Encryption minn tarf sa tarf, spjegat tassew

Dak li jgħidu l-fornituri meta jgħidu E2EE, u dak li ma jgħidux. Spjegazzjoni didattika tal-mekkaniżmu u l-limiti tiegħu, mingħajr it-tgeżwir tar-reklamar.

Biex inkunu ċari: WhatsApp jgħid li l-messaġġi tiegħek huma encrypted minn tarf sa tarf. Dan minnu — u mhux biżżejjed. Jekk il-backup imur għal iCloud jew Google Drive mingħajr encryption addizzjonali, l-encryption tinkiser fuq it-telefon tiegħek stess. Il-mistoqsija operattiva mhijiex jekk hux encrypted, iżda fejn jinsabu ċ-ċwievet.

Xi tfisser encryption, tassew

L-encryption ta' messaġġ tfisser li tibdlu f'xi ħaġa li tidher qisha ħoss għal kull min m'għandux ċerta informazzjoni msejħa ċavetta. L-operazzjoni ssir fuq l-apparat ta' min jibgħat u, biċ-ċavetta t-tajba, titreġġa' lura fuq l-apparat ta' min jirċievi. Bejniethom, il-messaġġ jivvjaġġa bħala suċċessjoni ta' bytes mingħajr tifsira apparenti. Dik hija l-idea sempliċi. Il-bqija tal-artiklu jittratta n-nuances li jibdluha, skont il-każ, f'garanzija reali jew f'tikketta tal-marketing.

L-aġġettiv *minn tarf sa tarf* — bl-Ingliż *end-to-end*, imqassar E2EE — iżid preċiżjoni. L-encryption ma ssirx biex server intermedju jkun jista' jaqraha u jwassalha. Isir sabiex iż-żewġ truf biss — l-apparat ta' min jibgħat u l-apparat ta' min jirċievi — ikollhom iċ-ċavetta. Kwalunkwe server li jgħaddi minnu l-messaġġ jara l-ħoss, mhux il-messaġġ. Dik hija d-differenza teknika bl-encryption *waqt it-tranżitu*, fejn il-kontenut jivvjaġġa encrypted minn server għal ieħor, iżda kull server li jgħaddi minnu jiddeċifrah biex jibagħtu mill-ġdid, u jirkupra temporanjament it-test ċar.

Il-paradoss tas-sigriet maqsum

Hemm problema ovvja. Biex żewġ persuni jkunu jistgħu jikkriptaw u jiddeċifraw messaġġi bejniethom, it-tnejn għandhom bżonn l-istess ċavetta. Iżda, kif jaqblu fuq din iċ-ċavetta jekk dak kollu li jibagħtu lil xulxin, b'definizzjoni, jgħaddi minn kanal fejn xi ħadd jista' jkun qed jisma'? Li wieħed jaqbel fuq iċ-ċavetta fl-istess kanal fejn aktar tard se jużaha jidher impossibbli: jekk l-attakkant jisimagħha meta jaqblu fuqha, ikun jista' jiddeċifra dak kollu ta' wara. Għal għexieren ta' snin, il-kriptografija klassika solviet dan bil-mod iebes: iċ-ċwievet kienu jitwasslu personalment, qabel ma jibdew jintużaw, f'laqgħat fiżiċi. L-ambaxxaturi kienu jġorru basktijiet ta' ċwievet meħjuta fil-kisja tal-kowt tagħhom.

Fl-email kontemporanja, dik is-soluzzjoni ma tiskalax. Kieku kellna mmorru fiżikament fid-dar ta' kull persuna li biħsiebna nikkomunikaw magħha b'mod encrypted, ma konniex nilħqu nitkellmu ma' ħadd. Il-mistoqsija magħmula ħamsin sena ilu mill-komunità kriptografika kienet din: huwa possibbli li żewġ persuni li ma jafux lil xulxin u li jaqsmu biss kanal pubbliku jaqblu, f'dak l-istess kanal pubbliku, fuq sigriet li ħadd li jisma' l-kanal ma jista' jkun jaf?

L-eleganza ta' Diffie-Hellman

Fl-1976, żewġ matematiċi msejħa Whitfield Diffie u Martin Hellman urew xi ħaġa li tidher impossibbli: li żewġ persuni, li jitkellmu biss permezz ta' kanal pubbliku — kanal fejn kulħadd jista' jisma' dak kollu li jgħidu — jistgħu jaqblu fuq password sigrieta mingħajr ma l-ebda semmiegħ ma jkun jista' jiskopriha. Tinstema' bħal maġija. Mhijiex: hija matematika. L-iskambju taċ-ċavetta Diffie-Hellman, kif inhu magħruf minn dakinhar, huwa l-bażi ta' prattikament il-komunikazzjoni kollha encrypted fuq l-internet, u nofs seklu ta' użu intensiv u skrutinju akkademiku dinji jikkonfermaw is-soliditá tiegħu. Kull min irid jara l-intuwizzjoni viżwali jew il-matematika jista' jkompli jaqra. Kull min jippreferi jafda li jaħdem jista' wkoll ikompli mingħajr ma jitlef il-fil tal-artiklu.

Għal min irid jaraha f'immaġni, hemm analoġija magħrufa bil-kuluri. Immaġina li Alicia u Bruno jaqblu b'mod miftuħ fuq kulur bażi — ngħidu aħna isfar — quddiem Eva, li tismagħhom. Kull wieħed jagħżel b'mod privat it-tieni kulur sigriet u jħallat is-sigriet tiegħu mal-isfar. Alicia tikseb oranġjo partikolari; Bruno jikseb aħdar partikolari. Huma jiskambjaw ir-riżultati quddiem Eva. Issa kull wieħed iħallat il-kulur riċevut mas-sigriet tiegħu stess, u t-tnejn jaslu għall-istess kulur finali, għax l-ordni tat-taħlitiet ma jimpurtax. Eva rat l-isfar u ż-żewġ taħlitiet intermedji, iżda mhux is-sigrieti; mingħajr ebda wieħed mis-sigrieti ma tista' tasal għall-kulur finali. Il-matematika reali tibdel il-kuluri għal esponenzjazzjonijiet fi gruppi modulari jew kurvi ellittiċi, iżda l-idea hija l-istess: is-sigriet kondiviż jinbena fil-pubbliku mingħajr ma ħadd fil-kanal ma jkun jista' jerġa' jibnih.

Fl-aritmetika, għal min jippreferi jara l-mekkaniżmu: Alicia tagħżel numru sigriet a, Bruno jagħżel b. Jiskambjaw g^a u g^b fil-miftuħ fuq il-kanal. Alicia tikkalkula $(g^b)^a$ u Bruno jikkalkula $(g^a)^b$; it-tnejn jaslu għall-istess g^{ab}. Eva tara g, g^a u g^b jgħaddu mill-kanal, iżda l-irkupru ta' a minn g^a — dik imsejħa l-problema tal-logaritmu diskret — teħtieġ ħin tal-kompjuter astronomikament ogħla mill-età tal-univers meta g jintgħażel fi grupp matematiku adattat.

Para quien quiera comprobarlo con números pequeños. El intercambio Diffie-Hellman se puede recorrer entero con cifras lo bastante reducidas como para hacer las cuentas a mano. Quien prefiera no entrar en aritmética puede saltarse este bloque sin perder el hilo del artículo;

quien quiera ver el mecanismo funcionando paso a paso lo encontrará aquí. **Las reglas públicas**, que cualquiera puede leer: un primo $p = 11$ (en el Diffie-Hellman real es de unas trescientas cifras; usamos once para que las cuentas quepan en una página), una base $g = 2$, y la convención de que toda la aritmética se hace *módulo p* — se calcula, se divide entre *p*, y se conserva el resto, como un reloj de once posiciones que vuelve al cero al rebasar el diez. **Las elecciones privadas**, una cada uno y jamás compartidas: Alicia elige $a = 4$. Bruno elige $b = 7$.

Paso 1. Alicia calcula $2^4 = 16$, luego $16 \bmod 11 = \mathbf{5}$. Envía el cinco. Eva lo anota.

Paso 2. Bruno calcula $2^7 = 128$, luego $128 \bmod 11 = \mathbf{7}$. Envía el siete. Eva también lo anota. Tras los dos envíos, la libreta de Eva contiene cuatro datos: $p = 11$, $g = 2$, A = 5, B = 7. Le falta el número compartido que Alicia y Bruno están a punto de derivar — y que Eva no podrá reconstruir.

Paso 3. Alicia toma el siete que Bruno le envió y lo eleva a su exponente privado $a = 4$. Para evitar manejar $7^4 = 2401$, se calcula por partes aplicando el módulo en cada paso:

$7^2 = 49$

$49 \bmod 11 = 5$

$7^4 = (7^2)^2 = 5^2 = 25$

$25 \bmod 11 = 3$

Alicia obtiene el número **3**.

Paso 4. Bruno toma el cinco que Alicia le envió y lo eleva a su exponente privado $b = 7$. De nuevo por partes:

$5^2 = 25 \bmod 11 = 3$

$5^4 = (5^2)^2 = 3^2 = 9 \bmod 11 = 9$

$5^6 = 5^4 \times 5^2 = 9 \times 3 = 27 \bmod 11 = 5$

Finalmente $5^7 = 5^6 \times 5 = 5 \times 5 = 25 \bmod 11 = \mathbf{3}$.

Bruno obtiene también **3**.

Los dos han llegado al mismo número, 3, trabajando en paralelo. Ninguno envió su exponente privado en ningún momento. Alicia no sabe que $b = 7$; Bruno no sabe que $a = 4$. Cada cual usó el valor público que el otro envió combinado con su propio exponente privado, y se encontraron en el mismo destino. **¿Por qué llegan al mismo número?** Lo que calculó cada uno: Alicia, $(g^b)^a = 2^{7\times4} = 2^{28} \bmod 11$. Bruno, $(g^a)^b = 2^{4\times7} = 2^{28} \bmod 11$. Es la misma cantidad porque el orden de multiplicación de exponentes no importa ($7 \times 4 = 4 \times 7$). Cada cual llegó por un camino distinto al mismo destino.

¿Y Eva? Tiene en su libreta $p = 11$, $g = 2$, A = 5, B = 7, y quisiera el 3. Para calcularlo necesitaría conocer *a* o *b* — pero ninguno ha viajado por el canal. Su única vía es preguntarse: «¿para qué exponente *a* se cumple $2^a \bmod 11 = 5$?». Con *p* tan pequeño puede probar 0, 1, 2, 3, 4… y encontrarlo en menos de un minuto. Pero al sustituir 11 por un primo de trescientas cifras, el espacio de exponentes posibles tiene más elementos que átomos hay en el universo observable. **No existe a día de hoy ningún algoritmo conocido por la humanidad que pueda recorrer ese espacio en menos de miles de millones de años.** Es el llamado *problema del logaritmo discreto*: fácil hacia adelante, computacionalmente imposible hacia atrás. Y es la razón por la que el cifrado resiste aunque Eva haya seguido toda la conversación letra por letra.

Tres ingredientes simples —aritmética sobre un reloj, exponenciación, y conmutatividad de la multiplicación ($a \cdot b = b \cdot a$)— combinados producen un protocolo del que media humanidad depende cada día para sus comunicaciones privadas. Ninguna de las tres piezas, por separado, parece especial. Lo decisivo es el ensamblaje.

Minn Diffie-Hellman għall-protokoll Signal

L-encryption minn tarf sa tarf li jużaw illum l-applikazzjonijiet tal-messaġġi professjonali tistrieħ, kważi mingħajr eċċezzjoni, fuq verżjoni eleganti u mwebbsa tal-iskambju Diffie-Hellman. Il-protokoll Signal, iddisinjat minn Trevor Perrin u Moxie Marlinspike bejn l-2013 u l-2016, huwa r-referenza. Jgħaqqad żewġ ideat ewlenin. L-ewwel, l-iskambju ta' ċwievet f'kurvi ellittiċi (X25519), li jipproduċi s-sigriet kondiviż inizjali bejn żewġ apparati. It-tieni, l-ħekk imsejjaħ Double Ratchet — ratch doppju —, li jġedded iċ-ċwievet awtomatikament ma' kull messaġġ, sabiex il-kompromess tal-apparat illum ma jippermettix id-deċifrar ta' messaġġi tal-passat, u lanqas messaġġi futuri ladarba r-ratch ikun ġie mdawwar.

F'Zig, l-iskambju X25519 li jipproduċi s-sigriet kondiviż bejn żewġ apparati jidħol f'sitt linji, billi tuża l-librerija standard:

```
const std = @import("std");
const X25519 = std.crypto.dh.X25519;

// Alicia y Bruno generan cada uno un par (privada, pública).
const par_alicia = X25519.KeyPair.generate(io);
const par_bruno  = X25519.KeyPair.generate(io);

// Cada parte recibe la clave pública de la otra y deriva el mismo secreto.
const secreto_alicia = X25519.scalarmult(par_alicia.secret_key, par_bruno.public_key) catch unreachable;
```

```
const secreto_bruno  = X25519.scalarmult(par_bruno.secret_key,  par_alicia.public_key) catch unreachable;
// secreto_alicia == secreto_bruno  (32 bytes)
```

Dak li jiġri f'dawk is-sitt linji: Iċ-ċwievet pubbliċi jivvjaġġaw fil-miftuħ. Iċ-ċwievet privati qatt ma jitilqu mill-apparat rispettiv. Kull parti derivata, ibbażata fuq il-privat tagħha u l-pubbliku tal-oħra, l-istess sigriet ta' tnejn u tletin bytes li ħadd fil-kanal ma jista' jirkupra. Dak is-sigriet iservi aktar tard bħala żerriegħa biex jikkripta l-messaġġi skambjati. Id-Double Ratchet tal-protokoll Signal iżid rotazzjoni kostanti ta' dak il-materjal sabiex il-kompromess ta' instant ma jikkompromettix il-bqija tal-konversazzjoni.

U x'hemm eżattament ġewwa `std.crypto.dh.X25519`? L-ebda maġija moħbija. Huma żewġ funzjonijiet qosra li jistgħu jinqraw fl-intier tagħhom fil-librerija standard ta' Zig stess. L-ewwel waħda toħroġ iċ-ċavetta pubblika minn dik privata — il-«g^{a}» tal-iskambju:

```
pub fn recoverPublicKey(secret_key: [secret_length]u8) IdentityElementError![public_length]u8 {
    const q = try Curve.basePoint.clampedMul(secret_key);
    return q.toBytes();
}
```

Fil-lingwaġġ tal-artiklu: iċ-ċavetta privata tiġi «multiplikata» — fis-sens ellittiku, mhux dak aritmetiku elementari — bil-punt bażi tal-kurva Curve25519, u r-riżultat jiġi serjalizzat fi tnejn u tletin byte. L-operazzjoni `clampedMul` hija l-verżjoni msaħħa ta' dik il-multiplikazzjoni skalari: tinkorpora s-salvagwardji li l-komunità kriptografika żiedet matul is-snin biex tirreżisti familji magħrufa ta' attakki. Żewġ linji ta' korp tal-funzjoni.

It-tieni funzjoni tgħaqqad iċ-ċavetta privata tiegħek maċ-ċavetta pubblika li l-parti l-oħra tibgħatlek. Huwa l-«$(g^{b})^{a}$» tal-iskambju, li jipproduċi s-sigriet kondiviż ta' tnejn u tletin byte li ħadd minnkom qatt ma trażmetta:

```
pub fn scalarmult(secret_key: [secret_length]u8, public_key: [public_length]u8) IdentityElementError![shared_length]u8 {
    const q = try Curve.fromBytes(public_key).clampedMul(secret_key);
    return q.toBytes();
}
```

Żewġ linji oħra. Iċ-ċavetta pubblika riċevuta hija interpretata bħala punt fuq il-kurva, u tiġi «multiplikata» biċ-ċavetta privata tiegħek stess. Permezz tal-kommutattività tal-operazzjoni tal-kurva — analoga għall-kommutattività tal-multiplikazzjoni tal-esponenti li rajna fl-eżempju numeriku — iż-żewġ partijiet jispiċċaw bl-istess punt serjalizzat: eżattament is-sigriet kondiviż li jitkellem dwaru l-artiklu.

Dak kollox. Dak li f'applikazzjoni jidher qisu maġija huwa, fir-realtà, żewġ funzjonijiet ta' tliet linji kull waħda. Il-kumplessità teknika hija kkonċentrata f'operazzjoni waħda, `clampedMul`, li hija miktuba aktar 'l isfel fl-istess librerija standard, riveduta għal għexieren ta' snin mill-komunità kriptografika internazzjonali, u disponibbli għal kull min irid jaqraha ittra b'ittra. M'hemm l-ebda kaxxa sewda la fl-applikazzjoni tagħna u lanqas fil-librerija standard ta' Zig. Hemm kodiċi open source li bniedem jista' jifhem, billi jagħżel il-pass li bih irid jidħol fih.

Dak li jipproteġi l-encryption minn tarf sa tarf

Dak li jipproteġi sew l-E2EE, jekk wieħed jassumi implimentazzjoni korretta, huwa l-kontenut tal-messaġġ waqt it-tranżitu. Server intermedju li jirċievi u jibgħat mill-ġdid id-dejta encrypted se jara suċċessjoni ta' bytes inintelliġibbli. Attakkant b'aċċess għall-kejbil, għar-router, għall-punt ta' aċċess wifi, se jara l-istess ħaġa. Fornitur tas-servizz li jżomm kopji tat-traffiku ma jkunx jista' jaqrah aktar tard. Gvern li jordna lill-operatur tas-servizz biex iwassal il-kontenut jirċievi l-istess bytes inintelliġibbli li s-server kellu fl-ewwel lok.

Dan, f'termini prattiċi, huwa ħafna. Hija d-differenza bejn li tikteb ittra ġewwa envelop opak u li tiktebha fuq kartolina. It-tnejn jaslu. Wieħed biss jippreserva l-kontenut quddiem il-pustier.

Dak li ma jipproteġix l-encryption minn tarf sa tarf

Tajjeb li tkun tafha bl-istess mod. L-E2EE ma jipproteġix il-metadejta: is-server għadu jaf li l-utent A jibgħat dejta lill-utent B, f'liema ħin, b'liema frekwenza u minn fejn, għalkemm ma jafx x'jgħid. Din il-metadejta, kif diġà argumentajna fi *Li tikkripta mhuwiex li tkun privat*, ħafna drabi hija aktar rivelanti mill-kontenut. Li tkun taf li xi ħadd ċempel lil ditta legali speċjalizzata fid-divorzji nhar ta' Ġimgħa fl-22:00 għal tletin minuta jirrakkonta storja li l-kontenut tas-sejħa qatt ma rrakkonta. Hija l-istess sitwazzjoni bħal li tara persuna tidħol u toħroġ bosta drabi minn klinika onkoloġika: m'hemmx bżonn tisma' xejn minn dak li jingħad ġewwa biex timmaġina x'qed jiġri. Metadejta waħda iżolata tista' ma tfisser xejn; bosta minnhom inkroċjati bejniethom jiġbdu xi ħaġa wisq simili għall-verità. L-E2EE ma jipproteġix it-truf: jekk l-apparat tar-riċevitur jiġi kompromess minn programm malizzjuż, il-messaġġ jiġi deċifrat b'mod normali għal dak ir-riċevitur u l-programm malizzjuż jaqrah. L-E2EE ma jipproteġix kontra l-identità tal-interlokutur fiha nnifisha: jekk Alicia temmen li qed titkellem ma' Bruno iżda attakkant daħal bejniethom fil-bidu (*man in the middle*) u l-protokoll ma jinkludix verifika indipendenti, iż-żewġ partijiet jispiċċaw jitkellmu mal-intruż jaħsbu li qed jitkellmu ma' xulxin.

Hemm ir-raba' ħaġa li ta' min jifformulahom mingħajr ambigwità. L-E2EE ma jipprevjenix fornitur li jiddikjara li joffrih milli jżomm ukoll kopja tal-messaġġ mhux kriptat fis-sistemi tiegħu stess. Id-dikjarazzjoni «il-messaġġi tiegħi huma encrypted minn tarf sa tarf» u d-dikjarazzjoni «il-fornitur ma jżommx il-kontenut tiegħi» mhumiex l-istess. Applikazzjoni tista' tikkonforma mal-ewwel waħda waqt li tikser it-tieni waħda; rajnieha fl-aħbarijiet ripetutament mill-2018. L-utent, sakemm il-kodiċi tal-klijent ma jkunx verifikabbli, m'għandux mod tekniku kif jiddistingwi każ mill-ieħor mingħajr investigazzjoni esperta. L-aktar każ magħruf fil-pubbliku ġenerali: WhatsApp jikkripta l-messaġġi minn tarf sa tarf waqt it-tranżitu, iżda jekk l-utent jattiva l-backup f'iCloud jew Google Drive mingħajr encryption addizzjonali, dik il-kopja tiġi maħżuna b'mod li tista' tinqara fl-infrastruttura ta' parti terza, u l-encryption tinkiser fit-tarf tal-utent stess.

Il-mistoqsija li l-operatur ma jridx jisma'

Applikazzjoni li tiddikjara li tikkripta minn tarf sa tarf tista', teknikament, tagħmel waħda minn tliet affarijiet rigward iċ-ċwievet:

1. **Iċ-ċwievet jinsabu biss fuq l-apparati.** Jiġu ġġenerati u jinsabu esklussivament fuq l-apparati tal-utenti; l-operatur ma jafhomx u ma jaħżinhomx. Huwa l-każ ottimali.
2. **L-operatur jista' jaċċessa jekk irid.** L-operatur għandu ċ-ċwievet tal-utenti (jew jista' jiġġenerahom kif irid) u jżommhom fid-databases tiegħu. Jekk irid jew jiġi sfurzat, jista' jaqra l-kontenut. Dan huwa l-każ tal-biċċa l-kbira tas-servizzi «cloud».
3. **L-operatur ma jistax jaċċessa skont id-disinn, iżda jikkontrolla l-aċċess.** L-operatur m'għandux iċ-ċwievet, iżda għandu kontroll fuq l-applikazzjoni li tiġġenerahom. Jekk jiġi sfurzat, jista' jibgħat aġġornament malizzjuż li jaqbad iċ-ċwievet jew il-kontenut qabel l-encryption. Dan huwa l-każ ta' bosta servizzi E2EE kummerċjali.

Il-mistoqsija operattiva, għalhekk, mhijiex jekk xi ħaġa hijiex encrypted, iżda min għandu l-kontroll tal-apparat u tas-softwer li jamministra ċ-ċwievet. F'Solo2, iċ-ċwievet jinsabu biss fil-Bóveda tiegħek (IndexedDB encrypted bil-password tiegħek) u s-softwer huwa kodiċi miftuħ verifikabbli.

Għall-qarrej professjonali

L-encryption minn tarf sa tarf huwa għodda għas-sovranità diġitali. Iżda bħal kull għodda, l-effettività tagħha tiddependi fuq l-id li żżommha u l-art li tistrieħ fuqha.

1. Fejn jiġu ġġenerati ċ-ċwievet kriptografiċi u fejn jirrisjedu fiżikament? Jekk l-operatur jista' jaċċessahom (saħansitra temporanjament, anke taħt il-qoxra ta' rkupru), l-E2EE huwa nominali.
2. Hemm verifika indipendenti tal-interlokutur (numri tas-sigurtà, kodiċijiet QR, paragun out-of-band) li tevita attakk man-in-the-middle waqt l-istabbiliment tal-konversazzjoni?
3. Il-kodiċi tal-klijent huwa awditjabbli — miftuħ, ippubblikat, riproduċibbli — jew jeħtieġ li tafda l-kelma tal-fornitur dwar x'jagħmel tassew il-klijent?
4. X'metadejta jiġġenera u jżomm is-servizz, u għal kemm żmien? Anke jekk il-kontenut huwa opakk, il-metadejta tista' tibni mill-ġdid parti kbira mill-informazzjoni sensittiva.

Dawn l-erba' mistoqsijiet ma jitolbux informazzjoni teknika avvanzata; jitolbu informazzjoni li kwalunkwe operatur onest jista' jwieġeb fid-dokumentazzjoni pubblika tiegħu. Il-kwalità u l-preċiżjoni tat-tweġiba tgħid daqstant dwar il-prodott daqs it-tweġiba nnifisha.

L-encryption minn tarf sa tarf, magħmul tajjeb, huwa wieħed mill-ifjen kostruzzjonijiet li l-kriptografija kontemporanja tat lill-prattika ta' kuljum. L-idea oriġinali — li żewġ persuni jistgħu jaqblu fuq sigriet f'kanal pubbliku — tappartjeni lil Whitfield Diffie u Martin Hellman, 1976; nofs seklu wara għadna ngħixu fil-konsegwenza tiegħu. Iżda, bħal kull wegħda teknika, il-valur tiegħu jiddependi fuq it-twettiq reali, mhux fuq it-tikketta. Il-mistoqsija tal-professjonist onest mhijiex «huwa kkodifikat?», iżda «min għandu ċ-ċwievet?». It-tweġibiet għandhom konsegwenzi differenti. Tajjeb li tkun tafhom.

Sorsi u aktar qari

- Diffie, W.; Hellman, M. — *New Directions in Cryptography*, IEEE Transactions on Information Theory, Novembru 1976. Artiklu pedamentali tal-kriptografija taċ-ċavetta pubblika.
- Perrin, T.; Marlinspike, M. — *The Double Ratchet Algorithm*, speċifikazzjoni pubblika minn Open Whisper Systems, reviżjoni 2016. Bażi tal-protokoll Signal u d-derivattivi industrijali tiegħu.
- RFC 7748 — Elliptic Curves for Security (IETF, Jannar 2016). Speċifikazzjoni normattiva tal-kurvi X25519 u X448 użati fl-iskambji moderni taċ-ċwievet.
- Ferguson, N.; Schneier, B.; Kohno, T. — *Cryptography Engineering: Design Principles and Practical Applications* (Wiley, 2010). Kapitoli dwar l-iskambju ta' ċwievet u l-protokolli ta' encryption awtentikati.
- Regolament (UE) 2024/1183 dwar il-qafas tal-identità diġitali Ewropea (eIDAS 2) — jistabbilixxi oqfsa fejn il-verifika indipendenti tal-interlokutur takkwista appoġġ istituzzjonali, u fejn id-distinzjoni bejn encryption nominali u reali għandha konsegwenzi legali differenti.

← PreċedentiKill switch u l-qbid istituzzjonaliLi jmiss →Il-mudell tan-negozju bħala sinjal ta' fiduċja

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 154cc1a56e1dfe9edeec48a2e803fcb1d895784c7d4a4561cc7229aefc36dfd7

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