

Zifraketa sarrera, esteganografia, laburpen algoritmoak

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus

Zifraketa sarrera, esteganografia, laburpen algoritmoak

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

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



Zifraketa sarrera, esteganografia, laburpen algoritmoak

- Zifraketa sarrera
- Esteganografia
- Laburpen algoritmoak

Zifraketa sarrera

Kriptografia: informazioa zifratu

Segurtasun mekanismo oso zaharra (Aintzinekoa)

Konfidentzialtasuna, Osotasuna, Kautotzea bermatzen ditu

Zifraketa sarrera

Kriptoanalisia: mezu zifratuak deszifratzeko teknikak

Kriptologia: Kriptografia + Kriptoanalisia

Zifraketa sarrera

Kriptoanalisia:

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

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**

Kerckhoffs-en printzipoak

- Gako kriptografiko edo pasahitzak erraz gogoratzeko modukoa izan behar du, inon idazteko beharrik ez izateko modukoa eta erraz aldatzeko modukoa
- Kriptogramak telegrafo bidez transmititzeko modukoa izan behar du, karaktere alfanumerikoetan idazteko modukoa

Kerckhoffs-en printzipoak

- 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

Zifraketa 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

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)

Zifraketa sarrera

Kriptografia: informazioa **zifratu**

Esteganografia: informazioa **ezkutatu**

Hash algoritmoak: informazioa **laburtu**

Esteganografia

"steganos": ezkutua; "graphos": idazkera

Informazioa ezkutatzean 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

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)

Laburpen algoritmoak (Digest)

Jatorrizko eduki osoa ordezkatzeko duen kriptograma ekoizten dute:

- **Tamaina finkokoa**, jatorrizko edukia edozein izanda
- **Jatorrizko eduki guztia** ordezkatzeko du
- Edukia apur bat aldatzen bada ere **guztiz aldatzen da**
- Eduki berdinentzat beti ekoizten du **bera**

Hash funtzioak

- Ez daukate alderantzizko funtziorik (one-way function): ezin da edukia lortu kriptogramatik
- Ezin dira deszifratu, ez dutelako zifratzen (laburtu)

Laburpen algoritmoak: Erabilpenak

Informazioaren Osotasuna ziurtatu

Pasahitzak gorde

Datu edo fitxategien identifikatzailea

Lan froga -Proof of Work- ([Bitcoin](#))

Sinadura digitala inplementatu ([Zifraketa asimetrikoa: sinadura digitala](#))

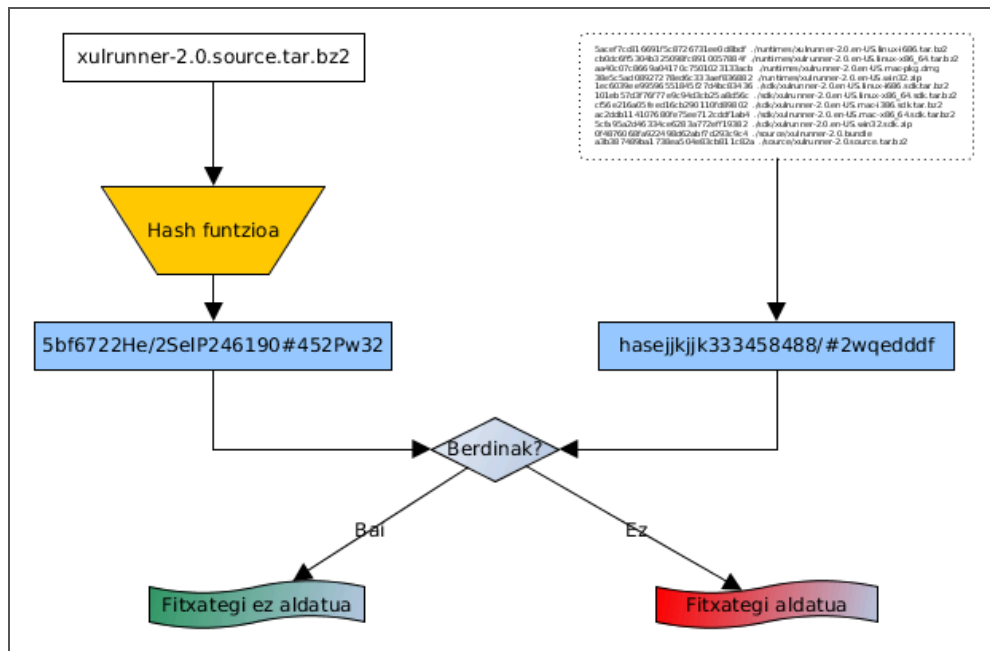
Informazioaren Osotasuna ziurtatu

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

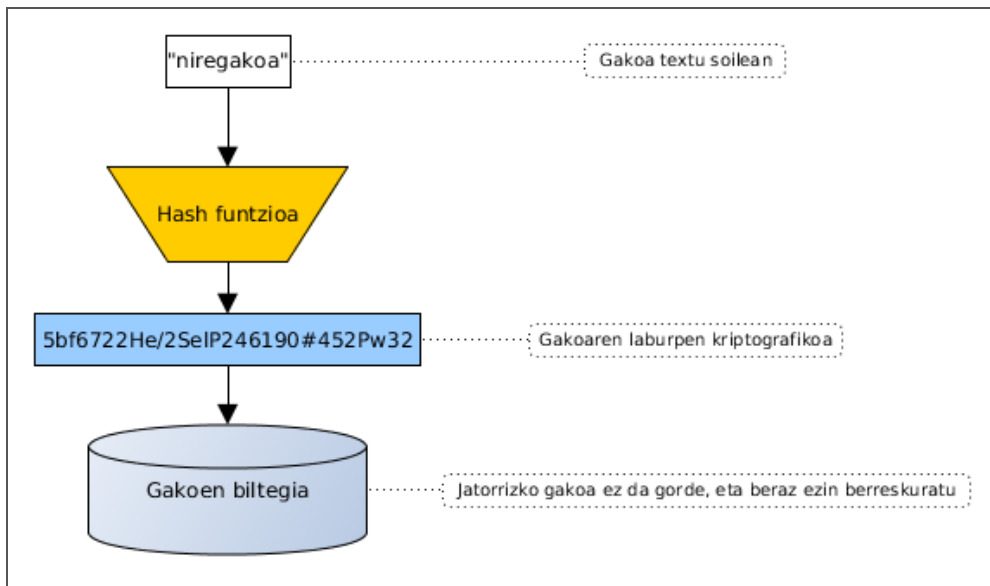
```
5acef7cc816691f5c8726731ee0d8bdf ./runtimes/xulrunner-2.0.en-US.linux-i686.tar.bz2
cb0dc6ff5304b325098fc8910057884f ./runtimes/xulrunner-2.0.en-US.linux-x86_64.tar.bz2
aa40c07c86669a04170c7501023133acb ./runtimes/xulrunner-2.0.en-US.mac-pkg.dmg
38e5c5ad08927278ed6c333aef836882 ./runtimes/xulrunner-2.0.en-US.win32.zip
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
```

Nola baieztatu osotasuna?

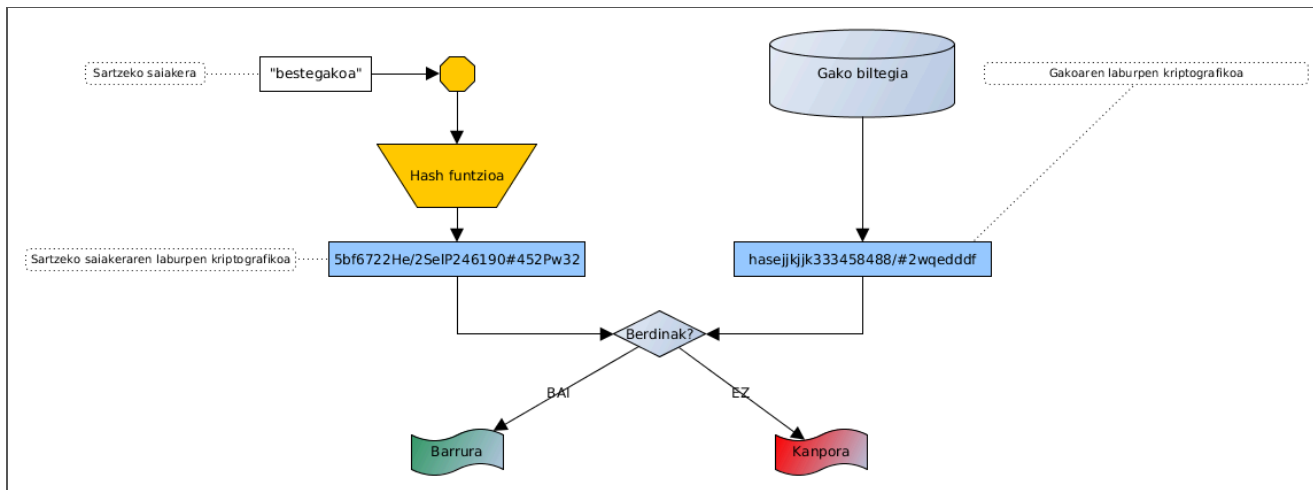
Informazioaren Osotasuna ziurtatu



Pasahitzak gorde



Pasahitzak gorde: identifikatu

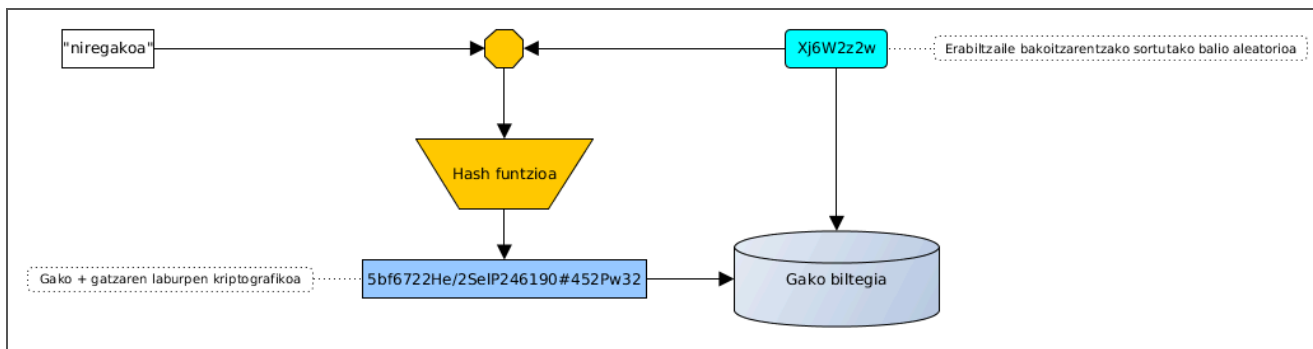


Pasahitzak gorde: arazoak

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

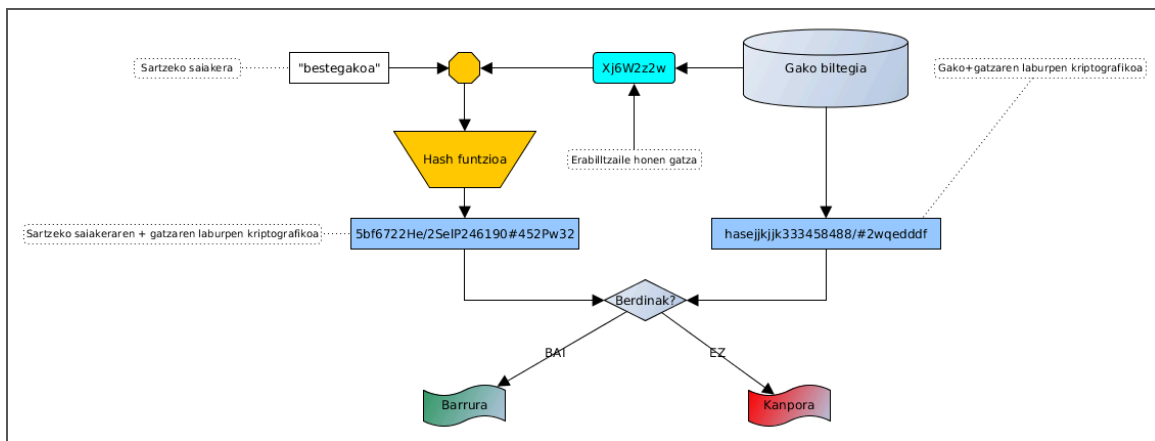
Pasahitzak gorde: arazoak

Soluzioa: "gatza" (Salt) edo hazia erabiltzea



Pasahitzak gorde

Identifikazioa gatza gehituta



Pasahitzak gorde

Gatza erabiltzearen abantailak

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

Pasahitzak gorde

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: ausazko katea

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)

Datu edo fitxategien identifikatzailea

Git bertsio kontrol sisteman, identifikatzeko:

- Commit-ak
- Blobs (Binary Large Objects)
- Zuhaitzak: beste direktorio batzuei eta blob-ei erreferentziak dituzten direktorioak

Datu edo fitxategien identifikatzailea

Git bertsio kontrol sisteman:

- Edukia de-duplikatzeko
- Aldaketen antzematea
- Aldaketa maltzurren kontrako osotasuna mantentzea

Datu edo fitxategien identifikatzailea

BitTorrent-en identifikatzeko:

- Artxibo zatiak
- .bittorrent artxiboak
- Magnet link-ak

Datu edo fitxategien identifikatzailea

Programazio hizkuntzatan datu egituretan:

- Bilaketa azkarra
- Osotasuna bermatzea
- Banakotasuna bermatzea

Datu edo fitxategien identifikatzailea

Programazio hizkuntzatan datu egituretan:

- Python: Dicts, Sets
- Java: HashMap, HashSet
- JavaScript: Object, Map

Laburpen algoritmo ezagunenak

MD5

SHA-3

RIPEMD

MD5

Kriptografikoki apurtuta baina oraindik erabiltzen da, batez ere osotasuna bermatzeko

128 bit-eko hash-ak

SHA-3

SHA-3 (Secure Hash Algorithm 3) [NIST](#) (National Institute for Standards and Technology) erakundeak garatua

SHA-0..2 MD5-an oinarrituta zeuden (Apurtuta), SHA-3-ek egitura ezberdina du

SHA-3

Sinadura digitalak: DSA (Digital Signature Algorithm) eta ECDSA (Elliptic Curve Digital Signature Algorithm)

SSL/TLS agiriak: [Open SSL](#)

Kriptomonetak: [Ethereum](#)

RIPEMD

RIPEMD (RACE Integrity Primitives Evaluation Message Digest): alternatiba
SHA eta MD5 aurrean

Oso segurua

SHA-256-rekin erabiltzen da [Bitcoin helbideak](#) sortzeko gako publikoetatik
abiatuta

Laburpen algoritmoen aurkako arazoak

- Talkak: textu ezberdinek laburpen berdina sortzea
- Indarrezko erasoak (Adib. urtebetetzearen paradoxa) edo SHA 1-en kontrako [shattered](#) bezalako teknika finagoak
- Osotasuna: hash berdina duen dokumentu faltsu batekin ordezkatu benetazko dokumentua
- TLS/SSL agiriak: zerbitzu bat bezala agertu agiri faltsu batekin