Cad is SHA-256 ann i ndáiríre

Lorg mhatamaiticiúil a oireann i seasca a ceathair carachtar agus a athraíonn go hiomlán má bhogtar camóg amháin sa bhuntéacs. Cén fáth a dtugaimid séala céir digiteach air.

Chun é a chur go simplí: Samhlaigh meaisín a léann téacs ar bith agus a sheolann seicheamh 64 carachtar ar ais. Má théann an téacs céanna isteach, tagann an seicheamh céanna amach. Má bhogann tú camóg amháin, tá an seicheamh go hiomlán difriúil. Is é an seicheamh sin an séala céir digiteach.

An smaoineamh simplí taobh thiar den ainm teicniúil

Samhlaigh go bhfuil meaisín ann le sliotán amháin agus scáileán amháin. Tríd an sliotán cuireann tú téacs isteach: focal, frása, úrscéal iomlán. Ar an scáileán feictear, chuimhneacháin ina dhiaidh sin, seicheamh de seasca a ceathair carachtar go díreach. Tugaimid *hash* nó *achoimre chripteagrafach* ar an seicheamh sin don léitheoir gairmiúil; don léitheoir ginearálta, is féidir linn lorg mhatamaiticiúil an téacs a thabhairt air faoi láthair, mar atá lorg méire duine.

Má chuireann tú an téacs céanna isteach faoi dhó, taispeánann an meaisín an lorg céanna an dá uair. Má chuireann tú téacs atá beagán difriúil isteach — camóg amháin bogtha, ceannlitir a bhíonn ina litir bheag — taispeánann an meaisín lorg atá go hiomlán difriúil ón gcéad cheann. Ní cosúil leis: difriúil. Is iad an dá airí sin le chéile — an cinntitheachas agus an íogaireacht — an smaoineamh simplí. Is é an chuid eile de SHA-256 an innealra a fhágann go gcomhlíonann siad go maith.

Is fiú a rá ón tús cad nach ndéanann an meaisín. Ní chriptíonn sé an téacs. Ní chuireann sé i bhfolach é. Ní shábhálann sé é. Féachann an meaisín ar an téacs, ríomhann sé an lorg, agus déanann sé dearmad ar an téacs. Ní féidir an téacs a tháirg é a athchruthú ón lorg; ní ligeann sé ach, i bhfianaise téacs iarrthóra, seiceáil an bhfuil sé ag teacht leis an mbunleagan nó nach bhfuil. Sin an fáth a deirimid gur achoimre *aon treo* é: téann sé, ní thagann sé ar ais.

Ní hionann hash agus criptiú

Is minic a bhíonn mearbhall ann agus is fiú é a ghlanadh suas: is oibríochtaí difriúla iad criptiú agus haiseáil. Is éard atá i gceist le criptiú ná téacs a athrú sa chaoi is nach féidir ach le sealbhóir an eochair é a chur ar ais ina bhunfhoirm. Is éard atá i gceist le haiseáil ná lorg an téacs a tháirgeadh nach féidir an buntéacs a aisghabháil uaidh go deo, le heochair nó gan í. Tá an chéad cheann inchúlaithe de réir dearadh; an dara ceann, do-aisiompaithe de réir dearadh.

Is tábhachtach an toradh praiticiúil. Nuair a deir aip «coimeádaimid do phasfhocal criptithe», tá duine éigin ann a bhfuil an eochair aige chun é a dhíchriptiú — an aip féin, ar aon nós. Nuair a deir aip «coimeádaimid do phasfhocal haiseáilte», ní féidir leis an aip féin an bunphasfhocal a léamh fiú más mian léi; ní féidir léi ach seiceáil an dtáirgeann an ceann a scríobhann tú an lorg céanna arís. Tá an dara samhail, déanta go maith, i bhfad níos fearr ná an chéad cheann chun pasfhocail a stóráil. Feicfimid níos déanaí cén fáth a dteastaíonn rud éigin níos mó ná SHA-256 amháin le «déanta go maith».

Na ceithre airí a fhágann go bhfuil hash cripteagrafach úsáideach

Comhlíonann feidhm hash a bhfuil an aidiacht *cripteagrafach* tuillte aici ceithre airí:

1. **Cinntitheachas.** Táirgeann an t-ionchur céanna an lorg céanna i gcónaí.
2. **Éifeacht maoime.** Táirgeann athrú beag ar an ionchur lorg atá go hiomlán difriúil, gan aon chosúlacht infheicthe leis an gceann roimhe sin.

3. **Friotaíocht in aghaidh inbhéartaithe.** I bhfianaise loirg, ní féidir go ríomhaireachtúil an téacs a tháirg é a fháil.
4. **Friotaíocht in aghaidh imbhuailtí.** Ní féidir go ríomhaireachtúil dhá théacs dhifriúla a fháil a tháirgeann an lorg céanna.

Ní chiallaíonn «ní féidir go ríomhaireachtúil» «go bhfuil sé dodhéanta go matamaiticiúil». Ciallaíonn sé go sáraíonn an costas in am, i bhfuinneamh agus in airgead chun é sin a bhaint amach méid an chumais ríomhaireachta go léir atá ar fáil go réasúnta. Maidir le SHA-256, déantar an teorainn sin a thomhas sna mílte trilliún bliain fiú do na cuir chuige is dóchaí le crua-earraí speisialaithe. Rud atá, chun críocha praiticiúla an léitheora, mar an gcéanna le «ní féidir é a dhéanamh».

SHA-256, go sonrach

Deir an t-ainm go léir é. Seasann SHA do *Secure Hash Algorithm*: algartam hash slán. Léiríonn an uimhir 256 méid an loirg i ngiotáin: dhá chéad caoga a sé giotán, is é sin tríocha a dó beart, atá le feiceáil i heicsidheachúil mar na seasca a ceathair carachtar a aithníonn an léitheoir cheana féin. D'fhoilsigh NIST na Stát Aontaithe, an comhlacht a dhéanann caighdeánú ar an gcineál seo feidhmeanna, an caighdeán in 2001 mar chuid den teaghlach SHA-2; is as 2015 an leagan reatha den caighdeán, FIPS 180-4.

Dóibh siúd nach bhfuil a fhios acu go fóill cad is giotáin agus bearta ann:

```
1 giotán    →  0 nó 1       (lasc: casta air nó as)
1 beart     →  8 ngiotán    (256 teaglaim fhéideartha)
32 beart    →  256 giotán   (an lorg SHA-256)
```

Inis an uimhir 256 ag deireadh an ainm méid an loirg i ngiotáin. In heicsidheachúil — córas uimhrithe le sé shiombail déag in ionad a deich — oireann na 256 giotán sin i 64 carachtar go díreach. Is iad sin na 64 carachtar a fheiceann tú ag bun gach Cuaderno.

Is fiú na toisí nóiméad a thabhairt dóibh. Ligeann dhá chéad caoga a sé giotán do dhá cheann cumhacht dhá chéad caoga a sé luach difriúil: uimhir le seachtó a hocht ndigit dheachúla, i bhfad níos mó ná an líon measta adamh sa chruinne inbhraite. Titeann gach téacs ar domhan — gach leabhar, gach ríomhphost, gach teachtaireacht — ar cheann de na luachanna sin. Tá an dóchúlacht go dtiocfaidh dhá théacs dhifriúla le chéile trí thaisme, chun críocha praiticiúla, doríofa ó nialas.

Cén chaoi a bhfeiceann sé i gcód

I Zig, an teanga ina scríobhaimid na píosaí a thacaíonn le Solo2, tá ríomh séala SHA-256 de théacs mar seo:

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

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

D'iarr muid díreach ar leabharlann chaighdeánach Zig an SHA-256 den téacs idir comharthaí athfhriotail a ríomh. Tar éis an ghlao, tá an tríocha a dó beart san athróg *resumen* a dhéanann suas an séala ina fhoirm amh; nuair a thaispeántar iad ar an scáileán i heicsidheachúil, is iad na seasca a ceathair carachtar iad a fheiceann tú ag bun an ailt seo. Dá n-athróimis *Cuadernos Lacre* go *Cuadernos lacre* — ceannlitir amháin níos lú — d'athródh an séala go hiomlán. Sin é, i gcúig líne, an t-airí lárnach a thacaíonn leis an gcuid eile. Dóibh siúd ar mian leo feiceáil conas a oibríonn sé go hinmheánach, ag deireadh an ailt tá leagan inléite den algartam le tuairimí céim ar chéim san áireamh.

Cén fáth a dtugaimid séala céir air

I gcomhfhreagras na hEorpa ón gcúigiú haois déag go dtí an naoú haois déag, dhún an chéir an litir. Braon de chéir leáite, séala brúite air, agus bhí an litir marcáilte ar bhealach nach bhféadfaí a athdhéanamh. Níor chosain sé an t-ábhar ón duine fiosrach — d'fhéadfaí an páipéar a léamh in aghaidh an tsolais, d'fhéadfaí an chéir a bhriseadh — ach léirigh sé é. Bhí aon athrú ar an dúnadh le feiceáil ag an bhfaighteoir fiú sular osclaíodh an páipéar. Níor choisc an chéir an damáiste; d'fhógair sé é.

Comhlíonann SHA-256 chorp gach Cuaderno an fheidhm chéanna ina leagan digiteach. Dá n-athródh focal amháin den alt idir an t-am a foilsíodh é agus an t-am a léann tú é, ní bheadh an séala heicsidheachúil ag bun an téacs ag teacht le SHA-256 an téacs atá os do chomhair a thuilleadh. D'fhéadfadh aon léitheoir le cúig líne de chód é a sheiceáil. Ní féidir leis an bhfoilseachán a stair a athscríobh gan an séala á nochtadh. Ní chosnaíonn sé in aghaidh damáiste; cuireann sé ar fáil é le fíorú.

An rud nach bhfuil i hash

Ceithre mheabhrúchán oibriúcháin don té a chinneann nó a dhéanann iniúchadh ar chórais:

1. **Criptiú.** Déanann hash achoimre; ní chuireann sé i bhfolach é. Más mian leat nach féidir an téacs a léamh, ní mór duit é a chriptiú, ní é a haiseáil.
2. **An t-údar a fhíordheimhniú.** Ní deir hash cé a scríobh an téacs, ach cén téacs a haiseáladh. Chun údar a cheangal leis an téacs, teastaíonn síniú cripteagrafach os cionn an hash, ní an hash amháin.
3. **Pasfhocail a stóráil.** Tá gaiste anseo ar fiú a thuiscint. Tá SHA-256 deartha chun a bheith an-tapa — rud atá go maith do go leor rudaí, ach go dona don cheann seo. Is féidir le hionsaitheoir le crua-earraí speisialaithe na billiúin pasfhocal in aghaidh an tsoicind a thriail in aghaidh hash SHA-256 go dtí go bhfaighidh sé do cheannsa. Chun pasfhocail a shábháil ní mór feidhmeanna díorthaithe eochair atá mall d'aon ghnó a úsáid ar nós Argon2, scrypt nó bcrypt, i gcomhar le *salann* (sonraí randamacha uathúla in aghaidh an úsáideora, rud a fhágann nach bhfuil an hash céanna ag beirt a bhfuil an pasfhocal céanna acu).
4. **Léigh an hash mar aitheantóir an údair.** Ní hé. Aithníonn hash an t-ábhar. Má haiseann beirt an focal *dia duit* le SHA-256, faigheann an bheirt acu an achoimre chéanna — agus sin an t-airí lárnach, ní locht: dá mba achoimrí difriúla iad, ní fhéadfaimis seiceáil an raibh an méid a foilsíodh ag teacht leis an méid a fuarthas.

Cá bhfeictear SHA-256 i do shaol laethúil

Cé nach bhfeiceann tú é, tacaíonn SHA-256 le cuid mhaith de na rudaí a úsáideann tú go laethúil ar an idirlíon. Tógtar blocshlabhra Bitcoin trí SHA-256 gach bloic a nascadh leis an gcéad bhloc eile; má athraítear bloc san am a chuaigh thart, ní mór an slabhra iomlán ina dhiaidh sin a athríomh. Déanann Git, an córas leis an bhfuil an cód de leath an domhain leaganaithe, gach deimhniú a aithint tríd an SHA-256 (i leaganacha le déanaí) nó trína réamhtheachtaí SHA-1 (i leaganacha níos sine) dá ábhar iomlán. Tá lorg SHA-256 bainteach leis na teastais HTTPS a fhíoraíonn céannacht suímh ghréasáin nuair a théann tú isteach. Is minic go mbíonn SHA-256 foilsithe ag an bhforbróir ag gabháil le híoslódálacha bogearraí ionas gur féidir leat a fhíorú nár athraíodh an comhad ar an mbealach. Agus, mar a dúirt muid, ag bun gach Cuadernos Lacre.

Don léitheoir gairmiúil

Ceithre mheabhrúchán oibriúcháin don té a chinneann nó a dhéanann iniúchadh ar chórais:

1. Ní hionann hash agus criptiú. Má chuireann soláthraí an dá théarma in iúl ina dhoiciméadú teicniúil, is fiú fiafraí cad go díreach atá i gceist aige.
2. Chun pasfhocail a stóráil, níor cheart SHA-256 amháin a úsáid go deo. Tá SHA-256 ró-tapa don tasc seo (féach pointe 3 de *An rud nach bhfuil i hash*). Is é **Argon2id** an caighdeán reatha: mall de réir dearadh, inchumraithe de réir cumas an fhreastalaí, i gcomhar le *salann* randamach difriúil in aghaidh an úsáideora.
3. Maidir le hiomláine doiciméad — conarthaí, comhaid, taifid — is é SHA-256 an caighdeán tagartha fós. Is é an ceann a úsáideann séalaithe ama cáilithe san AE.
4. Le haghaidh caomhnú fadtéarmach (blianta fada) is fiú SHA-3 nó SHA-512 a ríomh agus a chartlannú freisin in éineacht le SHA-256; molann stuama cripteagrafach gan brath ar fheidhm amháin le linn cartlanna céad bliain.

Go teicniúil, tugtar tógáil **Merkle-Damgård** ar an struchtúr atáite seo — áit a gcoimeádtar an staid idirmheánach idir bloic ionchuir —, an patrún ar a bhfuil SHA-1, SHA-2 (lena n-áirítear SHA-256) agus go leor feidhmeanna haise clasaiceacha eile bunaithe. Tréigeann SHA-3 an struchtúr Merkle-Damgård, áfach, i bhfabhar ailtireachta difriúla ar a dtugtar *spúinse*.

Conas a oibríonn SHA-256, céim ar chéim, i ngnáthchaint

Samhlaigh go bhfuil an ciorcad fada ceann de na dominoes is casta ar domhan tógtha agat: na mílte mír, na dosaenacha de dhrisí, droichid mheicniúla agus rampaí a théann trasna an tseomra ar fad, curtha go cúramach mír ar mhír.

Má thugann tú cnag don chéad mhír, titeann an slabhra i seicheamh beacht in-athdhéanta. An socrú céanna, an cnag tosaigh céanna → patrún deiridh céanna de mhír thite, arís agus arís eile.

Seo an rud suimiúil: bog **mír amháin** leath-cheintiméadar ar leataobh sula dtosaíonn tú agus cnag arís. Fanann rampa a bhí ceaptha a ghníomhachtú gan bogadh, ní thiteann droichead, scaoiltear dhris dhifriúil. Tá patrún deiridh na míreanna ar an urlár go hiomlán do-aitheanta i gcomparáid leis an gcéad cheann.

Is é SHA-256 an ciorcad seo go matamaiticiúil. Is é an téacs a scríobhann tú staid tosaigh na míreanna. Is é an t-algartam an cnag a scaoileann an easa. Agus is é an toradh deiridh — an rud ar a dtugaimid *hais* — an grianghraf seasta den urlár nuair atá gach rud stoptha. Athraigh camóg amháin sa bhuntéacs agus beidh an grianghraf go hiomlán difriúil. Chomh simplí sin, agus chomh suntasach sin.

Céim 1. An téacs a aistriú go mír dhénártha. Ní thuigeann ríomhairí litreacha; aistríonn siad iad ar dtús go huimhreacha (ASCII) agus na huimhreacha go dénártha (aonanna agus nialais). Déantar 8 mír bhána nó dhubha de gach litir: is é *A* ná `01000001`, is é *B* ná `01000010`, is é an spás ná `00100000`. Déantar líne fhada de mhíreanna bána agus dubha de do théacs ar fad — focal, conradh, úrscéal.

Céim 2. Líonadh suas go dtí an méid caighdeánach. Próiseálann an ciorcad an líne i *rannóga* de 512 mír go beacht. Mura sroicheann do theachtaireacht iolra de 512, cuirtear mír mharcála (le luach `10000000`) díreach i ndiaidh an téacs agus ansin nialais go dtí go mbeidh an rannóg iomlán. Coimeádtar na 64 suíomh deireanacha de gach rannóg chun fad bunaidh an téacs a thaifeadadh. Mar sin bíonn a fhios ag an gciorcad i gcónaí cá raibh deireadh leis an bhfíor-ábhar agus cá raibh tús leis an líonadh.

Céim 3. Na hocht mír mháistreachta a chur síos. Sula dtosaímid, leagaimid **ocht mír mháistreachta** ar an mbord i staid tosaigh bheacht. Ní rún iad na hocht mír seo: tá a luach tosaigh socraithe ag riail mhatamaiticiúil phoiblí (fréamhacha cearnacha na chéad ocht bhuimhreach phríomha — 2, 3, 5, 7, 11, 13, 17, 19 — agus na chéad bhiotaí de chuid dheachúil gach fréimhe). Tosaíonn gach duine, in aon áit ar an bpláinéad, leis na hocht mír mháistreachta chéanna sa staid chéanna. Is é an cinniúint atá acu ná go mbeidh an easa á mbrú agus á n-athrú.

Céim 4. An easa mhór: seasca a ceathair babhta brú. Seo an áit a dtosaíonn an taispeántas. Cuirtear an chéad rannóg de 512 mír de do théacs ag bualadh in aghaidh na n-ocht mír mháistreachta. Ach ní thiteann siad go léir ag an am céanna: déanann an meicníocht **seasca a ceathair babhta as a chéile**. I ngach babhta déantar trí oibríocht leis na míreanna:

- **An Timpeallán** (rothlú). Bogann na míreanna i gcioral: téann na cinn ar dheis go dtí an taobh clé. Ní chailltear aon mhír agus ní chuirtear aon mhír nua leis; déantar iad a athordú agus iad ag dul timpeall an timpealláin uair amháin go hiomlán. Is bealach saor in-athraithe é seo chun faisnéis a athdháileadh.
- **An Tonnadóir Loighciúil** (XOR). Téann na míreanna trí thonnadóir a chuireann i gcomparáid iad beirt ar bheirt: má tá an dath céanna orthu, tagann mír bhán amach; má tá siad difriúil, tagann mír dhubh amach. Is é seo an oibríocht is simplí den loighic dhénártha, ach nuair a chuirtear le chéile é le rothlú an timpealláin éiríonn sé thar a bheith cumhachtach chun faisnéis a mheascadh gan í a chailliúint.
- **An Ró-shreabhadh** (suimiú modúlach). Cuirtear an toradh le *mír bhrú thairiseach* a thagann ó liosta poiblí de sheasca a ceathair tairiseach (fréamhacha ciúbacha na chéad seasca a ceathair uimhir phríomha). Má ghineann an suimiú míreanna breise nach n-oireann sa spás de 32 mír atá beartaithe, caitear na míreanna breise sin amach. Níl spás ar an mbord ach do 32 mír, níl spás do cheann ar bith eile.

Ag deireadh bhabhta a seasca a ceathair, bhí tionchar ag gach ceann de na míreanna i rannóg do théacs ar staid na n-ocht mír mháistreachta. Tá fuinneamh an bhrú tar éis taisteal tríd an gciorcad ar fad.

Céim 5. An chéad rannóg eile a chur leis (gan atosú). Má bhí do théacs fada agus má tá rannóg eile de 512 mír le próiseáil, **ní dhéantar an ciorcad a atosú**. Fanann na hocht mír mháistreachta mar a d'fhág an chéad easa iad, agus scaoiltear an dara rannóg ina n-aghaidh chun seasca a ceathair babhta eile a thosú. Tá sé cosúil le seomra nua lán de dhominoes a chur ag deireadh an tseomra atá díreach tar éis titim: tá titim an dara seomra ag brath go hiomlán ar an mí-ord sa chéad seomra.

Céim 6. An grianghraf deiridh a thógáil. Nuair nach bhfuil aon rannóga eile le próiseáil, stopann an easa. Féachaimid ar an staid dheiridh ina bhfuil na hocht mír mháistreachta. Aistrímid an socrú sin go cód litreacha agus uimhreacha sa chóras heicsidheachúil. Is é an toradh ná teaghrán de sheasca a ceathair carachtar go beacht: is é sin do shéala SHA-256.

Tagann ceithre airí as an mbealach a bhfuil an ciorcad tógtha:

1. **Cinntitheacht.** Táirgeann an téacs céanna an grianghraf deiridh céanna i gcónaí, ar aon ríomhaire ar domhan. Nialas randamachta, nialas iontas.
2. **Éifeacht na heasa.** Camóg breise, litir mhór athraithe, síneadh fada dearmadta: beidh an grianghraf go hiomlán do-aitheanta. Is é seo an t-íogaireacht mhór a thuairiscigh muid ag an tús.
3. **Treo amháin amháin.** Bunaithe ar an ngrianghraf deiridh, ní féidir leat an buntéacs a athchruthú. Scriosann na rothluithe, na tonnadóirí agus na ró-shreafaí an fhaisnéis threorach ar fad faoi *cá as a tháinig gach biot* agus ní choimeádtar ach *an méid a suimíodh san iomlán*.
4. **Friotaíocht in aghaidh imbhuailtí.** I gcaitheamh cúig bliana is fiche de chripteanailís phoiblí, níor éirigh le duine ar bith dhá théacs dhifriúla a aimsiú a bhfuil an grianghraf deiridh céanna acu. Agus tá an deacracht a bhaineann leis sin lasmuigh de chumais ríomhaireachta aon sibhialtachta is féidir a shamhlú le réasún.

Cuireann an t-aguisín cóid a leanann na sé chéim seo i bhfeidhm go beacht i Zig. Anois is féidir leat é a léamh agus fios agat cad is brí le gach oibríocht bhiotaí, in ionad glacadh leis na hionramhálacha go dall.

Gluais theicniúil

Don léitheoir ar mian leis tuiscint a fháil ar cad a dhéanann gach oibríocht. Is féidir leat é seo a scipeáil go saor: tuigtear an t-alt fós gan é.

ASCII agus Unicode — conas a dhéantar uimhreacha de litreacha. Ní fheiceann ríomhairí litreacha; feiceann siad uimhreacha. Sanntar uimhir shonrach do gach carachtar méarchláir le caighdeán ar a dtugtar **ASCII** (*American Standard Code for Information Interchange*, ó 1963): is é 65 an *A*, is é 66 an *B*, is é 97 an *a*, is é 48 an *0*, is é 32 an spás, is é 44 an chamóg. Leathnaíonn córais nua-aimseartha é seo le **Unicode**, a shannann uimhir do gach carachtar de gach aibítir ar domhan: Coireallach, Arabach, Síneach, Seapánach, agus fiú emoji. Nuair a scríobhann tú carachtar nó nuair a osclaíonn tú comhad téacs, léann an ríomhaire an uimhir sa chúlra, ní an cruth ar an scáileán. Oibríonn SHA-256 ar na huimhreacha seo, ag déileáil le haon téacs mar sheicheamh fada d'uimhreacha. Sin an fáth gur féidir leis alt i Spáinnis, dán i Seapáinis agus comhad dénártha a shéalú leis an algartam céanna.
XOR — an comparadóir biot ar bhiot. Tá XOR (fuaimnithe *«exor»*, ón mBéarla *exclusive or*, «nó eisiach») ar cheann de na hoibríochtaí is simplí is féidir le ríomhaire a dhéanamh le dhá uimhir dhénártha. Cuireann sé dhá bhiot i gcomparáid suíomh ar shuíomh agus tugann sé ar ais: **1** má tá go beacht ceann amháin den bheirt acu mar 1 (ceann amháin ach ní an bheirt acu), **0** má tá an bheirt acu mar an gcéanna (iad araon mar 0 nó iad araon mar 1). Sampla: is é `0110` an XOR de `1010` agus `1100`. Tá airí suntasach aige: tá sé in-athraithe — má dhéanann tú XOR faoi dhó leis an eochair chéanna, filleann tú ar an mbunleagan. Sin an fáth gurb é capall oibre na cripteagrafaíochta é: meascann sé biotacha gan faisnéis a chailliúint, ach ní nochtann an toradh aon rud faoi na hionchuir mura bhfuil ceann acu ar eolas agat.
Heicsidheachúil — comhaireamh i mbonn 16. Úsáideann beagnach gach uimhir sa ghnáthshaol deich ndigit (0-9). Úsáideann an córas heicsidheachúil sé cinn déag: na gnáth-uimhreacha 0-9 móide sé litir a sheasann do na luachanna seo a leanas: `A` = 10, `B` = 11, `C` = 12, `D` = 13, `E` = 14, `F` = 15. Cén fáth sé cinn déag? Toisc go smaoiníonn ríomhairí i ngrúpaí de cheithre bhiot, agus is féidir le ceithre bhiot sé luach déag dhifriúla a léiriú go beacht — mar sin, comhfhreagraíonn carachtar heicsidheachúil amháin go glan do cheithre bhiot. Tá rian SHA-256 256 biot ar fhad, is é sin go beacht **64 carachtar heicsidheachúil**. Dá scríobhfaimis é i ngnáth-dheachúlacha, thógfadh sé thart ar 78 digit agus bheadh sé níos deacra. Is rogha aeistéitiúil agus dhlúth í; is é an uimhir chéanna atá sa chúlra.
Rothlú biotacha — an timpeallán dénártha. Samhlaigh sraith de sheacht mbolgán solais, cuid acu ar lasadh (1) osa chuid acu múchta (0): `1 0 1 1 0 0 1`. Is éard atá i gceist le rothlú ar dheis suíomh amháin ná an bolgán ar dheis ar fad a thógáil, é a thabhairt go dtí an taobh clé ar fad agus na cinn eile a bhogadh áit amháin ar dheis: `1 1 0 1 1 0 0`. Ní chaillтear aon bholgán agus ní chuirtear aon cheann nua leis: ní dhéanann siad ach damhsa i gcioral. Úsáideann SHA-256 rothlú biotacha na céadta uair i ngach ríomh; is bealach saor gan chaillteanas é chun faisnéis a athdháileadh laistigh den staid.
Tairisigh *«nothing-up-my-sleeve»* — cén fáth a dtagann siad ó uimhreacha príomha. Níor roghnaíodh na hocht mír mháistreachta agus na seasca a ceathair tairiseach babhta de SHA-256 go randamach. Tagann siad ó na fréamhacha cearnacha agus ciúbacha de na chéad uimhreacha príomha. Cén fáth? Mar gheall go raibh tairisigh *«gan aon rud i bhfolach»* (*«nothing-up-my-sleeve»*) ag teastáil óna ndearthóirí: luachanna ar féidir le duine ar bith a mbunús a fhíorú. Dá ndéarfadh duine éigin *«bíodh muinín agat asam: úsáid an uimhir randamach 32-biot seo»*, bheadh amhras ort go réasúnta faoi laige i bhfolach nó faoi dhoras cúil. Ach is féidir le duine ar bith a bhfuil áireamhán aige a sheiceáil gurb iad na chéad 32 biot de fhréamh chearnach 2 ná `0x6a09e667`. Is luachanna matamaiticiúla, poiblí agus in-athdhéanta iad: ní féidir le haon chleas i bhfolach sleamhnú isteach san oideas.

Aguisín: SHA-256 i gcód inléite

Tá an t-aguisín seo don léitheoir ar mian leis an algartam a fheiceáil ón taobh istigh. Is cur i bhfeidhm didactach é i Zig a leanann an tsonraíocht FIPS 180-4. Ní hé an leagan a úsáideann Solo2 é — tá an fíorleagan i `std.crypto.hash.sha2.Sha256` de leabharlann chaighdeánach Zig, optamaithe agus iniúchta. Ach tá an t-algartam mar an gcéanna: is é an méid a fheiceann tú anseo, céim ar chéim, an méid a tharlaíonn nuair a dhéanann an glao cúig charachtar sin a chuid oibre.

```
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
}
```

Táirgeann aon athscríobh i dteanga eile a leanann an struchtúr céanna — tairisigh tosaigh, leathnú an sceidil, seasca a ceathair babhta, carnadh — an toradh céanna. Níl aon rúin ag an algartam: is é an luach atá leis ná go leanann na hairíonna atá liostaithe thuas ag seasamh tar éis fiche bliain de chripteasholáthar poiblí thar na mílte súl.

Má théann tú ar ais go dtí bun an ailt seo, feicfidh tú séala heicsidheachúil seasca a ceathair carachtar. Is é SHA-256 an téacs a léigh tú díreach, sa teanga seo. Dá n-aistreofaimis an t-alt, bheadh an séala difriúil; dá n-athródh focal den leagan Spáinnise, d'athródh an séala Spáinnise. Ní chosnaíonn an séala an t-ábhar — tá uirlisí eile ann chuige sin — ach aithníonn sé é go huathúil. Agus is leor sin, chomh measartha agus a fhuaimeann sé, ionas nach féidir le haon chéim den slabhra eagarthóireachta an méid a dúradh a athrú gan é a thabhairt faoi deara. Tógtar an chuid eile — criptiú, síniú, aithint — ar an smaoineamh simplí seo.

Nóta eagarthóireachta: nuair a ainmníonn na Cuadernos seo cuideachtaí nó táirgí, ní chun cúiseamh a dhéanamh é. Déanann na daoine a thógann iad obair a úsáideann agus a dtaitníonn na milliúin daoine léi. Is é an rud a léirímid ná struchtúrach — an múnla, ní an branda. Dealraíonn brandaí mar shamplaí toisc gurb iad na cinn a n-aithníonn an léitheoir iad.

Foinsí agus léitheoireacht bhreise

- NIST — *FIPS PUB 180-4: Secure Hash Standard (SHS)*, Lúnasa 2015. Sonraíocht oifigiúil an teaghlaigh SHA-2, lena n-áirítear SHA-256.
- RFC 6234 — *US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)*, IETF, Bealtaine 2011. Leagan normatach d'fhorbróirí.
- Ferguson, N.; Schneier, B.; Kohno, T. — *Cryptography Engineering: Design Principles and Practical Applications* (Wiley, 2010). Clúdaíonn Caibidlí 5 agus 6 feidhmeanna hash agus a n-úsáidí dlisteanacha agus neamhdhlisteanacha.
- Nakamoto, S. — Bitcoin: A Peer-to-Peer Electronic Cash System (2008). Sampla praiticiúil de SHA-256 a úsáid chun bloic a nascadh i struchtúr do-athraithe trí thógáil.
- Rialachán (AE) 910/2014 (eIDAS) — creat do shéalaithe ama cáilithe. Is é SHA-256 an fheidhm thagartha do shínithe agus séalaí leictreonacha cáilithe a eisítear san AE.
- Cur i bhfeidhm tagartha i Zig: `std.crypto.hash.sha2.Sha256` i stóras oifigiúil na teanga (*github.com/ziglang/zig* → `lib/std/crypto/sha2.zig`). Is é an leagan optamaithe agus iniúchta é a úsáideann Solo2 i ndáiríre. Úsáideach chun codarsnacht a dhéanamh leis an gcur i bhfeidhm didactach san aguisín.

← Roimhe seoSchrems II, cúig bliana níos déanaíAr aghaidh →Kill switch agus an gabháil institiúideach

Léitheoireacht le déanaí

- Anailís · 18 Bealtaine 2026 Príobháideacht iarbhír vs príobháideacht dhealraitheach: na ceisteanna ba chóir duit a chur ort féin
- Anailís · 18 Bealtaine 2026 Féin-óstáil mar chleachtas gairmiúil
- Coincheap · 18 Bealtaine 2026 Na 24 focal: cad is féiniúlacht chripteagrafach ann

Beir an t-alt seo leat áit ar bith a dteastaíonn sé uait.

↓ Markdown ↓ Téacs simplí ↓ PDF

Íoslódálfar an comhad chuig do ghléas. Ón áit sin is féidir leat é a shábháil, é a iompórtáil go Solo2 nó é a roinnt cibé áit is mian leat. Ní chinneann Cuadernos an ceann scríbe duitse.

Séala céir · SHA-256 6e60eec7b5da7f8778d0743d7085b52e29ee143013d5b32b804355371af23f44

Cuadernos Lacre · Foilseachán de chuid Menzuri Gestión S.L. ·
scríofa ag R.Eugenio · curtha in eagar ag foireann Solo2.

Ní úsáideann an suíomh seo fianáin agus ní lódálann sé acmhainní ó thríú páirtithe. Úsáideann sé córas tomhais anaithnid arna óstáil (Umami, ar ár bhfreastalaí Eorpach) agus an t-íosmhéid JavaScript is gá don dá rialaitheoir ceanntáisc: téama solais nó dorcha, agus roghnóir teanga. Gan rianairí, gan próifíliú, gan comhroinnt sonraí. Más mian leat sinn a leanúint: RSS.