

Zifraketa

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus



Zifraketa

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

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



Aurkibidea

- Sarrera
- Esteganografia
- Enkriptazio metodoak
 - Indarrezko erasoak
 - Laburpen algoritmoak
 - Pasahitzak sistema eragiletan
- Enkriptazio asimetrikoa

Sarrera

Kriptografia: informazioa zifratu

Segurtasun mekanismo oso zaharra (Aintzinekoa)

Bermatzen ditu:

- Konfidentzialtasuna (Zifraketa)
- Osotasuna (Laburpen algoritmoak)
- Kautotzea (Ziurtagarri digitala)

Sarrera

Esteganografia: informazioa **ezkutatu**

Kriptografia: informazioa **zifratu**

Sarrera

Kriptografiaren historia:

- 1948 arte, Kriptografia aurre-zientifikoa
- 1948-an, Claude Shannon-ek Informazioaren Teoriaren eta Kriptografia modernoaren oinarriak ezartzen ditu
- 1976-an Diffie & Hellman-ek gako publikoko Kriptografia kontzeptua plazaratzen dute

Sarrera

Kriptoanalisia: mezu zifratuak deszifratzeko teknikak

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

Kriptologia: Kriptografia + Kriptoanalisia

Sarrera

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

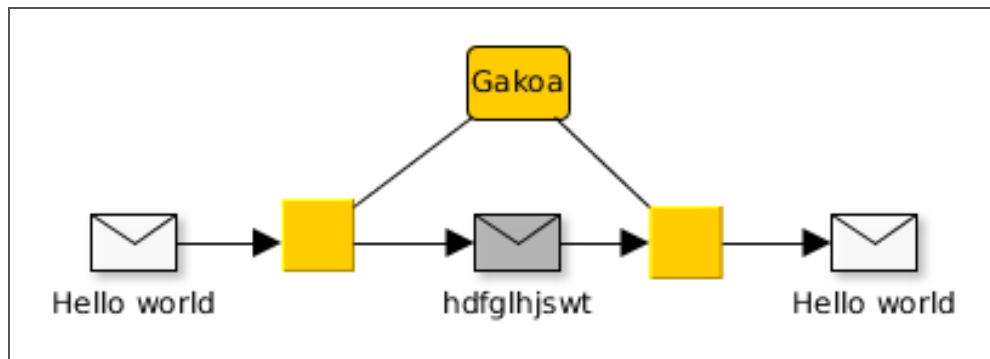
- M: zifratu gabeko mezuak
- C: zifratutako mezuak (kriptogramak)
- K: gako posibleak
- E: enkriptazio algoritmoa
- D: desenkriptazio algoritmoa

Sarrera

Kriptosistemak

- Simetrikoak edo gako pribatukoak
 - Gako bakarra enkriptatu eta desenkriptatzeko
 - Zifratua blokeetan edo fluxu moduan
- Asimetrikoak edo gako publikokoak
 - Gako batek enkriptatu eta beste batek desenkriptatu
 - Gako bikoteak: batek enkriptatzen duena, besteak enkriptatzen du

Gako pribatuko kriptosistemak



Gako pribatuko kriptosistemak

Gako ahulak

- Algoritmo bakoitzaren ezaugarrien arabera agertu daitezke
- Jokaera desegokia duten gakoak
 - $E_K(M)=M$
 - $E_K(E_K(M))=M$
 - $D_{K2}(E_{K1}(M))=M$

Esteganografia

Informazioa ostentzean datza, ikusgarria izateko gakoa dakienarentzat soilik

Gakoa jakin barik, badirudi ez dagoela informazioa ezkutaturik

Kriptografiaren aitzindaria

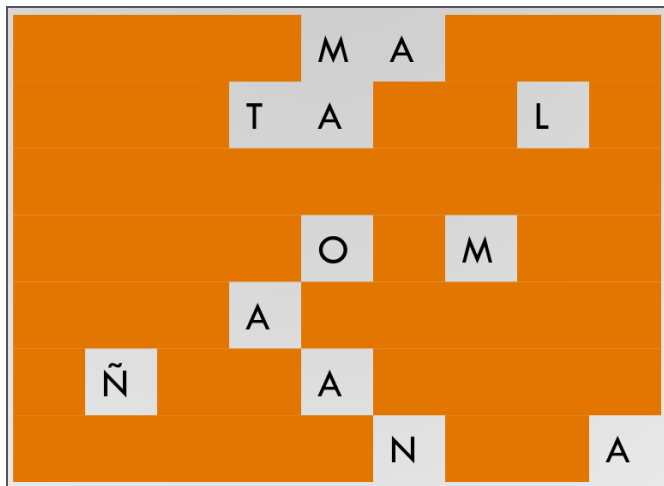
Esteganografia

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



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.

Esteganografia

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

Esteganografia

Adibidez, textua ezkutatzeko nahi dugun hizkiaren ASCII kodea txertatzen dugu

A → 65 → 01000001

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

Enkriptazio metodoak

Helburuak

- Mezua ulertezin bihurtu
- Zifratutako informazioa berreskuratu
- Inplementazioa ahalik eta sinpleena

Enkriptazio metodoak

Oinarrizko teknikak kriptografia klasikoan

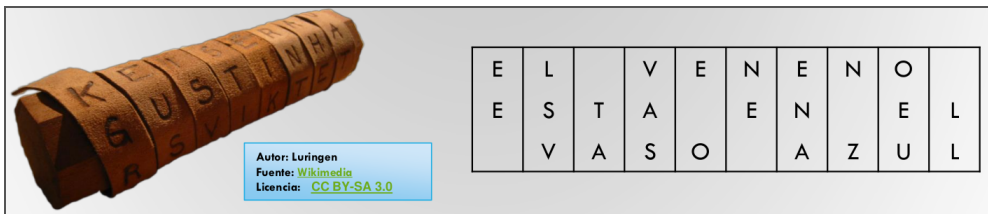
- Transposizioa (jatorrizko hizkiak lekuz aldatzen dira soilik)
- Ordezkapena (jatorrizko hizkiak beste hizkiekin aldatzen dira)

Esparta-ko Escitaloren metodoa

Paper tira bat makila batean kiribildu eta mezua idatzi

Papera askatu eta mezua bidali

Esparta-ko Escitaloren metodoa



EE_LSV_TAVASE_ONE_ENAN_ZOEU_LL

Esparta-ko Escitaloren metodoa

Mezua deszifratzeko makila berdina beharrezkoa da

Paper tira makilaren inguruan kiribildu eta mezua irakurri

Sistema honen gakoa makilaren diametroa da

Escitaloren metodoa 2.0


Mezua zutabetan banatu

Gakoa: zutabe kopurua eta ordena

Escitaloren metodoa 2.0

Clave 32154

1	2	3	4	5
E	L		P	E
R	R	O		D
E		S	A	N
	R	O	Q	U
E		N	O	T
I	E	N	E	
R	A	B	O	.



3	2	1	5	4
	L	E	E	P
O	R	R	D	
S		E	N	A
O	R		U	Q
N		E	T	O
N	E	I		E
B	A	R	.	O

_OSONNBLR_R_EAERE_EIR_EDNUT_.P_AQOEO

Escitaloren metodoa 2.0

Kriptoanalisia

- Konbinatorian oinarritzen da
- Blokeen tamaina kalkulatu
- Blokeak orden ezberdinean konbinatu zentzua duen mezua aurkitu arte

Atbash metodoa (Ispilua)

Zifraketa monoalfabetikoa

Hebrear alfabetotik datorren teknika

Hizki bakoitza bere "aurkakoarekin" aldatu

Atbash metodoa (Ispilua)

a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z
Z	Y	X	W	V	U	T	S	R	Q	P	O	Ñ	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Quedamos a las dos → Jfvwzñlh z ozh wlh

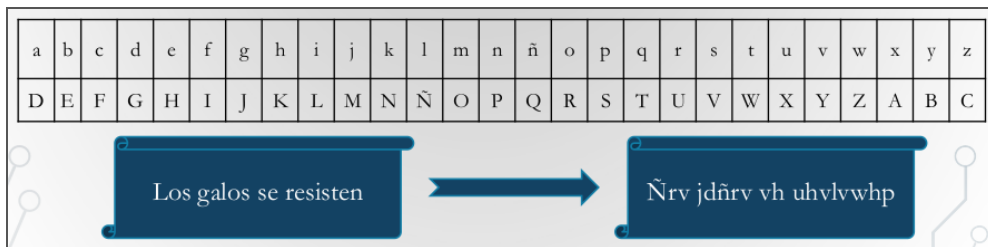
Cesar Metodoa

Zifraketa monoalfabetikoa

Julius Caesar-ek erabilia

Hikzki bakoitzak alfabetoan duen posizioari 3 gehitzean datza

Cesar Metoda



Afin metodoa

Zifraketa monoalfabetikoa

Cesar Metodoaren orokortzea

$$E_{(a;b)}(M) = (aM + b) \bmod N$$

N alfabetoaren hizki zenbakia da

Cesar: afin $E(1,3)$

Hiztegi metodoa

Zifraketa monoalfabetikoa

Korrespondentzien taula "eskuz" sortu

a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z
K	V	D	M	J	L	E	A	N	T	F	Q	X	Z	B	P	Y	R	O	G	C	I	Ñ	S	H	W	U

Desordenado

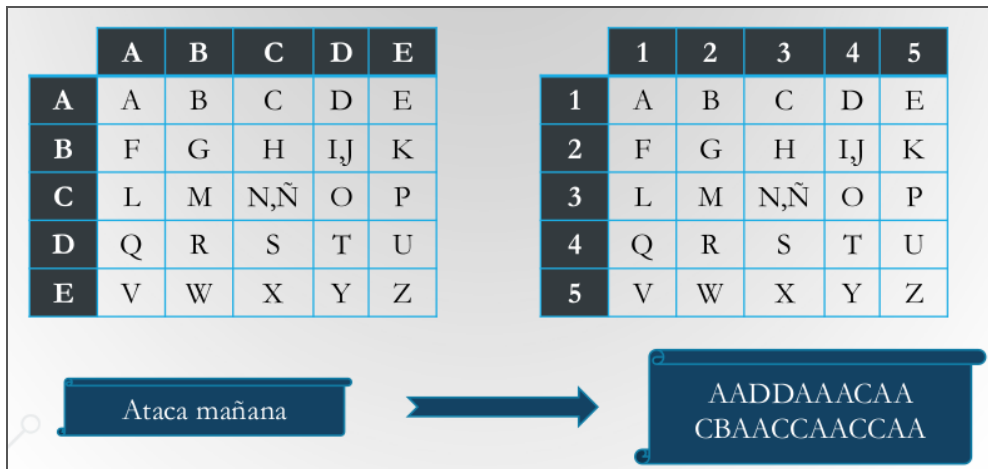
a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z
M	U	R	C	I	E	L	A	G	O	B	D	F	H	J	K	N	Ñ	P	Q	S	T	V	W	X	Y	Z

En base a una palabra

Polybius metodoa

Zifraketa monoalfabetikoa

Zenbakiak edo hizkiak



Ordezkapen metodo monoalfabetikoak

Estatistikan oinarritutako metodoa

Al-Kindi-k 9 mendean sortua

Jatorrizko hizkia beti ordezkutzen da hizki berdinetatik

Hizkuntza bakoitzean badakigu hizki bakoitza zenbat agertzen den

Badakizkigu zeintzuk diren gehien agertzen diren $2/3/4$ hizkiko hitzak
hizkuntza bakoitzean

Ordezkapen metodo monoalfabetikoak

Probak egin, ondorioztatu

Zifratutako textua zenbat eta luzeago, hobeto

Jatorrizko mezuaren textuaren hizkuntza jakin behar dugu

Ordezkapen metodo monoalfabetikoak

Gaztelerazko hizkien portzentaiak

e - 16,78%	r - 4,94%	y - 1,54%	j - 0,30%
a - 11,96%	u - 4,80%	q - 1,53%	ñ - 0,29%
o - 8,69%	i - 4,15%	b - 0,92%	z - 0,15%
l - 8,37%	t - 3,31%	h - 0,89%	x - 0,06%
s - 7,88%	c - 2,92%	g - 0,73%	k - 0,00%
n - 7,01%	p - 2,776%	f - 0,52%	w - 0,00%
d - 6,87%	m - 2,12%	v - 0,39%	

Adibidea: frekuentzien analisisian oinarritutako deszifraketa

Ordezkapen metodo monoalfabetikoak

Kriptoanalisia zailtzeko metodoak

- Hutsuneak kendu
- Jatorrizko textua aldatu, esanahia mantenduz (Adib. SMS, WhatsApp, ...)
- Esanahia duten piktogramak erabili (kodeen liburua)
- 1-1 korrespondentzia ekidin, hizki berdina behin baino gehiagotan erabiliz
(Sistema Polialfabetikoak)

Alberti-ren diskoa

Lehenengo sistema polialfabetikoa

Bi disko zentrokide, barrukoa mugikorra

Zifraketan barrukoa mugitzen doa, X alfabeto (Korrespondentzia) ezberdin erabiltzen dugularik

Gakoa jatorrizko posizioa da, zenbat hizki pasa ondoren biratzen den diskoa, zenbat biratzen den diskoa, eta zein zentzutan

Alberti-ren diskoa

The Alberti and Jefferson Code Disks



Enigma makina

Historia osoko elementu kriptografiko ezagunena

Jatorrian gizartean erabiltzeko

Erabilera militararako eraldatua, batez ere Naziak

Enigma makina

158,962,555,217,826,360,000 (Enigma Machine) - Numberp...



Enigma makina

Marian Rejewski matematikari poloniarrek Enigma desenkriptatzeko oinarriak ezarri zituen:

- "Bonba" deituriko makina elektromekanikoak
- Nazi-ek 2 gurpil gehitu zioten Enigmari eta "Bonbak" ez ziren gai

Enigma makina

[Alan Turing](#)-en taldea informazio horretatik abiatuz "bonba" berriak sortu zituen

Flaw in the Enigma Code - Numberphile

