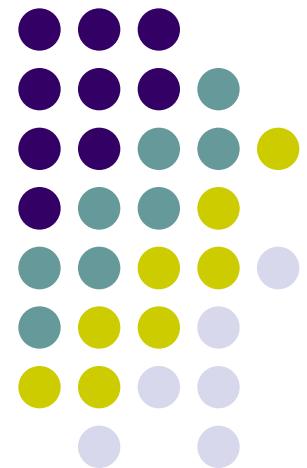


# Informazio Sistemen Arkitektura

Ingeniaritza Telematika Arloa

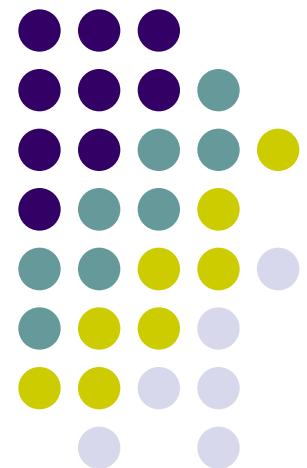
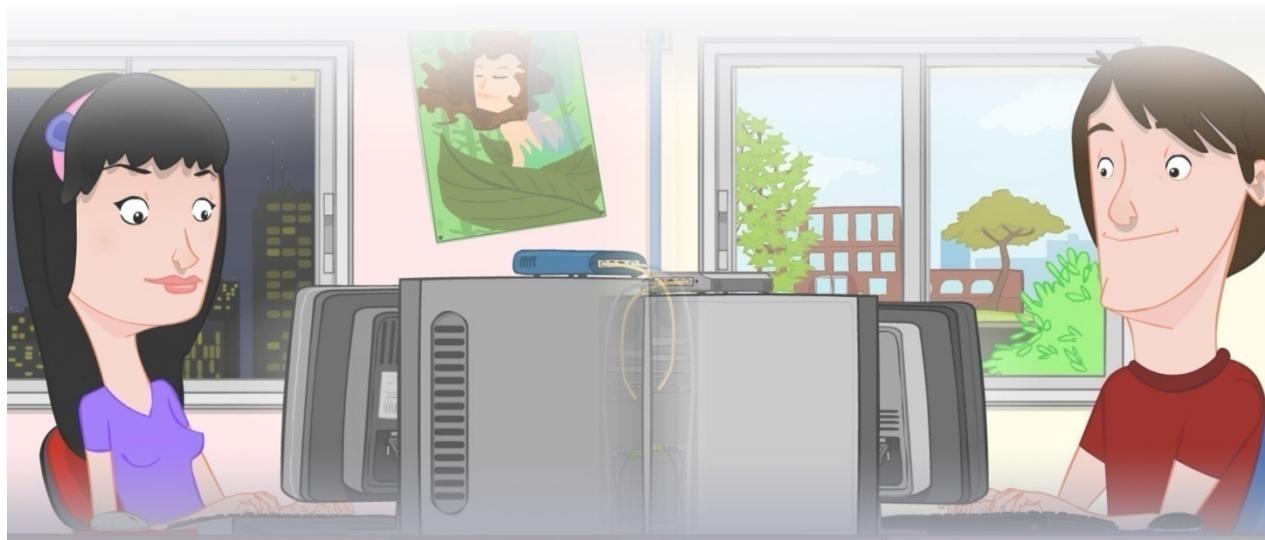


**TELEK:O**  
UPV/EHU Bilbao

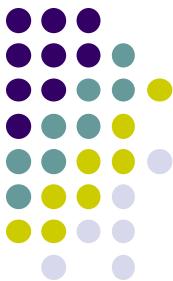
# 2. Atala: Segurtasuna Informazio Sistemetan

Informazio Sistemen Arkitektura

Telekomunikazio Teknologiaren Ingeniaritzako Gradua (3. Maila)



**TELEK:O**  
UPV/EHU Bilbao



# Aurkibidea

- Sarrera
- Segurtasunaren oinarriak Informazio Sistemetan
- Teknika kriptografikoak
  - Kriptografiari buruzko oinarrizko kontzeptuak
  - Zifratzea
  - Mezu Autentifikazio Kodeak (MAC, Message Authentication Code)
  - Sinadura Digitalak
  - Mezuen freskotasuna
  - Gakoen banaketa
- Segurtasuna Informazio Sistemetan
- Segurtasunaren egungo egoera
- Segurtasunaren kudeaketa



# Aurkibidea

- Sarrera
- Segurtasunaren oinarriak Informazio Sistemetan
- **Teknika kriptografikoak**
  - Kriptografiari buruzko oinarrizko kontzeptuak
  - Zifratzea
  - Mezu Autentifikazio Kodeak (MAC, Message Authentication Code)
  - Sinadura Digitalak
  - Mezuen freskotasuna
  - Gakoen banaketa
- Segurtasuna Informazio Sistemetan
- Segurtasunaren egungo egoera
- Segurtasunaren kudeaketa



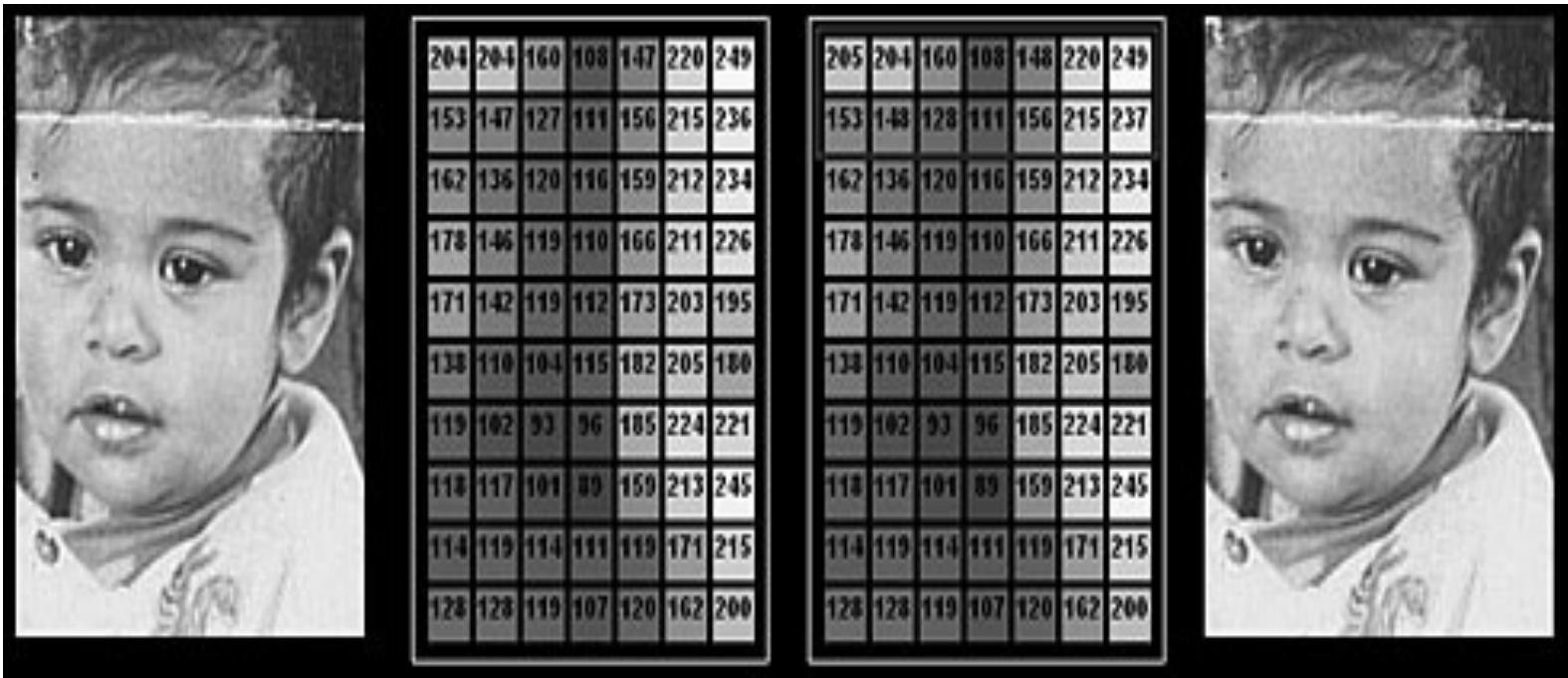
# Kriptografia: Definizioak

- Esteganografia
  - Helburua: mezu baten existentzia ezkutatzea
- Kriptografia
  - Bere helburua mezu baten esanahia edo edukia ezkutatzea da, kodifikazioa bezala ezagutzen den prozesua.
- Kriptologia
  - Igorle eta hartzale baten artean komunikazio kanal baten bidez kodifikatutako mezuen elkar trukearen segurtasunarekin loturiko arazo teorikoak tratatzen dituen zientzia.
    - Kriptografia + Kriptoanalisia



# Kriptografia: Definizioak

- Esteganografia: adibidea



Iturria: [https://equalit.ie/esecman/chapter2\\_8.html](https://equalit.ie/esecman/chapter2_8.html)



# Kriptografia: Definizioak

## ● Kriptografia

- Mezuen adierazpen linguistikoak aldatzera zuzendutako zifratze edo kodifikazio teknikak, ez baimendutako hartzaleentzat ulertezinak bihurtzeko xedearekin.
- Tradizionalki zifratzearekin erlazionatuta bakarrik:
  - Kriptografiaren helburu bakarra mezuen konfidentzialtasuna lortzea zen.
- Gaur egun:
  - Hurrengoek ikertetaz arduratzen den kriptologiaren arloa: algoritmoak, protokolo kriptografikoak, informazioa babesteko erabiltzen diren sistemak eta bai komunikazioetan bai komunikatzen diren entitateetan segurtasuna implementatzeko erabiltzen diren sistemak.

[Iturria: [Wikipedia](#)]



# Kriptografia motak

- Sistema kriptografikoak hurrengoan arabera sailkatzen dira:
  - Testu arrunta (plaintext) zifratutako testua (ciphertext) bihurtzeko erabilitako eragiketa motak:
    - Ordezkapena eta transposizioa
  - Erabilitako gako kopurua:
    - Simetrikoa eta asimetrikoa
  - Testu arrunta (plaintext) prozesatzeko era:
    - Bloke edo fluxua (stream)

Gako kopuruaren arabera sailkatu: A->B

- Gako BAKARRA: K\_AB

Gako SEKRETU bakarra

- Gako bikote bat entitateko:

A-> K\_A-(pribatu) eta K\_A+(publiko)

B-> K\_B-(pribatu) eta K\_B+(publiko)

Sekretua != Pribatua!

[Fuente: Wikipedia]

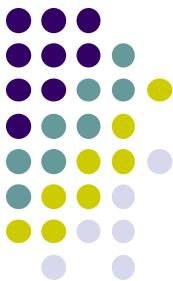


# Kriptografia motak

- Oinarrizko zifratze motak erabilitako eragiketa moten arabera:
  - Ordezkapenetan oinarrituta:
    - Jatorriko testuko unitateak zifratutako testuarekin ordezkatzen dira sistema erregular bat jarraituz.
  - Transposizioetan oinarrituta:
    - Jatorriko testuko unitateak, orden ezberdin, eta, normalean, oso konplexu bat erabiliz aldatzen dira, baina unitateak berez ez dira aldatzen.

[Iturria: Wikipedia]

Gaur egun bi eragiketen arteko nahasteak!



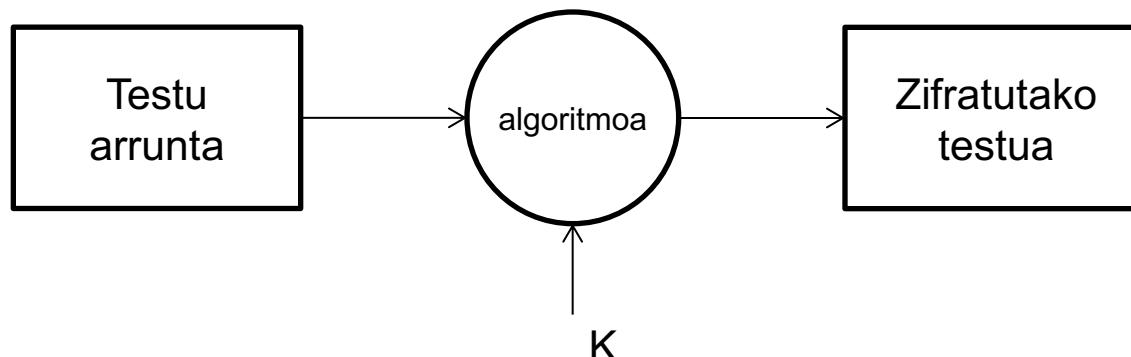
# Aurkibidea

- Sarrera
- Segurtasunaren oinarriak Informazio Sistemetan
- **Teknika kriptografikoak**
  - Kriptografiari buruzko oinarrizko kontzeptuak
  - Zifratzea
  - Mezu Autentifikazio Kodeak (MAC, Message Authentication Code)
  - Sinadura Digitalak
  - Mezuen freskotasuna
  - Gakoen banaketa
- Segurtasuna Informazio Sistemetan
- Segurtasunaren egungo egoera
- Segurtasunaren kudeaketa



# Zifratzea: Oinarrizko Kontzeptuak

- Zifratzea: jatorrizko testu bat (testu arrunta, *plaintext*) gako batekin parametrizatutako funtzioko bidez gakoan jarri (zifratutako testua, *ciphertext*).
  - KONFIDENTZIALTASUNAren aurkako erasoetatik babesten du



- Kasu honetan kriptoanalisia:
  - Zifratutako testuak deszifratzeko kriptosistema hondatzen, eta dagokien testu arruntak lortzeko aukera ematen duten sistemak ikertzen dituen zientzia.



# Zifratzea: Oinarrizko Kontzeptuak

## ● Ordezkapenetan oinarritutako zifratza:

- “Unitateak” honakoak izan daitezke: letra bakar bat (kasurik ohikoena), letra pareak, hirukoteak, aurrekoen nahasteak, etab.
- Hartzaileak kontrako ordezkapena egin behar du testua deszifratzeko.
- Motak:
  - Simplea: letra simpleekin eragiten badu.
    - Monoalfabetikoa: ordezkapen simplea erabiltzen bada mezu osorako. (Homofoniko)
    - Polialfabetikoa: ordezkapen ezberdinak erabiltzen baditu mezu baten parte ezberdinetan.
  - Poligrafikoa: Letra taldeak erabiltzen baditu.

[Iturria: Wikipedia]



# Zifratzea: Oinarrizko Kontzeptuak

- Kriptoanalisia:
  - Sistemetan ahultasunak aurkitzeko eta euren segurtasuna apurtzeko xedearekin sistema kriptografikoen azterketara zuzendutako kriptologiaren partea.
    - Zifratutako testuak deszifratzeko kriptosistema (kodea) hondatza.
    - Kriptoanalisian jarduten duten pertsonei kriptoanalista deitzen zaie.

[Iturria: Wikipedia]



# Zifratzea: Oinarrizko Kontzeptuak

- Kriptoanalisia:

- Eraso motak erasotzailearen aurretiko ezagutzaren arabera:
  - “ciphertext-only” erasoak:
    - Zifratutako testua bakarrik daukaguenan.
    - Adibideak:
      - Indarrez (brute force).
      - Maiztasunen azterketan oinarritutakoa.
      - Kasiski metodoa.

[Fuente: Wikipedia]



# Zifratzea: Oinarrizko Kontzeptuak

## ● Kriptoanalisia:

- Eraso motak erasotzailearen aurretiko ezagutzaren arabera:
  - “known-plaintext” erasoa:
    - Erasotzaileak testu arrunta ezagutzen du
      - Orduan, ez da eratzeko ezer geratzen! EZ!!!
  - Batzuetan erasotzaileak testu arruntaren parte bat ezagutzen du edo probablea den hitzen bat (“probable-word” attack).

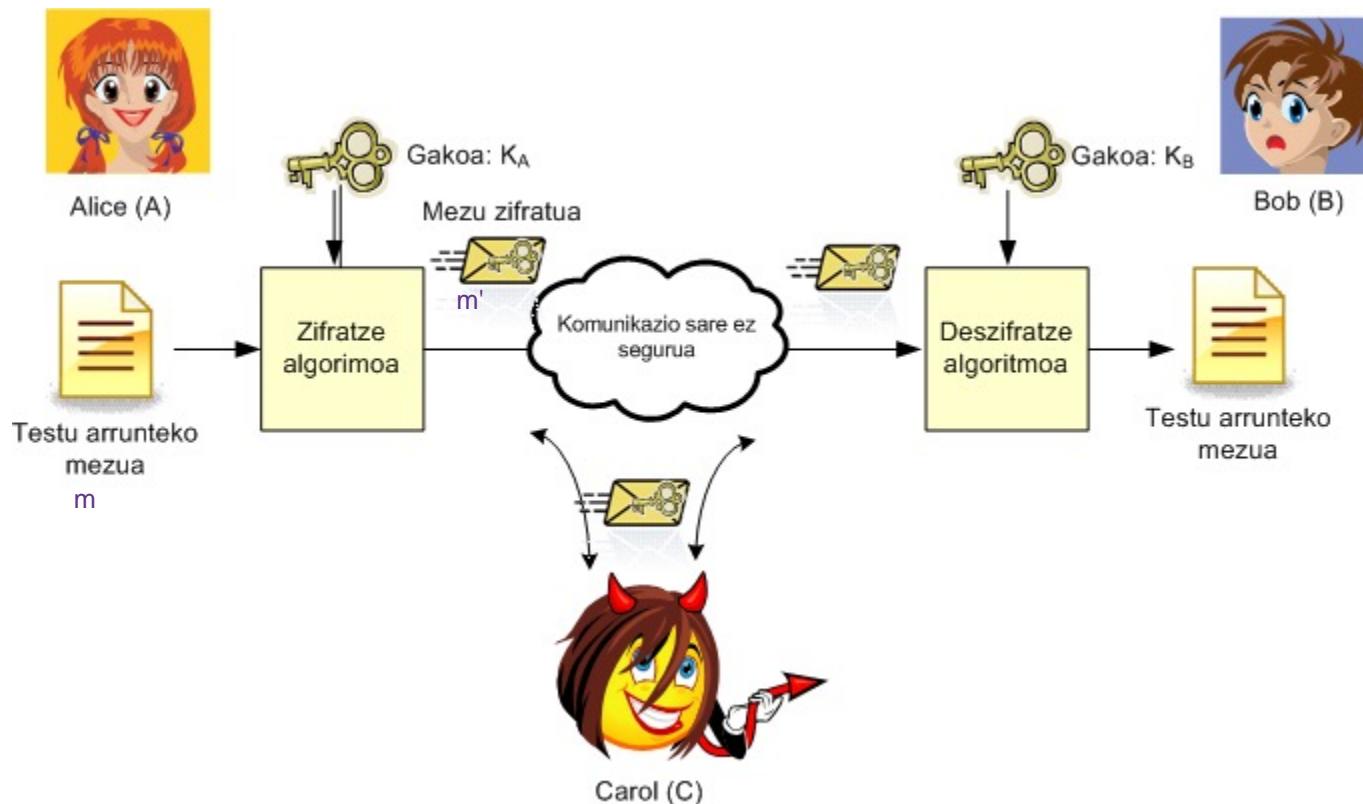


# Zifratzea: Oinarrizko Kontzeptuak

- Kriptoanalisia:
  - Eraso motak erasotzailearen aurretiko ezagutzaren arabera:
    - “chosen-plaintext” erasoa
      - Erasotzailea bere testu arrunta definitu, zifratzailean sartu eta sortutako zifratutako testua aztertzeko gai da.
        - Ez dirudi oso egoera problablea. Adibidea: kriptografia publikoa.
      - Helburua: zifratzaile horrek zifratutako edozein testu deszifratzeko gai izatea.
    - “chosen-plaintext” erasoen aurka segurua den edozein sistema “known-plaintext” eta “ciphertext-only” erasoen aurka segurua da ere.



# Zifratzea: Oinarrizko Kontzeptuak



## ● Sistemaren elementu nagusiak:

- Testu arrunta eta zifratutako testua.
- Zifratze/deszifratze algoritmoak.
- Zifratze gakoa ( $K_A$ ) eta deszifratze gakoa ( $K_B$ )



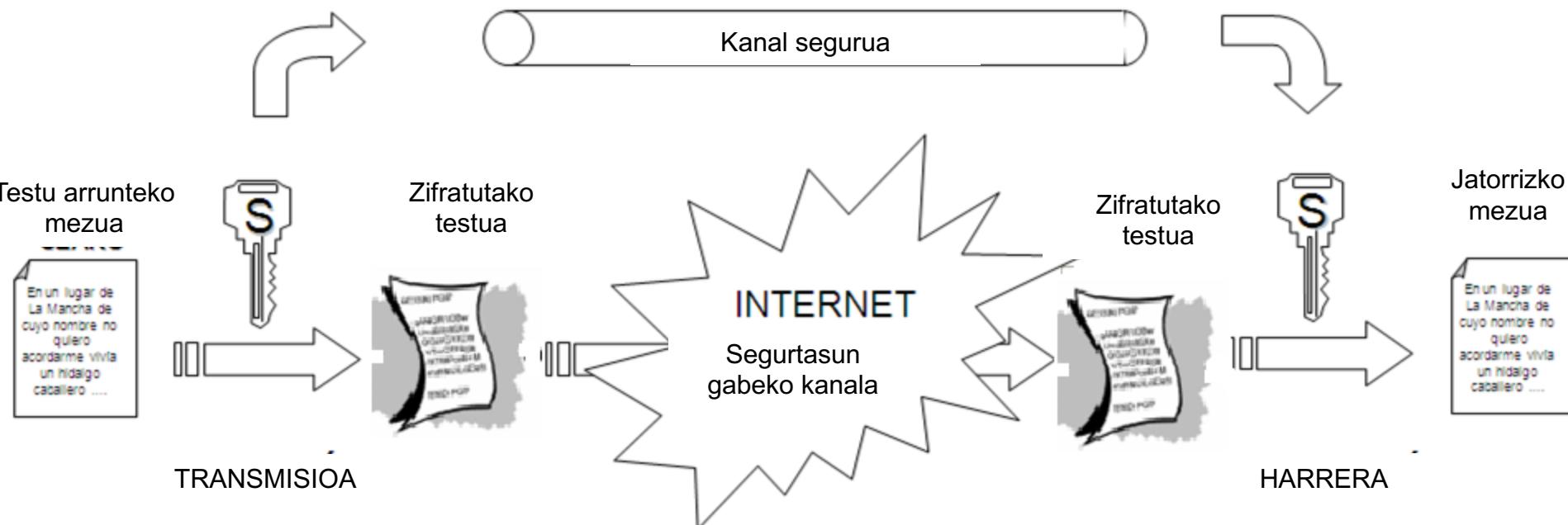
# Zifratzea: Oinarrizko Kontzeptuak

- Gako sekretudun edo simetrikodun kriptografia (I):
  - Gako bera erabiltzen da informazioa zifratzeko eta deszifratzeko:
$$K_A = K_B = K_{AB}$$
$$K_{AB}(K_{AB}(m))$$
$$m' = \{m\}K_{AB}$$
$$m = \{\{m'\}K_{AB}\}K_{AB}$$
  - Gako **sekretua** ( $K_{AB}$ ), komunikazioan parte hartzen duten benetako bi entitateek ezagutzen dute (Alice eta Bob) eta beraiek bakarrik.



# Zifratzea: Oinarrizko Kontzeptuak

- Gako sekretudun edo simetrikodun kriptografia (II):



# Zifratzea: Oinarrizko Kontzeptuak

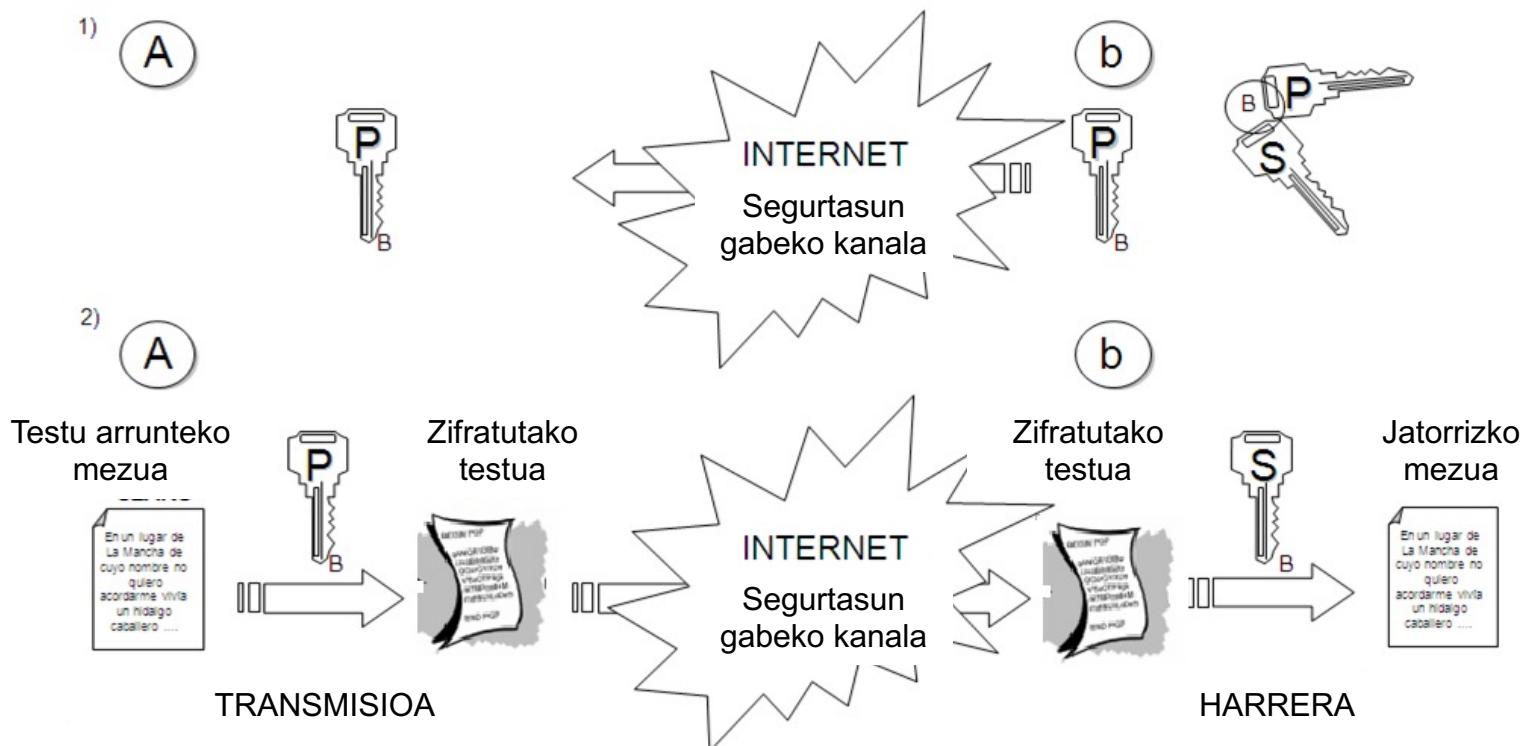


- Gako publikodun edo asimetrikodun kriptografia (I):
  - 70. hamarkadaren erdialdea
  - Erabiltzaile bakoitzak gako publiko ( $K^+$ )/pribatu ( $K^-$ ) pare bat dauka.
    - Alice:  $K_A^+ / K_A^-$  eta Bob:  $K_B^+ / K_B^-$
  - $K^+$  gako publikoa jakinda, dagokion gako pribatua  $K^-$  lortzea konputazionalki bideraezina da.
  - Gako **pribatua** sekretua da eta beraz, bere benetako jabeak ezagutzen du bakarrik.
  - Gako **publikoa**, berriz, publikoa da eta beraz, edonork ezagutzen du.

# Zifratzea: Oinarrizko Kontzeptuak



- Gako publikodun edo asimetrikodun kriptografia (II):



# Zifratzea: Oinarrizko Kontzeptuak



- Gako publikodun edo asimetrikodun kriptografia (III):
  - Gako publikoarekin zifratzen den guztia dagokion gako pribatuarekin deszifratu daiteke bakarrik eta alderantziz.
    - $K^+(K^-(m)) = m \text{ ó } K^-(K^+(m)) = m$
  - Bob-eri bidalitako mezuen konfidentzialtasuna bermatzeko igorle guztiekin mezuak Bob-en gako publikoarekin ( $K_B^+$ ), guztiekin ezagutzen dutena, zifratu behar dituzte.
    - Alice:  $m \rightarrow K_B^+(m)$
  - Bob da mezuak bere gako pribatuarekin ( $K_B^-$ ), berak bakarrik ezagutzen duena, deszifratu ditzakeen bakarra:
    - Bob:  $K_B^-(K_B^+(m)) = m$



# Zifratzea: historia apur bat...

- Algoritmo zaharrenek kriptografia simetrikoa erabiltzen dute.
- Ordezkaren bidezko zifratzea.
  - Gako sekretua ordezkaren taula batean datza.

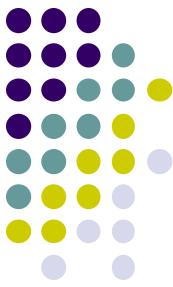
$K_{AB} =$

a -> c  
b -> w  
⋮  
z -> a

## Adibideak:

Testu arrunteko mezua: “bcza”

$K_{AB}$  gakoarekin zifratutako mezua: “wnac”



# Zifratzea: historia apur bat...

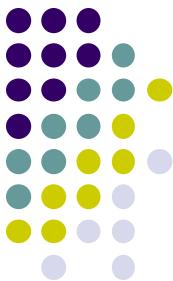
- César-en zifratzea:
  - Ordezkaren bidezko zifratzearen adibide konkretu bat.
    - Julio César-ek asmatuta bere jeneralekin komunikatzeko (D). -> Beste edozein hizkirekin izen bera hartzen du.
  - Ez da benetako zifratze algoritmo bat, gakorik ez baita existitzen, gakoa finkoa da.
    - Desplazamendu konstantea.

Alfabeto original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto cifrado	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

## Adibidea:

Testu arrunteko mezua: “Kaixo”

Zifratutako mezua: “Ndilar”



# Zifratzea: historia apur bat...

- Ordezkaren bidezko zifratzearen arazoa:
  - Zifratze erabat ez segurua.
    - Oso erraza da zifratza “haustea”.
  - “Brute-force” attack, zenbat konbinazio posible daude?
    - 26
    - $26!$
    - $2^{26}$
    - $26^2$
    - $26! \approx 2^{88}$  Shannon-en bakartasun distantzia  $\log_2(N!)/D$ 
      - 88 bit gako bakoitzarentzat -> segurtasun onargarria
  - Gakoa gehitu!!!
    - Orokortasuna:  $C=(a*m+b) \bmod N \rightarrow$  César  $k=(1,3)$ 
      - A eta b < N
      - $\text{z.k.h}(a,N)=1$
    - Transposizioa



# Zifratzea: historia apur bat...

- Ordezkapen bidezko zifratzearen arazoa :
  - Oinarria: letra ezberdinek erabilpen maiztasun ezberdinak dituzte.
    - Ingeles-ez gehien erabiltzen diren letrak dira:
      - ‘e’ -> %12.7, ‘t’->%9.1, ‘a’->%8.1...
    - Eta gehien erabiltzen diren letra pareak:
      - “he”, “in”, “an”, “th”,...
  - “Ciphertext-only” motako erasoak dira.



# Zifratzea: historia apur bat...

- Vigenère-ren zifratzea (16. mendea, Erroma)
  - Gakoa letra sekuentzia bat da, eta mezu osoa zifratzeko behar den bezain beste bider errepikatzen da.
  - Adibidea:  
$$(m+k) \text{ mod } 26$$
  
\*Hizkien posizioa 0tik hasten da

$k =$	C R Y P T O C R Y P T O C R Y P T
$m =$	W H A T A N I C E D A Y T O D A Y
$c =$	Y Y Y I T B K T C S T M V F B P R



# Zifratzea: historia apur bat...

- Vigenère-ren zifratzea (16. mendea, Erroma)
  - “Hausteko” erraza: “chipertext-only” attack
  - Gakoaren luzera ezagututa:

$k =$	C	R	Y	P	T	O	C	R	Y	P	T	O	C	R	Y	P	T
$m =$	W	H	A	T	A	N	I	C	E	D	A	Y	T	O	D	A	Y
$c =$	Y	Y	Y	I	T	B	K	T	C	S	T	M	V	F	B	P	R

Diagram illustrating the Vigenère cipher decryption process. The key  $k$  is repeated as  $C R Y P T O C R Y P T O C R Y P T$ . The message  $m$  is  $W H A T A N I C E D A Y T O D A Y$ . The ciphertext  $c$  is  $Y Y Y I T B K T C S T M V F B P R$ . Arrows point from the first four letters of the key ( $C, R, Y, P$ ) to the first four letters of the ciphertext ( $Y, Y, Y, I$ ). The second group of letters ( $T, B, K, T$ ) is highlighted with yellow arrows, indicating they correspond to the second letter of the key ( $R$ ).

- Sarrien agertzen den 1. letra ‘H’-a dela suposatuz:
  - ‘H’ – ‘E’ = ‘D’
  - Horrela gako osoa lortu daiteke
- Gakoaren luzera ezaguna ez bada:
  - Luzera=1-etik aurrera luzera ezberdinekin frogatu zentzua daukan testua lortu arte.



# Zifratzea: historia apur bat...

- Vigenère-ren zifratzea. Beste bertsio bat.

Tablero de Vigenère																										
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y



# Zifratzea: historia apur bat...

- Vigenère-ren zifratzea. Beste bertsio bat.
  - Adibidea:
    - Gakoa = **AZUL**
    - Bidali beharreko testua: **el ejército está preparado**

E	L	E	J	E	R	C	I	T	O	E	S	T	A	P	R	E	P	A	R	A	D	O
A	Z	U	L	A	Z	U	L	A	Z	U	L	A	Z	U	L	A	Z	U	L	A	Z	U

- Zifratutako mezua:

**EK YUEQWTTN YDTZ JCEOUCACI**



# Zifratzea: historia apur bat...

Tablero de Vigenère

0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

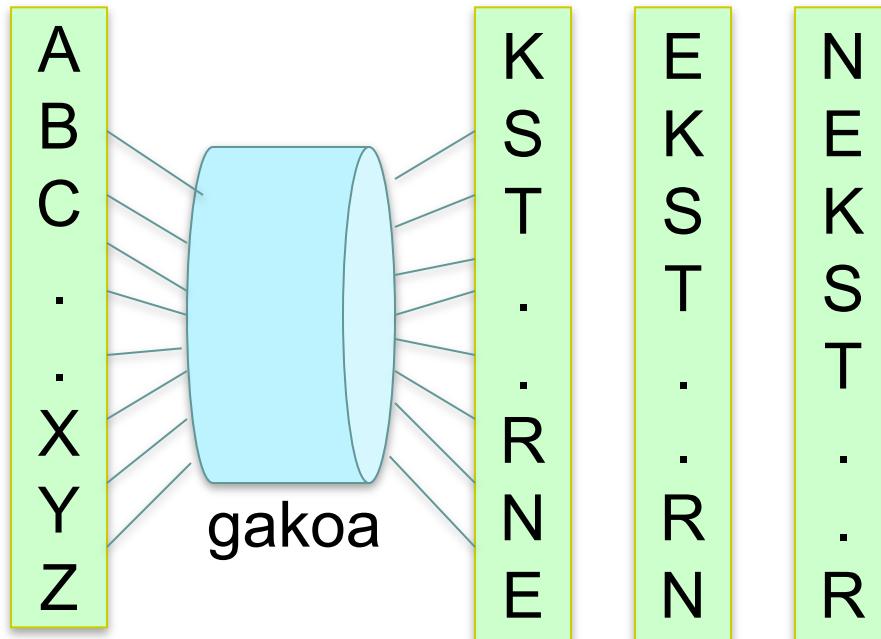
E	L	E	J	E	R	C	I	T	O	E	S	T	A	P	R	E	P	A	R	A	D	O
A	Z	U	L	A	Z	U	L	A	Z	U	L	A	Z	U	L	A	Z	U	L	A	Z	U

E K Y U E Q W T T N Y D T Z J C E O U C A C I



# Zifratzea: historia apur bat...

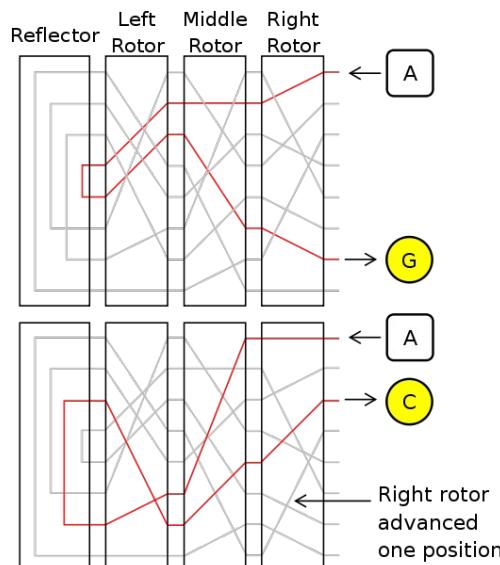
- Errotore makinak (1870 – 1943)
  - Adibide goiztiarra:
    - Hebern makina(errotore bakarra)





# Zifratzea: historia apur bat...

- Errotore makinak (1870 – 1943)
  - Errotore makinarik famatuena:
    - Enigma (3-5 errotore)



Guztirako gako posible kopurua:  
216,767,120,751,581,400,000



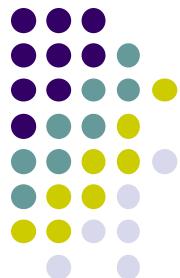
# Zifratzea: historia apur bat...

- Aro digitala:
  - 1974: DES (Data Encryption Standard) :
    - 1976. urtean estandar federal bezala onartu zen.
    - 2005. urtea arte erabilia
    - NSA-ren (National Security Agency) atzeko ate baten susmoa.
    - Gako luzera laburra: 56 bit
      - “Brute-force” motatako eraso batekin, 24 ordutan “hauts” daiteke.
    - DES-ren bertsio seguruagoa:
      - 3-DES: datu bakoitzeko sekuentzialki hiru gako erabiltzea.
      - Zifratutako blokeen kateatzea erabiltzen du.



# DES

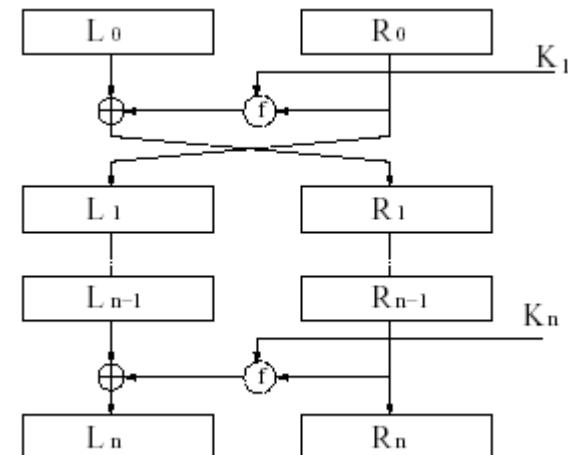
- Kodifikazioa eta dekodifikazioa oso antzekoak edo berdinak
  - HW sistemetan implementatzea errazten du
  - Gakoa aldatzea bakarrik da beharrezko
- Algoritmoa:
  - Feistel ordezkapen – transposizio sare bat
  - Blokeka ematen da
  - Aldaera:
    - Feistel Sare ez-orekatuak: L0 eta R0 atalek ez dute luzera berdina (SkipJack)



# DES

- Gakoa: 56bits (64bits - paritate bitak)

- Bloke tamaina: 64bits
  - Betetzearen beharrizana



- Dekodifikatzeko: k<sub>i</sub> alderantzizko ordenean
- 3DES/TDES
  - 3 aldiz DES zifratzea
  - Gako luzera: 168bits (3x56 bits)
    - Berez, 112bits: Man-in-the-middle erasoa
    - Bakarrik da segurua, 3 gako desberdin erabilita
  - Erabilera: Microsoft Office, Firefox, Ordaintze-sistemak...
  - 2023 arte

Iturria: <https://ciberseguridad.com/guias/prevencion-proteccion/criptografia/cifrado-3des/>



# Zifratzea: historia apur bat...

- Aro digitala:
  - Lehenengo gako publikodun algoritmoak:
    - 1976 -> **Diffie-Hellman** gako ezarpena.
    - 1977 -> RSA zifratzea.
    - 1984 -> ElGamal zifratzea.
  - Egungo gako sekretudun zifratzaileak:
    - AES (2001), Salsa20 (2008) eta askoz gehiago.



# AES

- 2001. urtean estandar federal bezala onartu zen.
- Gako tamaina: 128, 192 eta 256 bits
- Bloke tamaina: 128 bits
- Algoritmoa:
  - Rijndael ordezkaren – transposizio sare bat
  - Blokeka ematen da
- Algoritmo efiziente bat da
- DES-ekin konparaketa:

<https://barcelonageeks.com/diferencia-entre-cifrados-aes-y-des/>



# Zifratzea: Gakoen Iuzera

- Gakoen Iuzera segurtasun maila berdintsua eskaintzeko:

Symm. Cipher key-size

80 bit  
128 bit  
256 bit (AES)

Asymm. Cipher key-size

1024 bit  
3072 bit  
**15360** bit



# Aurkibidea

- Sarrera
- Segurtasunaren oinarriak Informazio Sistemetan
- Teknika kriptografikoak
  - Kriptografiari buruzko oinarrizko kontzeptuak
  - Zifratzea
  - Mezu Autentifikazio Kodeak (MAC, Message Authentication Code)
  - Sinadura Digitalak
  - Mezuen freskotasuna
  - Gakoen banaketa
- Segurtasuna Informazio Sistemetan
- Segurtasunaren egungo egoera
- Segurtasunaren kudeaketa



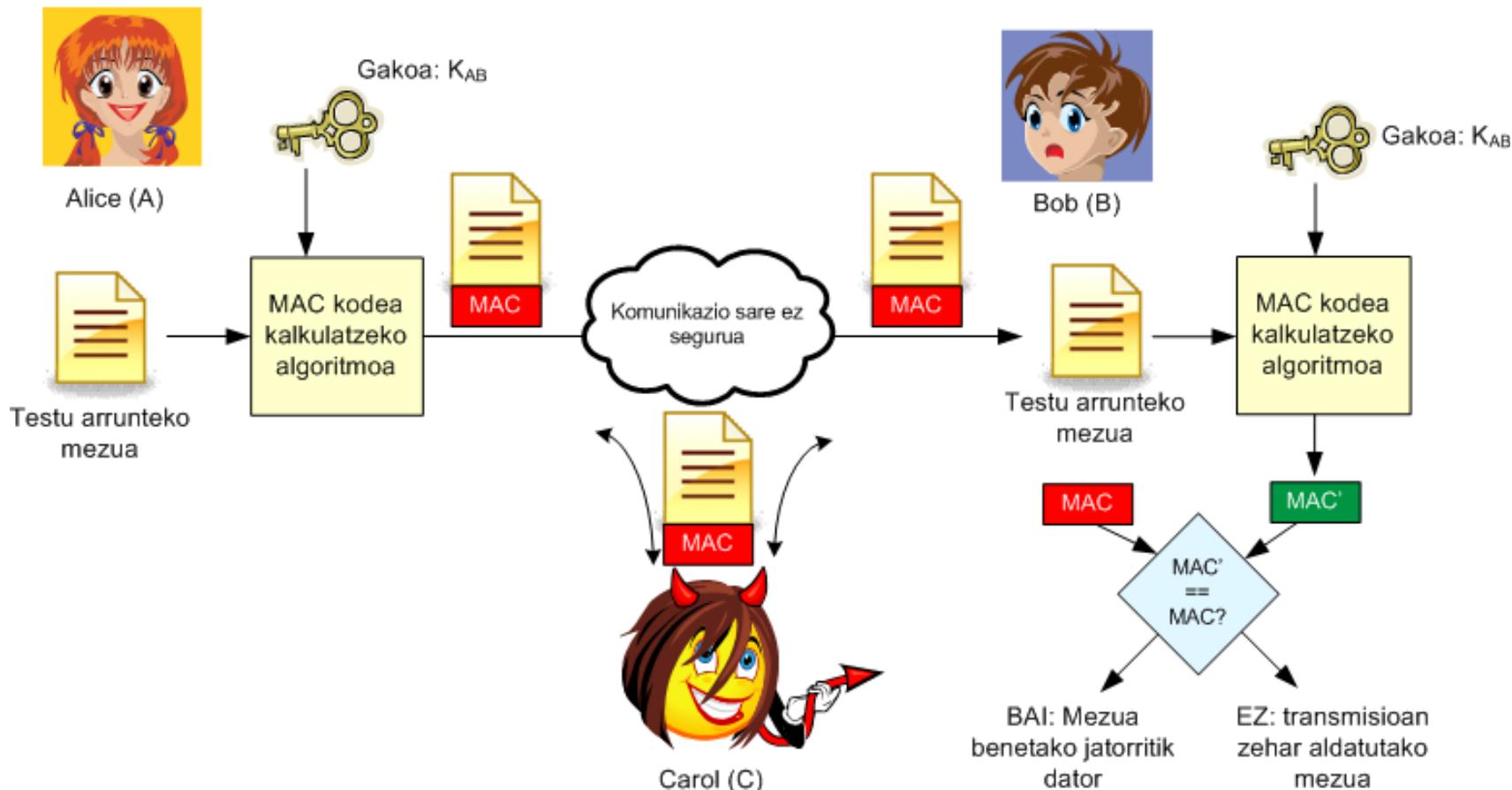
# Mezu autentifikazio kodeak

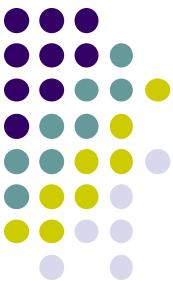
- Mezuen OSOTASUNA eta JATORRIZKO AUTENTIKOTASUNA babesten dute:
  - Mezuaren jatorria benetan berak dioena dela eta mezua transmisioan zehar aldatu ez dela bermatzea.
    - Sinonimotzat har daitezke: mezu bat bere transmisioan zehar aldatzen bada, mezuaren jatorria aldatzen da. Mezuaren jatorria dagoeneko ez da hasierako igorlea, baizik eta mezua aldatu duena.
- Batzuetan mezu baten osotasuna bermatzea beharrezkoa izan daiteke, baina ez bere konfidentzialtasuna:
  - Fitxategi bitarrak diskoetan, iragarki bandak (banner) web orrialdeetan, etab.



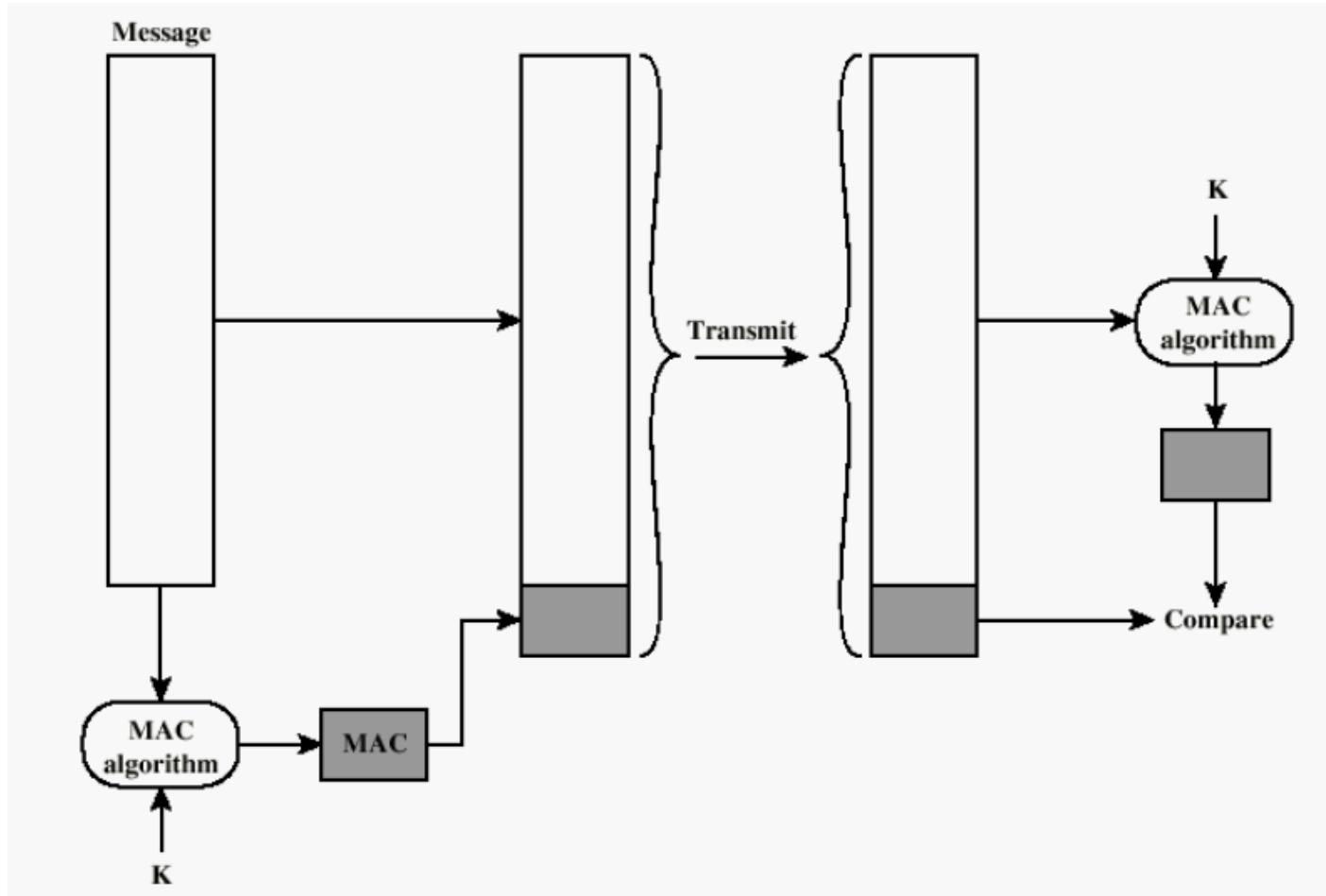
# Mezu autentifikazio kodeak

- Mezuen OSOTASUNA eta JATORRIZKO AUTENTIKOTASUNA babesten dute:

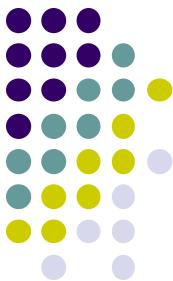




# Mezu autentifikazio kodeak



Jatorria: [http://ldc.usb.ve/~figueira/cursos/Seguridad/Material/criptografia\\_hash.pdf](http://ldc.usb.ve/~figueira/cursos/Seguridad/Material/criptografia_hash.pdf)



# Mezu autentifikazio kodeak

- Oinarritzko kontzeptuak:

- Sakabanatze funtziokoak (*hash*):

- $h$  deritzon hash funtzioko batek hautazko luzerako bit kateak  $n$  bitetako luzera finkoko kateak bihurtzen ditu (hatz-aztarna).
    - Adibidea: CRC kodeak
    - Datuak sinatzeko erabiltzen da

- MAC (Message Authentication Code):

- Gako simetrikodun teknika kriptografikoen bidez mezuen autentifikazioa ahalbidetzen duen kodea.
    - MAC algoritmoek bi parametro (mezu bat eta gako simetriko bat) hartzen dituzte sarrera bezala eta luzera finkoko irteera bat sortzen dute. Gakoa ezagutu barik irteera berbera sortzea konputazionalki bideraezina delaren ezaugarriarekin.
    - Zifratzeak, mezua ez irakurtzea ahalbidetzen du, honek, mezua ez dela aldatu.
    - Adibidea: CBC-MAC.



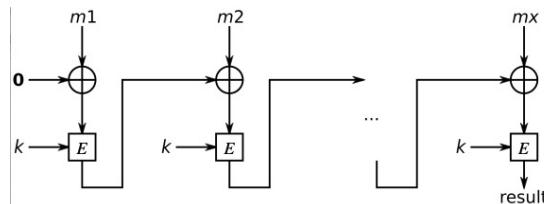
# Mezu autentifikazio kodeak

- Oinarrizko kontzeptuak:
  - Hash funtzioen ezaugarriak:
    - Konpresioa:
      - Hautazko lutzerako sarrera bat luzera finkoko irteera batera bihurtzen dute.
    - Kalkulu erraztasuna:
      - $h$  hash funtzi bat eta  $x$  sarrera bat emanda,  $h(x)$  irteera kalkulatzea konputazionalki erraza da.
    - Norabide bakarrekoa (itzulezina):
      - $y$  balio bat emanda,  $h(x')=y$  betetzen duen  $x'$  balio berri bat aurkitzea konputazionalki bideraezina da.
    - Talkarik gabekoa:
      - $h(x)=h(x')$  betetzen duten bi sarrera ezberdin  $x$ ,  $x'$  aurkitzea konputazionalki bideraezina da.



# Mezu autentifikazio kodeak

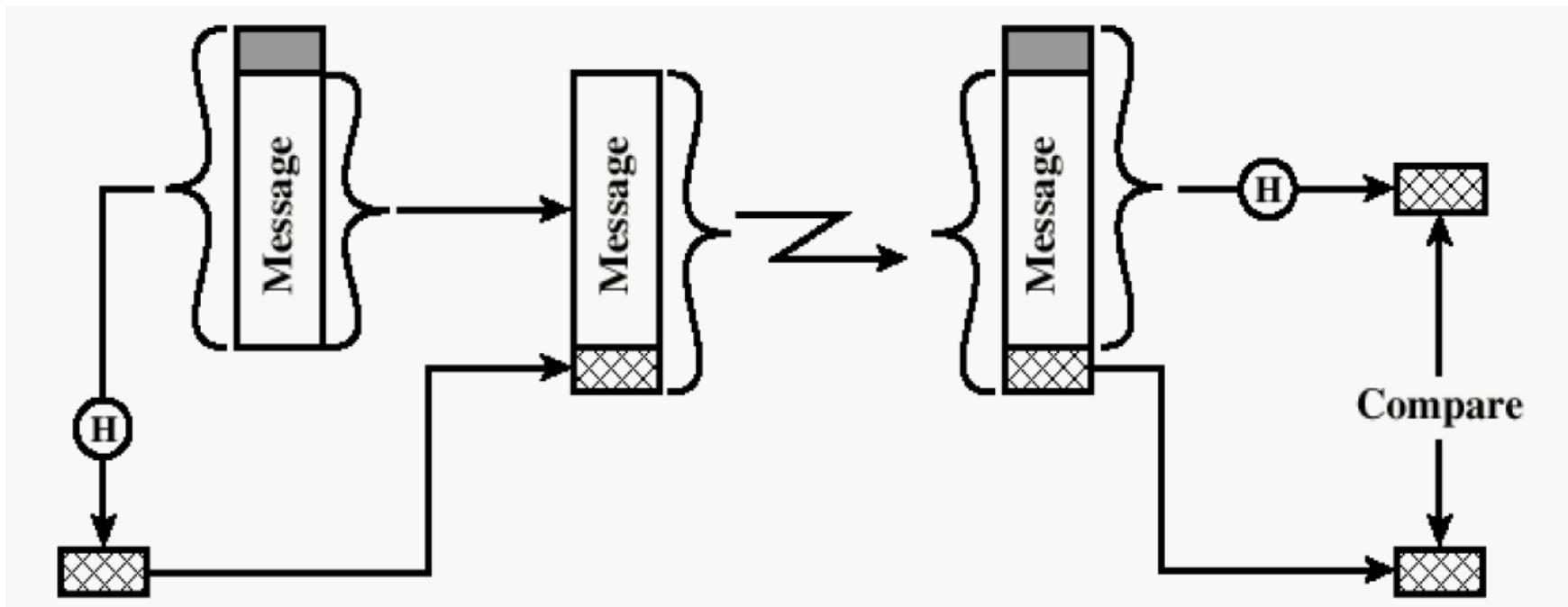
- MAC kodeen adibideak:
  - CBC-AES-MAC:
    - Zifratze algoritmo baten erabilpenean oinarrituta.
      - Lehenengo terminoak (CBC) zifratzea burutzeko erabilitako modua definitzen du eta bigarrenak (AES) erabilitako zifratze algoritmoa zehazten du.
      - CBC: Blokekako zifratzea berrelikadurarekin.
  - HMAC (Hash-based Message Authentication Code):
    - MAC kode mota espezifiko bat.
    - Hash funtzioen erabilpenean oinarrituta:
      - MAC kodea kalkulatzeko erabiltzen den algoritmoa hash funtzioen erabilpenean oinarrituta dago, beste mekanismo batzuetan, adibidez zifratze algoritmoetan, oinarrituta egon beharrean.
    - Adibideak: MD5, SHA-1, RIPEMD-160, etab.

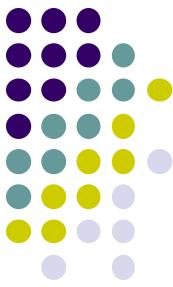




# Mezu autentifikazio kodeak

- HMAC kodeak kalkulatzeko mekanismoa:





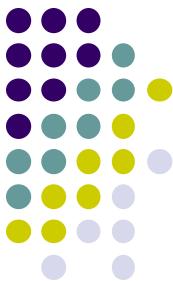
# Aurkibidea

- Sarrera
- Segurtasunaren oinarriak Informazio Sistemetan
- **Teknika kriptografikoak**
  - Kriptografiari buruzko oinarrizko kontzeptuak
  - Zifratzea
  - Mezu Autentifikazio Kodeak (MAC, Message Authentication Code)
  - **Sinadura Digitalak**
  - Mezuen freskotasuna
  - Gakoen banaketa
- Segurtasuna Informazio Sistemetan
- Segurtasunaren egungo egoera
- Segurtasunaren kudeaketa



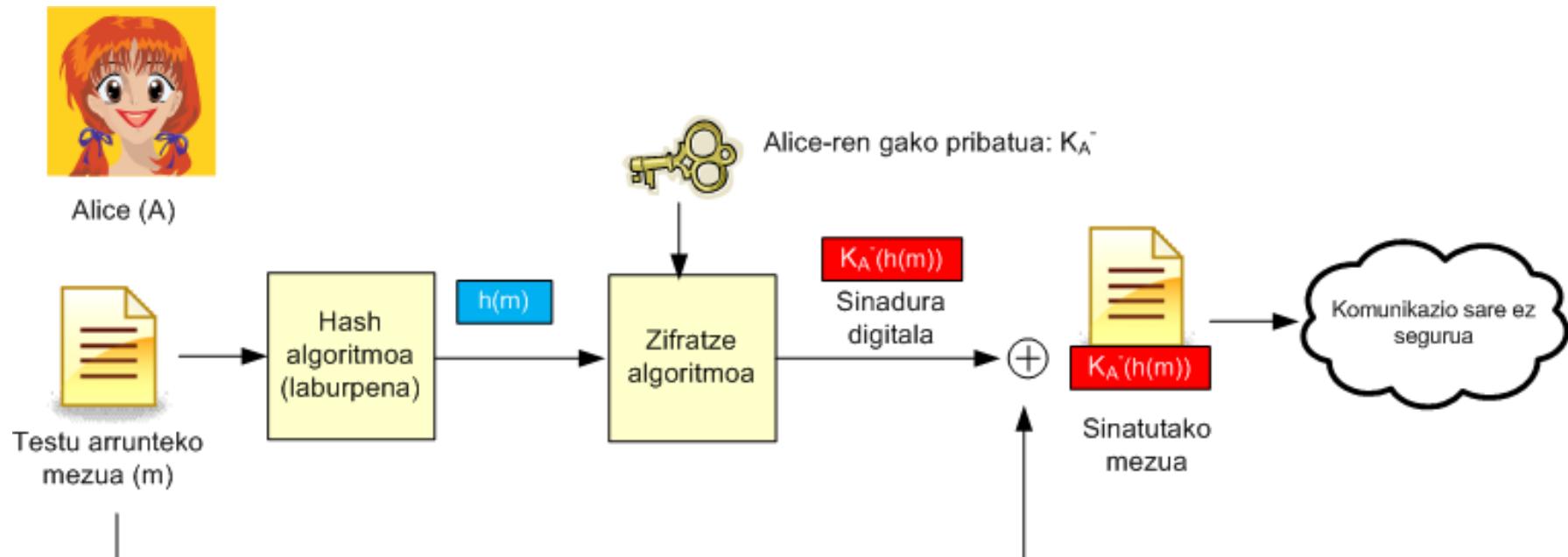
# Sinadura digitala

- Eskuz egindako sinaduren antzeko teknika kriptografikoa.
- Mezu baten osotasuna edo jatorrizko autentifikazioa bermatzen du.
- MAC-en baliokidea baina gako publiko bat erabiliz.
- Egiaztagarria, faltsutu ezina: helmugako entitateak (Bob) hirugarren parte bati frogatzea diezai oke Alice-ek, eta ez beste pertsona batek (Bob barne), dokumentua sinatu duela.
- Mezuaren laburpena (hash) zifratua.



# Sinadura digitala

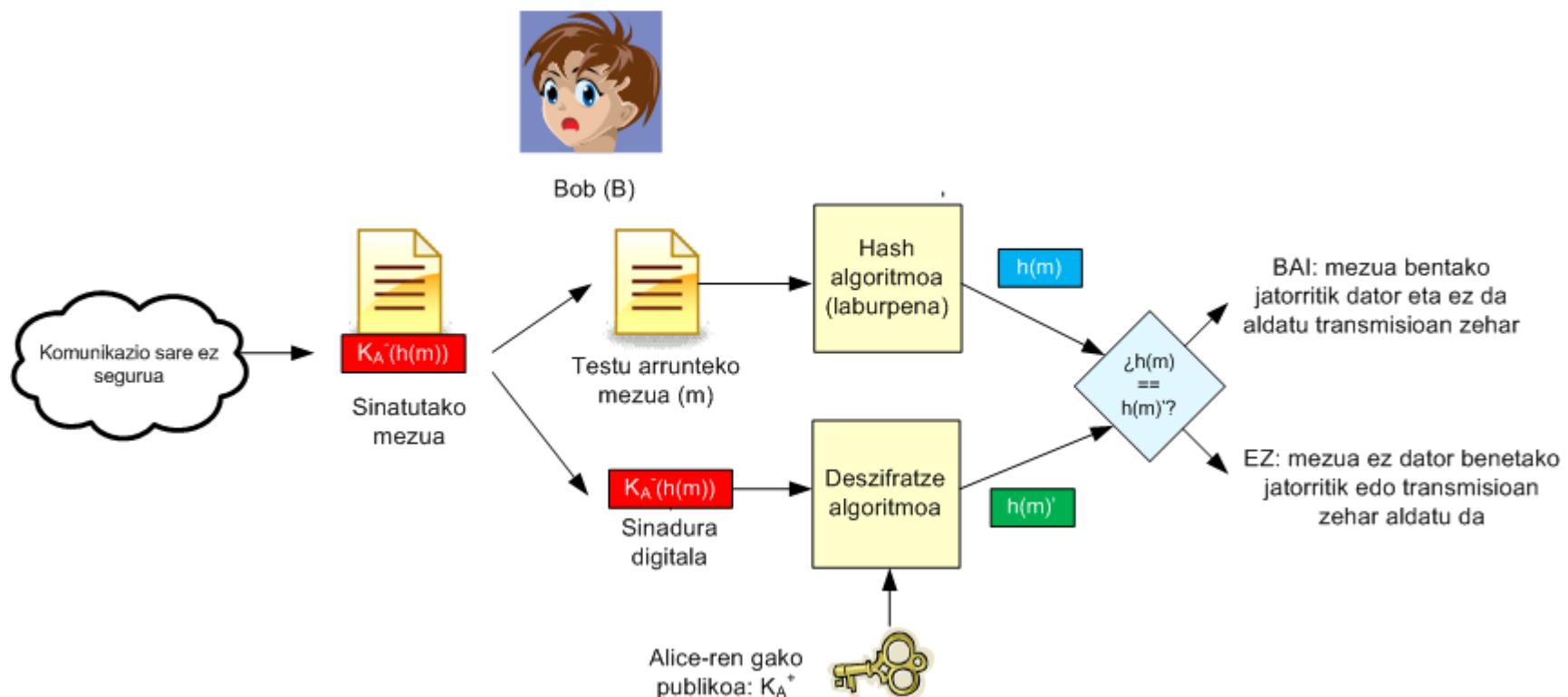
- Mezu baten sinadura sortzeko prozesua:





# Sinadura digitala

- Mezu baten sinadura egiaztatzeko prozesua:





# Sinadura digitala

- Hash, MAC eta sinadura digitalen arteko ezberdintasunak:

Cryptographic primitive Security Goal	Hash	MAC	Digital signature
Integrity	Yes	Yes	Yes
Authentication	No	Yes	Yes
Non-repudiation	No	No	Yes
Kind of keys	none	symmetric keys	asymmetric keys

<https://en.wikipedia.org/wiki/Non-repudiation>



# Aurkibidea

- Sarrera
- Segurtasunaren oinarriak Informazio Sistemetan
- **Teknika kriptografikoak**
  - Kriptografiari buruzko oinarrizko kontzeptuak
  - Zifratzea
  - Mezu Autentifikazio Kodeak (MAC, Message Authentication Code)
  - Sinadura Digitalak
  - **Mezuen freskotasuna**
  - Gakoen banaketa
- Segurtasuna Informazio Sistemetan
- Segurtasunaren egungo egoera
- Segurtasunaren kudeaketa



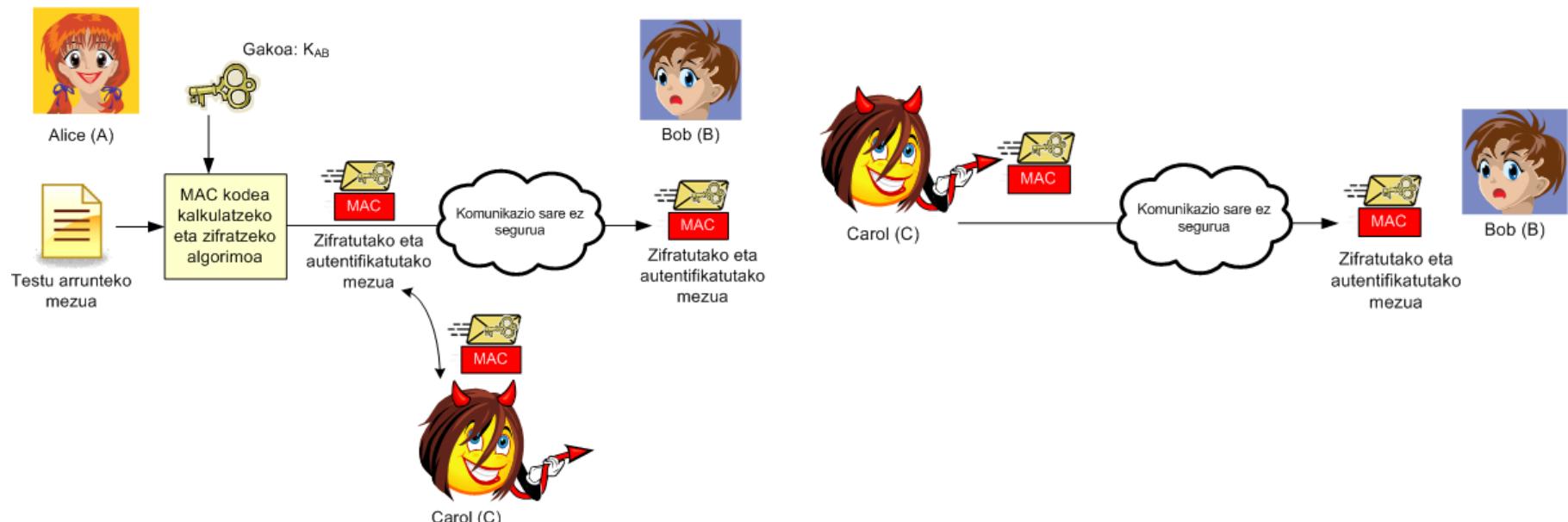
# Mezuen freskotasuna

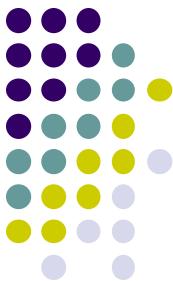
- Nahiz eta mezu bat zifratu eta autentifikatu (MAC kodearen edo sinadura digitalaren bidez) oraindik posiblea da erasotzaile batek mezu bat saretik kapturatzea eta geroago errepikatzea benetako jatorriaren lekua hartuz.
  - Birbidaltze erasoa (Replay attack)
- Mezuen freskotasuna (freshness) bermatu behar da.



# Mezuen freskotasuna

- Mezuen birbidaltze erasoa:
  - Bob-ek Alice-ek bidalitako mezu berri bat jaso duela uste du, baina benetan Carol-ek birbidalitako mezu zahar bat da.





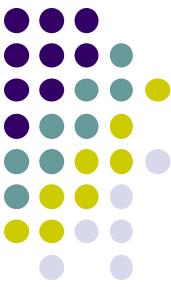
# Mezuen freskotasuna

- Freskotasun mekanismoak:
  - Data-zigiluak
    - Datuak sortu ziren “momentua” identifikatzen dituzten datuak.
    - Erlojuen erabilera edo data-zigilu logikoetan (sekuentzia zenbakiak) oinarritutik egon daitezke.
  - Nonce balioak
    - Erabilera bakarrerako sartzen den zenbakia da (one-time identification)
    - Normalean ausazko zenbaki bat da.
    - Freskotasuna emateko balio dute aldez aurretik erabili ez diren zenbakiak sortzen direla suposatuz.



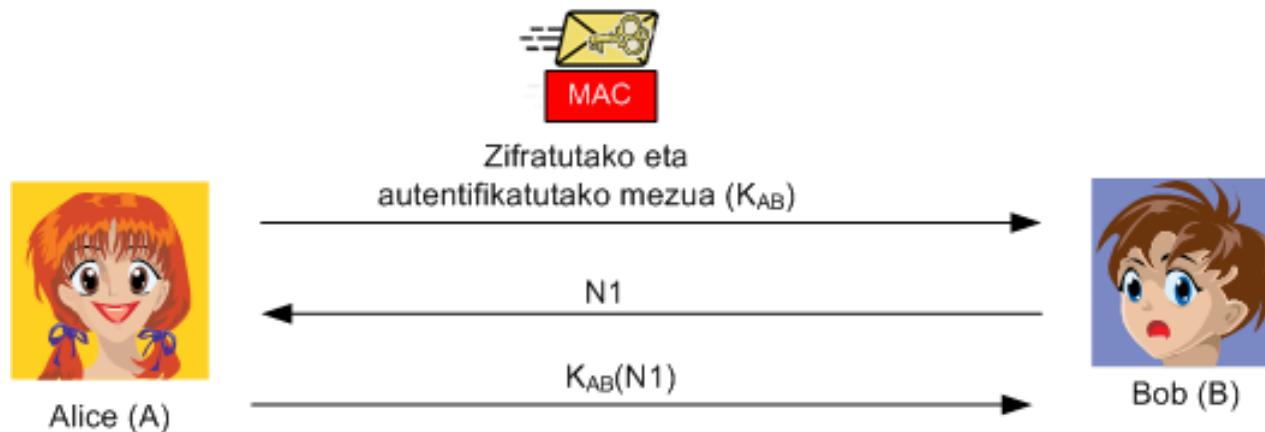
# Mezuen freskotasuna

- Data-zigilua (Timestamp):
  - Alice-ek mezuaaren sortze data/ordua (data-zigilua) sartu egiten du jatorrizko mezuan.
  - Bob-ek mezua jasotzen duenean, mezuan sartutako data-zigilua momentu horretako data/orduarekin alderatu egiten du.
  - Mezuaren latentzia komunikazio sarearen latentzia normala baino handiagoa izan bada, mezua baztertu egiten da:
    - Ez da mezu berri bat, errepikatutako mezu bat da.
  - Desabantaila: Alice eta Bob-en erlojuak sinkronizaturik egon behar dira beti.



# Mezuen freskotasuna

- nonce balioen erabilpena
  - Erabilera bakarreko bit kateak.
  - Balio bakarrak eta aurretik jakin ezinak.

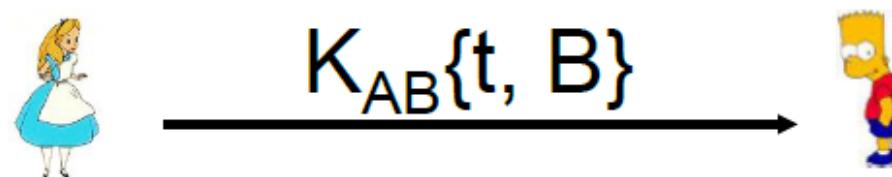


- $N1$ -eri desafio (challenge) deitzen zaio.

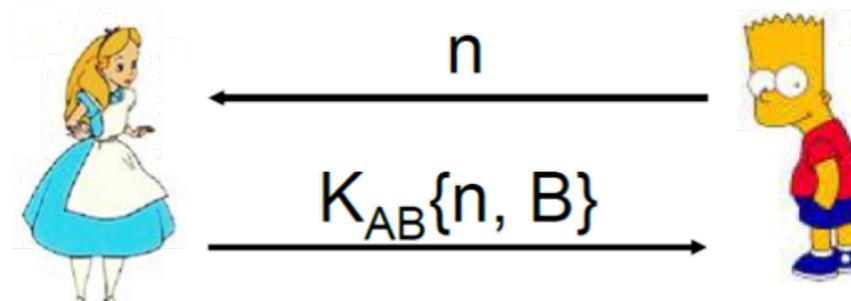


# Mezuen freskotasuna

- Freskotasun mekanismoak.
  - Aldebakarreko gako simetrikoa:
    - Autentifikazioa A-k sortutako data-zigiluarekin.
      - A eta B-ren erlojuak sinkronizaturik egon behar dira.
      - B-k mezua denbora tarte finko baten barnean heltzen bada hartzen du.



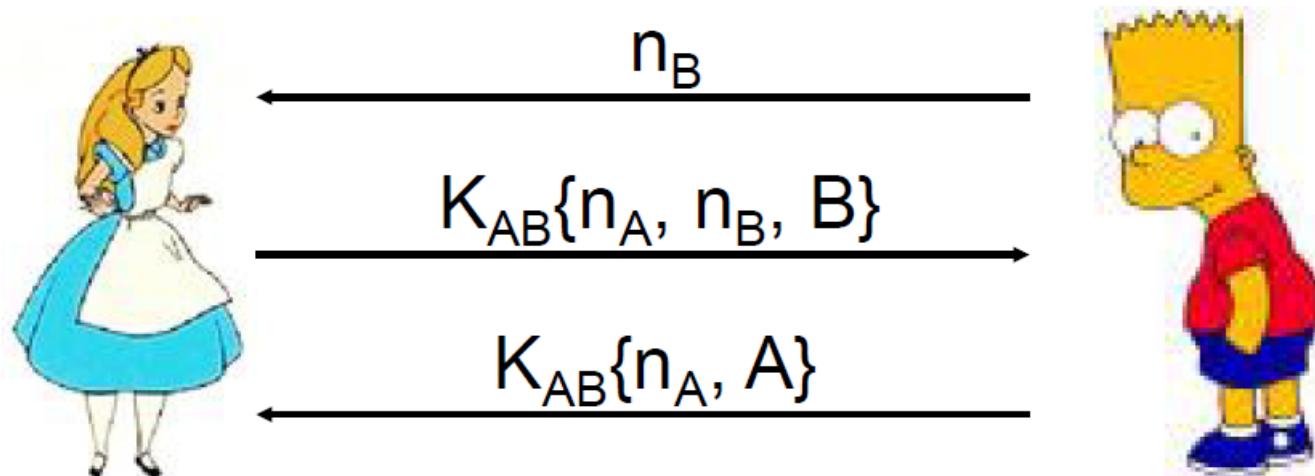
- Aldebakarreko autentifikazioa *nonce* balioekin.





# Mezuen freskotasuna

- Freskotasun mekanismoak.
  - Elkarrekiko gako simetrikoa.
    - Nonce balioak erabiliz.





# Aurkibidea

- Sarrera
- Segurtasunaren oinarriak Informazio Sistemetan
- **Teknika kriptografikoak**
  - Kriptografiari buruzko oinarrizko kontzeptuak
  - Zifratzea
  - Mezu Autentifikazio Kodeak (MAC, Message Authentication Code)
  - Sinadura Digitalak
  - Mezuen freskotasuna
  - Gakoen banaketa
- Segurtasuna Informazio Sistemetan
- Segurtasunaren egungo egoera
- Segurtasunaren kudeaketa



# Gakoen banaketa

- Derrigorrez autentifikazio prozesuari loturik:
  - Ez dauka zentzurik autentifikatu gabeko erabiltzaile batekin gako bat partekatzea:
    - Benetan hau da komunikatu nahi naizen erabiltzailea?
  - Ez dauka zentzurik erabiltzaile bat autentifikatzea eta gakorik ez banatzea:
    - Behin autentifikazio prozesua amaituta, nola jakin dezaket komunikazioaren beste aldea lehen autentifikatutako erabiltzaile bera dela?



# Gakoen banaketa

- Gako simetrikodun kriptografia:
  - Arazoak:
    - Nola komunika dezakete bi entitateek partekaturiko gako sekretu bat komunikazio sare ez seguru baten bidez?
    - Gako bat behar da erabiltzaile pare bakoitzeko:
      - n partaideentzat behar den gako kopurua:
$$n * (n-1) / 2$$



# Gakoen banaketa

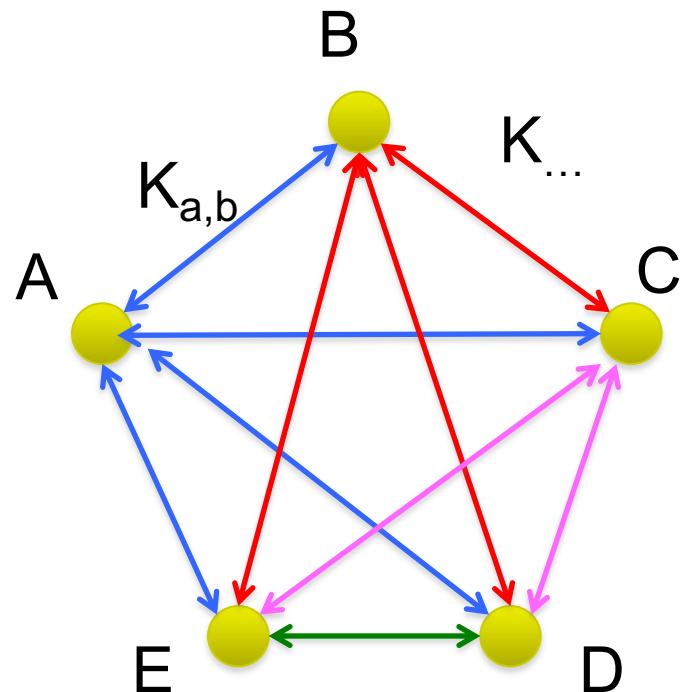
- Gako simetrikodun kriptografia:
  - Arazoak:
    - Nola komunika dezakete bi entitateek partekatutako gako sekretu bat komunikazio sare ez seguru baten bidez?
    - Gako bat behar da erabiltzaile pare bakoitzeko:
      - n partaideentzat behar den gako kopurua:
$$n * (n-1) / 2$$
  - Erantzuna:
    - Gako banaketa gunea (KDC, Key Distribution Centre)
      - Gako bat partekatu nahi duten bi entitateek fidagarritzat hartzen duten bitarteko bezala jokatzen du.



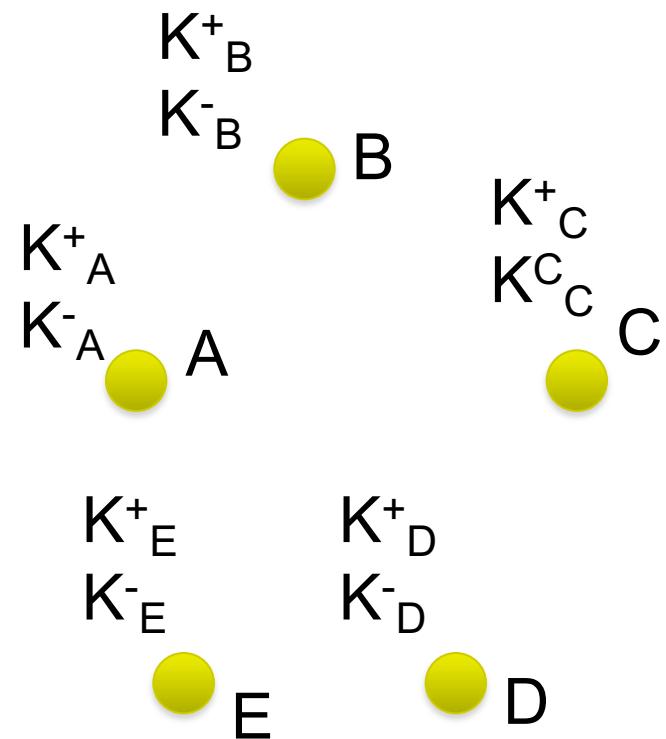
# Gakoen banaketa

- Gako kopuruaren konparaketa:

N=5



$$4+3+2+1 = (5 * (5-1) / 2) = 10$$

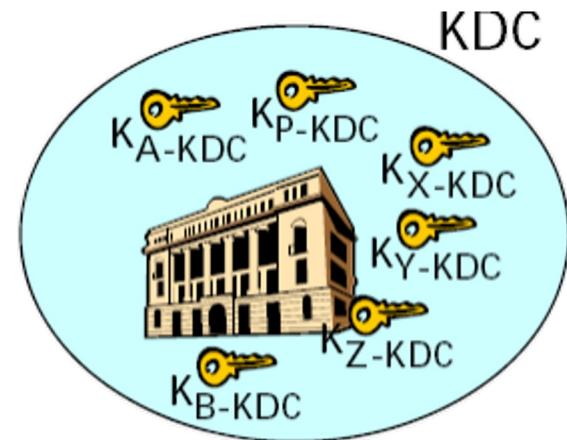
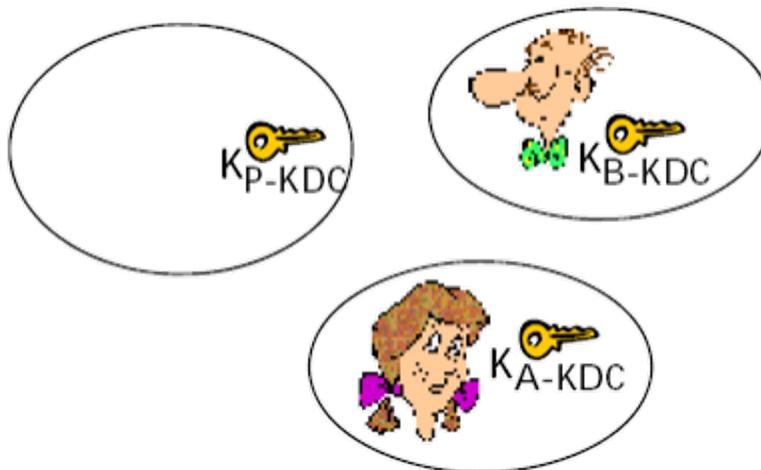


5 gako bikote:  $2 \times 5 = 10$  gako?



# Gakoen banaketa

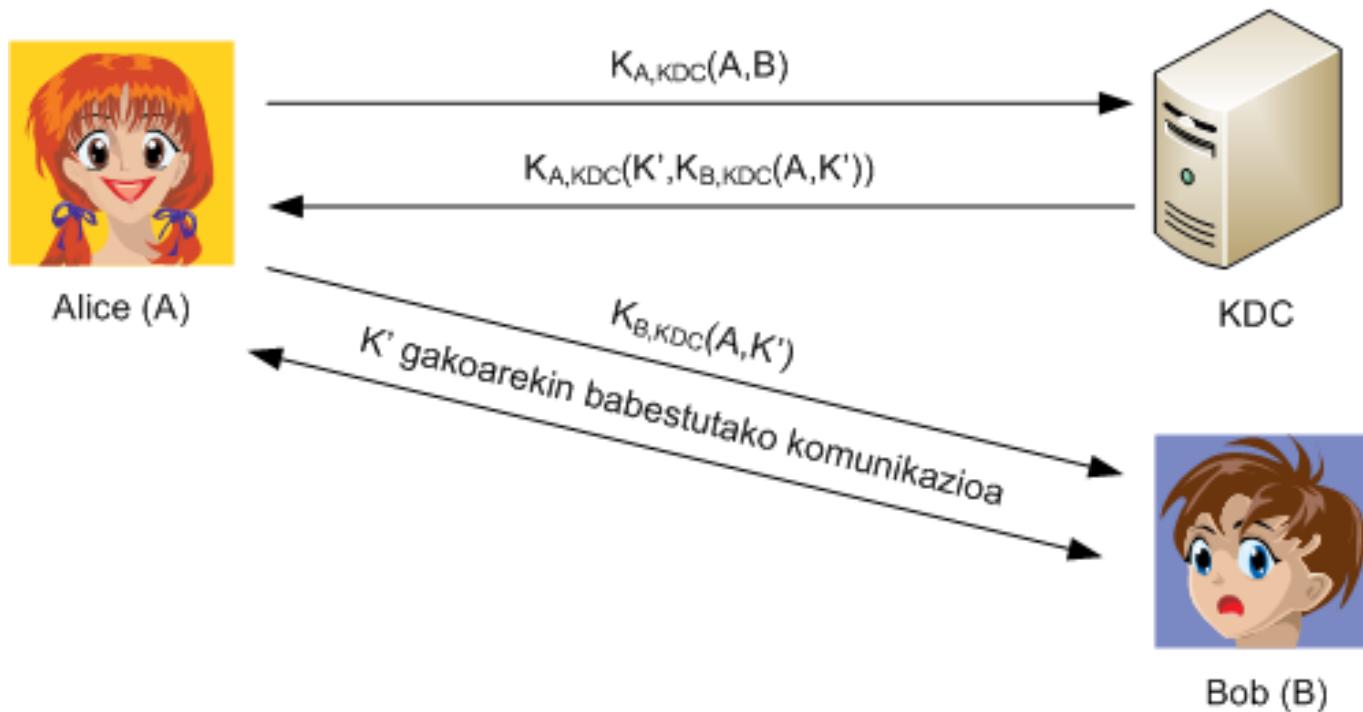
- Gako banaketa gunea (KDC)
  - Sisteman erregistratutako erabiltzaile bakoitzak gako sekretu bat partekatzen du KDC-arekin:
    - $K_{A,KDC}$ : Alice eta KDC-aren artean partekaturiko gakoa,
    - $K_{B,KDC}$ : Bob eta KDC-aren artean partekaturiko gakoa,
    - Etab.





# Gakoen banaketa

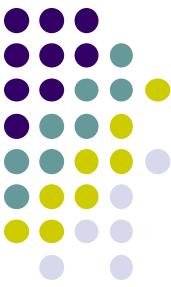
- Gako banaketa gunea (KDC):
  - K' gakoaren banaketa saio gako bezala Alice eta Bob-ren arteko komunikazio seguruak ahalbidetzeko.





# Gakoen banaketa

- Kerberos: sistema ezagunetariko bat
  - MIT-en garatua Athena proiektuaren barnean.
    - Azkeneko bertsioa: 5 (RFC 4120, 2005).
  - Gako simetrikodun kriptografian oinarritua
    - Luzapenak: Gako asimetrikodun kriptografiarentzat.
  - TTP bat, KDC bat, behar du.
  - TCP eta UDP erabiltzen ditu garraio mailako protokolo bezala, beraz, berak eman behar du zifratze geruza.
  - Zerbitzarien esku gelditzen da, erabiltzaileek dituzten pribilegioak, nahiko diren beraien zerbitzuak erabiltzeko.



# Gakoen banaketa

- Kerberos: sistema ezagunetariko bat
  - KDC-a bi zerbitzariek osatzen dute:
    - Autentifikazio Zerbitzaria (AS, Authentication Server).
    - Ticket Emate Zerbitzaria (TGS, Ticket Granting Server).
  - Eskalagarritasuna:
    - Erreinu (realm) ezberdinen existentzia ahalbidetzen du.
    - Erreinu bakoitzak bere KDC-a dauka eta erreinu ezberdinako KDC-ek segurtasun elkartekatik ezartzen dituzte beraien artean.
  - Single-Sign On mekanismoak implementatzea ahalbidetzen du:
    - TGT-ari esker, erabiltzaileak nahi bezain beste Zerbitzu Ticket lor ditzake berriro AS-aren aurka autentifikatu behar gabe.



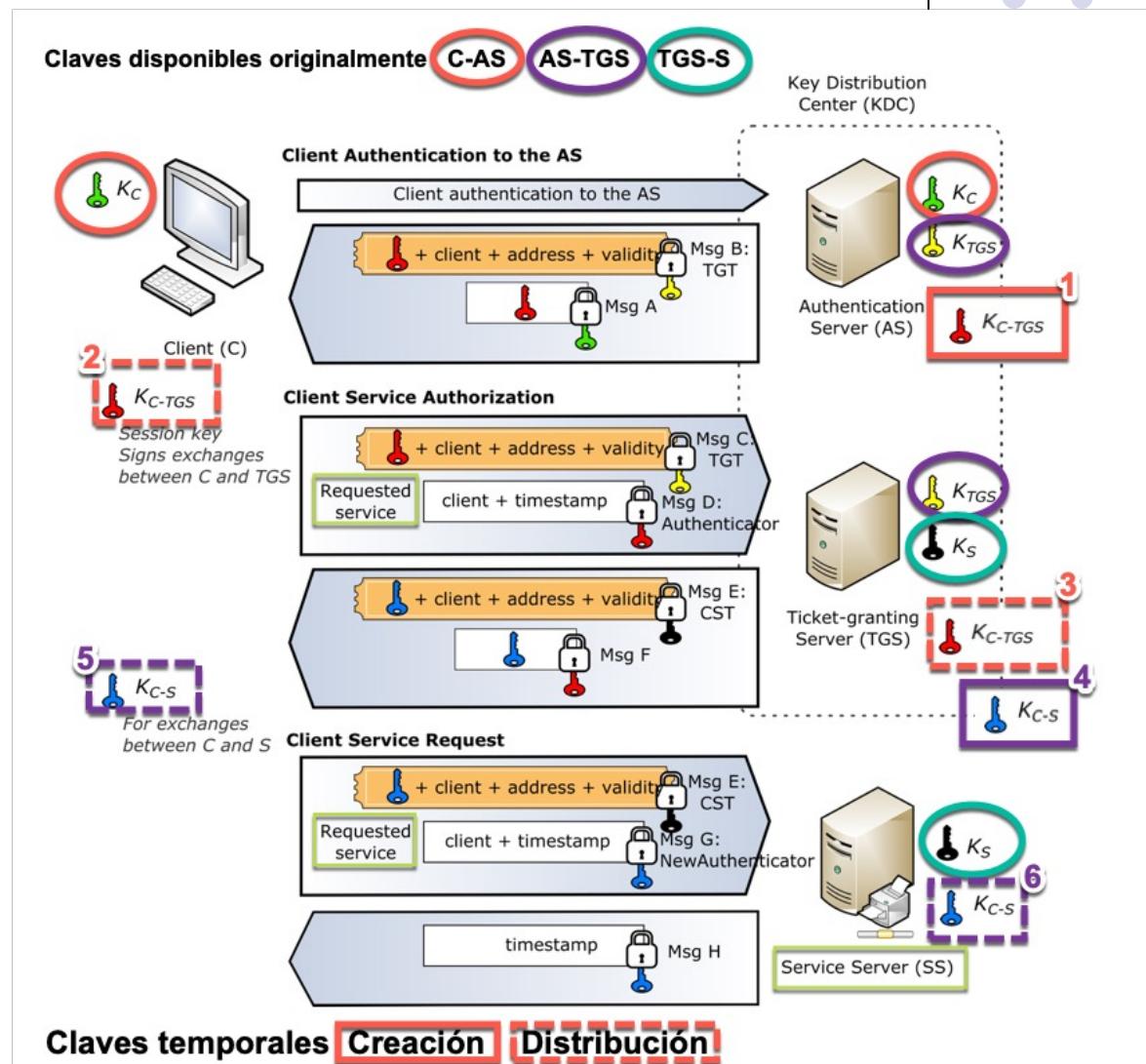
# Gakoen banaketa

- Kerberos: sistema ezagunetariko bat
  - Erabiltzailearen autentifikazioa 2 fasetan gertatzen da:
    - Autentifikazio fasea:
      - Erabiltzailea Kerberos-eko AS-aren aurka autentifikatu egiten da.
      - Erabiltzaileak TGT (Ticket Granting Ticket) bat lortzen du:
        - TGT: erabiltzailea dagoeneko autentifikatu egin dela bermatzen duen ticket orokor baten modukoa da.
    - Ticket-en kontzesio fasea:
      - Erabiltzaileak Kerberos-eko TGS-tik Zerbitzuko Ticket bat lortzen du:
        - Zerbitzuko Ticket-a: erabiltzaileak urruneko entitateari aurkeztu behar dion egiaztagiria bere identitatearen froga gisa.
  - Ticket-en bizitza erabilgarria mugatua dago: Ticket bakoitzak autentifikazio balio guztiak gordeko dituen denbora marka bat du.

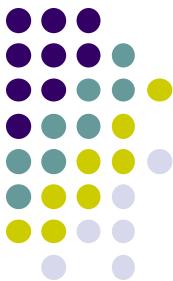
# Gakoen banaketa



- Kerberos. Funtzionamendua.



Iturria: By Jeran Renz - Own work, CC BY-SA 4.0,  
<https://commons.wikimedia.org/w/index.php?curid=98722081>



# Gakoen banaketa

- Kerberos:
  - Microsoft-ek erabiltzen du sareetan autentifikatzeko mekanismo estandar bezala.
  - Sistema eragile askotan eskuragarri.
  - Ekipo guztien arteko sinkronizazioa behar du.
  - Lotutako estandarra: "The Kerberos Network Authentication Service (V5)" (RFC 4120).



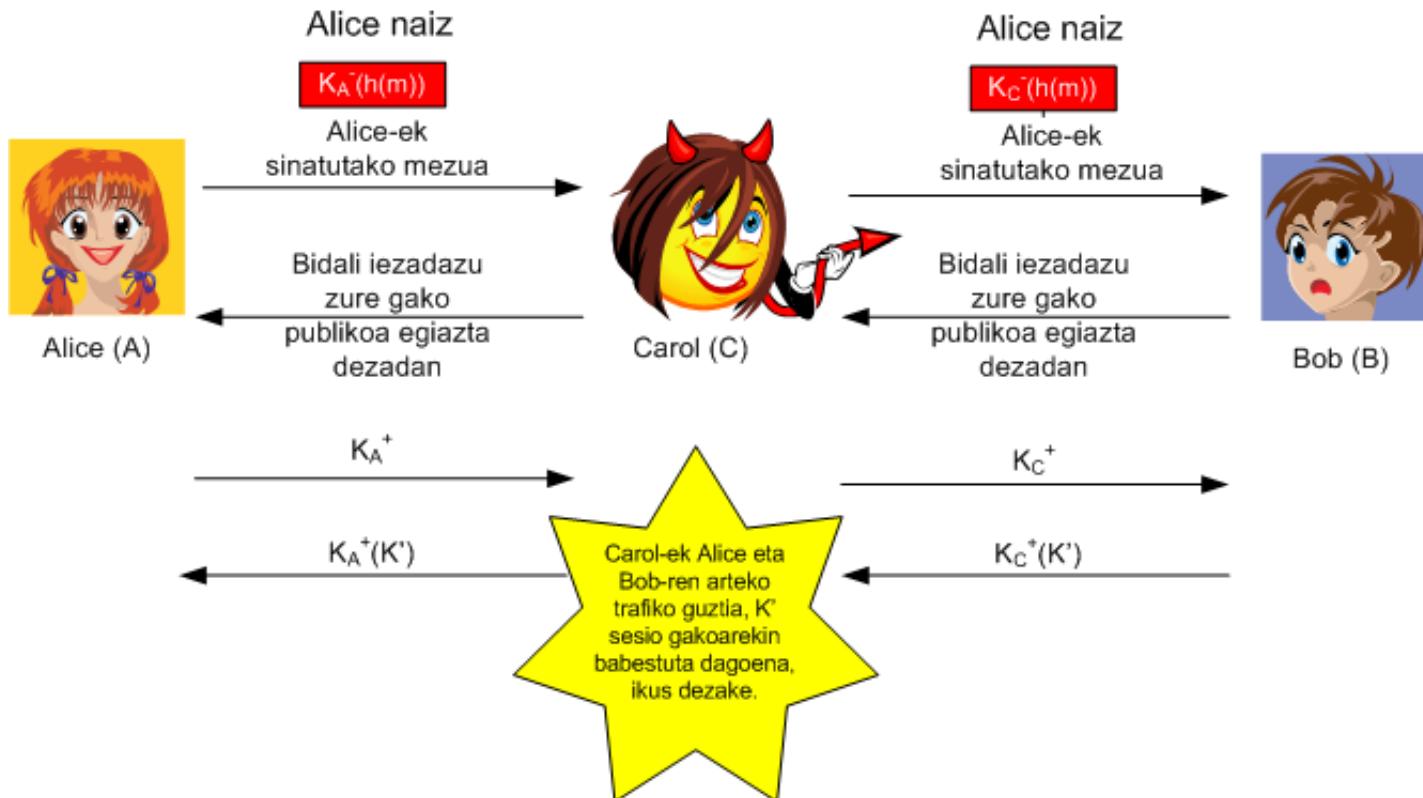
# Gakoen banaketa

- Gako publikodun kriptografia:
  - Arazoa:
    - Bob-ek Alice-ren gako publikoa lortzen duenean (web orrialde batetik, posta elektronikoaren bidez, etab.), nola egon daiteke ziur benetan Alice-ren gako publikoa dela eta ez Alice-ren lekua hartu nahi duen beste erabiltzaile batena?
    - Erdiko gizonaren erasoa (Man in the Middle Attack).



# Gakoen banaketa

- Man In The Middle Attack (MITM):





# Gakoen banaketa

- Gako publikodun kriptografia:
  - Arazoa:
    - Bob-ek Alice-ren gako publikoa lortzen duenean (web orrialde batetik, posta elektronikoaren bidez, eta.), nola egon daiteke ziur benetan Alice-ren gako publikoa dela eta ez Alice-ren lekua hartu nahi duen beste erabiltzaile batena?
    - Erdiko gizonaren erasoa (Man in the Middle Attack).
  - Erantzuna:
    - Ziurtagiri-Autoritate fidagarria (CA, Certification Authority)



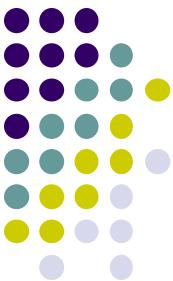
# Gakoen banaketa

- Gako publikodun kriptografia:
  - Ziurtagiri-Autoritateen, X.509 ziurtagirien eta direktorio zerbitzuen erabilpenean oinarrituta.
  - Ziurtagiri digitala:
    - Ziurtagiri-Autoritate fidagarri batek sinatutako dokumentu digitala, gako publiko bat identitate bateri lotzen duena.
  - Bi erabiltzaile CA ezberdinek sinatutako ziurtagiriak baldin baditzte, bi CA hauen arteko ziurtagiri bide bat egin behar da.
  - CA askoren gako publikoak nabigatzaleen barnean daude.



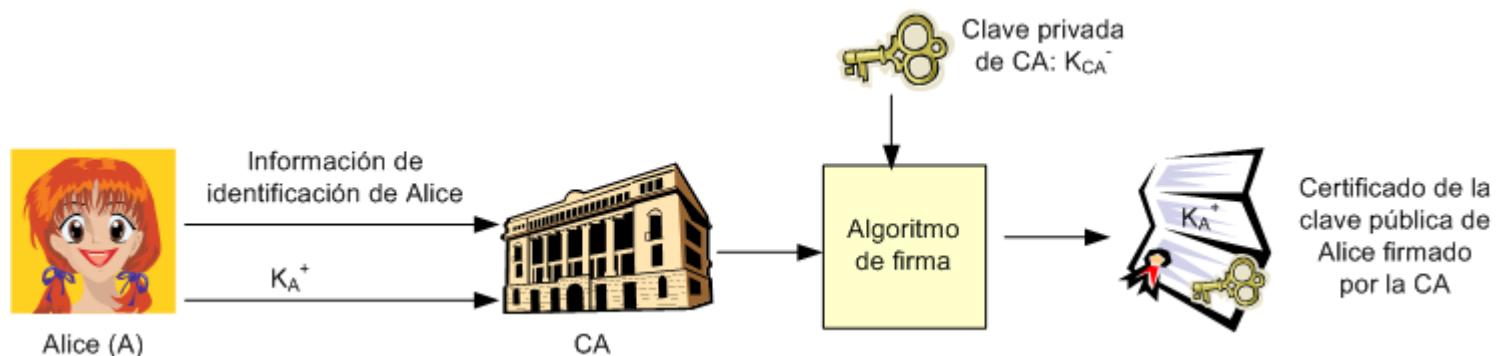
# Gakoen banaketa

- CA-k ziurtagiriak sortzeko prozesua:
  - E (pertsona edo makina) bere gako publikoa erregistratzen du CA-rekin:
    - E benetan berak esaten duena dela egiaztatzeko mekanismoak eskaini behar dira.
  - E-k bere gako publikoa ( $K_E^+$ ) eta dagokion gako pribatuaren ( $K_E^-$ ) “jabetza frogua” bat eman behar dio CA-ri:
    - $\{K_E^+\}$  eta  $K_E^-\{K_E^+\}$
  - CA-k E bere gako publikoarekin lotzen duen ziurtagiria sortzen du:
    - Ziurtagiriak E-ren gako publikoa dauka, CA-k sinatuta:  $K_{CA}^-\{E, K_E^+\}$
    - Edonork egiazta dezake E-ren ziurtagiria CA-ren gako publikoa erabiliz:  $K_{CA}^+\{K_{CA}^-\{E, K_E^+\}\}$
    - CA-en gako publikoa CA-en ziurtagirietatik lortzen da eta CA-en ziurtagiriak arakatzaileetan instalatuta egon ohi dira



# Gakoen banaketa

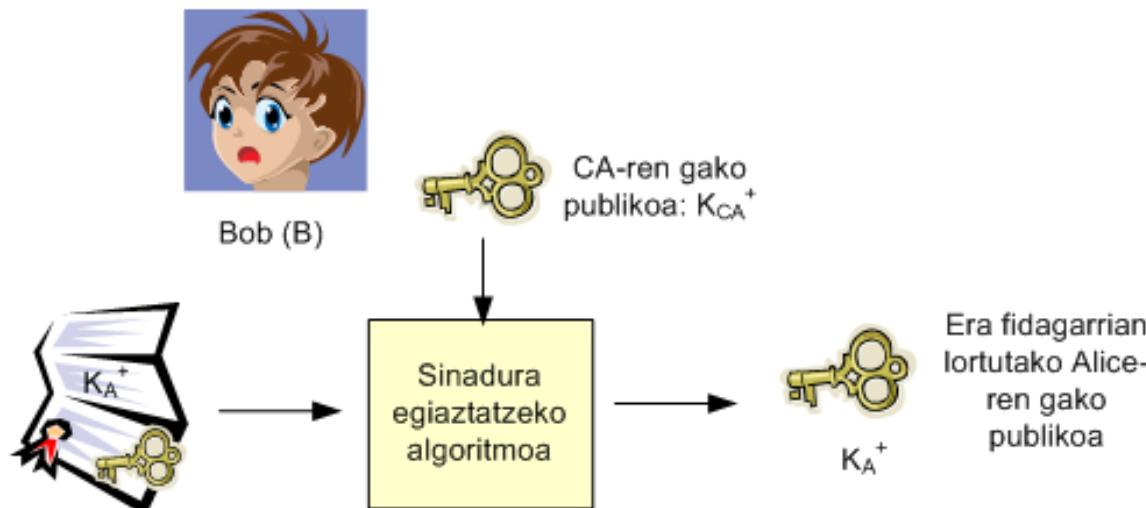
- CA-k ziurtagiriak sortzeko prozesua grafikoki:





# Gakoen banaketa

- Bob-ek Alice-ren gako publikoa nahi duenean:
  - Alice-ren ziurtagiria lortzen du (Alice-reна edo edonorena).
  - CA-ren gako publikoa erabiltzen du Alice-ren ziurtagiria egiazatzeko:
    - Alice-ren gako publikoa lortzen du.

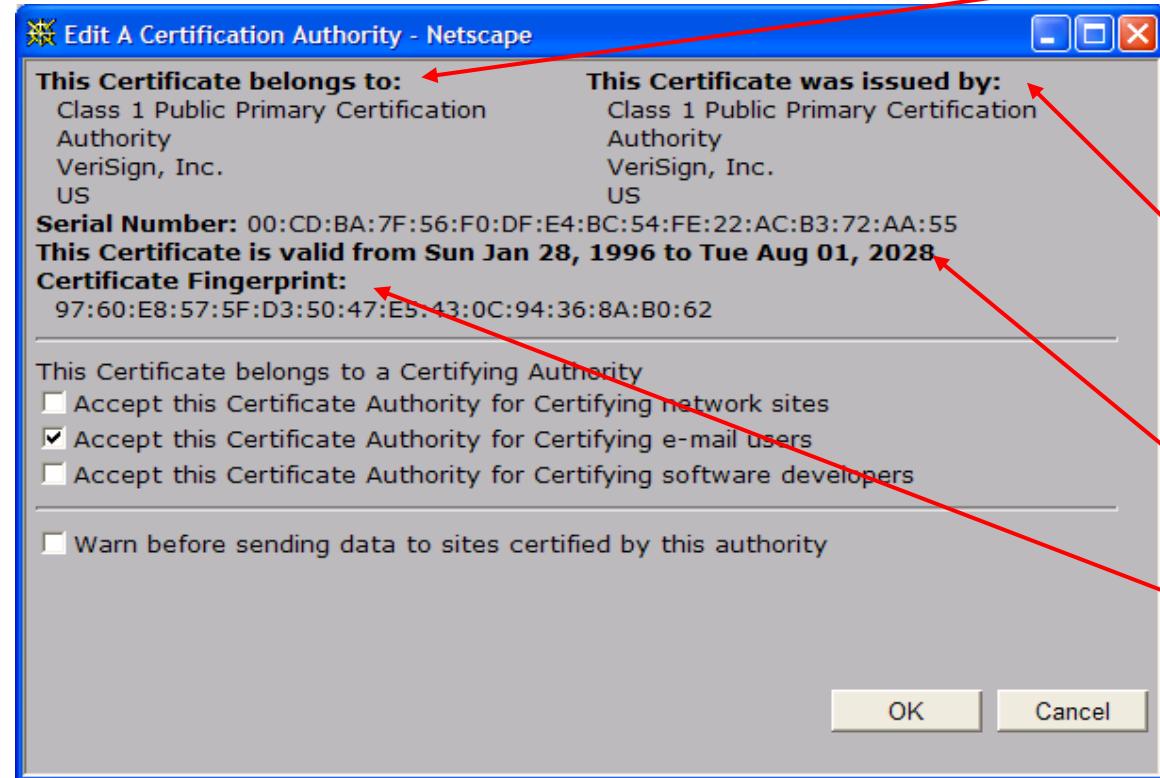




# Gakoen banaketa

- X. 509 ziurtagiri digital baten formatoa:
  - CA batek bere buruarentzat sinatutako ziurtagiri baten kasua

Serie zenbakia (CA bakoitzarentzat bakarra).

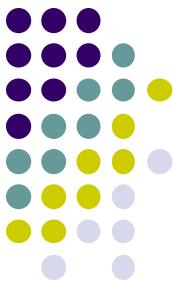


Ziurtagiriaren jabeari buruzko informazioa, erabilitako algoritmoa eta gakoaren balioa barne (irudian ez da ikusten).

Ziurtagiria igorri duen CA-ri buruzko informazioa.

Balio denbora.

Ziurtagiria igorri duen CA-ren sinadura digitala.



# Gakoen banaketa

- Ziurtagiri gurutzatuak:
  - 2 erabiltzaile (A eta B) 2 CA ezberdinek (CA1 eta CA2) sortutako ziurtagiriak dituztelarik
  - A-k zera dauka:
    - CA1-en ziurtagiria:  $K_{CA1^-}\{CA1, K_{CA1^+}\}$
    - CA2-k sortutako B-ren ziurtagiria:  $K_{CA2^-}\{B, K_B^+\}$
  - B-k zera dauka:
    - CA2-ren ziurtagiria:  $K_{CA2^-}\{CA2, K_{CA2^+}\}$
    - CA1-ek sorutako A-ren ziurtagiria:  $K_{CA1^-}\{A, K_A^+\}$
  - Erabiltzaile bakoitzak ezin du beste erabiltzailearen ziurtagiria modu seguru batean egiaztatu, ez daukalako dagokion CA-ren (beste CA-ren) ziurtagiria.



# Gakoen banaketa

- Ziurtagiri gurutzatuak behar ditugu:
  - CA1-ek sortutako CA2-ren ziurtagiria (A-k egiaztatu dezakeena):
    - $K_{CA1}^{-}\{CA2, K_{CA2}^{+}\}$
  - CA2-k sortutako CA1-en ziurtagiria (B-k egiaztatu dezakeena):
    - $K_{CA2}^{-}\{CA1, K_{CA1}^{+}\}$
- Orain:
  - A-k zera dauka:
    - CA1-en ziurtagiria:  $K_{CA1}^{-}\{CA1, K_{CA1}^{+}\}$
    - CA1-ek sortutako CA2-ren ziurtagiria:  $K_{CA1}^{-}\{CA2, K_{CA2}^{+}\}$ 
      - $K_{CA1}^{+}$  erabiliz CA2-ren ziurtagiri hau egiaztatu eta  $K_{CA2}^{+}$  modu seguru batean lortu dezake:  $K_{CA1}^{+}\{K_{CA1}^{-}\{CA2, K_{CA2}^{+}\}\} \rightarrow K_{CA2}^{+}$
    - CA2-k sortutako B-ren ziurtagiria:  $K_{CA2}^{-}\{B, K_B^{+}\}$ 
      - $K_{CA2}^{+}$  erabiliz B-ren ziurtagiria egiaztatu eta  $K_B^{+}$  modu seguru batean lortu dezake:  $K_{CA2}^{+}\{K_{CA2}^{-}\{B, K_B^{+}\}\} \rightarrow K_B^{+}$



# Gakoen banaketa

- Orain:
  - B-k zera dauka:
    - CA2-ren ziurtagiria:  $K_{CA2}^{-}\{CA2, K_{CA2}^{+}\}$
    - CA2-k sortutako CA1-en ziurtagiria:  $K_{CA2}^{-}\{CA1, K_{CA1}^{+}\}$ 
      - $K_{CA2}^{+}$  erabiliz CA1-en ziurtagiri hau egiazta eta  $K_{CA1}^{+}$  modu seguru batean lortu dezake:  $K_{CA2}^{+}\{K_{CA2}^{-}\{CA1, K_{CA1}^{+}\}\} \rightarrow K_{CA1}^{+}$
    - CA1-ek sorutako A-ren ziurtagiria:  $K_{CA1}^{-}\{A, K_A^{+}\}$ 
      - $K_{CA1}^{+}$  erabiliz A-ren ziurtagiria egiazta eta  $K_A^{+}$  modu seguru batean lortu dezake:  $K_{CA1}^{+}\{K_{CA1}^{-}\{A, K_A^{+}\}\} \rightarrow K_A^{+}$



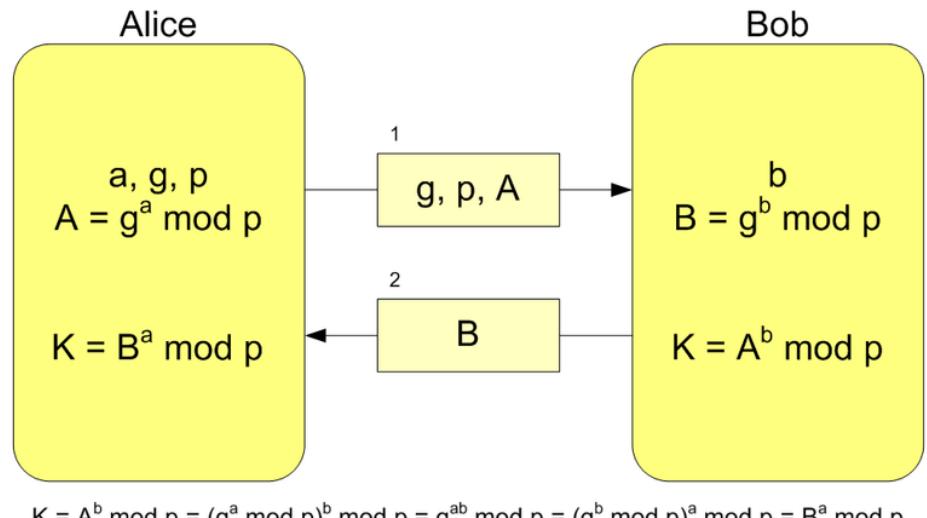
# Gakoen banaketa

- Diffie-Hellman protokolo kriptografikoa:
  - Gakoen banaketarako protokoloa da.
    - Aldez aurretik kontakturik izan ez duten entitateen artean.
    - Kanal ez seguru bat erabiliz.
    - Era anonimoan (aldez aurretik autentifikatu gabe).
  - Sesio bati dagokion informazioa zifratzeko erabiliko diren gako simetrikoetan ados jartzeko erabiltzen da (sesio gakoa ezartzeko).
    - Hala ere, autentifikatu gabeko protokoloa izanik, zenbait autentifikatutako protokoloen oinarriak ezartzen ditu.
  - Man In The Middle erasoen xedea izan daiteke:
    - Gainetik autentifikazioren bat erabili behar da.

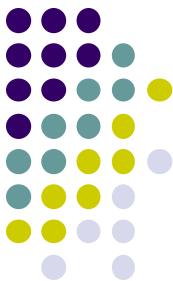


# Gakoen banaketa

- Diffie-Hellman protokoa:
  - Deskribapena



- Zenbaki lehen bat ( $p$ ) eta sortzaile bat ( $g \in Z_p^*$ ). Hauek publikoak dira, beraz edonork ezagu ditzake.
- Alice-ek ausazko  $a \in Z_{p-1}$  aukeratzen du,  $A=g^a \text{ mod } p$  kalkulatzen du eta  $A$  bidaltzen dio Bob-eri.
- Bob-ek ausazko  $b \in Z_{p-1}$  aukeratzen du,  $B=g^b \text{ mod } p$  kalkulatzen du eta  $B$  bidaltzen dio Alice-eri.
- Informazio honekin Alice eta Bob-ek  $K=g^{ab} \text{ mod } p$  kalkula dezakete bakoitzak bere aldetik:
  - Alice-ek:  $B^a \text{ mod } p = (g^b \text{ mod } p)^a \text{ mod } p = g^{ab} \text{ mod } p = K$
  - Bob-ek :  $A^b \text{ mod } p = (g^a \text{ mod } p)^b \text{ mod } p = g^{ab} \text{ mod } p = K$

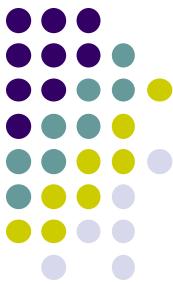


# Gakoen banaketa

- Diffie-Hellman. Adibidea:
  - Zenbaki baxuekin (benetako egoeretan zenbaki askoz altuagoak erabiltzen dira):
  - Aukeratzen dugu:  $g=7$  eta  $p=23$ 
    - 1. Alice-ek  $x = 3$  aukeratzen du eta  $R_1 = 7^3 \text{ mod } 23 = 21$  kalkulatzen du.
    - 2. Bob-ek  $y = 6$  aukeratzen du eta  $R_2 = 7^6 \text{ mod } 23 = 4$  kalkulatzen du.
    - 3. Alice-ek 21 zenbakia bidaltzen dio Bob-eri.
    - 4. Bob-ek 4 zenbakia bidaltzen dio Alice-eri.
    - 5. Alice-ek gako simetrikoa kalkulatzen du:  $K = 4^3 \text{ mod } 23 = 18$ .
    - 6. Bob-ek gako simetrikoa kalkulatzen du:  $K = 21^6 \text{ mod } 23 = 18$ .
  - K balioa bera da Alice eta Bob-rentzat.

$$g^{xy} \text{ mod } p = 7^{18} \text{ mod } 23 = 18$$

# Gako simetrikodun eta asimetrikodun kriptografia



- Gakoen kudeaketarako konparazioa:

## Zifratze simetrikoa

n partaideentzat erabili  
behar diren gako  
kopurua:

$$n * (n-1) / 2$$

## Zifratze asimetrikoa

n partaideentzat erabili  
behar diren gako  
kopurua:

$$2 * n$$

### Adibidea

$n=100$  partaideentzat

- Simetrikoa:  $100*99/2=4950$  gako
- Asimetrikoa:  $2*100= 200$  gako

# Gako simetrikodun eta asimetrikodun kriptografia



- Beste alderdien konparazioa:

## Kriptografia simetrikoak

Gakoaren luzera  
 $\geq 128$  bit

Gakoen bizitza denbora  
- normalean sesio gako bezala:  
- oso laburra (seg. edo min.)

## Kriptografia asimetrikoak

Gakoaren luzera  
 $\geq 1024$  bit

Gakoen bizitza denbora:  
- Luzea (hilabeteak edo urteak)

# Gako simetrikodun eta asimetrikodun kriptografia



- Beste alderdien konparazioa:

## Kriptografia simetrikoak

Sinadura abiadura

- Oso altua
- 100 edo 1000 aldiz azkarragoak

Segurtasuna:

- Gakoaren segurtasunean datza

Mezuaren tamaina:

- Edozein

## Kriptografia asimetrikoak

Sinadura abiadura

- Oso baxua
- Erabilerak:

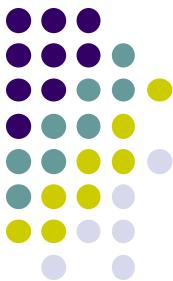
- sesio gakoak
- sinadura digitala (f. hash)

Segurtasuna:

- Gako publikoa ezagututa, gako pribatua lortzeko zaitasunean datza

Mezuaren tamaina:

- Gakoaren luzera baino gutxiago



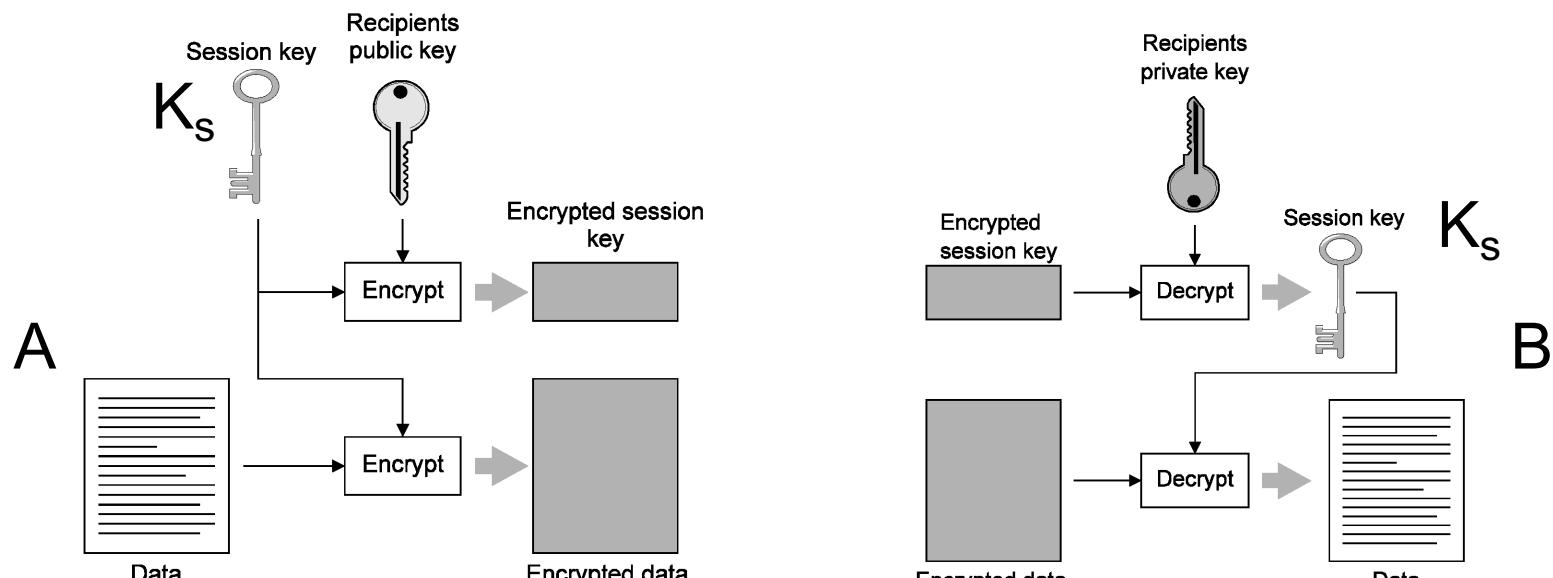
# Errealitatean...

- Kriptografia hibridoa:
  - Bi algoritmo erabiltzen ditu
    - Gako publikodun algoritmoa:
      - Gako simetrikoa bidaltzean zifratzeko (informazio kopuru txikia)
      - Seguruagoa.
    - Gako simetrikkodun algoritmoa:
      - Datu mezuak zifratzeko.
      - Kostu konputazionala txikiagotu egiten da.

# Errealitatean...



- Kriptografia hibridoa. Adibidea (II):



$K_s\{M\} \parallel K^+_B\{K_s\}$  (M-ren konfidentzialitasuna)

A → B

$K_s\{M\} \parallel K^+_B\{K_s\} \parallel K^-_A\{H(M)\}$

(M-ren konfidentzialitasuna, jatorriko autentikotasuna eta ez ukatzea)