Esteganografia

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus

Universidad del País Vasco
Euskal Herriko Unibertsitatea
BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

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 gobernatzailea) 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

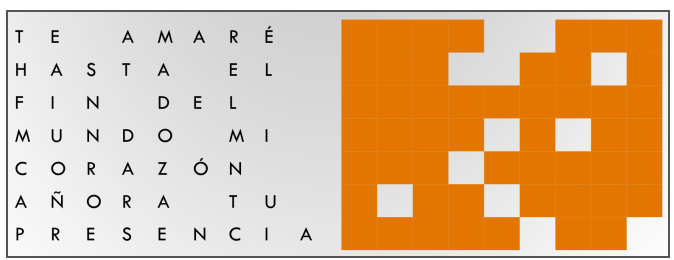
Bigarren Mundu Gerra

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

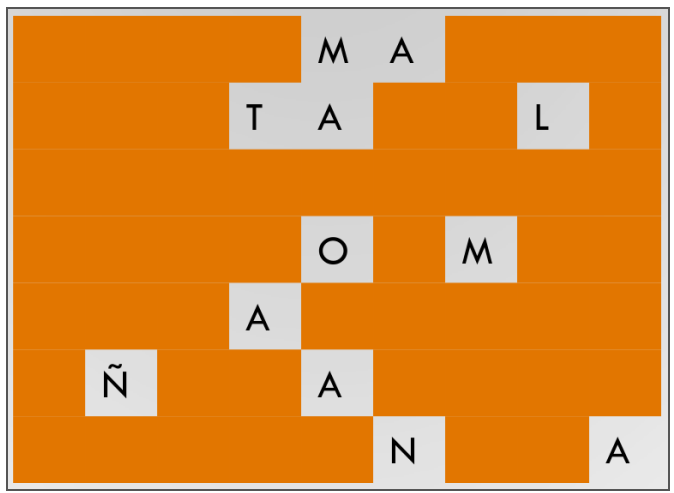
Esteganografia

Txantiloi batekin

Gakoa forma da

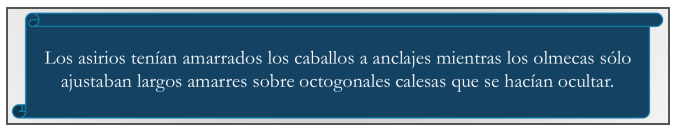


Esteganografia

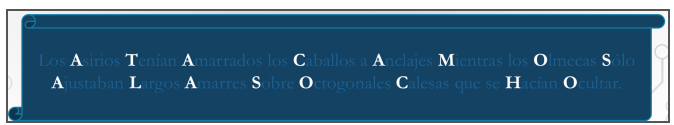


Esteganografia

Karaktere batzuk hautatuz



Gakoa: hitz ez-monosilabiko bakoitzaren lehenengo hizkia



Gaur eguneko esteganografia

Informazio garrantzitsua **fitxategi edukiontzian** txertatzea

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

Bit-ak ordezkatzea

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 ordezkatzea

Adibidez, textua ezkutatzeko nahi dugun hizkiaren ASCII kodea txertatzen dugu

A → 65 → 01000001

(1 1 0 1 1 0 1 **0**) (0 1 0 0 1 0 0 **1**) (0 1 0 0 0 0 1 **0**)
(0 0 0 1 1 1 1 **0**) (0 1 0 1 1 0 1 **0**) (1 1 0 1 1 1 1 **0**)
(0 0 0 0 1 1 1 **0**) (0 1 0 0 0 1 1 **1**) (0 0 0 0 0 1 1 1)

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)