Kunċett · 19 ta' Mejju 2026

← Preċedenti·Li jmiss →

X'inhu verament SHA-256

Marka tas-swaba' matematika li toqgħod f'erba' u sittin karattru u li tinbidel kollha kemm hi jekk tinbidel biss virgola waħda fit-test oriġinali. Għaliex insejħulha siġill tax-xama' diġitali.

Biex niftehmu: Immaġina magna li taqra kwalunkwe test u tagħti sekwenza ta' 64 karattru. Jekk it-test jidħol identiku, is-sekwenza toħroġ identika. Jekk iċċaqlaq komma waħda biss, is-sekwenza tkun waħda kompletament differenti. Dik is-sekwenza hija x-xama' tas-siġill diġitali.

L-idea sempliċi wara l-isem tekniku

Immaġina li teżisti magna b'fetħa waħda u skrin wieħed. Mill-fetħa ddaħħal test: kelma, frażi, rumanz sħiħ. Fuq l-skrin tidher, mumenti wara, sekwenza ta' eżattament erba' u sittin karattru. Dik is-sekwenza, lill-qarrej professjonali nsejħulha *hash* jew *sommarju kriptografiku*; lill-qarrej ġenerali, nistgħu nsejħulha għalissa marka tas-swaba' matematika tat-test, bħalma l-marka tas-swaba' hija ta' persuna.

Jekk iddaħħal l-istess test darbtejn, il-magna turi l-istess marka ż-żewġ darbiet. Jekk iddaħħal test kemxejn differenti — virgola waħda mċaqalqa, ittra kbira li ssir żgħira— il-magna turi marka kompletament differenti mill-ewwel waħda. Mhux simili: differenti. Dawn iż-żewġ proprjetajiet flimkien —id-determiniżmu u s-sensittività— huma l-idea sempliċi. Kulma fadal mix-SHA-256 hija l-makkinarju li jagħmilhom jaħdmu tajjeb.

Tajjeb li ngħidu mill-bidu x'ma tagħmilx il-magna. Ma tikkriptax it-test. Ma taħbihx. Ma tissejvjahx. Il-magna tħares lejn it-test, tikkalkula l-marka, u tinsa t-test. Il-marka ma tippermettix li jerġa' jinbena t-test li pproduċieha; tippermetti biss, meta jingħata test kandidat, li jiġi ċċekkjat jekk jaqbilx jew le mal-oriġinal. Għalhekk ngħidu li huwa sommarju *f'direzzjoni waħda*: tmur u ma terġax lura.

Hash mhux l-istess bħal ikkriptar

Il-konfużjoni hija frekwenti u tajjeb li niċċarawha: l-ikkriptar u l-hashing huma operazzjonijiet differenti. L-ikkriptar jikkonsisti f'li tittrasforma test b'tali mod li s-sid taċ-ċavetta biss jista' jreġġgħu lura għall-forma oriġinali tiegħu. Il-hashing jikkonsisti fil-produzzjoni ta' marka tat-test li minnha t-test oriġinali qatt ma jista' jiġi rkuprat, la biċ-ċavetta u lanqas mingħajrha. L-ewwel hija riversibbli b'disinn; it-tieni hija irriversibbli b'disinn.

Il-konsegwenza prattika hija importanti. Meta applikazzjoni tgħid «inżommu l-password tiegħek ikkriptata», hemm xi ħadd li għandu ċ-ċavetta biex jiddekriptaha — l-applikazzjoni stess, f'kull każ. Meta applikazzjoni tgħid «inżommu l-password tiegħek hashed», l-applikazzjoni stess ma tistax taqra l-password oriġinali anke jekk trid; tista' biss tiċċekkja jekk dik li tikteb int terġax tipproduċi l-istess marka. It-tieni mudell, jekk isir sew, huwa ħafna preferibbli mill-ewwel wieħed biex jinħażnu l-passwords. Aktar 'il quddiem naraw għaliex «isir sew» jeħtieġ xi ħaġa aktar minn SHA-256 waħdu.

L-erba' proprjetajiet li jagħmlu hash kriptografiku utli

Funzjoni hash li tixraqilha l-aġġettiv *kriptografiku* tissodisfa erba' proprjetajiet:

1. **Determiniżmu.** L-istess input dejjem jipproduċi l-istess marka.
2. **Effett valanga.** Bidla żgħira fl-input tipproduċi marka kompletament differenti, mingħajr ebda xebh viżibbli ma' dik ta' qabel.
3. **Reżistenza għall-inverżjoni.** Mogħtija marka, mhuwiex vijabbli komputazzjonalment li ssib it-test li pproduċieha.

4. **Reżistenza għall-ħabtiet.** Mhuwiex vijabbli komputazzjonalment li ssib żewġ testi differenti li jipproduċu l-istess marka.

«Mhux vijabbli komputazzjonalment» ma jfissirx «huwa matematikament impossibbli». Ifisser li l-ispiża f'ħin, enerġija u flus biex jinkiseb dan taqbeż b'diversi ordnijiet ta' kobor is-somma tal-kapaċità kollha tal-kompjuters raġonevolment disponibbli. Għax-SHA-256, dak il-limitu jitkejjel f'eluf ta' biljuni ta' snin anke għall-approċċi l-aktar ottimisti b'hardware speċjalizzat. Li, għall-għanijiet prattiċi tal-qarrej, huwa l-istess bħal «ma jistax isir».

SHA-256, b'mod partikolari

L-isem jgħid kollox. SHA huma l-inizjali ta' *Secure Hash Algorithm*: algoritmu ta' hash sigur. In-numru 256 jindika d-daqs tal-marka f'bits: mitejn u sitta u ħamsin bit, jiġifieri tnejn u tletin byte, li meta jintwerew f'hexadecimal huma l-erba' u sittin karattru li l-qarrej diġà jagħraf. L-istandard ġie ppubblikat min-NIST tal-Istati Uniti, l-organiżmu li jinnormalizza dan it-tip ta' funzjonijiet, fl-2001 bħala parti mill-familja SHA-2; il-verżjoni attwali tal-istandard, FIPS 180-4, hija tal-2015.

Għal min għadu mhux familjari ma' x'inhuma bits u bytes:

```
1 bit    →  0 jew 1        (swiċċ: mixgħul jew mitfi)
1 byte   →  8 bits         (256 kombinazzjoni possibbli)
32 bytes →  256 bits       (il-marka SHA-256)
```

In-numru 256 fl-aħħar tal-isem jgħid id-daqs tal-marka f'bits. F'hexadecimal —sistema ta' numerazzjoni b'sittax-il simbolu minflok għaxra— dawk il-256 bit joqogħdu f'eżattament 64 karattru. Dawk huma l-64 karattru li tara f'qiegħ kull Cuaderno.

Id-dimensjonijiet jixirqilhom mument. Mitejn u sitta u ħamsin bit jippermettu tnejn mibgħuta għal mitejn u sitta u ħamsin valur differenti: numru bi tmienja u sebgħin ċifra deċimali, bosta ordnijiet ta' kobor akbar min-numru stmat ta' atomi fl-univers osservabbli. Kull test tad-dinja —kull ktieb, kull email, kull messaġġ— jaqa' fuq wieħed minn dawk il-valuri. Il-probabbiltà li żewġ testi differenti jaqblu b'kumbinazzjoni hija, għall-għanijiet prattiċi, indistingwibbli minn żero.

Kif jidher f'kodiċi

F'Zig, lingwa li biha niktbu l-partijiet li jżommu Solo2, il-kalkolu tas-siġill SHA-256 ta' test jidher hekk:

```
const std = @import("std");

const texto = "Cuadernos Lacre";
var resumen: [32]u8 = undefined;
std.crypto.hash.sha2.Sha256.hash(texto, &resumen, .{});
```

Għadna kemm talabna lill-librerija standard ta' Zig biex tikkalkula x-SHA-256 tat-test fil-virgoli. Wara s-sejħa, il-varjabbli *resumen* fiha t-tnejn u tletin byte li jiffurmaw is-siġill fil-forma mhux ipproċessata tiegħu; meta jintwerew fuq l-iskrin f'hexadecimal, huma l-erba' u sittin karattru li jidhru f'qiegħ dan l-artiklu. Jekk inbiddlu *Cuadernos Lacre* f'*Cuadernos lacre* —ittra kbira waħda inqas— is-siġill jinbidel kollu kemm hu. Dik hija, f'ħames linji, il-proprjetà ċentrali li ssostni l-kumplament. Għal min irid jara kif jaħdem internament, fl-aħħar tal-artiklu ninkludu verżjoni li tista' tinqara tal-algoritmu b'kummenti pass pass.

Għaliex insejħulu siġill tax-xama'

Fil-korrispondenza Ewropea tas-sekli ħmistax sad-dsatax, ix-xama' kienet tissiġilla l-ittra. Qatra xama' mdiba, siġill ippressat fuqha, u l-ittra kienet tibqa' mmarkata b'mod li ma jistax jiġi ripetut. Ma kinitx tipproteġi l-kontenut minn min irid jittajjar —il-karta setgħet tinqara kontra d-dawl, ix-xama' setgħet tinkiser— iżda kienet turi evidenza. Kull tibdil fis-siġill kien ikun viżibbli għad-destinatarju qabel ma jiftaħ il-karta. Ix-xama' ma kinitx tipprevjeni l-ħsara; kienet tiddikjaraha.

Ix-SHA-256 tal-korp ta' kull Cuaderno jaqdi l-istess funzjoni fil-verżjoni diġitali tiegħu. Jekk kelma waħda fl-artiklu tinbidel bejn il-mument li ġie ppubblikat u l-mument li taqrah int, is-siġill hexadecimal f'qiegħ it-test ma jibqax jaqbel max-SHA-256 tat-test li għandek quddiemek. Kull qarrej b'ħames linji ta' kodiċi jista' jiċċekkja dan. Il-pubblikazzjoni ma tistax terġa' tikteb l-istorja tagħha mingħajr ma s-siġill jikxfilha. Ma jipproteġix kontra l-ħsara; jagħmilha verifikabbli.

Dak li mhuwiex hash

Erba' użi xi kultant jintalbu minn SHA-256 li ma jikkorrispondux miegħu:

1. **Ikkriptar.** Hash jiġbor fil-qosor; ma jaħbix. Jekk trid li t-test ma jkunx jista' jinqara, għandek bżonn tikkriptah, mhux tagħmillu hashing.
2. **Awtentikazzjoni tal-awtur.** Hash ma jgħidlekx min kiteb it-test, biss liema test ġie hashed. Biex tassoċja awturija hemm bżonn ta' firma kriptografika fuq il-hash, mhux il-hash waħdu.
3. **Ħażna ta' passwords.** Hawnhema hemm nassa li tajjeb li tifhimha. SHA-256 huwa ddisinjat biex ikun veloċi ħafna —li hija ħaġa tajba għal ħafna affarijiet, iżda ħażina għal dan il-għan. Attakkant b'hardware speċjalizzat jista' jipprova biljuni ta' passwords kull sekonda kontra hash SHA-256 sakemm isib tiegħek. Biex taħżen passwords għandhom jintużaw funzjonijiet ta' derivazzjoni ta' ċavetta deliberatament bil-mod bħal Argon2, scrypt jew bcrypt, ikkombinati ma' *sal* (salt - data każwali unika għal kull utent, li tipprevjeni li żewġ persuni bl-istess password ikollhom l-istess hash).
4. **Aqra l-hash bħala identifikatur tal-awtur.** Mhuwiex. Hash jidentifika l-kontenut. Jekk żewġ persuni jagħmlu hash tal-kelma *hola* b'SHA-256, it-tnejn jiksbu l-istess sommarju — u dik hija l-proprjetà ċentrali, mhux difett: kieku kienu sommarji differenti, ma nkunux nistgħu niċċekkjaw qbil bejn dak ippubblikat u dak riċevut.

Fejn jidher SHA-256 fil-ġurnata tiegħek

Għalkemm ma tarahx, SHA-256 isostni parti kbira minn dak li tuża kuljum fuq l-internet. Il-blockchain ta' Bitcoin tinbena billi tikkatenat SHA-256 ta' kull blokka għal dik li jmiss; li tbiddel blokka tal-passat iġġiegħel li terġa' tikkalkula l-katina kollha ta' wara. Git, is-sistema li biha jiġi rreġistrat il-kodiċi ta' nofs id-dinja, tidentifika kull konferma (commit) bix-SHA-256 (f'verżjonijiet reċenti) jew bil-predeċessur tiegħu SHA-1 (f'verżjonijiet eqdem) tal-kontenut sħiħ tagħha. Iċ-ċertifikati HTTPS li jivverifikaw l-identità ta' sit web meta tidħol fih għandhom marka SHA-256 assoċjata. It-tniżżil ta' softwer spiss jiġi akkumpanjat minn SHA-256 ippubblikat mill-iżviluppatur biex tivverifika li l-fajl ma nbidilx matul it-triq. U, kif għidna, f'qiegħ kull Cuaderno Lacre.

Għall-qarrej professjonali

Erba' tfakkiriet operattivi għal min jiddeċiedi jew jawditja sistemi:

1. Hash mhuwiex ikkriptar. Jekk fornitur iħawwad iż-żewġ termini fid-dokumentazzjoni teknika tiegħu, tajjeb li tistaqsi xi jrid jgħid eżattament.
2. Biex taħżen passwords qatt m'għandu jintuża SHA-256 waħdu. SHA-256 huwa veloċi wisq għal dan ix-xogħol (ara l-punt 3 ta' *Dak li mhuwiex hash*). L-istandard attwali huwa **Argon2id**: bil-mod b'disinn, konfigurabbli skont il-kapaċità tas-server, ikkombinat ma' *sal* (salt) każwali differenti għal kull utent.
3. Għall-integrità tad-dokumenti —kuntratti, fajls, arkivji— SHA-256 jibqa' l-istandard ta' referenza. Huwa dak li jintuża mis-siġillaturi tal-ħin kwalifikati fl-UE.
4. Għal konservazzjoni fit-tul (għexieren ta' snin) tajjeb li tikkalkula u tissejvja wkoll SHA-3 jew SHA-512 flimkien max-SHA-256; il-prudenza kriptografika tirrakkomanda li ma tiddependix fuq funzjoni waħda biss matul arkivji ta' sekli sħaħ.

Teknikament, din l-istruttura iterata — fejn l-istat intermedju jinżamm bejn il-blokok tad-dħul — hija magħrufa bħala kostruzzjoni **Merkle-Damgård**, id-disinn li fuqu huma bbażati SHA-1, SHA-2 (inkluż SHA-256) u ħafna funzjonijiet hash klassiċi oħra. Mill-banda l-oħra, SHA-3 jabbanduna Merkle-Damgård favur arkitettura differenti msejħa *sponża*.

Kif jaħdem SHA-256, pass pass, fi kliem sempliċi

Immaġina li bnejt l-aktar ċirkwit tad-domino elaborat fid-dinja: eluf ta’ biċċiet, għexieren ta’ friegħi, pontijiet mekkaniċi u rampi li jaqsmu l-kamra kollha, pożizzjonati bir-reqqa biċċa biċċa.

Jekk tagħti daqqa fuq l-ewwel biċċa, il-katina taqa' f'sekwenza preċiża u ripetibbli. L-istess tqassim, l-istess daqqa inizjali → l-istess disinn finali ta' biċċiet li jkunu waqgħu, darba wara l-oħra.

Hawn huwa dak li hu interessanti: mexxi **biċċa waħda biss** nofs ċentimetru mal-ġenb qabel tibda u erġa' agħti daqqa. Rampa li suppost kellha tattiva ruħha tibqa' inerta, pont ma jaqax, tiskatta fergħa differenti. Id-disinn finali ta' biċċiet fuq l-

art huwa kompletament mhux rikonoxxibbli meta mqabbel mal-ewwel wieħed.

Matematikament SHA-256 huwa dan iċ-ċirkwit. It-test li tikteb huwa l-pożizzjoni inizjali tal-biċċiet. L-algoritmu huwa d-daqqa li tirrilaxxa l-kaskata. U r-riżultat aħħari — dak li aħna nsejħulhom *hash* — huwa r-ritratt fiss tal-art meta kollox ikun waqaf. Ibdel virgola waħda biss mit-test oriġinali u r-ritratt ikun drastikament differenti. Sempliċi daqshekk, u daqshekk drastiku.

Pass 1. It-traduzzjoni tat-test f'biċċiet binarji. Il-kompjuters ma jifhmux l-ittri; l-ewwel jittraduċuhom f'numri (ASCII) u n-numri f'binarju (ones u zeros). Kull ittra tinbidel fi 8 biċċiet bojod jew suwed: l-*A* hija `01000001`, il-*B* hija `01000010`, l-ispazju huwa `00100000`. It-test sħiħ tiegħek — kelma, kuntratt, rumanz — isir ringiela twila ta' biċċiet bojod u suwed.

Pass 2. Il-mili sad-daqs standard. Iċ-ċirkwit jipproċessa r-ringiela fi *blokki* ta' eżattament 512-il biċċa. Jekk il-messaġġ tiegħek ma jilħaqx multiplu ta' 512, tiżdied biċċa tal-immarkar (dik bil-valur `10000000`) eżatt wara t-test u mbagħad zeros sa ma jitlesta l-blokk. L-aħħar 64 pożizzjoni ta' kull blokk huma riżervati biex jinnotaw it-tul oriġinali tat-test. B'hekk iċ-ċirkwit dejjem ikun jaf fejn spiċċa l-kontenut reali u minn fejn beda l-mili.

Pass 3. It-tqegħid tat-tmien biċċiet prinċipali. Qabel nibdew, inpoġġu fuq il-mejda **tmien biċċiet prinċipali** f'pożizzjoni inizjali preċiża. Dawn it-tmien biċċiet mhumiex sigriet: il-valur inizjali tagħhom huwa ffissat b'regola matematika pubblika (l-għeruq kwadrati tal-ewwel tmien numri primi — 2, 3, 5, 7, 11, 13, 17, 19 — u l-ewwel bits tal-parti deċimali ta' kull għerq). Kulħadd, f'kull rokna tal-pjaneta, jibda bl-istess tmien biċċiet prinċipali fl-istess pożizzjoni. Id-destin tagħhom huwa li jiġu mbuttati u trasformati mill-valanga.

Pass 4. Il-valanga kbira: erbgħa u sittin round ta' mbuttaturi. Hawn jibda l-ispettaklu. L-ewwel blokk ta' 512-il biċċa tat-test tiegħek jibda jaħbat mat-tmien biċċiet prinċipali. Imma ma jaqgħux f'daqqa waħda: il-mekkaniżmu jwettaq **erbgħa u sittin round konsekuttiv**. F'kull round jagħmel tliet operazzjonijiet bil-biċċiet:

- **Il-Carousel** (rotazzjoni). Il-biċċiet jimxu f'ċirku: dawk ta' fuq il-lemin jgħaddu għax-xellug. L-ebda biċċa ma tintilef jew tiżdied; sempliċiment jerġgħu jiġu ordnati billi jagħmlu dawra sħiħa mal-carousel. Huwa mod irħis u riversibbli biex terġa' tqassam l-informazzjoni.
- **Il-Lembut Loġiku** (XOR). Il-biċċiet jgħaddu minn lembut li jqabbilhom tnejn tnejn: jekk it-tnejn ikunu tal-istess kulur, toħroġ waħda bajda; jekk ikunu differenti, toħroġ waħda sewda. Hija l-operazzjoni l-aktar sempliċi tal-loġika binarja, iżda magħquda mar-rotazzjonijiet tal-carousel issir waħda b'saħħitha ħafna biex tħallat l-informazzjoni mingħajr ma titlifha.
- **Il-Fluss** (żieda modulari). Ir-riżultat jingħadd ma' *biċċa ta' mbuttatura kostanti* meħuda minn lista pubblika ta' erbgħa u sittin kostanti (l-għeruq kubi tal-ewwel erbgħa u sittin numru prim). Jekk l-għadd jiġġenera biċċiet żejda li ma joqogħdux fl-ispazju tat-32 biċċa previst, dawn il-biċċiet żejda jintremew. Il-mejda għandha spazju biss għal 32 biċċa, u l-ebda waħda oħra.

Fi tmiem l-erbgħa u sittin round, kull waħda mill-biċċiet tal-blokk tat-test tiegħek influwenzat il-pożizzjoni tat-tmien biċċiet prinċipali. L-enerġija mill-imbuttatura vjaġġat maċ-ċirkwit kollu.

Pass 5. Iż-żieda tal-blokk li jmiss (mingħajr restart). Jekk it-test tiegħek kien twil u għad fadal blokk ieħor ta' 512-il biċċa x'jiġi pproċessat, **iċ-ċirkwit ma jsirlux restart**. It-tmien biċċiet prinċipali jibqgħu eżatt kif ħallithom l-ewwel valanga, u t-tieni blokk jintefa' kontrihom biex jattiva erbgħa u sittin round oħra. Dan qisu kif iżżid kamra ġdida mimlija dominoes fit-tarf ta' dik li tkun għadha kif waqgħet: id-diżordni tal-ewwel waħda tikkonnizzjona għalkollox kif se taqa' t-tieni waħda.

Pass 6. Ir-ritratt aħħari. Meta ma jkun fadal l-ebda blokk ieħor xi jsirlu l-ipproċessar, il-valanga tieqaf. Inħarsu lejn il-pożizzjoni aħħarija fejn waqfu t-tmien biċċiet prinċipali. Nittraduċu l-konfigurazzjoni tagħhom f'kodiċi ta' ittri u numri fis-sistema eżadeċimali. Ir-riżultat huwa sekwenza ta' eżattament erbgħa u sittin karattru: dak huwa s-siġill SHA-256 tiegħek.

Erba' karatteristiċi joħorġu waħedhom mill-mod kif ġie mmuntat iċ-ċirkwit:

1. **Id-determiniżmu.** L-istess test dejjem jipproduċi l-istess ritratt finali, fi kwalunkwe kompjuter fid-dinja. Żero każwalità, żero sorpriżi.
2. **L-effett tal-valanga.** Virgola miżjuda, ittra kapitali mibdula, aċċent minsi: ir-ritratt isir kompletament mhux rikonoxxibbli. Din hija s-sensittività estrema li diġà ddeskrivejna fil-bidu.
3. **F'direzzjoni waħda.** Mir-ritratt finali, m'intix kapaċi terġa' tibni t-test oriġinali. Ir-rotazzjonijiet, il-lembuti u l-flussi jeqirdu l-informazzjoni direzzjonali kollha dwar *minn fejn ġie kull bit* u jippreservaw biss *dak li ngħadd b'kollox*.

4. **Ir-reżistenza għall-kolliżjonijiet.** F'ħamsa u għoxrin sena ta' kryptoanaliżi pubblika, ħadd ma rnexxielu jsib żewġ testi differenti fejn ir-ritratti finali tagħhom ikunu jaqblu. U d-diffikultà biex isir dan hija lil hinn mill-firxa komputazzjonali ta' kwalunkwe ċiviltà li wieħed jista' raġonevolment jimmaġina.

L-appendiċi tal-kodiċi li ġejja timplimenta eżattament dawn is-sitt passi f'Zig. Issa tista' taqrah bil-għarfien ta' x'tfisser kull operazzjoni tal-bits, minflok ma taċċetta l-manipulazzjonijiet l-agħma.

Glossarju tekniku

Għall-qarrej li jixtieq jifhem x'tagħmel kull operazzjoni. Tista' taqbeż din il-parti b'mod ħieles: l-artiklu xorta waħda jiftiehem mingħajrha.

L-ASCII u l-Unicode — kif l-ittri jsiru numri. Il-kompjuters ma jarawx ittri; jaraw numri. Standard imsejjaħ **ASCII** (*American Standard Code for Information Interchange*, mill-1963) jassenja lil kull karattru tat-tastiera numru speċifiku: l-*A* hija 65, il-*B* hija 66, l-*a* hija 97, iż-*0* hija 48, l-ispazju huwa 32, il-virgola hija 44. Is-sistemi moderni jespandu dan permezz tal-**Unicode**, li jassenja numru lil kull karattru f'kull alfabett tad-dinja: Ċirilliku, Għarbi, Ċiniż, Ġappuniż, u anke l-emojis. Meta tikteb karattru jew tiftaħ file ta' test, il-kompjuter jaqra n-numru fl-isfond, u mhux il-forma fuq l-iskrin. SHA-256 jaħdem fuq dawn in-numri, u jittratta kwalunkwe test bħala sekwenza twila ta' ċifri. Huwa għalhekk li jista' jissiġilla artiklu bl-Ispanjol, poeżija bil-Ġappuniż, u file binarju bl-istess algoritmu.
Ix-XOR — il-komparatur minn bit għal bit. Ix-XOR (imfisser *«exor»*, mill-Ingliż *exclusive or*, «jew esklużiv») hija waħda mill-aktar operazzjonijiet sempliċi li kompjuter jista' jagħmel b'żewġ numri binarji. Tqabbel żewġ bits pożizzjoni b'pożizzjoni u tirritorna: **1** jekk eżattament wieħed mit-tnejn ikun 1 (wieħed iżda mhux it-tnejn), **0** jekk it-tnejn ikunu l-istess (it-tnejn 0 jew it-tnejn 1). Eżempju: XOR ta' `1010` u `1100` hija `0110`. Għandha karatteristika eċċezzjonali: tista' titqalleb lura — jekk tagħmel XOR darbtejn bl-istess ċavetta, terġa' lura għall-oriġinal. Huwa għalhekk li hija ż-żiemel tat-tagħbija fil-kriptografija: tħallat il-bits mingħajr ma tintilef l-informazzjoni, imma r-riżultat ma jiżvela xejn dwar id-dħul jekk ma tkunx taf waħda minnhom.
L-Eżadeċimali — tgħodd fil-bażi 16. Kważi n-numri kollha ta' kuljum jużaw għaxar ċifri (0-9). L-eżadeċimali juża sittax: iż-0-9 tas-soltu flimkien ma' sitt ittri li jirrappreżentaw il-valuri li ġejjin: `A` = 10, `B` = 11, `C` = 12, `D` = 13, `E` = 14, `F` = 15. Għaliex sittax? Għax il-kompjuters jaħsbu fi gruppi ta' erba' bits, u l-erba' bits jistgħu jirrappreżentaw eżattament sittax-il valur differenti — għalhekk, karattru eżadeċimali wieħed jikkorrispondi eżatt għal erba' bits. Hash (siġill) SHA-256 jkejjel 256 bit, li jiġu eżattament **64 karattru eżadeċimali**. Kieku nkiktbuha fid-deċimali normali, kienet tieħu madwar 78 ċifra u kienet tkun anqas prattika. L-għażla hija estetika u kompatta; il-valur fl-isfond jibqa' l-istess.
Ir-rotazzjoni tal-bits — il-carousel binarju. Immaġina ringiela ta' seba' bozoz, xi whud mixgħula (1) u oħrajn mitfija (0): `1 0 1 1 0 0 1`. Jekk iddawwar pożizzjoni waħda lejn il-lemin tikkonsisti filli tieħu l-bozza l-aktar fuq il-lemin, teħodha fl-estremità tax-xellug, u tmexxi l-oħrajn post wieħed lejn il-lemin: `1 1 0 1 1 0 0`. L-ebda bozza ma tintilef jew tiżdied: huma sempliċiment jiżfnu f'ċirku. SHA-256 juża r-rotazzjoni tal-bits mijiet ta' drabi f'kull kalkolu; huwa metodu irħis u mingħajr telf sabiex terġa' tqassam l-informazzjoni fl-istat.
Il-kostanti *«nothing-up-my-sleeve»* — għaliex joriġinaw minn numri primi. It-tmien biċċiet prinċipali u l-erbgħa u sittin kostanti tar-round ta' SHA-256 ma ġewx magħżula b'mod każwali. Huma ġejjin mill-għeruq kwadrati u kubi tal-ewwel numri primi. Għaliex? Għaliex id-disinjaturi tagħhom riedu kostanti *«mingħajr xejn fil-komma»*: valuri li kwalunkwe persuna tista' tivverifika l-oriġini tagħhom. Li kieku xi ħadd qallek *«afda lili: uża dan in-numru każwali ta' 32-bit»*, raġonevolment tista' tissuspetta xi dgħufija moħbija jew xi backdoor. Imma kwalunkwe persuna b'kalkolatur tista' tiċċekkja li l-ewwel 32 bit tal-għerq kwadrat ta' 2 huma `0x6a09e667`. Il-valuri huma matematiċi, pubbliċi u jistgħu jiġu riprodotti: l-ebda nassa moħbija ma tista' tinfiltra fir-riċetta.

Appendiċi: SHA-256 f'kodiċi li jinqara

Dan l-appendiċi huwa għall-qarrej li jrid jara l-algoritmu minn ġewwa. Hija implimentazzjoni didattika f'Zig li ssegwi l-ispeċifikazzjoni FIPS 180-4. Mhix il-verżjoni li juża Solo2 —dik vera tinsab f'`std.crypto.hash.sha2.Sha256` tal-librerija standard ta' Zig, ottimizzata u awditjata—. Iżda l-algoritmu huwa l-istess: dak li tara hawnhekk huwa, pass pass, dak li jiġri meta dik is-sejħa ta' ħames karattri tesegwixxi xogħolha.

```
const std = @import("std");

// SHA-256 — implementación didáctica.
// Sigue la especificación FIPS 180-4. Prioriza la claridad sobre la
// velocidad y la robustez frente a entradas hostiles. Para producción,
// usa std.crypto.hash.sha2.Sha256, que está optimizada y auditada.
```

```
// H0: las ocho palabras del estado inicial. Primeros 32 bits de la parte
// fraccionaria de las raíces cuadradas de los primeros ocho primos
// (2, 3, 5, 7, 11, 13, 17, 19).
const H0 = [_]u32{
    0x6a09e667, 0xbb67ae85, 0x3c6ef372, 0xa54ff53a,
    0x510e527f, 0x9b05688c, 0x1f83d9ab, 0x5be0cd19,
};

// K: 64 constantes de ronda. Primeros 32 bits de la parte fraccionaria
// de las raíces cúbicas de los primeros 64 primos.
const K = [_]u32{
    0x428a2f98, 0x71374491, 0xb5c0fbcf, 0xe9b5dba5, 0x3956c25b, 0x59f111f1, 0x923f82a4, 0xab1c5ed5,
    0xd807aa98, 0x12835b01, 0x243185be, 0x550c7dc3, 0x72be5d74, 0x80deb1fe, 0x9bdc06a7, 0xc19bf174,
    0xe49b69c1, 0xefbe4786, 0x0fc19dc6, 0x240ca1cc, 0x2de92c6f, 0x4a7484aa, 0x5cb0a9dc, 0x76f988da,
    0x983e5152, 0xa831c66d, 0xb00327c8, 0xbf597fc7, 0xc6e00bf3, 0xd5a79147, 0x06ca6351, 0x14292967,
    0x27b70a85, 0x2e1b2138, 0x4d2c6dfc, 0x53380d13, 0x650a7354, 0x766a0abb, 0x81c2c92e, 0x92722c85,
    0xa2bfe8a1, 0xa81a664b, 0xc24b8b70, 0xc76c51a3, 0xd192e819, 0xd6990624, 0xf40e3585, 0x106aa070,
    0x19a4c116, 0x1e376c08, 0x2748774c, 0x34b0bcb5, 0x391c0cb3, 0x4ed8aa4a, 0x5b9cca4f, 0x682e6ff3,
    0x748f82ee, 0x78a5636f, 0x84c87814, 0x8cc70208, 0x90befffa, 0xa4506ceb, 0xbef9a3f7, 0xc67178f2,
};

// Rotación circular a la derecha de un u32.
inline fn rotr(x: u32, n: u5) u32 {
    return std.math.rotr(u32, x, n);
}

// Lee 4 bytes consecutivos como un u32 big-endian.
inline fn readU32(b: []const u8) u32 {
    return @as(u32, b[0]) << 24 | @as(u32, b[1]) << 16 | @as(u32, b[2]) << 8 | @as(u32, b[3]);
}

// Escribe un u32 como 4 bytes consecutivos big-endian.
inline fn writeU32(b: []u8, v: u32) void {
    b[0] = @truncate(v >> 24);
    b[1] = @truncate(v >> 16);
    b[2] = @truncate(v >> 8);
    b[3] = @truncate(v);
}

// Compresión de un bloque de 64 bytes sobre el estado del hash. Sigue §6.2.2 de FIPS 180-4.
fn compress(state: *[8]u32, block: [16]u32) void {

    // 1. Expansión del schedule: 16 palabras → 64. Las nuevas se obtienen
    //    combinando cuatro anteriores con dos funciones de mezcla (s0 y s1)
    //    que usan rotación, XOR y desplazamiento. El "+%" es suma con
    //    truncado u32 (overflow-wrap), tal como exige el estándar.
    var w: [64]u32 = undefined;
    for (0..16) |i| w[i] = block[i];
    for (16..64) |i| {
        const s0 = rotr(w[i-15], 7) ^ rotr(w[i-15], 18) ^ (w[i-15] >> 3);
        const s1 = rotr(w[i-2], 17) ^ rotr(w[i-2], 19) ^ (w[i-2] >> 10);
        w[i] = w[i-16] +% s0 +% w[i-7] +% s1;
    }

    // 2. Variables de trabajo: copia del estado actual.
    var a = state[0]; var b = state[1]; var c = state[2]; var d = state[3];
    var e = state[4]; var f = state[5]; var g = state[6]; var h = state[7];

    // 3. 64 rondas de mezcla no lineal.
    //    S1, S0  : combinaciones rotacionales de 'e' y 'a'.
    //    ch      : "choose" — multiplexor bit a bit, elige entre f y g según e.
    //    maj     : "majority" — bit mayoritario entre a, b, c.
    //    t1 + t2 : se inyecta al top de la cascada cada ronda.
    for (0..64) |i| {
        const S1 = rotr(e, 6) ^ rotr(e, 11) ^ rotr(e, 25);
        const ch = (e & f) ^ (~e & g);
        const t1 = h +% S1 +% ch +% K[i] +% w[i];
        const S0 = rotr(a, 2) ^ rotr(a, 13) ^ rotr(a, 22);
        const maj = (a & b) ^ (a & c) ^ (b & c);
        const t2 = S0 +% maj;
        h = g; g = f; f = e; e = d +% t1;
```

```
        d = c; c = b; b = a; a = t1 +% t2;
    }

    // 4. Acumular las variables de trabajo en el estado.
    state[0] +%= a; state[1] +%= b; state[2] +%= c; state[3] +%= d;
    state[4] +%= e; state[5] +%= f; state[6] +%= g; state[7] +%= h;
}

// Hash completo: procesa el mensaje en bloques, padea el último, escribe el resumen.
pub fn sha256(msg: []const u8, out: *[32]u8) void {
    var state = H0;
    var block: [64]u8 = undefined;
    var block_w: [16]u32 = undefined;

    // Procesar bloques completos del mensaje original.
    var i: usize = 0;
    while (i + 64 <= msg.len) : (i += 64) {
        @memcpy(block[0..64], msg[i..i+64]);
        for (0..16) |j| block_w[j] = readU32(block[j*4..j*4+4]);
        compress(&state, block_w);
    }

    // Padding del último bloque: byte 0x80, después ceros, después la
    // longitud original (en bits) como u64 big-endian en los 8 últimos bytes.
    const remaining = msg.len - i;
    @memcpy(block[0..remaining], msg[i..]);
    block[remaining] = 0x80;
    const bit_len: u64 = @as(u64, msg.len) * 8;

    if (remaining + 1 + 8 <= 64) {
        // El padding cabe en el mismo bloque.
        for (remaining + 1..56) |k| block[k] = 0;
        var k: usize = 0;
        while (k < 8) : (k += 1) block[56 + k] = @truncate(bit_len >> @as(u6, @intCast((7 - k) * 8)));
        for (0..16) |j| block_w[j] = readU32(block[j*4..j*4+4]);
        compress(&state, block_w);
    } else {
        // El padding requiere un bloque adicional.
        for (remaining + 1..64) |k| block[k] = 0;
        for (0..16) |j| block_w[j] = readU32(block[j*4..j*4+4]);
        compress(&state, block_w);
        for (0..56) |k| block[k] = 0;
        var k: usize = 0;
        while (k < 8) : (k += 1) block[56 + k] = @truncate(bit_len >> @as(u6, @intCast((7 - k) * 8)));
        for (0..16) |j| block_w[j] = readU32(block[j*4..j*4+4]);
        compress(&state, block_w);
    }

    // Escribir el estado final como 32 bytes big-endian.
    for (0..8) |j| writeU32(out[j*4..j*4+4], state[j]);
}

// Ejemplo de uso.
pub fn main() void {
    var resumen: [32]u8 = undefined;
    sha256("Cuadernos Lacre", &resumen);
    for (resumen) |byte| std.debug.print("{x:0>2}", .{byte});
    std.debug.print("\n", .{});
    // Imprime: ae6bdea6bbf5476889e0651a31f3dc1612fc61497477e21a95cabae2a6886c3e
}
```

Kull kitba mill-ġdid f'lingwa oħra li ssegwi l-istess struttura —kostanti inizjali, espansjoni tal-iskeda (schedule), erba' u sittin rawnd, akkumulazzjoni— tipproduċi l-istess riżultat. L-algoritmu m'għandux sigrieti: il-valur tiegħu jinsab f'li l-proprjetajiet elenkati hawn fuq jibqgħu jinżammu wara għoxrin sena ta' kriptanaliżi pubblika fuq eluf ta' għajnejn.

Jekk tmur lura f'qiegħ dan l-artiklu, tara siġill hexadecimal ta' erba' u sittin karattru. Huwa x-SHA-256 tat-test li għadek kemm qrajt, f'din il-lingwa. Jekk nittradux l-artiklu, is-siġill ikun ieħor; jekk tinbidel kelma tal-verżjoni Maltija, is-siġill Malti jinbidel. Is-siġill ma jipproteġix il-kontenut —għal dan hemm għodod oħra— iżda jidentifikah b'mod uniku. U dan,

anke jekk jinstema' modest, huwa biżżejjed biex l-ebda pass fil-katina editorjali ma jkun jista' jbiddel dak li ntqal mingħajr ma jinnota ħadd. Il-bqija —ikkriptar, iffirmar, identifikazzjoni— jinbena fuq din l-idea sempliċi.

Nota editorjali: meta dawn il-Cuadernos isemmu kumpaniji jew prodotti, mhux biex jakkużaw. Dawk li jibnuhom jagħmlu xogħol li miljuni ta' nies jużaw u japprezzaw. Dak li qed nindikaw huwa strutturali — il-mudell, mhux il-marka. Il-marki jidhru bħala eżempju għax huma dawk li l-qarrej jagħraf.

Sorsi u aktar qari

- NIST — *FIPS PUB 180-4: Secure Hash Standard (SHS)*, Awwissu ta' 2015. Speċifikazzjoni uffiċjali tal-familja SHA-2, inkluż SHA-256.
- RFC 6234 — *US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)*, IETF, Mejju ta' 2011. Verżjoni normativa għall-implimentaturi.
- Ferguson, N.; Schneier, B.; Kohno, T. — *Cryptography Engineering: Design Principles and Practical Applications* (Wiley, 2010). Kapitoli 5 u 6 ikopru funzjonijiet hash u l-użi leġittimi u illegali tagħhom.
- Nakamoto, S. — Bitcoin: A Peer-to-Peer Electronic Cash System (2008). Eżempju prattiku tal-użu ta' SHA-256 biex jikkatenaw blokki fi struttura immutabbli b'kostruzzjoni.
- Regolament (UE) 910/2014 (eIDAS) — qafas tas-siġillaturi tal-ħin kwalifikati. SHA-256 hija l-funzjoni ta' referenza għall-firem u s-siġilli elettroniċi kwalifikati maħruġa fl-UE.
- Implimentazzjoni ta' referenza f'Zig: `std.crypto.hash.sha2.Sha256` fir-repożitorju uffiċjali tal-lingwa (*github.com/ziglang/zig* → `lib/std/crypto/sha2.zig`). Hija l-verżjoni ottimizzata u awditjata li fil-fatt juża Solo2. Utli biex tikkuntrasta mal-implimentazzjoni didattika tal-appendiċi.

← PreċedentiSchrems II, ħames snin waraLi jmiss →Kill switch u l-qbid istituzzjonali

Letturi riċenti

- Analiżi · 18 ta' Mejju 2026 Privatezza reali vs apparenti: il-mistoqsijiet li jaqbel li tistaqsi lilek innifsek
- Analiżi · 18 ta' Mejju 2026 Self-hosting bħala prattika professjonali
- Kunċett · 18 ta' Mejju 2026 L-24 kelma: x'inhi identità kriptografika

Ħu dan l-artiklu miegħek kull fejn għandek bżonnu.

↓ Markdown ↓ Test sempliċi ↓ PDF

Il-fajl se jitniżżel fuq it-tagħmir tiegħek. Minn hemm tista' ssalvah, timportah f'Solo2 jew taqsmu kull fejn tixtieq. Cuadernos ma jiddeċidix id-destinazzjoni għalik.

Siġill tax-xama' · SHA-256 da096be67b1a95c770a2dc29c6dd976c502beae4b9c6ddce33c952fb2e8d1a5f

Cuadernos Lacre · Pubblikazzjoni ta' Menzuri Gestión S.L. ·
miktuba minn R.Eugenio · editjata mit-tim ta' Solo2.