APLIKAZIO GERUZA
HTTPS
HYPERTEXT TRANSFER PROTOCOL SECURE

3. GAIA

Gaizka Saldaña
Dpto. Ingeniería de Sistemas y Automática

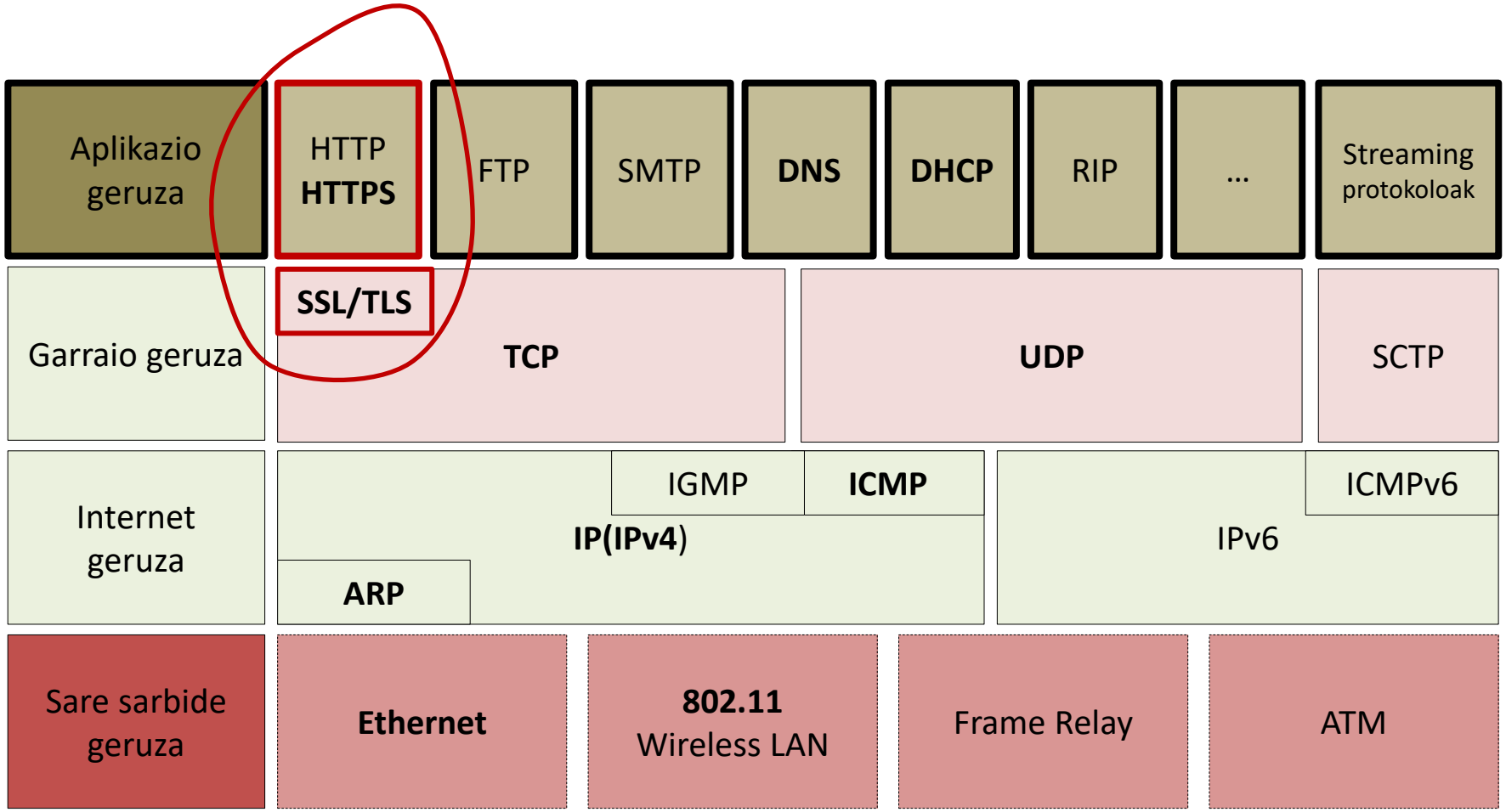
HTTPS SARRERA

- 1990ean internet jaio zen. Hasieratik, Hipertestua Transferitzeko Protokoloa (HTTP) erabili du informazioa munduan zehar mugitzeko. Horregatik, web helbideen hasiera HTTP-rekin hasten da.
- **HTTP EZ da segurua informazioa testu arruntean** daramalako. Horrek esan nahi du trafikoa atzematen duen edonork irakur dezakeela.
- Interneten datu konfidentzialak (adibidez, kreditu txartelen zenbakiak) bidaltzeko, babesteko modua aurkitu behar zen.
- 1994an, Netscape Communications-ek HTTP kriptografia apur batekin hobetu zuen.
- **Secure Socket Layer** (**SSL**) izeneko zifratze protokoloa erabili zuten jatorrizko HTTPrako. Hau "HTTP bidez SSL", "HTTP segurua" edo **HTTPS - Hypertext Transfer Protocol Secure**.
- Denbora luzez, SSL HTTPSek erabiltzen zuen protokolo estandarra izan zen. SSLren bertsio berriagoari orain **Transport Layer Security (TLS)** deritzo.

- **Zergatik enkriptatu Internet?**
  - **Segurtasuna**: saihestu datuak irakurtzea edo kodea txertatzea gure web saioetan.
  - **Pribatutasuna**: ISPek, gobernuek eta datu bilketa enpresa handiek gure trafikoa ikusi eta gordetzen dute. Informazio hori beti da erabilgarria norbaiti, eta horregatik nahi du eta gorde egiten du. Horregatik, webgune askok beren trafikoa zifratzea aukeratzen dute, nahiz eta informazio sentikorra ez bidali. Haien ustez, lineako portaerak ahalik eta pribatuena izan behar du.

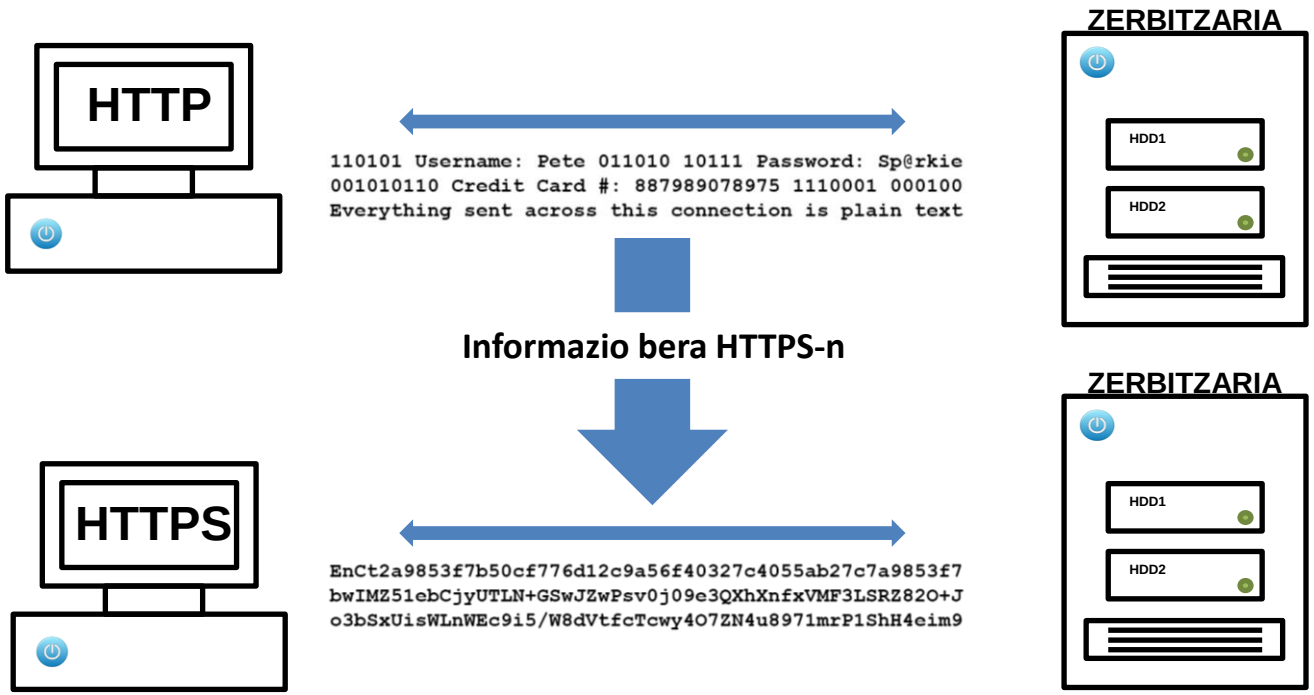
RFC 2818

APLIKAZIO GERUZA
HTTPS



HTTPS
SARRERA

- **HTTPS** (**Hypertext Transfer Protocol Secure**), HTTP seguruagoa.
- HTTPS, bai HTTP SSL (Secure Socket Layer) bidez, bai HTTP TLS (Transport Layer Security) bidez deritzo. TLS, SSL 3.0-aren bertsio eguneratua da. SSL / TLS datuak zifratzea ahalbidetzen duten protokolo kriptografikoak dira.
- HTTPk 80 ataka erabiltzen du, eta HTTPSek 443.
- **HTTPSek datuak ezkutuan gordetzen ditu arakatzailearen eta web zerbitzariaren artean mugitzen diren bitartean enkriptatuz**. Horrek ziurtatzen du elkarrizketa entzuten duen edonork (ISP zerbitzaria, hackerrak, gobernu maltzurrak ...) ezin duela ezer irakurri.



FUNTZIONAMENDUA
ZIFRAKETA PROTOKOLOA- SSL/TLS

KRIPTOGRAFIA: metodo eta trena matematikoak erabiltzen dituen zientzia da, mezu edo artxibo bat algoritmo baten bidez zifratzeko, eta, hortaz, babesteko helburuarekin. Horretarako, bi gako kode (clave) erabiltzen dira konfidentzialtasuna, benetakotasuna edo bak batera lortzeko. Datuak kode bihurtzean datza, irakurri ez daitezen.

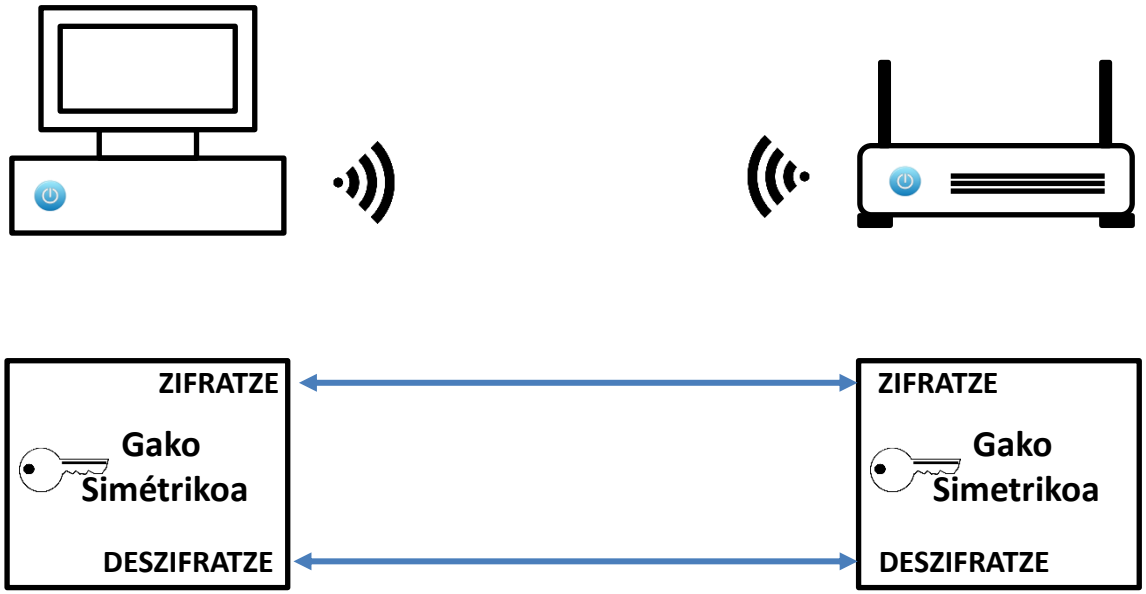
Jorge Ramió (@criptored) eta Alfonso Muñoz (@mindcrypt)

Zifratzeko helburu nagusia duten metodo eta tresna matematikoak erabiltzen dituen zientziari **KRIPTOGRAFIA** deritzo, baina **ezkutatzeko teknika / prozedurari ZIFRAKETA** (Ez enkriptatzioa)

- Hiru gauza behar dira datuak zifratzeko:
  - Zifratu nahi diren **datuak**.
  - **Zifratze gako** bakarra (ausazko testu kate luzea besterik ez)
  - **Zifratze algoritmoa** (funtzio matematikoa). Honek datuak eta gakoa algoritmoan konektatzen ditu eta testu enkriptatua lortuko dugu.
- Testua deszifratzeko, prozesua alderantzikatu besterik ez da egin behar, gako bera erabiliz, datuen jatorrizko forma leheneratuz.
- **Gakoa sekretuan** gordetzea da prozesu osoa funtzionatzen egiten duena. Datuen hartzaileek soilik eduki beharko lukete.
- Gako bakarra duen zifratze sistema honi simetrikoa deritzo.

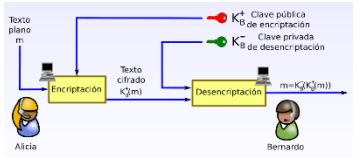
FUNTZIONAMENDUA
SSL/TLS

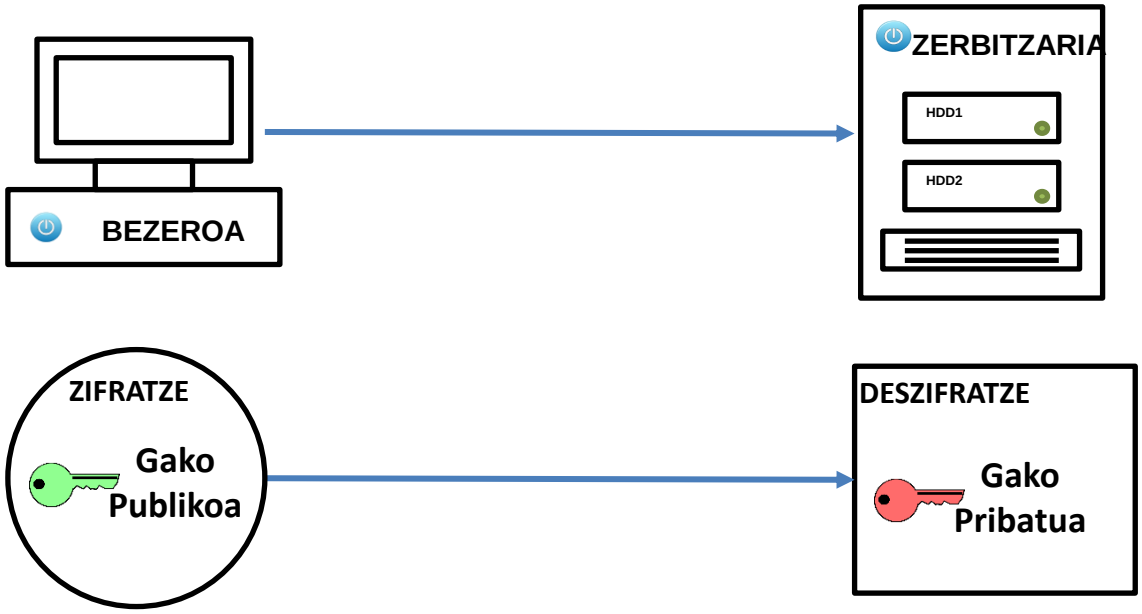
- **Bi muturretan zifratze gako bera erabiltzen duzunean, ZIFRATZE SIMETRIKOA deitzen zaio.** Hau da etxeko WiFiak erabiltzen duena. Haririk gabeko bideratzailea eta ordenagailu eramangarrira konektatzen duen gako bakarra edo "pasahitza" besterik ez dago.



FUNTZIONAMENDUA SSL/TLS

- Konplexuagoa interneteko webgune batera konektatzean. Zifratze simetrikoak, berez, ez du funtzionatuko konexioaren beste muturra kontrolatuta ez dagoelako. Nola partekatu gako sekretu bat bezeroaren eta zerbitzariaren artean Interneten norbaitek erdian atzemateko arriskurik gabe?
- Arazo hau **ZIFRATZE ASIMETRIKOArekin** konpontzen da. **Bi gako desberdin** erabiltzen dira, **bata zifratzeko eta bestea deszifratzeko**. **Gako publikoaren kriptografia** ere deitzen zaio internet publikoan konexio seguruak ezartzeko modua delako.





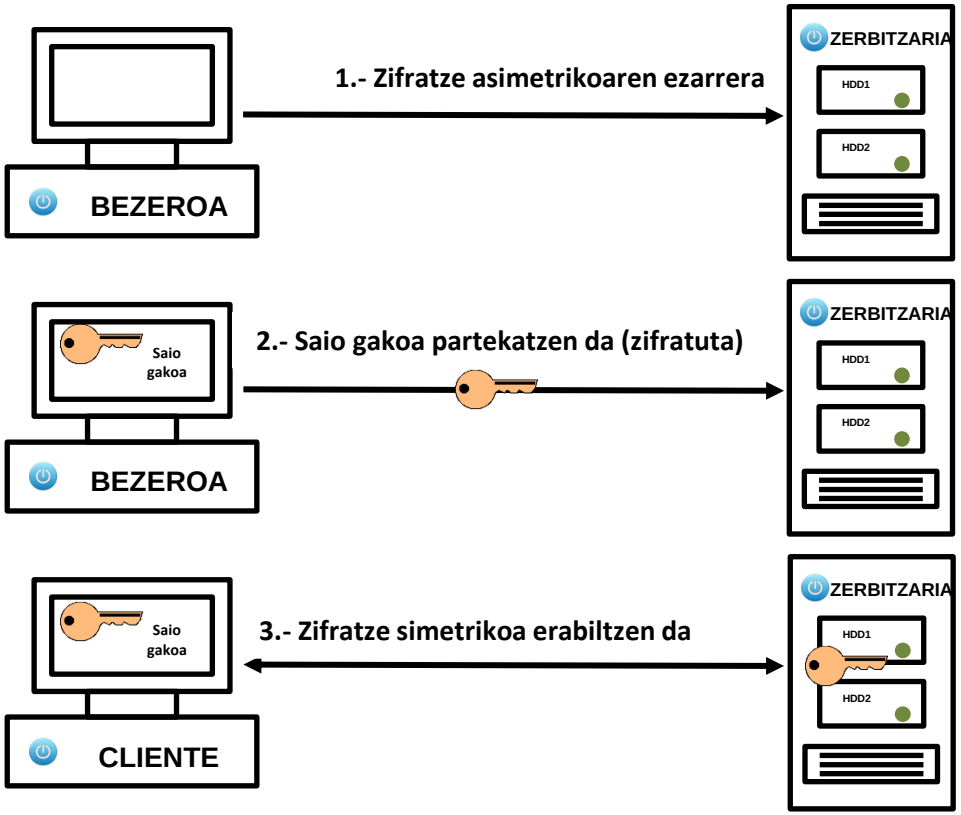
Non egon daiteke arazoa?

FUNTZIONAMENDUA
SSL/TLS – GAKO PAREAK

- Zifratze asimetrikoa ulertzeko, jakin behar da **bi gako ezberdinak datu berak nola zifratu eta deszifratu ditzaketen**.
- **Erantzuna**: zenbaki oso handiko matematika arazoa besterik ez da. Besteak beste, zenbaki lehen oso handiak eta aritmetika modularra erabiltzen dituen prozesu matematiko berezia behar du.
- Zenbaki lehen oso handiak haien artean biderkatzen direnean, funtsean ezinezkoa da hauek faktorizatu jatorrizko zenbakiak zein ziren jakin gabe. Ez da magia, matematikak zenbaki lehenekin funtzionatzeko modua da. Zifratua kentzeko, biderkatutako zenbaki lehenen produktua faktorizatu beharko genuke. Teknikoki posible da norbaitek egun batean nola egin asmatzea, baina gure egungo konputazio ahalmenaren arabera, aurreikusi ahal den etorkizuna segurua dirudi. Informatika kuantikoa heldu arte behintzat.
- Normalean (ez beti) gako publikoak eta pribatuak batera kalkulatzen dira aldi berean, prozesu matematiko berean. Horrek esan nahi du, matematikoki hitz eginez, oso lotuta daudela. Harreman hori dela eta, datu berak zifratzeko / deszifratzeko erabil daitezke. Hori da, gainera, gako bikote desberdinen gako publiko eta pribatuak elkarrekin lan ezin egitearen arrazoia. Web zerbitzari bakoitzak bere multzo berezia du, beraz, webgunerako konexioa beste gune batzuetatik bakarra da.
- Hala ere, prozesua norabide bakarrean joan daiteke. Datu batzuk zifratzeko gakoetako bat (publikoa edo pribatua) erabiltzen denean, beste gakoa bakarrik erabil daiteke deszifratzeko.
- Beraz, ez du axola gako publikoa nork duen datuak enkriptatu ondoren. Web zerbitzarian ezkutuan gordetzen den gako pribatuarekin bakarrik desenkriptatu daitezke.

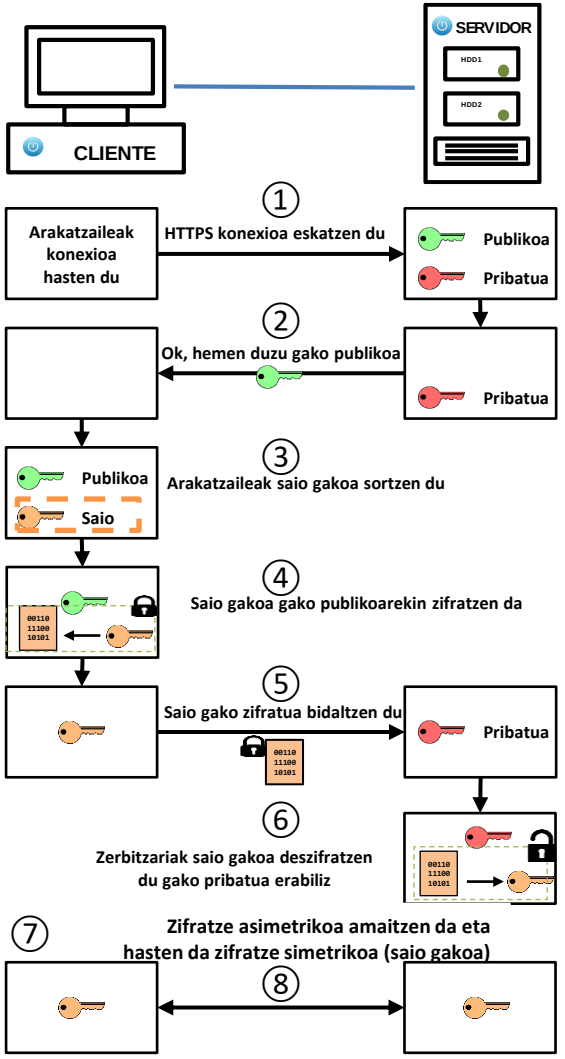
FUNTZIONAMENDUA
SSL/TLS – GAKO PUBLIKOKO KRIPTOGRAFIA

- **PKI - Public Key Infrastructure**-n, bi zifratze mota erabiltzen dira. Zifratze asimetrikoa (gako publikoa) erabiltzen da lehendabizi konexioa ezartzeko, eta, ondoren, zifratze simetrikoarekin (*saio* izeneko saio gakoa) denbora guztian jarraitzen da.



FUNTZIONAMENDUA
SSL/TLS – GAKO PUBLIKOKO KRIPTOGRAFIA

1. Arakatzaileak webguneko zerbitzariarekin konexioa eskatzen du.
2. Zerbitzariak **gako publikoa** bidaltzen du. **Gako pribatua** sekretuan gordetzen du.
3. Arakatzaileak **saio gakoa** izeneko hirugarren gakoa sortzen du.
4. Saioaren gakoa bezeroaren ordenagailuan (arakatzaileak) zifratzen da zerbitzariak emandako gako publikoa erabiliz.
5. Zifratutako saio gakoa zerbitzariarekin partekatzen da.
6. Zerbitzariak gako sekretu pribatua erabiliz jasotako saioaren gakoa deszifratzen du. Orain bi muturrek bezeroaren ordenagailuak sortutako saio gakoa dute.
7. Gako zifratu asimetrikoa edo publikoa amaitu, eta zifratze simetrikoarekin ordezkatzen da.
8. Bezeroa zifratze simetrikoa soilik erabiltzen duen zerbitzariarekin saioan dago, webgunea utzi arte.



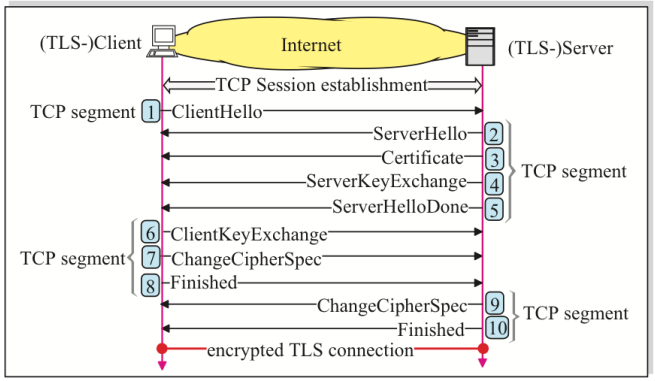
Gaizka Saldaña
Dpto. Ingeniería de Sistemas y Automática

FUNTZIONAMENDUA SSL/TLS

- Gako publikoa (asimetrikoa) **zifratzea** laburki erabiltzen da hasieran gainerako konexiorako erabiliko den hirugarren gakoa trukatzeko. Zifratze asimetrikoaren gaineko gastu matematikoa askoz ere handiagoa da eta, beraz, konputazio ahalmen askoz ere handiagoa behar du. Ez da egokia saio luzeetarako.
- **Zifratze gako simetrikoak askoz ere laburragoak izan daitezke**, ez baitago horien zati bat inoiz publiko egiten.
- Izaera publikoaren erruz **zifratze asimetrikoak gako luzeak eskatzen ditu**. Gako publikoa duzunean, dagoeneko erantzunaren zati bat duzulako. Erantzunaren gainerakoa (gako pribatua) kalkulatzea erraza izango litzateke erantzuna laburra balitz. Gako esponentzialki handiagoak izateak gako pribatuak pribatuan mantentzea bideragarri egiten du.
  - **Zifratze gako simetrikoa**
    C8D5897DCC56D6D462B8F32D464303161ACE11E536F04AE1
  - **Zifratze gako asimetrikoa**

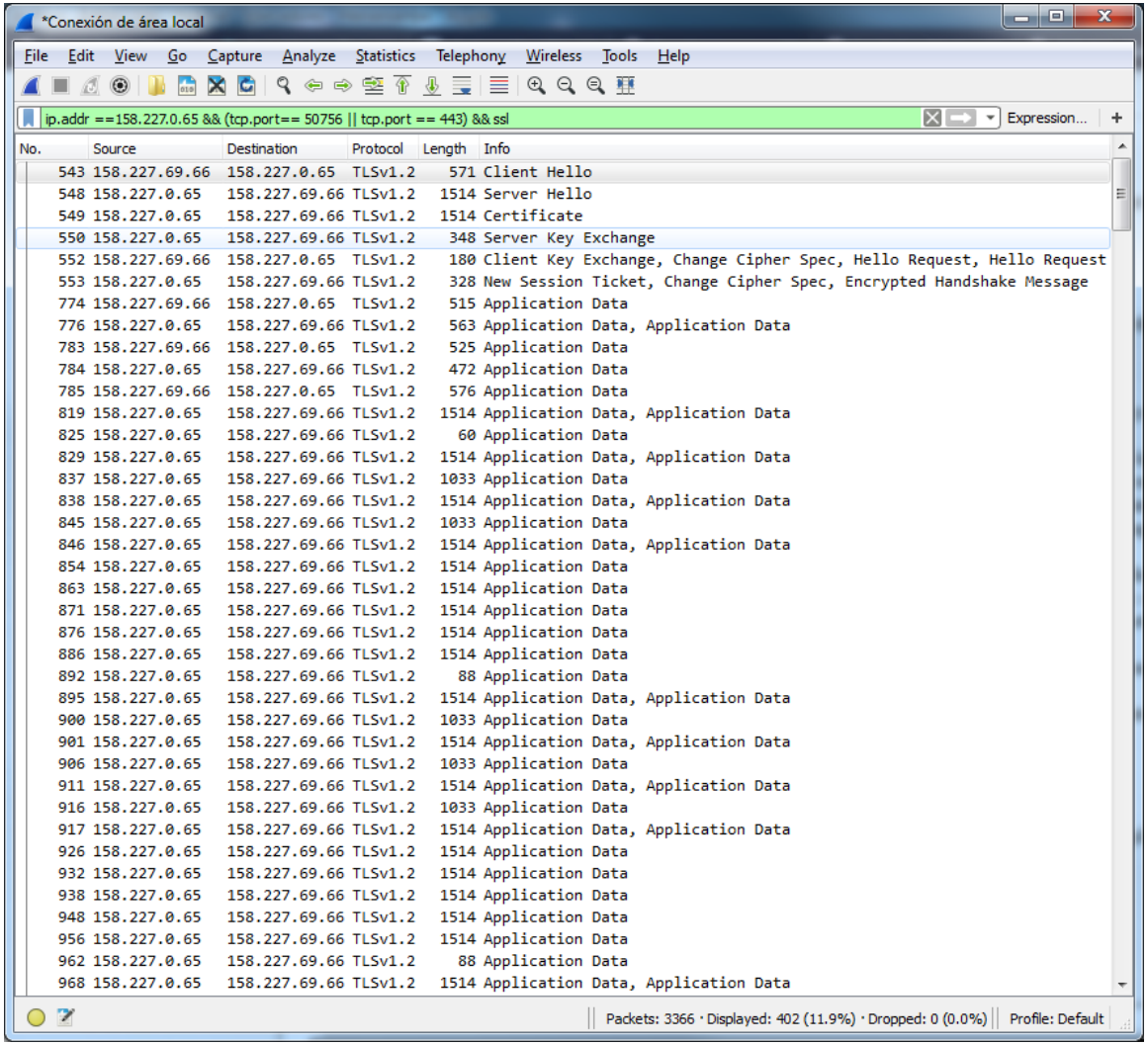
```
MIIEogIBAAKCAQBl1esMuCZXUjwiBaUJsZlHrcGJ988fblnhcTjtpnaovHYp7IZW
0EMIkKMuF6tILPuJBMd2FoFHC2ZUVcmGrFabK/zRzrEb74djiH4l1gQHZDsQYybv
Qm6bJEsT5Cy+lwRCvXznEnWmQu62HX09CThtXUPNwfGLcAEFQLzgKPOcU4DZboY9
Tlm/Repe9w6h0KEzB7MHFIt446RPh9FalQwfrjfxGNHb+8V9BVlpRetXxd6aj1oo
WEsg5TqrZB8Cr17l/KXh+goqlyFmsz6WMpbv5oLbG+535PhyZjJ/VjiuTi6jsD9N
Skgq+iEbx74ZE855Ba7iYlJma6vxAj3ILdyLAgMBAAECggEAB41BjQPq8/bJNsys
XHerIkGkZJLX7UDFsY4v5o+9pO205Y8At1diYTQ4paZjsUqErLiKAhvRIm+Z+w8R
jscg9QjiCr0FLUkqBRuOH0grrFCmgKSZsox+n0qltqfpGYkha8GZjZk02EuGYEL3
kpsocBPGf2+udeSsbrNKTmU7C5CdOp+Fzmw4goltgmS3Sn8FWBaWOgblcUIFyupB
ETAzxUiH2qQom3plosMb11NzVNw8LajyGNmphB5szRHx+6Y6fGuhEacIePez8LJE
zRUdcjomzNNsft1iAduc0cZSRfPCMMmP989l+tWck2d/i9QWtuRoDhxsXyAaCieZ
dDnAIQKBgQDGrxF1WRum9N+D4D2MRTntseiNyZAKzgcPmXqyWoyPFDKsiTsk/Qe2
/KIQjJf11JcpZ+12UNNRFjghiFyl3Bh1E+pT6kzTPUZ5Ewws0hjm5CL667RkWCtn
4N4BoWPLmM5KFXMvmoK3iNyMLI+LZmI3HQ2wLcpC2+I1cpVmyQHoZQKBgQCDNotl
s2tuzNOKUsgrYl3SGk3MgOHe147h/Q32/x+dahIihVz6N3/nCiVpmliySGuLlxOu
OsWJby7XNuana7AVt59pE7G87pHtNFpLvhmN8oBDgvzbH2pLta/fQM9yjDokyk0I
4jhn2cMDE6qpx1yLnR8Hogb393GXqmAB/RtKLwKBgCF1yE3n9NU4NhBCinr+CZRz
OsPuJxj6u4uwAE7bGwLZlvMhpVlEV7FEeJKq6siWxeJOQ1qCoCPuxwM2sMup9mB5
OyRouAl3L1AimhFOTK1NzGpPmbCwfJbg8uJ5aJIYKN2nIR/qOItqPCJLOt1yH6ZC
eVSrUX3TBBSWOHz36x9VAoGAPyB8zD8XzsTIeWH+X7EBhlWVXHAdOwLmAR+oGk7/
vNINS4JyCwesh1FAUqApUAy7gPr8QvSPmOFe3bfSHHYYzzn6fak197mnh0GKt6oL
zVkAEHryf9GLaEVPCc+6flesmYqiqUV88am4wsAxeWEqyxialyeCxsXLZrZXXl2R
RY0CgYEAioZF15++gWnRzVKL/xFMj6Si53hekXHMrAsyYkxDB7Drjz3Qg9QN7fG1
gzBXLeRPa0tnkfcWgeXIdbHNZywfqrhaUO+k4t5Ei5n8ZXDKeqtNAGSrVdG282/a
OXL64xujKmZG27kZjK43bRe27obUHXbV7X0unT98QyYyWmkXdKk=
```

FUNTZIONAMENDUA
WIRESHARK- EN BIDEZ ANALISIA



https://www.fehcom.de/qmail/smtptls.html

- Bezeroaren eta zerbitzariaren arteko komunikazioa ezartzerakoan hiru **agur mota (Handshake**) egon daitezke :
- **Agur osoa**: zerbitzariak eta bezeroak ziurtagiriak trukatzen dituzte
- **Agur erraza**: zerbitzaria, eta bezeroa ez, autentifikatzen da ziurtagiria entregatzean
- **Agurra laburtura**: konexioa ezartzerakoan, zerbitzariak eta bezeroak saio IDa trukatuko dute, bezeroak zerbitzariaren IP eta atariarekin lotuko duena, bezeroak berriro konektatzen denean ID hori erabil dezan. Zerbitzariak bezeroak eskaintzen duen saio IDa cache-an duela egiaztatuko du eta kasu horretan aurretik negoziatutako parametroekin konexioa berriro egitea erabaki dezake edo ID berri bat eskaini agur osoa berriro egitera behartuz (noizean behin bakarrik erabili behar den metodoa)



HTTPS
EZ DU EGITEN

- EZ ditu ezkutatzen bisitatzen ari zaren webguneen izenak
- EZ du babesten webgune maltzurra bisitatzetik, HTTPS-k ez du webgunea segurua denik ziurtatzen. Segurtasunez konektatzeak ez du esan nahi pertsona gaiztoek zuzendutako webgune batera konektatzen ez zarenik. *Agintari ziurtagiri fidagarriak* (Trusted Certificate Authotities) arazoa konpontzen saiatzen ari dira, baina sistema ez da perfektua.
- EZ du anonimotasunarik ematen. HTTPS-k ez du zure kokapen fisikoa edo identitate pertsonala ezkutatzen. Zure IP helbidea zifratutako datuen kanpoaldean erantsi behar da, Internetek ere ez lukeelako jakingo nora bidali zure IP helbidea ere zifratuta egongo balitz. Eta ez du zure identitatea ezkutatzen bisitatzen ari zaren webgunean ere.
- EZ du birusak izaterik eragozten. HTTPS ez da iragazkia. Baliteke birusak eta bestelako malware jasotzea HTTPS konexioaren bidez. Web zerbitzaria kutsatuta badago edo malware banatzen duen webgune kaltegarri batean bazaude, HTTPS korrontearen barruan bidaliko da beste guztia bezala. Hala eta guztiz ere, HTTPS-k bitarteko edozeinek zure trafikoan malwarea txertatzea eragozten du.
- EZ du babesten ordenagailua hackeatzeagatik. HTTPS-k datuak babesten ditu ordenagailuaren eta web zerbitzariaren artean mugitzen denean. Horrek esan nahi du konexioaren mutur batean trafikoa kontrolatzen duen malware bat badago, HTTPS korrontean zifratu aurretik eta ondoren irakur dezakeela trafikoa.

HTTPS-k zure informazioa kableetatik igarotzen denean bakarrik babesten du. Ezin ditu zure ordenagailua, zure identitatea babestu edo bisitatzen ari zaren guneak ezkutatu. HTTPS Internet seguruago baten zati bat besterik ez da.