

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

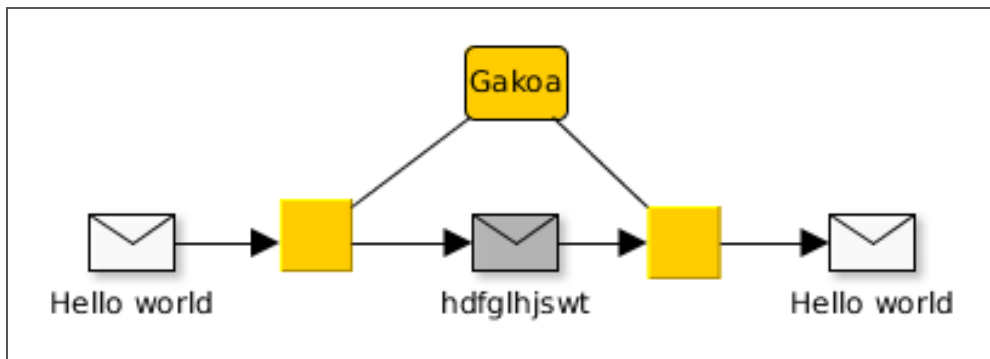
- M: zifratu gabeko mezuak
- C: zifratutako mezuak (kriptogramak)
- K: gako posibleak
- E: enkriptazio algoritmoa
- D: desenkriptazio algoritmoa

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 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

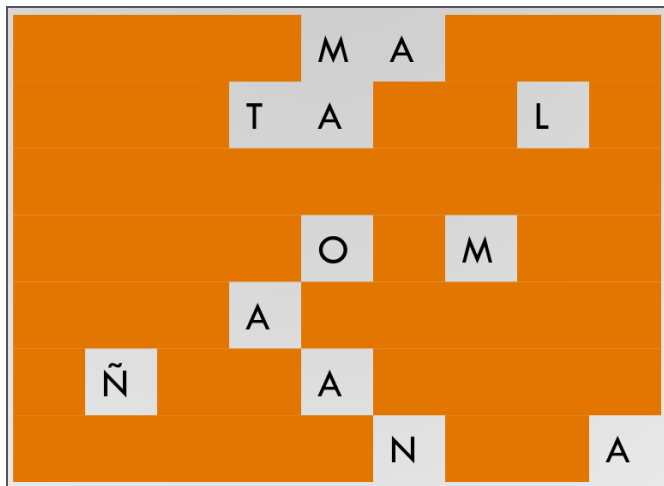
Esteganografia

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.

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

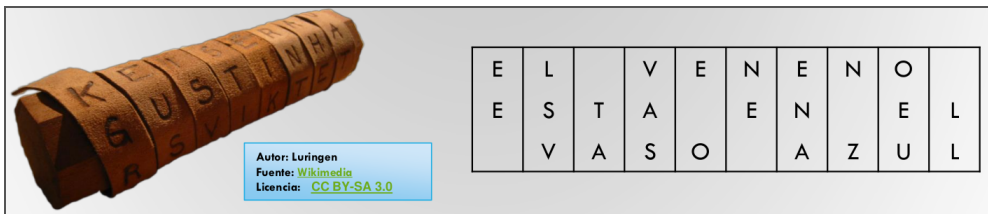
- Transposizioa (jatorrizko hizkiak lekuz aldatzen dira soilik)
- Ordezkapena (jatorrizko hizkiak beste hizkiekin aldatzen dira)

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 berdin-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 Metodoa

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
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Los galos se resisten → Ñrv jdñrv vh uhvhwph

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

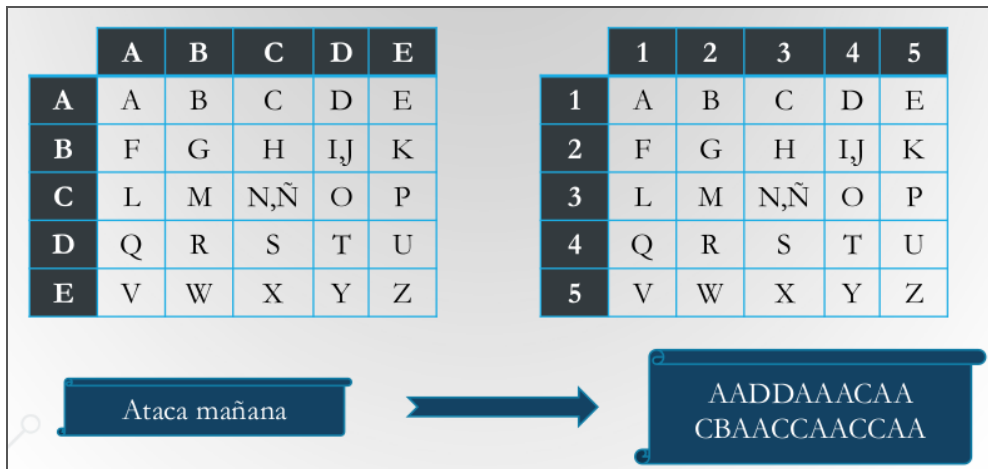
a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z
M	U	R	C	I	E	L	A	G	O	B	D	F	H	J	K	N	Ñ	P	Q	S	T	V	W	X	Y	Z

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



Ordezkapen metodo polialfabetikoak

Kriptoanalisia

- Metodo estatistikoak
- Gakoen tamaina txikitzeko patroiak, zati ezberdinen ordena, etab. bilatzen dira
- Sistema monoalfabetikotan baino textu zifratu gehiago behar da

Fluxu zifraketa metodoak

Mezu osoa zifratu ordez, bit bakoitza zifratzen dute, banan-bana

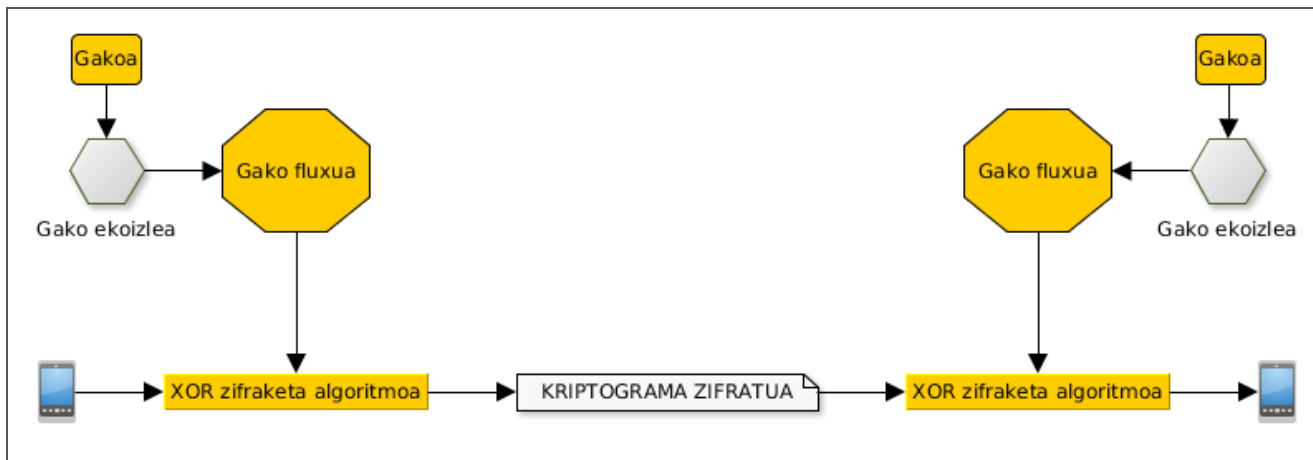
Denbora errealeko komunikaziotan erabilia (Ezin da itxaron mezu osoa izan arte zifratzeko eta bidaltzeko)

Fluxu zifraketa metodoak

Gakotik abiatuta, ekoizle sasi-aleatorioa erabiltzen da gako-fluxua sortzeko

Kriptograma sortzeko XOR eragiketa egiten da zifratu behar den bit-a eta gako-fluxuaren artean

Fluxu zifraketa metodoak



Vernam metodoa

XOR eragiketa textua eta luzera berdineko gakoa aleatorio baten artean egiten du (Ekoizlea benetan aleatorioa da)

Gakoa (gako-fluxua) "erabilpen bakarreko libreta" da:

- Behin bakarrik erabili ahal da
- Mezu irakurleari aurretik bidali behar zaio
- Matematikoki frogatua dago apurtezina dela

Beste fluxu zifraketa metodoak

Vernam-en metodoan oinarrituak

Gako pseudo-aleatorioak erabiltzen dituzte, hazi batetik eta ekoizpen algoritmo batetik sortuak

Hazia eta ekoizpen algoritmoa jakinda, gako pseudo-aleatorioa bereraikitzea dago (Hazi posible ezberdinen kopuruaren arabera)

Beste fluxu zifraketa metodoak

Ez dira matematikoki apurtezinak

Adibideak:

- RC4 (ARC4): TLS/SSL , WEP eta WPA-an (Apurtua)
- A5/1: GSM-an (A5/1 eta A5/2 apurtuak)

Blokeka zifratzeko metodoak

Jatorrizko mezua tamaina berdinetko blokeetan zatitu:

- Blokeen tamaina oso txikia bada, fluxu zifraketa da
- Mezuaren tamaina ez bada blokeen multiploa, badaude algoritmoak gainerakoa betetzeko

Blokeka zifratzeko metodoak

Jatorrizko bloke bakoitzak zifratutako bloke bat sortzen du

Blokeen arteko iterazioak, permutazioak eta beste operazioak gehitu daitezke

Blokeka zifratzeko metodoak

DES (Data Encryption Standard) - 1975:

- 64 bit-eko blokeak
- 56 biteko gakoak
- 16 itzuli

Blokeka zifratzeko metodoak

Triple DES - 1998: DES hiru aldiz (Zifratu – Deszifratu - Zifratu):

- 2 gako erabili: $(E_{k_1} (D_{k_2} (E_{k_1})))$
- 3 gako erabili: $(E_{k_1} (D_{k_2} (E_{k_3})))$
- Kreditu txarteletan oso erabilia

Blokeka zifratzeko metodoak

IDEA - 1991:

- 64 bit-eko blokeak
- 128 biteko gakoak
- 8 itzuli

Blokeka zifratzeko metodoak

KASUMI (A5/3) – 2000:

- 64 bit-eko blokeak
- 128 biteko gakoak
- 8 itzuli
- 3G sareetan erabilia

Blokeka zifratzeko metodoak

AES (Advanced Encryption Standard) - 2001:

- Erabilera oso hedatua
- 128 bit-eko blokeak
- 128, 192, 256 biteko gakoak
- 8 itzuli, 12 itzuli, 14 itzuli

Blokeka zifratzeko metodoak

4G sareak:

- Algoritmo bikoteak (bat apurtzen bada, besteak dirau)
- EEA atzizkia Konfidentzialtasuna bermatzen duten algoritmoentzako
- EIA atzizkia Osotasuna bermatzen duten algoritmoentzako

Indarrezko erasoak

Beti aurkitzen dute soluzioa

Gako posible guztiak probatzean datza

Gako espazioa eta zifraketa algoritmoa ezagunak izan behar dira

Beti ez dira posible, denbora-kostua medio adibidez

Indarrezko erasoak

Gako espazioa:

- 56 bit: 2^{56} aukera
- 128 bit: 2^{128} aukera
- 256 bit: 2^{256} aukera

Indarrezko erasoak

Super-ordenagailu batekin:

- 56 bit: 0,04 segundu
- 128 bit: 7.193.522.047 milurte
- 256 bit: ...

Indarrezko erasoak

Erasoa inteligenteagoa egin ahal da:

- Hiztegia bat erabiliz
- Gakoaren jabearen datuekin
- ...

Laburpen algoritmoak

Dispersio funtzioak (one-way hash)

Tamaina finkoko kriptograma sortzen dute, jatorrizko eduki osoa ordezkatzeko duena (edukia apur bat aldatzen bada ere, laburpena guztiz aldatzen da)

Ez dauka alderantzizko funtziorik

Ezin da deszifratu

Laburpen algoritmoak

Erabilpenak:

- Informazioaren Osotasuna ziurtatu
- Gakoak gorde
- Sinadura digitala implementatu

Laburpen algoritmoak

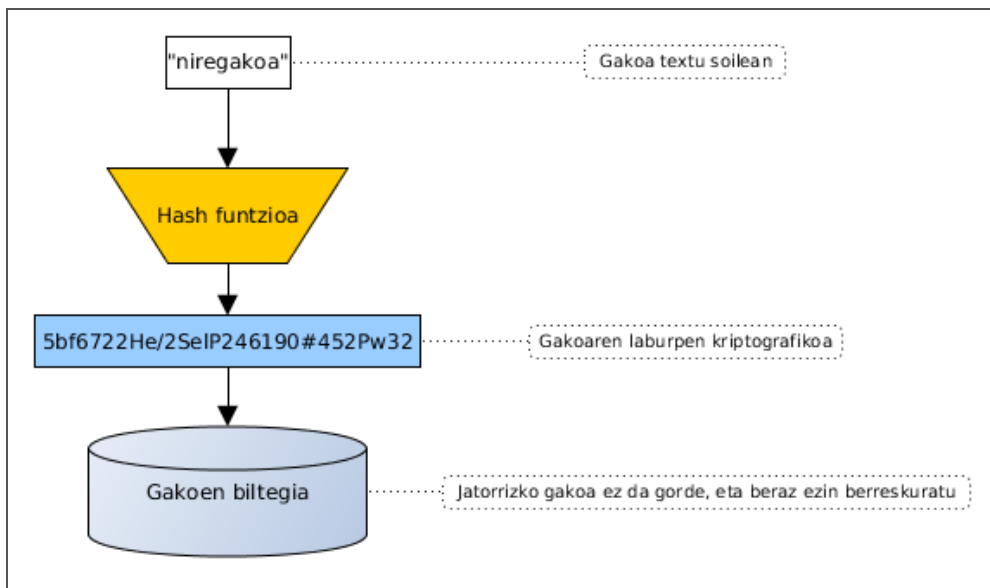
Informazioaren Osotasuna ziurtatu

<http://ftp.mozilla.org/pub/mozilla.org/xulrunner/releases/2.0/MD5SUMS>

```
5acef7cc816691f5c8726731ee0d8bdf ./runtimes/xulrunner-2.0.en-US.linux-i686.tar.bz2
cb0dc6ff5304b325098fc8910057884f ./runtimes/xulrunner-2.0.en-US.linux-x86_64.tar.bz2
aa40c07c8669a04170c7501023133acb ./runtimes/xulrunner-2.0.en-US.mac-pkg.dmg
38e5c5ad08927278ed6c333aef836882 ./runtimes/xulrunner-2.0.en-US.win32.zip
1ec6039ee99596551845f27d4bc83436 ./sdk/xulrunner-2.0.en-US.linux-i686.sdk.tar.bz2
101eb57d3f76f77e9c94d3cb25a8d56c ./sdk/xulrunner-2.0.en-US.linux-x86_64.sdk.tar.bz2
cf56e216a05feed16cb290110fd89802 ./sdk/xulrunner-2.0.en-US.mac-i386.sdk.tar.bz2
ac2ddb114107680fe75ee712cddf1ab4 ./sdk/xulrunner-2.0.en-US.mac-x86_64.sdk.tar.bz2
5cfa95a2d46334ce6283a772eff19382 ./sdk/xulrunner-2.0.en-US.win32.sdk.zip
0f4876068fa922498d62abf7d293c9c4 ./source/xulrunner-2.0.bundle
a3b387489ba1738ea504e83cb811c82a ./source/xulrunner-2.0.source.tar.bz2
```

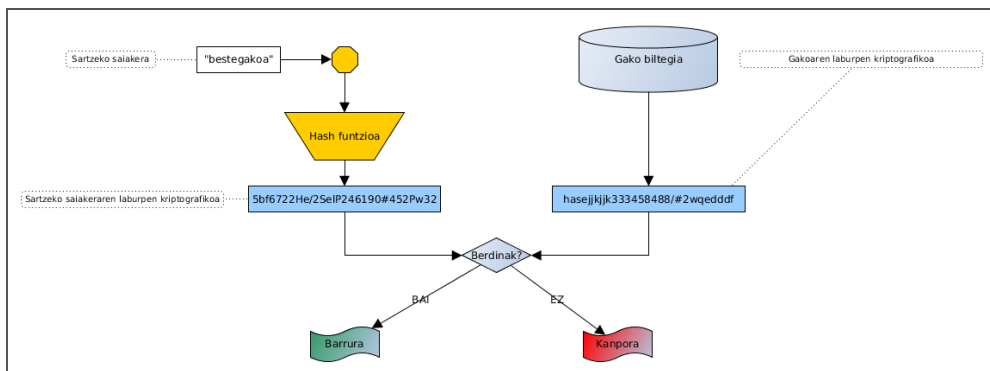
Laburpen algoritmoak

Gakoak gorde



Laburpen algoritmoak

Identifikatu



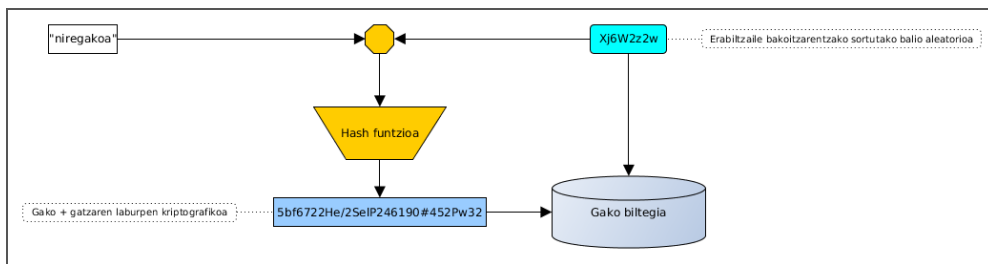
Laburpen algoritmoak

Arazoak

- Gako berdinek hash berdina sortuko dute
- Gako espazioko Hash guztiak pre-kalkulatu daitezke

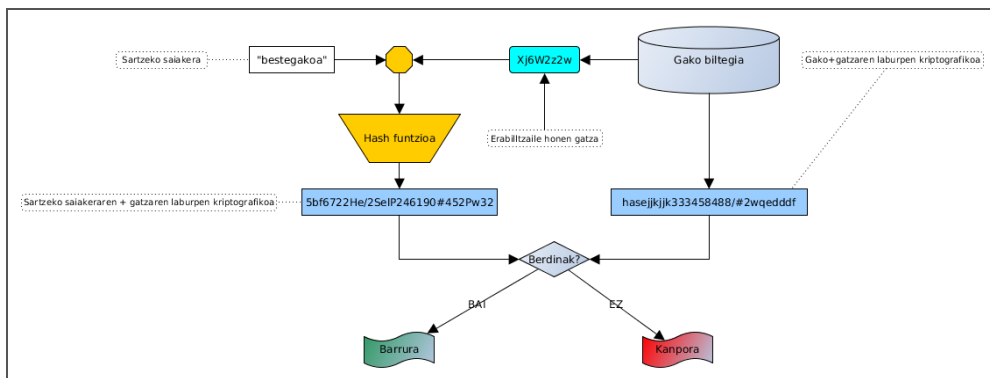
Laburpen algoritmoak

Soluzioa: "gatza" (Salt) edo hazia erabiltzea



Laburpen algoritmoak

Identifikazioa gatzaren gehituta



Laburpen algoritmoak

Gatza erabiltzearen abantailak

- Gakoa berberak kodifikazio ezberdina du aldi bakoitzean
- Indarrezko erasoak zailago egiten ditu

DB-a gakoekin eta gatzarekin lapurtzen badute, ez dago zereginik

Laburpen algoritmoak

Erabiliak:

- MD5
- SHA-1

Laburpen algoritmoak

Arazoak

- Talkak: bi testu ezberdinek laburpen berdina sortzea
- Algoritmoa ahultzen duten erasoak

Soluzioak

- Laburpen luzeagoak sortzen dituzten algoritmoak erabili
- SHA-224, SHA-256, SHA-384, SHA-512, ...

Pasahitzak sistema eragileetan

Linux:

- Kokapena: /etc/shadow
- Ikusteko: `sudo cat /etc/shadow`
- Formatua:

user:\$Erabilitakoalgoritmoa\$gatza\$LaburpenKriptografikoa:A:B:C:D:E:F:

Pasahitzak sistema eragileetan

Linux:

- Erabilitako algoritmoa: 1: MD5; 2: Blowfish; 3: NT; 5: SHA-256; 6: SHA-512
- Gatza: kate aleatorioa

Pasahitzak sistema eragileetan

Linux:

- A: zenbat egun pasa diren gakoak aldatu gabe (1970/01/01-tik)
- B: zenbat egun gakoak aldatu ahal izateko
- C: zenbat egun egon ahal den gakoak aldatu gabe

Pasahitzak sistema eragileetan

Linux:

- D: zenbat egun aurretik abisatu behar zaio erabiltzaileari pasahitza aldatzeko
- E: zenbat egun pasahitza iraungitzetik kontua desaktibatu arte
- F: zenbat egun kontua desaktibatu arte (1970/01/01-tik)

Klabe publikoko kriptografia

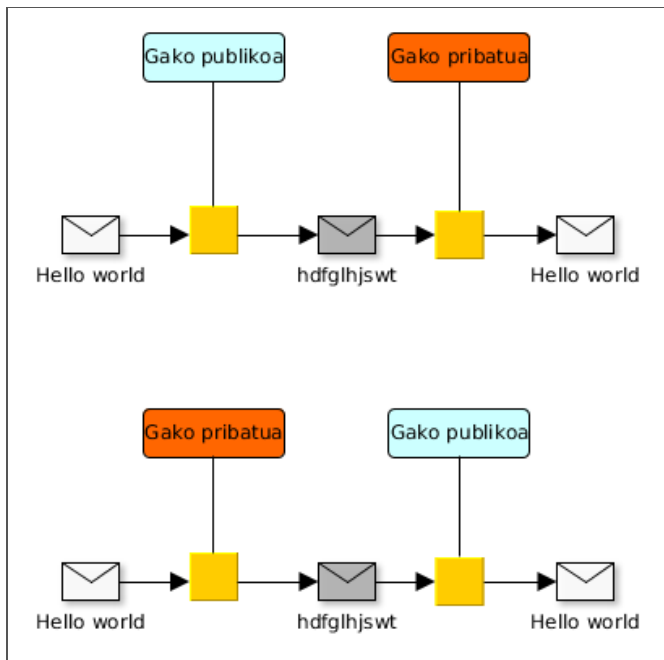
Gako asimetrikoko algoritmoak: zifratzen duen klabea ez da deszifratzen duena

Erabiltzaile bakoitzak bi klabe:

- Gako publikoa, mundu osoak ezagutzen duena
- Erabiltzaileak soilik ezagutzen duen gako pribatua

Gako batek zifratzen duena besteak deszifratzen du

Klabe publikoko kriptografia



Klabe publikoko kriptografia

- Ikerrek bere gako pribatua du, I_{pri} , eta mundu guztiak bere gako publikoa du, I_{pu}
- Mirenek bere mezua zifratzen du Ikerren gako publikoa erabiliz: $c = e (m , I_{pu})$
- Mirenek c kriptograma Ikerreri bidaltzen dio
- Ikerrek c jasotzen du
- Ikerrek c deszifratzen du bere I gako pribatua erabiliz: $m = d (c , I_{pri})$
- Konfidentzialtasuna. Ikerrek soilik deszifratu dezake mezua

Klabe publikoko kriptografia

Abantailak:

- Jasotzaileak soilik irakur dezake mezua
- Gako bakarra gorde behar da
- Edozeinek erabili dezake gako publikoa mezu konfidentziala bidaltzeko

Ikerreri

- Gako publikoa komunikatzeko ez dira beharrezkoak kanal seguruak

Klabe publikoko kriptografia

Arazoak:

- Gako pribatua pribatua mantendu behar da
- Gako publikotik gako pribatua ondorioztatzea ia ezinezkoa izan beharko litzateke
- (Des)zifraketa sistema simetrikotan baino geldoagoa da

Klabe publikoko kriptografia

Arazoak:

- Mirenek segurtasun osoz jakin behar du lkerren gako publikoa erabiltzen dagoela
- Gako publikoak lortzea erraza izan behar du

Klabe publikoko kriptografia

Erabiltzaile bakoitzak bere gako bikotea sortzen du (gako publikoa, gako pribatua) eta gako publikoa gakoaren zerbitzari batean argitaratzen du: Key Certification Authority edo Key Distribution Center (KDC)

Klabe publikoko kriptografia

Arazo gehiago:

- Nola daki Ikerrek mezua benetan Mirenena dela?
- Ikerrek erantzuten duenean, nola daki Mirenek benetan mezua Ikerrena dela?

Klabe publikoko kriptografia

- Ikerrek zifratzen badu bere gako pribatuarekin edonork deszifratu ahal du (Mundu osoak ezagutzen du I_{pu})
- Soluzioa:
 - Ikerrek bere gako pribatuarekin zifratzen du mezua: $C1 = e (m, I_{pri})$
 - Gero Mirenen gako publikoarekin berriro zifratzen du: $C2 = e (C1 , M_{pu})$

Klabe publikoko kriptografia

- Mirenek bakarrik deszifratu ahal du bere gako pribatuarekin:
 - Konfidentzialtasuna: Mirenek soilik deszifratu ahal du mezua: $C1 = d (C2, M_{pri})$
 - Kautotzea eta Zapuztezintasuna: Ikerrek soilik bidali ahal izan du mezua: $m = d (C1, I_{pu})$

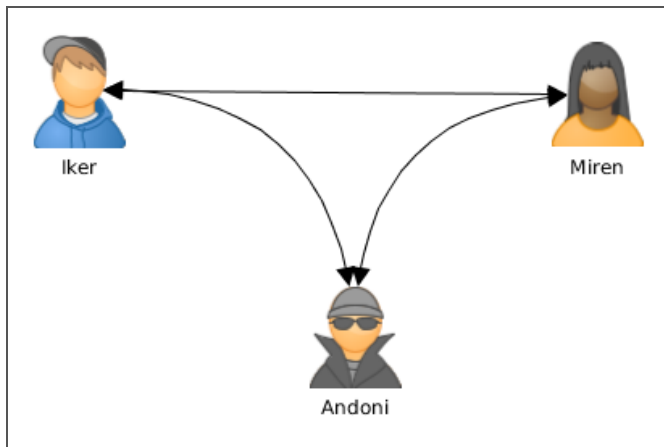
Klabe publikoko kriptografia

Zer gertatzen da baten bat komunikazio erdigunean jartzen bada

Man in the middle eraso:

- Bitartekari batek mezu guztiak jasotzen ditu partaideak jakin barik
- Partaideen komunikazio guztietan eskua sartu behar da

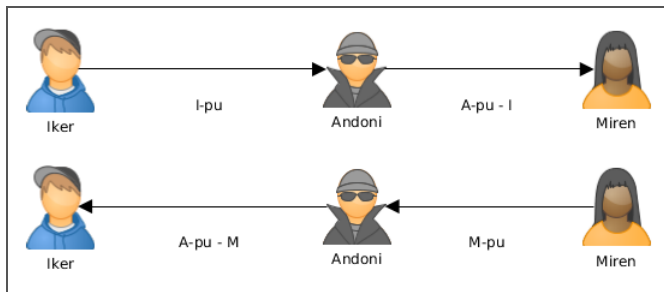
Klabe publikoko kriptografia



Klabe publikoko kriptografia

Ikerrek eta Mirenek komunikatzen hasi nahi dutenean, klabe publikoak trukatzeko dituzte

Andonik hartzen ditu eta bere klabearekin aldatzen ditu

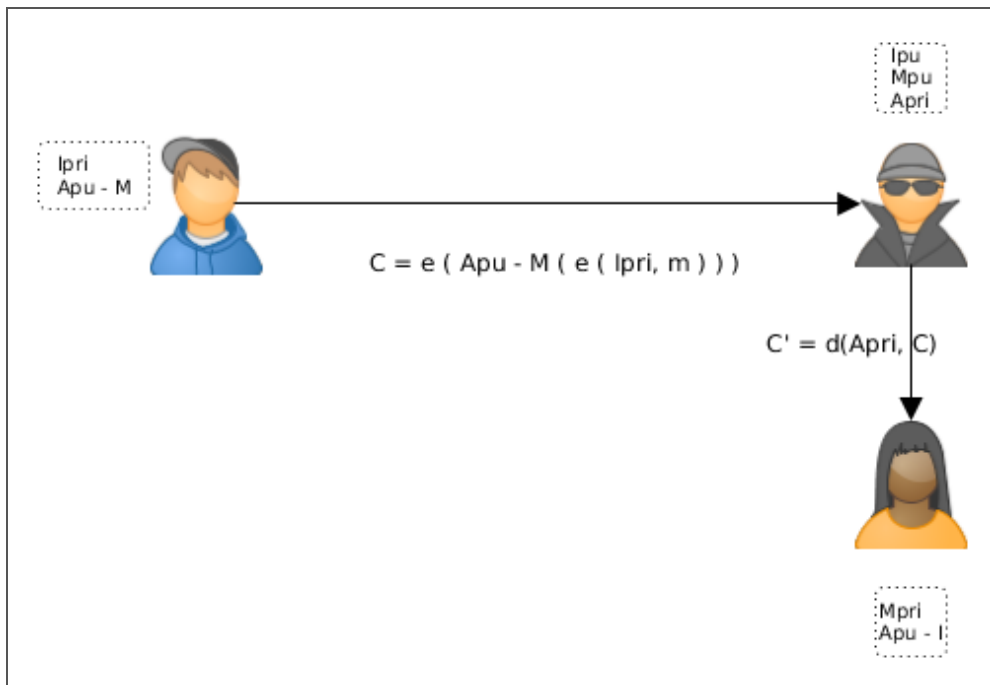


Klabe publikoko kriptografia

Ikerrek eta Mirenek mezuak zifratzen dituzte ustezko bestearen klabe publikoarekin eta beraien klabe pribatuarekin

Andonik mezuak jasotzen ditu, irakurtzen ditu, aldatzen ditu, eta bere klabe pribatuarekin zifratzen ditu

Klabe publikoko kriptografia



Klabe publikoko kriptografia

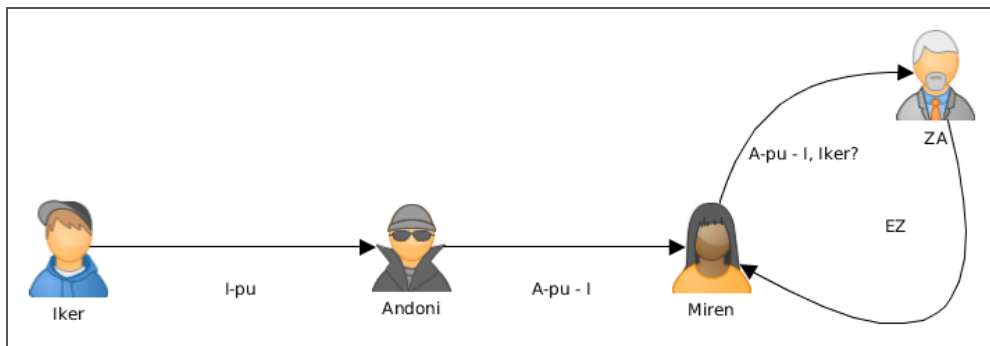
Ikerrek eta Mirenek modu seguruan komunikatzen ari direla uste dute

Andonik dena irakurtzen du eta nahi beste aldatzen

Ekiditeko:

- Klabeak kanal seguru bidez elkarbanatu
- Autoritate (erakunde) batek klabe publiko bat norbaiti dagokiola zertifikatzea: Zertifikazio Autoritatea

Klabe publikoko kriptografia



Zifratu hibridoa

Gako pribatuko sistemak gako publikokoak baino askoz azkarragoak dira

Askotan konbinazio bat erabiltzen da: gako publikoko sistema S gako sekretu bat elkarbanatzeko erabiltzen da, behin soilik erabiliko dena

Gako pribatuko sistemak S erabiltzen du mezua zifratzeko

Zifratu hibridoa

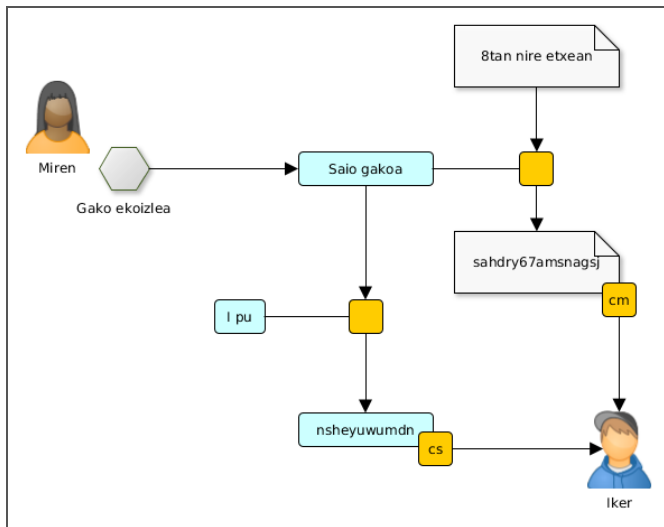
Mirenek S gako sekretua sortzen du, eta bere mezua zifratzeko erabiltzen du:

$$cm = e_1(m, S)$$

Mirenek S zifratzen du Ikerren gako publikoarekin: $cs = e_2(S, I_{pu})$

Mirenek $[cm, cs]$ bidaltzen dio Ikerreri

Zifratu hibridoa



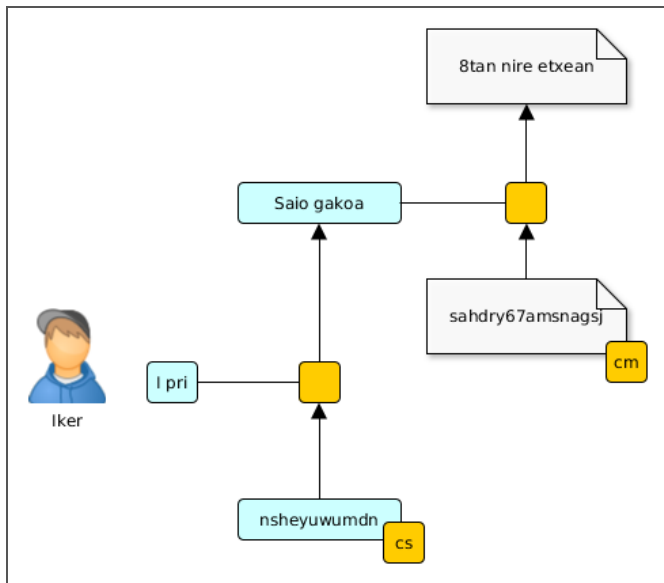
Zifratu hibridoa

Ikerrek [cm , cs] jasotzen du

Ikerrek S deszifratzen du bere gako pribatua erabiliz, $I_{pri}: d2 (cs , I_{pri}) = S$

Ikerrek S erabiliz m deszifratzen du: $d1 (cm , S) = m$

Zifratu hibridoa



Sinadura digitala

Mirenek Ikerreri mezua bidaltzen dio, gako publikoko sistema erabiliz

Edonork ezin du irakurri Mirenen Ikerrentzako mezua, baina edozeinek bidali ahal du

Nola daki Ikerrek Mirenek bidali diola edo inork ez duela mezua aldatu?

Soluzioa: Mirenek mezua sinatzen du

Sinadura digitala

Erabiltzaile zilegiak soilik sinatu ahal du bere dokumentua

Inork ezin du sinadura faltsutu

Edozeinek balioztatu ahal du sinadura digitala

Sinadura digitala

Ezin da sinadura bat berrerabili

Ezin da sinadura bat aldatu

Ezin da dokumentu bat sinatu izana ukatu

Ezin da dokumentu bat aldatu sinatu ostean

Kautotzea, Osotasuna eta Zapuztezintasuna

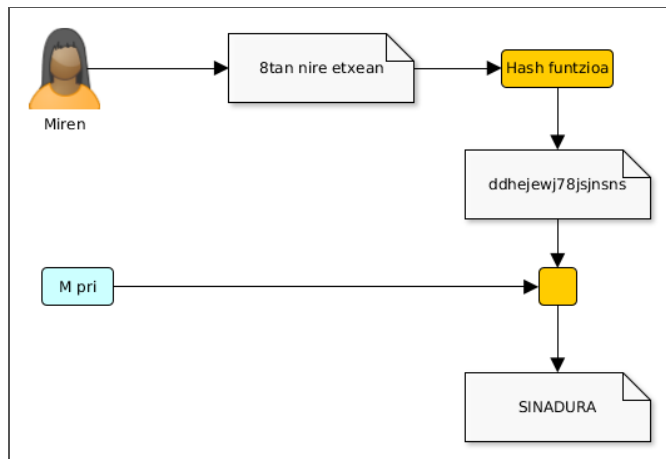
Sinadura digitala

Mirenek mezuaren laburpen kriptografikoa lortzen du: $RC = \text{hash}(m)$

Mirenek bere klabearekin zifratzen du laburpen kriptografikoa: $\text{Sinadura} = e(RC, M_{\text{pri}})$

Mirenek bere mezua (Zifratua edo zifratu gabe) eta bere sinadura bidaltzen ditu

Sinadura digitala



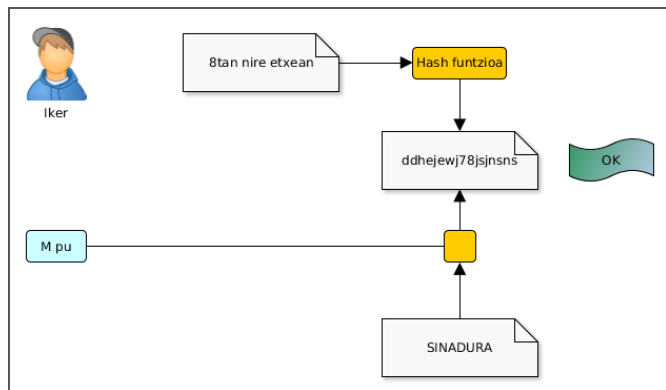
Sinadura digitala

Ikerrek sinadura deszifratzen du Mirenen gako publikoa erabiliz: $RC = (\text{Sinadura}, M_{pu})$

Ikerrek mezuaren laburpen kriptografikoa lortzen du: $RC' = \text{hash}(m)$

Ikerrek RC' eta RC alderatzen ditu ezer aldatu ez dela baieztatzeko

Sinadura digitala



Sinadura digitala

Sinatzeaz gain, Mirenek mezua zifratzen badu, Ikerrek bakarrik irakurriko du:

Konfidentzialtasuna, Osotasuna, Kautotzea, Zapuztezintasuna

Hurrengoak erabiltzea dauka:

- Kriptografia asimetrikoa
- Kriptografia hibridoa

Sinadura digitala

Kriptografia asimetrikoa. Ikerreri bidali:

- Mezu zifratuaren kriptograma (M_{pri} eta I_{pu} -rekin zifratua)
- Bere sinadura digitala (Laburpen kriptografikoa, M_{pri} -rekin zifratua)

Sinadura digitala

Kriptografia hibridoa. Ikerreri bidali:

- Saio gakoarekin zifratutako mezuaren kriptograma
- Saio gako zifratuaren kriptograma, I_{pu} -rekin zifratua
- Bere Sinadura digitala (Laburpen kriptografikoa, M_{pri} -rekin zifratua)

Gako publikoko algoritmoak

Diffie-Hellman - 1976

RSA - 1977

ElGamal - 1984

DSA - 1991

Kurba eliptikoak - 1985

Gako publikoko algoritmoak

Elliptic Curve Cryptography & Diffie-Hellman



Gako publikoko algoritmoak

Encryption and HUGE numbers - Numberphile



Gako publikoko algoritmoak

DNI elektronikoa (DNle 3.0):

- RSA
- SHA-1 / SHA-256
- TripleDES / AES

Gako publikoko algoritmoak

PGP:

- RSA / DSA
- IDEA / TripleDES

Gako publikoko algoritmoak

SSH:

- RSA / DSA

SSL / TLS:

- RSA / DSA / Diffie-Hellman
- IDEA / DES / TripleDES / AES

Sinaduren konfidantza

Sinadura digitalak erabilita ere:

- Nola dakigu sinadura bat esaten duenarena dela?
- Nola bermatzen du Zertifikazio Autoritate batek hori horrela dela?
- Ezin gara fidatu Zertifikazio Autoritate batek bermatu duen sinadura batetaz?

Sinaduren konfidantza

- PGP, GnuPG eta horrelakoak erabiltzen dira
- Erabiltzaile batek bermatzen du, bere gako pribatuarekin sinatuz, beste erabiltzaile baten gako publikoa fidagarria dela
- Konfidantza hedatzen doa, gakoak sinatzen dituzten erabiltzaileei ematen diegun konfidantzaren arabera

Konfidantza mailak

- Ezezaguna: erabiltzaile horrek sinatzen duenaz ez gara fidatzen (ezezaguna delako)
- Eza: erabiltzaile horrek sinatzen duenaz ez gara fidatzen (Badakigulako txarto egiten duela)
- Marginala: konfidantza marginala duten bi erabiltzailek sinatutako klabeengan konfidantza dugu
- Osoa: Erabiltzaile horrek sinatzen duen guztiaz fidatzen gara

Ziurtagiri digitalak

- Ziurtagiri digitala: konfidantzazko erakunde batek erabiltzaile baten gako publikoa sinatzea, bere gako pribatuarekin
- Erabiltzailea berak esaten duena dela bermatzeko balio du
- Bermea ematen duen erakundearenganako konfidantzaren arabera

Ziurtagiri digitalak

- X.509 estandarra
- Baliozkotasuna != konfidantza
 - Baliozkotasuna: sinadura baten eskakizunak betetzen ditu (iraungipena, etab.)
 - Konfidantza: sinadura horretaz fida gaitezke
- Sinadura batek baliozkotasuna eduki dezake, baina ez konfidantza
- Konfidantza duen baliogabeko sinadura batek ez dauka zentzurik

Ziurtagiri digitalak

Zertifikazio Autoritate batek sinadura baten baliozkotasuna bermatzen du

- Ziurtapen-zerbitzuen emaileak (PSC): Ley de Firma Electrónica (Ley 59/2003, LFE), Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (Ley 11/2007, LAESCP)
- PSC-ak beraien ziurtagirien indarraldia kontsultatzeko metodo bat eman behar dute: erakunde publikoen kasuan musutruk izan behar du

Ziurtagiri digitalak

Zertifikazio Hierarkia (RFC 1422)

Internet Policy Registration Authority (IPRA) >> Policy Certification

Authorities (PCA) >> Certification Authorities (CA): Verisign, Thawte, GeoTrust,
RapidSSL, DigiCertSSL

CA (Zertifikazio Autoritate) batek

- Distinguished Name eta CA subordinatuak gordetzen dituen DB-a
- Ziurtagirien baliogabetzea:
 - Erabiltzailearen klabe pribatua konprometitua
 - CA ziurtagiri bat okerreko norbaiteri eman dio
 - Erabiltzaileak CA-z aldatzen du
 - CA-aren segurtasuna apurtua
- CRL, Certification Revocation List: adibidez [GeoTrust](#)

CA (Zertifikazio Autoritate) batek

- OCSP (Online Certificate Status Protocol RFC 2560) protokoloak ziurtagiri baten egoera online balioztatzea bermatzen du
- CRL-ak baino eraginkorragoa da
- Abantaila: beti eguneratua
- Desabantaila: konprobatzeko konektatu behar

Ziurtagiri digitalak

Zerbitzua ematen duen CA bakoitzak OCSP zerbitzari bat mantentzen du

Eskakizun egokia egiten duten bezeroei erantzuten die

Ziurtagiri digitalak

Gako publikoko ziurtagiri motak:

- Autoritate ziurtagiriak
- Zerbitzari ziurtagiriak
- Ziurtagiri pertsonalak
- Software ziurtagiriak

Ziurtagiri digitalak

Ziurtagiri baten osagarriak:

- Bertsioa
- Serie zenbakia
- Sinadura algoritmoaren identifikatzailea
- Iraungipena
- ...

Ziurtagiri digitalak

- Konfidentzialtasuna informazioa enkriptatuz
- Informazioaren osotasuna hash eta sinadura bidez
- Kautotzea informazioa sinatua datorrelako
- Zapuztezintasuna informazioa sinatzean

Kriptografia kuantikoa

Quantum Cryptography in 6 Minutes

