

Esteganografia

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus



Esteganografia

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

<https://github.com/mikel-egana-aranguren/EHU-ISSKS-31>



Esteganografia

"steganos": ezkutua; "graphos": idazkera

Informazioa ostentzean datza, ikusgarria izateko gakoa dakienarentzat soilik

Gakoa jakin barik, badirudi ez dagoela informazioa ezkutaturik

Kriptografiaren aitzindaria

Esteganografia

Histaiaeo (Mileto-ko gobernatzalea) Dario I errege persiarraren kontra altxatzeko aliatuen bila zebilen

Inork detektatuko ez zituen mezuak bidali behar zituen:

- Mezulariei ilea ebaki
- Buruko azalan mezua idatzi
- Ilea berriro hazi arte itxaron, eta orduan helburura bidali
- Helburuan ilea ebaki eta mezua irakurri

Esteganografia

Bigarren Mundu Gerra

Alemaniarrek mikro puntuak erabiltzen zituzten testuetan informazioa ezkutatzeko, puntuazio-zeinuen itxura emanaz

Esteganografia

Txantiloï batekin

Gakoa forma da



Esteganografia



Esteganografia

Karaktere batzuk hautatuz

Los asirios tenían amarrados los caballos a anclajes mientras los olmecas sólo
ajustaban largos amarres sobre octogonales calesas que se hacían ocultar.

Gakoa: hitz ez-monosilabiko bakoitzaren lehenengo hizkia

Los **A**sirios **T**enían **A**marrados los **C**aballos a **A**ncclajes **M**ientras los **O**lmecas **S**ólo
Ajustaban **L**argos **A**marres **S**obre **O**ctogonales **C**alesas que se **H**icían **O**cultar.

Gaur eguneko esteganografia

Informazio garrantzitsua **fitxategi edukiontzian** txertatzea

- Bit-ak ordezkatzeta
- Bitak amaieran txertatzea, EOF (End Of File) markaren ondoren
- Ezkutatu beharreko informaziotik abiatuta beren-beregi fitxategi edukiontzia sortzea

Bit-ak ordezkatzeta

Informazioa ezkutatzea multimedia artxibotan (normalean irudiak)

BMP formatuan pixel bakoitza RGB-n 3 byte dira

LSB (Less Significant Bit): byte bakoitzaren azken bit-a aldatzeak ez dauka efekturik

Bit-ak ordezkatzeta

Adibidez, testua ezkutatzeko nahi dugun hizkiaren ASCII kodea txertatzen dugu

A → 65 → 01000001

(11011010) (01001001) (01000010)
(00011110) (01011010) (11011110)
(00001110) (01000111) (00000111)

Gaur eguneko esteganografia

- Normalean pasahitzak erabiltzen dituzten programekin
- Nola sendotu sistema?
- Informazioa zifratu txertatu baino lehen (Kriptografia + esteganografia)

Gaur eguneko esteganografia: arazoak

- Fitxategi edukiontzia norbaitek aldatzen badu informazioa gal dezake (adib. JPEG --> BMP --> JPEG)
- Ez ditu **Kautotzea** ezta **Osotasuna** bermatzen (Baina **Konfidentzialtasuna** bai)