Laburpen algoritmoak

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

Laburpen algoritmoak

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

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

Laburpen algoritmoak (Digest)

Jatorrizko eduki osoa ordezkatzen duen kriptogramabat ekoizten dute:

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

Laburpen algoritmoak

Hash funtzioak:

- Ez dauka alderantzizko funtziorik (one-way function): ezin da edukia lortu kriptogramatik
- Ezin da deszifratu, ez duelako 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)

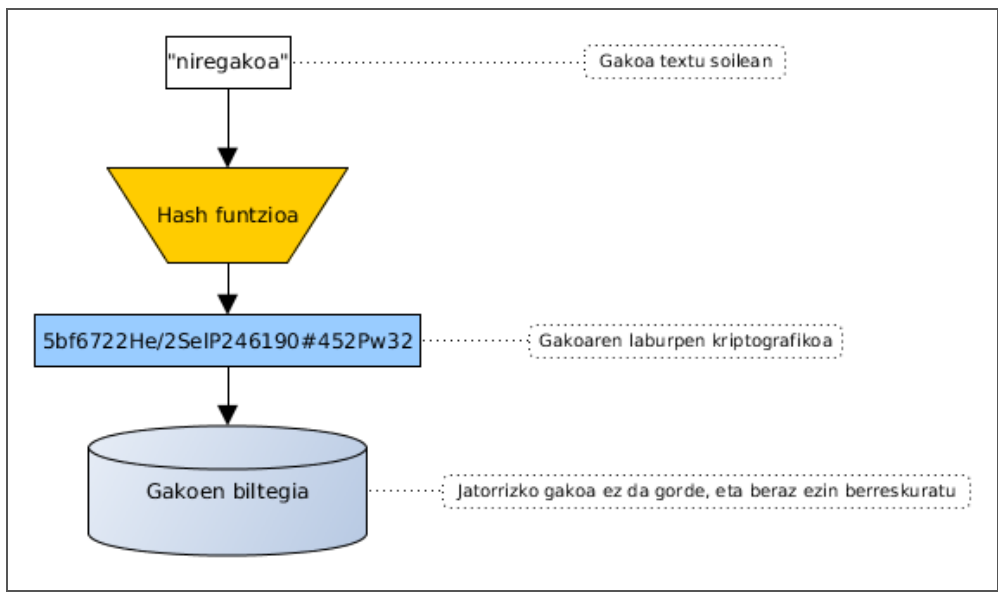
Informazioaren Osotasuna ziurtatu

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

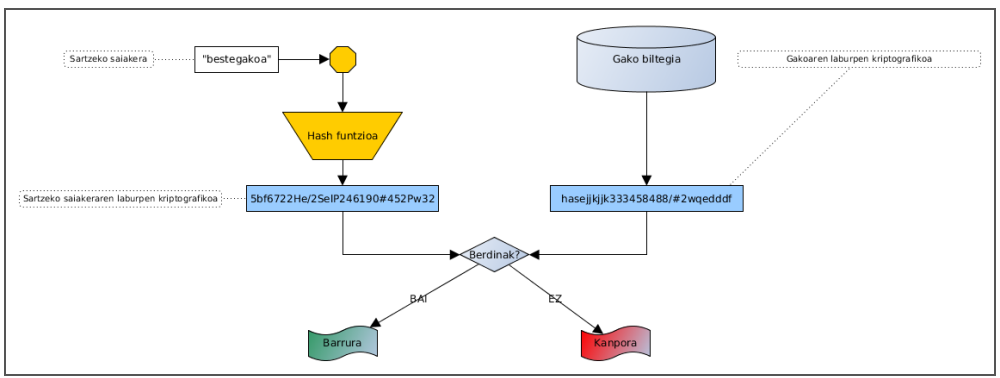
```
5acef7cc816691f5c8726731ee0d8bdf  ./runtimes/xulrunner-2.0.en-US.linux-i686.tar.bz2
cb0dc6ff5304b325098fc8910057884f  ./runtimes/xulrunner-2.0.en-US.linux-x86_64.tar.bz2
aa40c07c8669a04170c7501023133acb  ./runtimes/xulrunner-2.0.en-US.mac-pkg.dmg
38e5c5ad08927278ed6c333aef836882  ./runtimes/xulrunner-2.0.en-US.win32.zip
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
```

Nola baieztatu osotasuna?

Pasahitzak gorde



Pasahitzak gorde: identifikatu

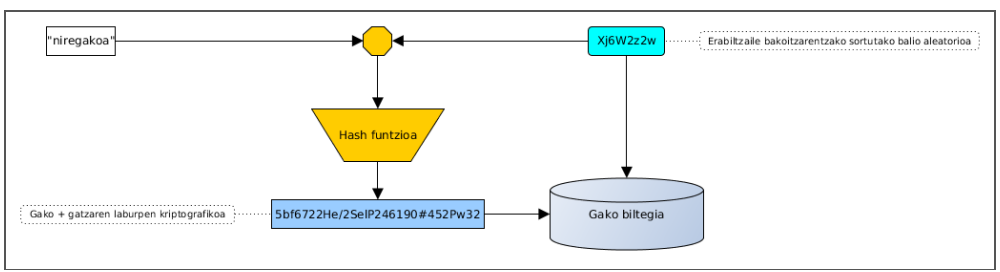


Pasahitzak gorde: arazoak

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

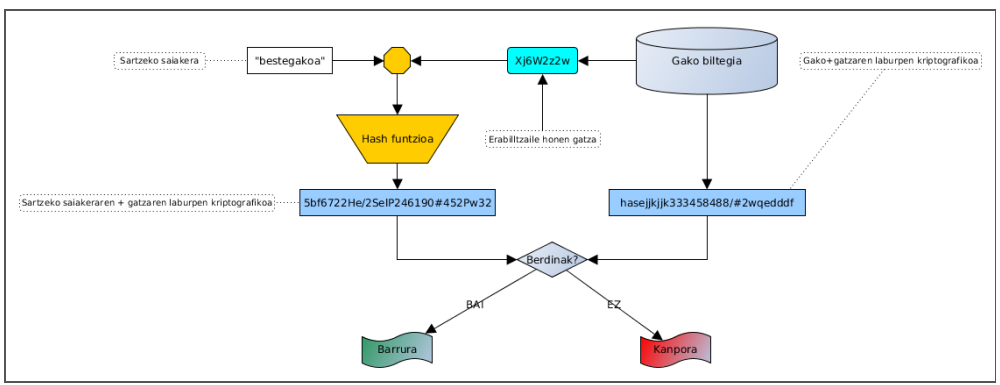
Pasahitzak gorde: arazoak

Soluzioa: "gatza" (Salt) edo hazia erabiltzea



Pasahitzak gorde

Identifikazioa gatza gehituta



Pasahitzak gorde

Gatza erabiltzearen abantailak

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

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

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 gakoa aldatu gabe (1970/01/01-tik)
- B: zenbat egun gakoa aldatu ahal izateko
- C: zenbat egun egon ahal den gakoa 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

Bertsioak kontrolatzeko sistemak, Git gisa, edukia sha1sum bidez identifikatzeko

Magnet URI-ak fitxategiak trukatzeko (Adib.: Magnet Links BitTorrenten)

Hash table datu-egitura programazio hizkuntza askotan

Laburpen algoritmo ezagunenak: MD5

Kriptografikoki apurtuta baina oraindik erabiltzen da, batez ere osotasuna bermatzeko

128 bit-eko hash-ak

Laburpen algoritmo ezagunenak: SHA-3

SHA-0..2 MD5-an oinarrituta zeuden, SHA-3 ez

224...512 bit

Open SSL, Ethereum, ...

Laburpen algoritmo ezagunenak: RIPEMD

128, 160, 256, 320 bit

Bitcoin-ek RIPEMD-160 erabiltzen du

Laburpen algoritmoak: Arazoak

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

Laburpen algoritmoak: Soluzioak

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