Zifraketa asimetrikoa

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus

Universidad del País Vasco
Euskal Herriko Unibertsitatea
BILBOKO INGENIARITZA ESKOLA
ESCUELA DE INGENIERÍA DE BILBAO

Zifraketa asimetrikoa

https://doi.org/10.5281/zenodo.4302267

https://github.com/mikel-egana-aranguren/EHU-SGSSI-01

Klabe publikoko kriptografia

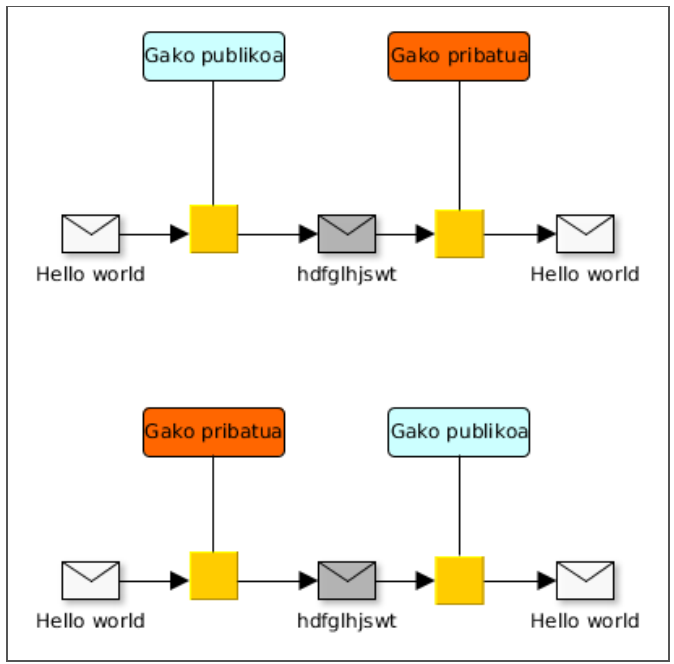
Gako asimetrikoko algoritmoak: zifratzen duen klabea ez da deszifratzen duena

Erabiltzaile bakoitzak bi klabe:

- Gako publikoa, mundu osoak ezagutzen duena
- Erabiltzaileak soilik ezagutzen duen gako pribatua

Gako batek zifratzen duena besteak deszifratzen du

Klabe publikoko kriptografia



Klabe publikoko kriptografia

- Ikerrek bere gako pribatua du, l_{pri}, eta mundu guztiak bere gako publikoa du, l_{pu}
- Mirenek bere mezua zifratzen du Ikerren gako publikoa erabiliz: $c = e (m , l_{pu})$
- Mirenek c kriptograma Ikerreri bidaltzen dio
- Ikerrek c jasotzen du
- Ikerrek c deszifratzen du bere l gako pribatua erabiliz: $m = d (c , l_{pri})$
- Konfidentzialtasuna. Ikerrek soilik deszifratu dezake mezua

Klabe publikoko kriptografia

Abantailak:

- Jasotzaileak soilik irakur dezake mezua
- Gako bakarra gorde behar da
- Edozeinek erabili dezake gako publikoa mezu konfidentziala bidaltzeko Ikerreri
- Gako publikoa komunikatzeko ez dira beharrezkoak kanal seguruak

Klabe publikoko kriptografia

Arazoak:

- Gako pribatua pribatua mantendu behar da
- Gako publikotik gako pribatua ondorioztatzea ia ezinezkoa izan beharko litzateke
- (Des)zifraketa sistema simetrikotan baino geldoagoa da

Klabe publikoko kriptografia

Arazoak:

- Mirenek segurtasun osoz jakin behar du Ikerren gako publikoa erabiltzen dagoela
- Gako publikoak lortzea erraza izan behar du

Klabe publikoko kriptografia

Erabiltzaile bakoitzak bere gako bikotea sortzen du (gako publikoa, gako pribatua) eta gako publikoa gakoen zerbitzari batean argitaratzen du: Key Certification Authority edo Key Distribution Center (KDC)

Klabe publikoko kriptografia

Arazo gehiago:

- Nola daki Ikerrek mezua benetan Mirenena dela?
- Ikerrek erantzuten duenean, nola daki Mirenek benetan mezua Ikerrena dela?

Klabe publikoko kriptografia

- Ikerrek zifratzen badu bere gako pribatuarekin edonork deszifratu ahal du (Mundu osoak ezagutzen du I_{pu})
- Soluzioa:
  - Ikerrek bere gako pribatuarekin zifratzen du mezua: C1 = e (m, I_{pri})
  - Gero Mirenen gako publikoarekin berriro zifratzen du: C2 = e (C1 , M_{pu})

Klabe publikoko kriptografia

- Mirenek bakarrik deszifratu ahal du bere gako pribatuarekin:
  - Konfidentzialtasuna: Mirenek soilik deszifratu ahal du mezua: C1 = d (C2 , M_{pri})
  - Kautotzea eta Zapuztezintasuna: Ikerrek soilik bidali ahal izan du mezua: m = d (C1, I_{pu})

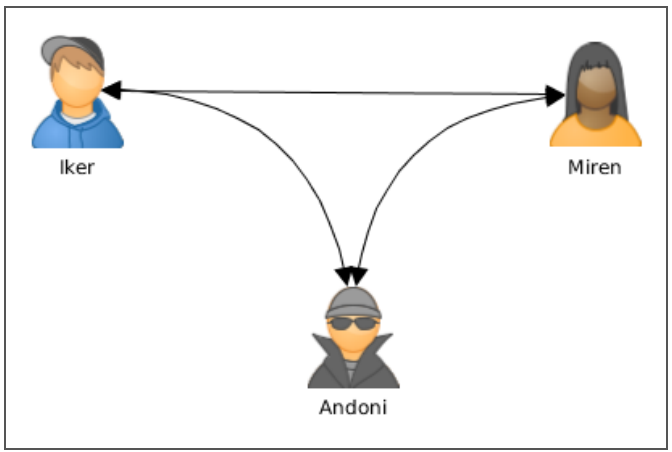
Klabe publikoko kriptografia

Zer gertatzen da baten bat komunikazio erdigunean jartzen bada

Man in the middle erasoa:

- Bitartekari batek mezu guztiak jasotzen ditu partaideak jakin barik
- Partaideen komunikazio guztietan eskua sartu behar da

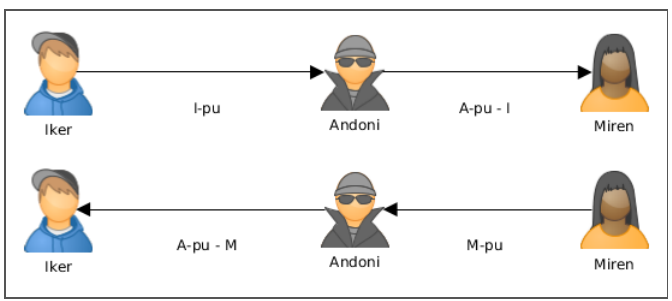
Klabe publikoko kriptografia



Klabe publikoko kriptografia

Ikerrek eta Mirenek komunikatzen hasi nahi dutenean, klabe publikoak trukatzen dituzte

Andonik hartzen ditu eta bere klabearekin aldatzen ditu

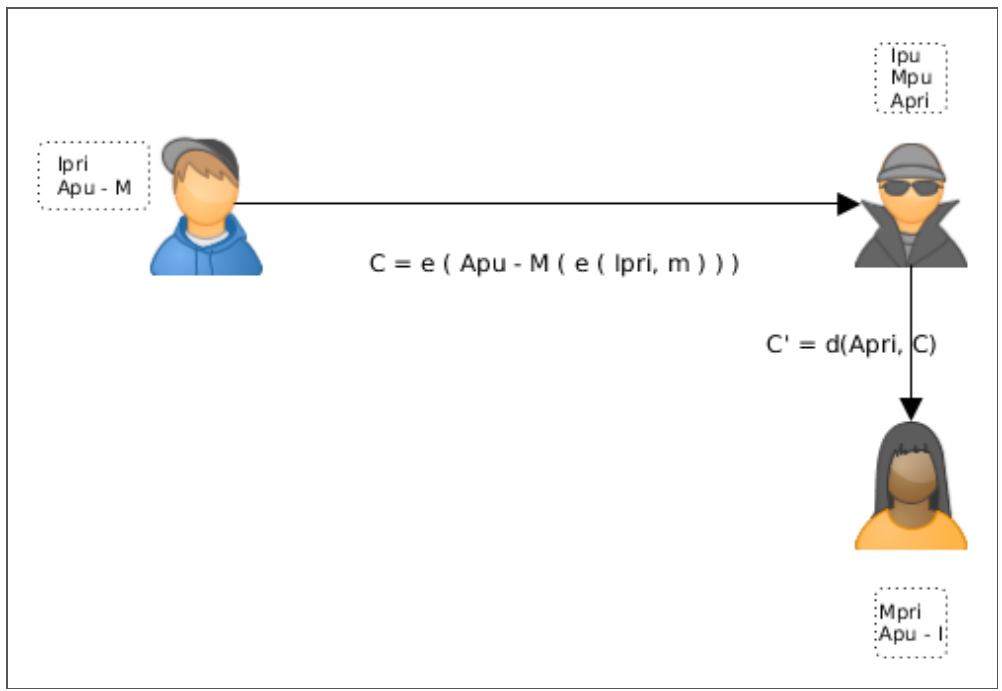


Klabe publikoko kriptografia

Ikerrek eta Mirenek mezuak zifratzen dituzte ustezko bestearen klabe publikoarekin eta beraien klabe pribatuarekin

Andonik mezuak jasotzen ditu, irakurtzen ditu, aldatzen ditu, eta bere klabe pribatuarekin zifratzen ditu

Klabe publikoko kriptografia



Klabe publikoko kriptografia

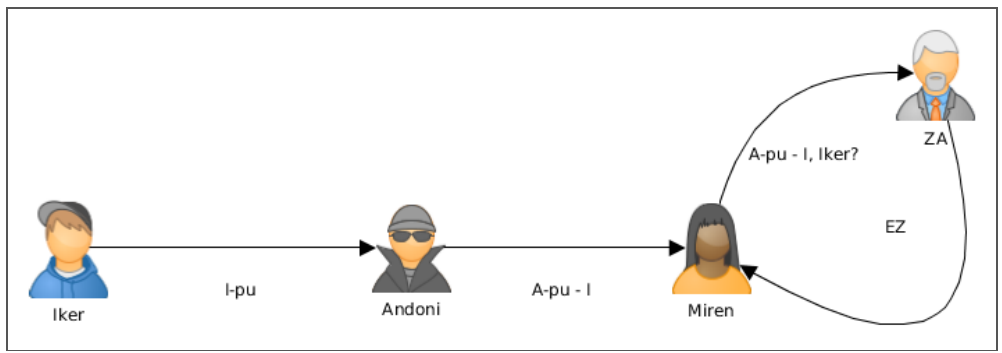
Ikerrek eta Mirenek modu seguruan komunikatzen ari direla uste dute

Andonik dena irakurtzen du eta nahi beste aldatzen

Ekiditeko:

- Klabeak kanal seguruen bidez elkarbanatu
- Autoritate (erakunde) batek klabe publiko bat norbaiti dagokiola zertifikatzea: Zertifikazio Autoritatea

Klabe publikoko kriptografia



Zifratu hibridoa

Gako pribatuko sistemak gako publikokoak baino askoz azkarragoak dira

Askotan konbinazio bat erabiltzen da: gako publikoko sistema S gako sekretu bat elkarbanatzeko erabiltzen da, behin soilik erabiliko dena

Gako pribatuko sistemak S erabiltzen du mezua zifratzeko

Zifratu hibridoa

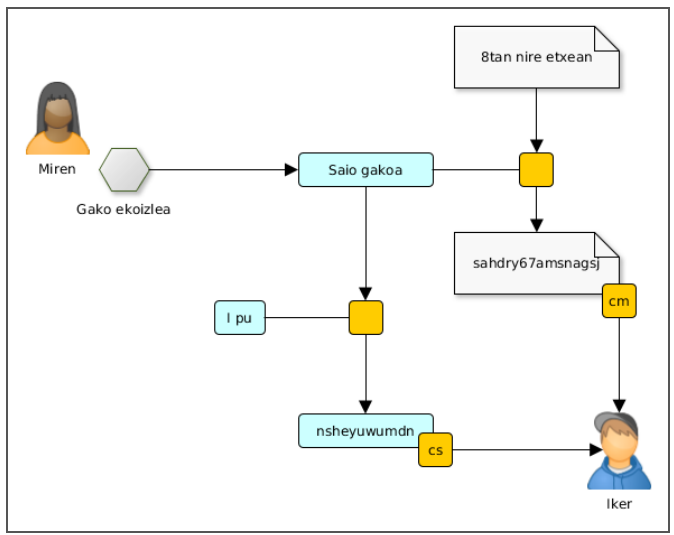
Mirenek S gako sekretua sortzen du, eta bere mezua zifratzeko erabiltzen du:

cm = e1 (m,S)

Mirenek S zifratzen du Ikerren gako publikoarekin: cs = e2 (S , I_{pu})

Mirenek [cm, cs] bidaltzen dio Ikerreri

Zifratu hibridoa



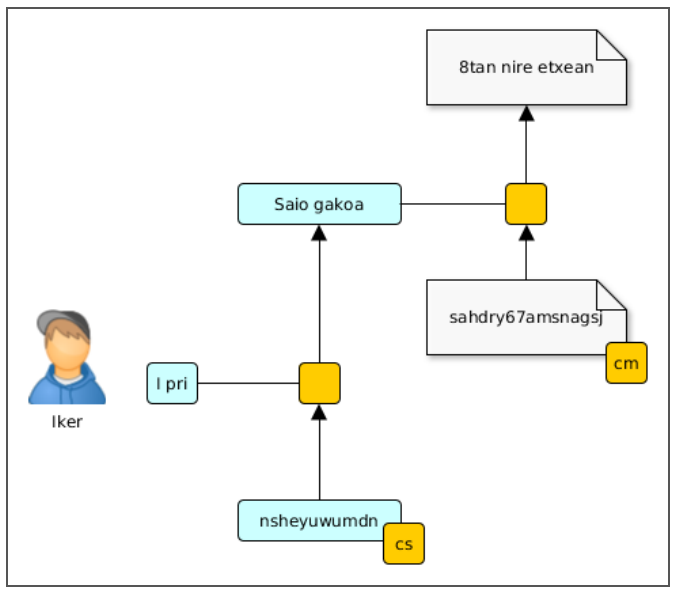
Zifratu hibridoa

Ikerrek [cm , cs] jasotzen du

Ikerrek S deszifratzen du bere gako pribatua erabiliz, l_{pri}: d2 (cs , l_{pri}) = S

Ikerrek S erabiliz m deszifratzen du: d1 (cm , S) = m

Zifratu hibridoa



Gako publikoko algoritmoak

Diffie-Hellman - 1976

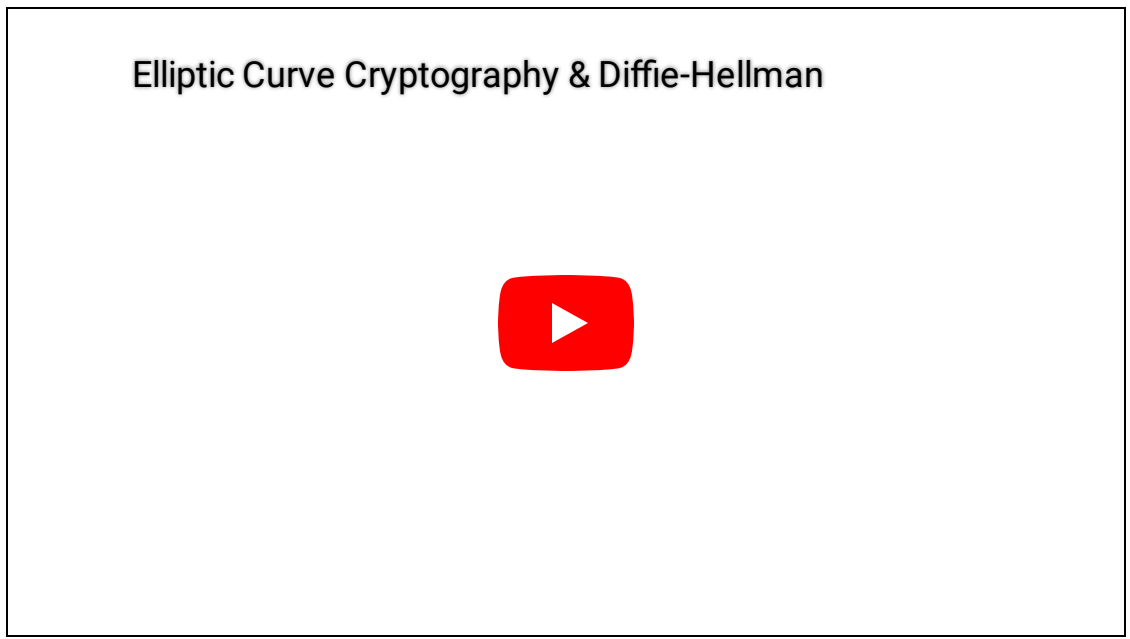
RSA - 1977

ElGamal - 1984

DSA - 1991

Kurba eliptikoak - 1985

Gako publikoko algoritmoak



Gako publikoko algoritmoak

Gako publikoko algoritmoak

DNI electronikoa (DNIe 3.0):

- RSA
- SHA-1 / SHA-256
- TripleDES / AES

Gako publikoko algoritmoak

PGP:

- RSA / DSA
- IDEA / TripleDES

Gako publikoko algoritmoak

SSH:

- RSA / DSA

SSL / TLS:

- RSA / DSA / Diffie-Hellman
- IDEA / DES / TripleDES /AES