HTTPS PROTOKOLOA

SARRERA

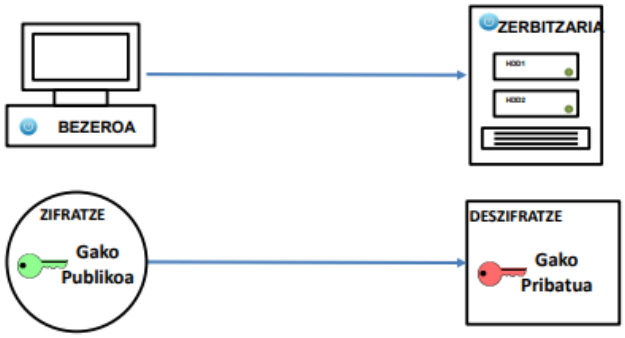
- 1990 → Informazioa mugitzeko HTTP bezala.
- HTTP ez da segurua → Zifratu gabea (trafikoa antzematen duen edonork irakurri dezake).
- Babesteko modu bat aurkitu behar → 1994an kriptografia apur bat gehitu.
- Secure Socket Layer (SSL) zifratze protokoloa erabili zuten HTTP gainean → HTTPS (Hypertext Transfer Protocol Secure).
- Orain SSL-ren ordez Transport Layer Security (TLS) bertsio berria erabiltzen da.
- Internet enkriptatzeko arrazoiak:
    - Segurtasuna: Datu irakurketa eta saioan kode txertaketa saihestu.
    - Pribatutasuna: ISPek, gobernua eta datu bilketa enpresa handiak gure trafikoa ikusi eta gorde egiten dute informazioa baliagarria izatekotan → Zifratu ahalik eta pribatuen mantentzeko informazio hori.
- HTTP → 80 ataka / HTTPS → 443 ataka.
- HTTPS datuak ezkutuan gorde arakatzaile eta web zerbitzari artean mugitzen diren bitartean enkriptatuz.

ZIFRAKETA PROTOKOLOA

- Beharrezkoa:
    - Datuak.
    - Zifratze gako bakarra (testu kate luzea).
    - Zifratze algoritmoa (funtzio matematiko) → Datuak eta gakoa algoritmoan konektatu testu enkriptatua lortuz.
- Deszifratzeko alderantzizko prozesua (gako bera erabili).
- Gakoa sekretuan mantendu host-ek bakarrik hau izanda → Zifratze sistema simetrikoa.
    - Etxeko wifi-a erabili: gako bakarra da pasahitza.

SSL/TLS

- Interneteko webgune batera konektatzean konplexuago → Zifratze simetrikoa ez funtzionatu beste muturra ez dagoelako kontrolatuta eta gako bat partekatu behar delako inork antzeman gabe.
- ZIFRATZE ASIMETRIKOA erabili horretarako → Bi gako bata zifratu eta bestea deszifratu (gako publikoaren kriptografia).



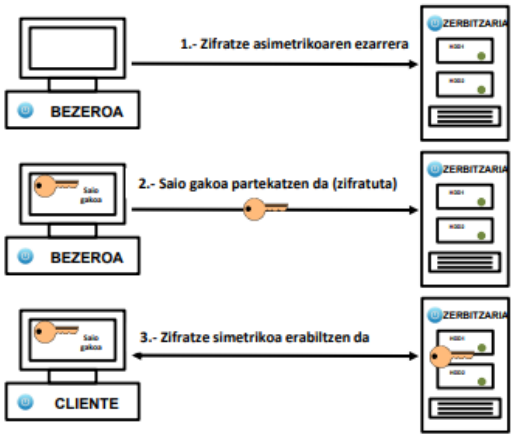
GAKO PAREAK

Bi gako ezberdinak datu berak zifratu edo deszifratu:

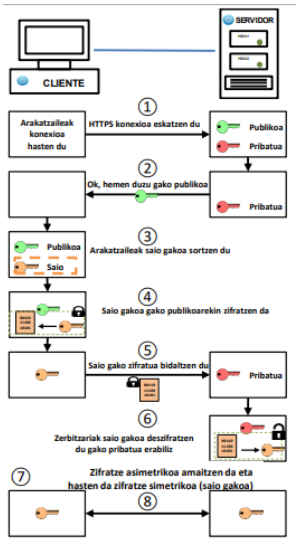
- Zenbaki lehen oso handiak eta aritmetika modularra erabiliz (prozesu matematikoa).
    - Zenbaki hauek haien artean biderkatzean, hauek faktorizatzea ezinezkoa da hasierako balioak ezagutu gabe.
- Gako publikoak eta pribatuak aldi berean kalkulatu prozesu beraren bidez → Oso lotuta daude eta beraz datu berdinak (des)zifratzeko erabili daiteke.
- Prozesua norabide bakarrean joan daiteke → Publikoa zifratzeko erabili bada pribatua deszifratzeko eta alderantziz.

GAKO PUBLIKOKO KRIPTOGRAFIA

- PKI-n (Public Key Infrastructure) bi zifratze mota erabili → Asimetrikoa lehen konexioa ezartzeko eta simetrikoa ostean saioko denbora guztian.



1. Arakatzaileak zerbitzariarekin konexioa eskatu.
2. Zerbitzariak gako publikoa bidali. Gako pribatua sekretuan gorde.
3. Arakatzaileak hirugarren gakoa (saio gako) sortu.
4. Saioaren gakoa bezeroaren ordenagailuan (arakatzaileak) zifratzen da zerbitzariak emandako gako publikoarekin.
5. Zifratutako saio gakoa zerbitzariarekin partekatu.
6. Zerbitzariak gako sekretu pribatua erabiliz jasotako saioaren gakoa deszifratu → Bi muturrek bezeroaren ordenagailuak sortutako saio gakoa dute.
7. Zifratze asimetrikoa zifratze simetrikoarekin ordezkatu.
8. Bezeroa zifratze simetrikoa soilik erabiltzen duen zerbitzariarekin saioan dago, webgunea utzi arte.



SSL/TLS

- Gako publikoa (asimetrikoa) zifratzea laburki erabili hasieran gainerako konexiorako erabiliko den hirugarren gakoa sortzeko.
    - Gastu matematikoa askoz handiagoa du → Konputazio ahalmen askoz handiagoa.
    - Saio luzeetarako ez.
- Zifratze gako simetrikoak askoz laburragoak izan daitezke → Inoiz ez publiko egiten.
- Izaera publikoa → Zifratze asimetrikoak gako luzeak eskatzen ditu.
    - Gako publikoa → Erantzunaren zati bat.
    - Erantzunaren gainerakoa (gako pribatua) kalkulatzea erraza laburra balitz.

HTTPS EZ DU EGITEN

- Bisitatzen ari zaren webguneen izenak ezkutatu.
- Webgune maltzurra bisitatzetik babestu:
    - Ez du webgunea segurua denik ziurtatzen.
    - Segurtasunez konektatu → Ez esan nahi pertsona gaiztoek zuzendutako webgune batera konektatzen ez zarenik.
- Anonimotasunarik eman.
    - HTTPS-k ez du zure kokapen fisikoa edo identitate pertsonala ezkutatzen.
    - IP helbidea zifratutako datuen kanpoaldean erantsi → Internetek ere ez lukeelako jakingo nora bidali zifratuta egongo balitz.
- Birusak izaterik eragozten (ez da iragazkia).
    - Baliteke birusak eta bestelako malware jasotzea.
    - Baina HTTPS-k bitarteko edozeinek zure trafikoan malwarea txertatzea eragoztu.
- Ordenagailua hackeatzeagatik babestu.
    - HTTPS-k datuak babesten ditu ordenagailuaren eta web zerbitzariaren artean mugitzen denean. → Konexioaren mutur batean trafikoa kontrolatzen duen malware bat badago, HTTPS korrontean zifratu aurretik eta ondoren irakur dezake trafikoa.
- **HTTPS-k informazioa kableetatik igarotzen denean bakarrik babestu**.