Muturretik muturrerako enkriptatzea, benetan azaldua

Hornitzaileek E2EE diotenean esaten dutena, eta esaten ez dutena. Mekanismoaren eta bere mugen azalpen didaktikoa, publizitate-bilgarririk gabe.

Uler dezagun elkar: WhatsApp-ek dio zure mezuak muturretik muturrera enkriptatuta daudela. Egia da — eta ez da nahikoa. Segurtasun-kopia iCloud-era edo Google Drive-ra badoa enkriptatze gehigarririk gabe, enkriptatzea zure telefonoan bertan hausten da. Galdera operatiboa ez da enkriptatuta dagoen, baizik eta gakoak non dauden.

Enkriptatzeak benetan esan nahi duena

Mezu bat enkriptatzea da hura bihurtzea gako deituriko informazio jakin bat ez duen edonorentzat zarata dirudien zerbait. Eragiketa bidaltzailearen gailuan egiten da eta, gako zuzenarekin, hartzailearen gailuan desegiten da. Tartean, mezua itxurazko esanahirik gabeko byte segida gisa bidaiatzen du. Hori da ideia erraza. Artikuluaren gainerako zatia kasuaren arabera hura berme real edo merkatu-etiketa bihurtzen duten nuanzeez arduratzen da.

Muturretik muturrerako adjektiboak —ingelesez *end-to-end*, E2EE laburtua— zehaztasun bat gehitzen du. Enkriptatzea ez da egiten bitarteko zerbitzari batek irakurri eta entregatu ahal izateko. Bi muturrek soilik —bidaltzailearen gailuak eta hartzailearenak— gakoa izan dezaten egiten da. Mezua igarotzen den edozein zerbitzarik zarata ikusten du, ez mezua. Hori da *trantsituan* enkriptatzearekiko alde teknikoa, non edukia enkriptatuta doan zerbitzari batetik hurrengora, baina igarotzen den zerbitzari bakoitzak desenkriptatu egiten baitu berriz bidaltzeko, testu argia aldi baterako berreskuratuz.

Sekretu partekatuaren paradoxa

Arazo bistako bat dago. Bi pertsonak mezuak elkarri enkriptatu eta desenkriptatu ahal izateko, biek gako bera behar dute. Baina, nola adosten dute gako hori bidaltzen duten guztia, definizioz, norbait entzuten egon daitekeen kanal batetik igarotzen bada? Gakoa geroago erabiliko duten kanal berean adostea ezinezkoa dirudi: erasotzaileak adostean entzuten badu, ondorengo guztia desenkriptatu ahal izango du. Hamarkadetan zehar, kriptografia klasikoak modu gogorrean konpondu zuen hau: gakoak pertsonalki ematen ziren, erabiltzen hasi aurretik, topaketa fisikoetan. Enbaxadoreek berokiaren forruan jositako gako-maletatxoak eramaten zituzten.

Gaur egungo posta elektronikoan, soluzio hori ez da eskalagarria. Enkriptatuta komunikatu nahi dugun pertsona bakoitzaren etxera fisikoki joan beharko bagenu, ez ginateke inorekin hitz egitera iritsiko. Komunitate kriptografikoak duela berrogeita hamar urte planteatutako galdera hau zen: posible al da elkar ezagutzen ez duten eta kanal publiko bat soilik partekatzen duten bi pertsonak, kanal publiko horretan bertan, kanala entzuten duen edonork ezagutu ezin duen sekretu bat adostea?

Diffie-Hellman-en dotoretasuna

1976an, Whitfield Diffie eta Martin Hellman izeneko bi matematikarik itxuraz ezinezkoa zen zerbait frogatu zuten: bi pertsonak, kanal publiko batetik soilik hitz eginez —edonork esaten duten guztia entzun dezakeen kanal bat—, sekretuzko pasahitz bat adostu dezaketela entzule batek ere deskubritu ezin izan gabe. Magia dirudi. Ez da: matematika da. Diffie-Hellman gako-trukea, harrezkero ezagutzen den bezala, interneteko komunikazio enkriptatu ia guztiaren oinarria da, eta mende erdi bateko erabilera intentsiboak eta mundu osoko azterketa akademikoak haren sendotasuna bermatzen dute. Intuizio bisuala edo matematika ikusi nahi duenak irakurtzen jarraitu dezake. Funtzionatzen duela fidatzea nahiago duenak ere jarraitu dezake artikuluaren haria galdu gabe.

Irudi batean intuitu nahi duenarentzat, koloreekin egindako analogia ezagun bat dago. Imajinatu Aliciak eta Brunok kolore oinarri bat —esan dezagun horia— adosten dutela agerian, entzuten ari den Evaren aurrean. Bakoitzak pribatuan bigarren kolore sekretu bat aukeratzen du eta bere sekretua horiarekin nahasten du. Aliciak laranja berezi bat lortzen du; Brunok berde berezi bat. Emaitzak trukatzen dituzte Evaren aurrean. Orain bakoitzak jasotako kolorea bere sekretuarekin nahasten du, eta biak iristen dira azken kolore berera, nahasketen ordenak ez baitu axola. Evak horia eta tarteko bi nahasketak ikusi ditu, baina ez sekretuak; sekretuetakoren bat izan gabe ezin da iritsi azken koloreraino. Matematika errealak koloreak talde modularretako edo kurba eliptikoetako berreketengatik aldatzen ditu, baina ideia bera da: sekretu partekatua publikoan eraikitzen da kanaleko inork berreraiki ahal izan gabe.

Aritmetikan, mekanismoa ikusi nahiago duenarentzat: Aliciak a zenbaki sekretua aukeratzen du, Brunok b aukeratzen du. g^a eta g^b agerian trukatzen dituzte kanaletik. Aliciak $(g^b)^a$ kalkulatzen du eta Brunok $(g^a)^b$ kalkulatzen du; biak g^{ab} berera iristen dira. Evak g, g^a eta g^b kanaletik igarotzen ikusten ditu, baina a berreskuratzeak g^a-tik —logaritmo diskretuaren arazoa deitua— unibertsoaren adina baino askoz handiagoa den konputazio denbora eskatzen du g talde matematiko egoki batean aukeratzen denean.

Zenbaki txikiekin egiaztatu nahi duenarentzat. Diffie-Hellman trukea oso-osorik egin daiteke kalkuluak eskuz egiteko bezain zifra txikiekin. Aritmetikan sartu nahi ez duenak bloke hau salta dezake artikuluaren haria galdu gabe; mekanismoa pausoz pauso martxan ikusi nahi duenak

hemen aurkituko du. **Arau publikoak**, edonork irakur ditzakeenak: $p = 11$ lehen bat (benetako Diffie-Hellman-ean hirurehun bat zifra ditu; hamaika erabiltzen dugu kontuak orrialde batean sar daitezen), $g = 2$ oinarri bat, eta aritmetika guztia *p modulu* egiten delako hitzarmena — kalkulatzen da, *p*-rekin zatitzen da eta hondarra gordetzen da, hamarra gainditzean zerora itzultzen den hamaika posizioko erloju baten gisa. **Aukera pribatuak**, bakoitzak bat eta inoiz partekatu gabeak: Aliciak $a = 4$ aukeratzen du. Brunok $b = 7$ aukeratzen du.

1. urratsa. Aliciak $2^4 = 16$ kalkulatzen du, ondoren 16 mod 11 = **5**. Bosta bidaltzen du. Evak apuntatu egiten du.

2. urratsa. Brunok $2^7 = 128$ kalkulatzen du, ondoren 128 mod 11 = **7**. Zazpia bidaltzen du. Evak ere apuntatzen du. Bi bidalketen ondoren, Evaren libreta lau daturekin geratu da: $p = 11$, $g = 2$, A = 5, B = 7. Falta zaio Alicia eta Bruno ateratzear dauden zenbaki partekatua — eta Evak ezingo duena berreraiki.

3. urratsa. Aliciak Brunok bidalitako zazpia hartzen du eta bere berretzaile pribatura igotzen du $a = 4$. $7^4 = 2401$ ez maneiatzeko, zatika kalkulatzen da pauso bakoitzean modulua aplikatuz:

$7^2 = 49$

49 mod 11 = 5

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

25 mod 11 = 3

Aliciak **3** zenbakia lortzen du.

4. urratsa. Brunok Aliciak bidalitako bosta hartzen du eta bere berretzaile pribatura igotzen du $b = 7$. Berriro zatika:

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

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

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

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

Brunok ere **3** lortzen du.

Biak iritsi dira zenbaki berberera, 3ra, paraleloan lan eginez. Bietako inork ez zuen bere berretzaile pribatua bidali inongo unetan. Aliciak ez daki $b = 7$ denik; Brunok ez daki $a = 4$ denik. Bakoitzak besteak bidalitako balio publikoa erabili zuen bere berretzaile pribatuarekin konbinatuta, eta helmuga berean elkartu ziren. **Zergatik iristen dira zenbaki berberera?** Bakoitzak kalkulatu zuena: Aliciak, $(g^b)^a = 2^{7 \times 4} = 2^{28} \bmod 11$. Brunok, $(g^a)^b = 2^{4 \times 7} = 2^{28} \bmod 11$. Kantitate bera da berretzaileen biderketa-ordenak ez baitu axola ($7 \times 4 = 4 \times 7$). Bakoitza bide desberdin batetik iritsi zen helmuga berera.

Eta Eva? Bere libretan $p = 11$, $g = 2$, A = 5, B = 7 ditu, eta 3a nahiko luke. Kalkulatzeko *a* edo *b* jakin beharko luke — baina bat ere ez da kanaletik bidaiatu. Bere bide bakarra bere buruari galdetzea da: «zer *a* berretzailerentzat betetzen da $2^a \bmod 11 = 5$?». *p* hain txikia izanik 0, 1, 2, 3, 4... probatu ditzake eta minutu bat baino gutxiagoan aurkitu. Baina 11ren ordez hirurehun zifrako lehen bat jartzean, berretzaile posibleen espazioak unibertso behagarrian dauden atomoak baino elementu gehiago ditu. **Gaur egun ez dago gizateriak ezagutzen duen algoritmorik espazio hori milaka milioi urte baino gutxiagotan zeharkatu dezakeenik.** Logaritmo diskretuaren *arazoa* deitzen zaio: erraza aurrerantz, konputazionalki ezinezkoa atzerantz. Eta hori da enkriptatzeak eustearen arrazoia, nahiz eta Evak elkarrizketa osoa letraz letra jarraitu izan.

Hiru osagai sinplek —erloju bateko aritmetikak, berreketak eta biderketaren trukakortasunak ($a \cdot b = b \cdot a$)— konbinatuta gizateriaren erdiak egunero bere komunikazio pribatuetarako menpe duen protokolo bat sortzen dute. Hiru ataletako batek ere ez dirudi berezia, bereizita. Erabakigarria mihiztadura da.

Diffie-Hellman-etik Signal protokolora

Gaur egun mezu profesionaletarako aplikazioek erabiltzen duten muturretik muturrerako enkriptatzea, ia salbuespenik gabe, Diffie-Hellman trukearen bertsio dotore eta gogortu baten gainean oinarritzen da. Signal protokoloa, Trevor Perrinek eta Moxie Marlinspikek 2013 eta 2016 artean diseinatua, erreferentzia da. Bi ideia nagusi konbinatzen ditu. Lehena, kurba eliptikoetako gako-trukea (X25519), bi gailuen arteko hasierako sekretu partekatua sortzen duena. Bigarrena, Double Ratchet deitua —engranaje bikoitza—, gakoak mezu bakoitzarekin automatikoki berritzen dituena, gaur gailua arriskuan jartzeak ez baitu uzten iraganeko mezuak desenkriptatzen, ezta etorkizunekoak ere engranajea biratu denean.

Zig-en, bi gailuren arteko sekretu partekatua sortzen duen X25519 trukea sei lerrotan sartzen da, liburutegi estandarra erabiliz:

```
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)
```

Sei lerro horietan gertatzen dena: Gako publikoak agerian doaz. Gako pribatuak ez dira inoiz ateratzen dagokien gailutik. Alderdi bakoitzak, bere pribatutik eta bestearen publikotik abiatuta, hogeita hamabi byteko sekretu bera deribatzen du, kanaleko inork berreskuratu ezin duena. Sekretu horrek hazi gisa balio du gero trukatutako mezuak enkriptatzeko. Signal protokoloko Double Ratchet-ak material horren biraketa konstante bat gehitzen du, une bateko konpromisoak elkarrizketaren gainerakoa arriskuan jar ez dezan.

Eta zer dago zehazki `std.crypto.dh.X25519` barruan? Ez dago ezkutuko magiarik. Zig-en liburutegi estandarrean bertan osorik irakur daitezkeen bi funtzio labur dira. Lehenengoak gako pribatutik publikoa deribatzen du — trukearen «g^a»:

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

Artikuluaren lengoaian: gako pribatua Curve25519 kurbaren oinarrizko puntuarekin «biderkatzen» da —zentzu eliptikoan, ez aritmetika oinarrizkoan—, eta emaitza hogeita hamabi bytetan serializatzen da. `clampedMul` eragiketa biderketa eskalar horren bertsio gogortua da: komunitate kriptografikoak eraso-familia ezagunei aurre egiteko urteetan zehar gehitu zituen babesak barneratzen ditu. Bi lerroko funtzio-gorputza.

Bigarren funtzioak zure gako pribatua beste alderdiak bidaltzen dizun gako publikoarekin konbinatzen du. Trukearen «$(g^b)^a$» da, bietako inork sekula transmititu ez zuen hogeita hamabi byteko sekretu partekatua sortzen duena:

```
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();
}
```

Beste bi lerro. Jasotako gako publikoa kurbaren gaineko puntu gisa interpretatzen da, eta norberaren gako pribatuarekin «biderkatzen» da. Kurba-eragiketaren trukakortasunagatik —adibide numerikoan ikusi genuen berretzaileen biderketaren trukakortasunaren analogoa— bi alderdiek serializatutako puntu berarekin amaitzen dute: artikuluak aipatzen duen sekretu partekatua zehazki.

Hori da guztia. Aplikazio batean magia dirudiena, errealitatean, hiru lerroko bi funtzio dira. Konplexutasun teknikoa eragiketa bakarrean pilatzen da, `clampedMul`, zeina liburutegi estandar berean aurrerago idatzita dagoen, komunitate kriptografiko internazionalak hamarkadetan zehar berrikusi duen, eta letraz letra irakurri nahi duen edonorentzat eskuragarri dagoen. Ez dago kutxa beltzik ez gure aplikazioan ez Zig-en liburutegi estandarrean. Gizaki batek uler dezakeen kode irekia dago, bertan murgildu nahi duen erritmoa aukeratuz.

Zer babesten duen muturretik muturrerako enkriptatzeak

E2EEk ondo babesten duena, inplementazio zuzen bat onartuz, mezuaren edukia da trantsituan dagoenean. Enkriptatutako datuak jaso eta berriz bidaltzen dituen bitarteko zerbitzari batek byte ulertezinen segida bat ikusiko du. Kablea, bideratzailea edo wifi sarbide-puntua atzitzeko aukera duen erasotzaile batek gauza bera ikusiko du. Trafikoaren kopiak gordetzen dituen zerbitzu-hornitzaile batek ezingo du geroago irakurri. Zerbitzuaren operadoreari edukia entregatzea agintzen dion gobernu batek zerbitzariak hasieran zituen byte ulertezin berak jasoko ditu.

Hori, termino praktikoetan, asko da. Gutun bat gutun-azal opaku baten barruan idaztearen eta postal batean idaztearen arteko aldea da. Biak iristen dira. Bakarrak mantentzen du edukia postariaren aurrean.

Zer babesten ez duen muturretik muturrerako enkriptatzeak

Berdin jakitea komeni da. E2EEk ez ditu metadatuak babesten: zerbitzariak oraindik badaki A erabiltzaileak B erabiltzaileari datuak bidaltzen dizkiola, zer ordutan, zein maiztasunekin eta nondik, zer dioten ez badaki ere. Metadatu hauek, *Enkriptatzea ez da pribatua izatea* artikuluan argudiatu dugun bezala, askotan edukia baino adierazgarriagoak dira. Norbaitek ostiralean 22:00etan hogeita hamar minutuz dibortzioetan espezializatutako abokatu-bulego batera deitu zuela jakiteak dei horren edukiak inoiz kontatu ez zuen istorio bat kontatzen du. Egoera bera da pertsona bat onkologia-klinika batean hainbat aldiz sartzen eta ateratzen ikustea: ez dago barruan hitz egiten denetik ezer entzun beharrik gertatzen ari dena imajinatzeko. Metadatu isolatu bakar batek agian ez du ezer esan nahi; elkarren artean gurutzatutako hainbatek egiatik hurbilegi dagoen zerbait marrazten dute. E2EEk ez ditu muturrak babesten: hartzailearen gailua programa gaizto batek arriskuan jarri badu, mezua normalean desenkriptatzen da hartzaile horrentzat eta programa gaiztoak irakurri egiten du. E2EEk ez du solaskidearen identitatearen aurka babesten berez: Aliciak Brunorekin hitz egiten ari dela uste badu baina erasotzaile bat hasieran tartekatu bada (*man in the middle* bat) eta protokoloak ez badu egiaztapen independenterik, bi alderdiak intrusoarekin hitz egiten amaitzen dute elkarrekin hitz egiten ari direla pentsatuz.

Laugarren gauza bat dago anbiguotasunik gabe formulatzea komeni dena. E2EEk ez du eragozten hura eskaintzen duela dioen hornitzaile batek, gainera, enkriptatu gabeko mezuaren kopia bat gordetzea bere sistemetan. «Nire mezuak muturretik muturrera enkriptatuta daude» baieztapena eta «hornitzaileak ez du nire edukia gordetzen» baieztapena ez dira berdinak. Aplikazio batek lehena bete dezake bigarrena hausten duen bitartean; 2018tik behin eta berriz ikusi dugu prentsako titularretan. Erabiltzaileak, bezeroaren kodea egiaztagarria ez bada behintzat, ez du modu teknikorik kasu bat bestetik bereizteko ikerketa aditurik gabe. Publiko orokorrean ezagunena den kasua: WhatsApp-ek mezuak muturretik muturrera enkriptatzen ditu trantsituan, baina erabiltzaileak iCloud edo Google Drive-n segurtasun-kopia enkriptatze gehigarririk gabe aktibatzen badu, kopia hori irakurgarri gordetzen da hirugarren baten azpiegituran, eta enkriptatzea erabiltzailearen muturrean bertan apurtzen da.

Operadoreak entzun nahi ez duen galdera

Muturretik muturrera enkriptatzen duela dioen aplikazio batek, teknikoki, hiru gauza hauetako bat egin dezake gakoei dagokienez:

1. **Gakoak gailuetan bakarrik daude.** Erabiltzaileen gailuetan bakarrik sortzen eta daude; operadoreak ez ditu ezagutzen ezta gordetzen ere. Kasu optimoa da.
2. **Operadoreak sarbidea izan dezake nahi badu.** Operadoreak erabiltzaileen gakoak ditu (edo nahi duen bezala sor ditzake) eta bere datu-baseetan gordetzen ditu. Nahi badu edo behartzen badute, edukia irakur dezake. Hori da «hodeiko» zerbitzu gehienen kasua.
3. **Operadoreak ezin du sarbiderik izan diseinuz, baina sarbidea kontrolatzen du.** Operadoreak ez ditu gakoak, baina gakoak sortzen dituen aplikazioaren kontrola du. Behartzen badute, eguneratze gaizto bat bidal dezake gakoak edo edukia enkriptatu aurretik kapturatzeko. Hori da E2EE zerbitzu komertzial askoren kasua.

Galdera operatiboa, beraz, ez da zerbait enkriptatuta dagoen, baizik eta nork duen gailuaren eta gakoak kudeatzen dituen softwarearen kontrola. Solo2-n, gakoak zure Bóvedan (zure pasahitzarekin enkriptatutako IndexedDB) baino ez daude eta softwarea kode ireki verificagarria da.

Irakurle profesionalarentzat

Muturretik muturrerako enkriptatzea subiranotasun digitalerako tresna bat da. Baina tresna oro bezala, bere eraginkortasuna heldu dion eskuaren eta bermatzen den lurraren mende dago.

1. Non sortzen dira gako kriptografikoak eta non daude fisikoki? Operadoreak horietara sarbidea badu (baita aldi baterako ere, baita berreskuratze aitzakiapean ere), E2EE nominala baino ez da.
2. Ba al dago solaskidearen egiaztapen independenterik (segurtasun-zenbakiak, QR kodeak, bandaz kanpoko konparazioa) elkarrizketa ezartzean man-in-the-middle eraso bat eragotziko duena?
3. Bezeroaren kodea ikuskagarria al da —irekia, argitaratua, erreproduzigarria— ala hornitzailearen hitzaz fidatzea eskatzen du bezeroak benetan egiten duenari buruz?
4. Zer metadatu sortzen eta gordetzen ditu zerbitzuak, eta zenbat denboraz? Edukia opakoa izan arren, metadatuek informazio sentikorraren zati handi bat berreraiki dezakete.

Lau galdera horiek ez dute informazio tekniko aurreraturik eskatzen; edozein operadore zintzok bere dokumentazio publikoan erantzun dezakeen informazioa eskatzen dute. Erantzunaren kalitateak eta zehaztasunak produktuaz erantzunak berak adina esaten du.

Muturretik muturrerako enkriptatzea, ondo egina, kriptografia garaikideak eguneroko praktikarako eman duen eraikuntzarik finenetako bat da. Jatorrizko ideia —bi pertsona kanal publiko batean sekretu bat adosteko gai izatea— Whitfield Diffie eta Martin Hellman-ena da, 1976koa; mende erdi geroago haren ondorioetan bizi gara oraindik. Baina, edozein promesa teknikorekin gertatzen den bezala, haren balioa betetze errealaren araberakoa da, ez etiketarena. Profesional zintzoaren galdera ez da «enkriptatuta dago?», baizik eta «nork ditu gakoak?». Erantzunek ondorio desberdinak dituzte. Komeni da jakitea.

Iturriak eta irakurgai gehiago

- Diffie, W.; Hellman, M. — *New Directions in Cryptography*, IEEE Transactions on Information Theory, 1976ko azaroa. Gako publikoko kriptografiaren oinarrizko artikulua.
- Perrin, T.; Marlinspike, M. — *The Double Ratchet Algorithm*, Open Whisper Systems-en espezifikazio publikoa, 2016ko berrikuspena. Signal protokoloaren eta haren eratorri industrialen oinarria.
- RFC 7748 — Elliptic Curves for Security (IETF, 2016ko urtarrila). Gako-truke modernoetan erabiltzen diren X25519 eta X448 kurben espezifikazio arauemailea.
- Ferguson, N.; Schneier, B.; Kohno, T. — *Cryptography Engineering: Design Principles and Practical Applications* (Wiley, 2010). Gako-trukeari eta enkriptatze autentifikatuaren protokoloei buruzko kapituluak.
- (EB) 2024/1183 Erregelamendua, nortasun digital europarraren esparruari buruzkoa (eIDAS 2) — solaskidearen egiaztapen independenteak babes instituzionala lortzen duen esparruak ezartzen ditu, eta enkriptatze nominalaren eta benetakoaren arteko bereizketak ondorio juridiko desberdinak dituenak.

← AurrekoaKill switch eta kaptura instituzionalaHurrengoa → Negozio-eredua konfiantza-seinale gisa

Azken irakurketak

- Analisia · 2026ko maiatzaren 18a Pribatutasun erreala vs itxurazkoa: geure buruari egin beharreko galderak
- Analisia · 2026ko maiatzaren 18a Self-hosting praktika profesional gisa
- Kontzeptua · 2026ko maiatzaren 18a 24 hitzak: zer den identitate kriptografiko bat

Eraman artikulu hau zurekin behar duzun lekura.

↓ Markdown ↓ Testu arrunta ↓ PDF

Fitxategia zure gailura deskargatuko da. Bertatik gorde, Solo2ra inportatu edo nahi duzun lekuan parteka dezakezu. Cuadernosek ez du helburua zure ordez erabakitzen.

Lakre-zigilua · SHA-256 2031fe094278c42b08e9e3a792607f94ae59956b8d4925824077ccd3749efcc8

Cuadernos Lacre · Menzuri Gestión S.L.ren argitalpena ·
R.Eugeniok idatzia · Solo2 taldeak editatua.