko

**Asimetrikoak edo gako publikokoak:** Gako batek enkriptatu eta beste batek desenkriptatu (Batek enkriptatzen duena, besteak enkriptatzen du)

# Sarrera

Kriptografia: informazioa **zifratu**

Esteganografia: informazioa **ezkutatu**

Hash algoritmoak: informazioa **laburtu**