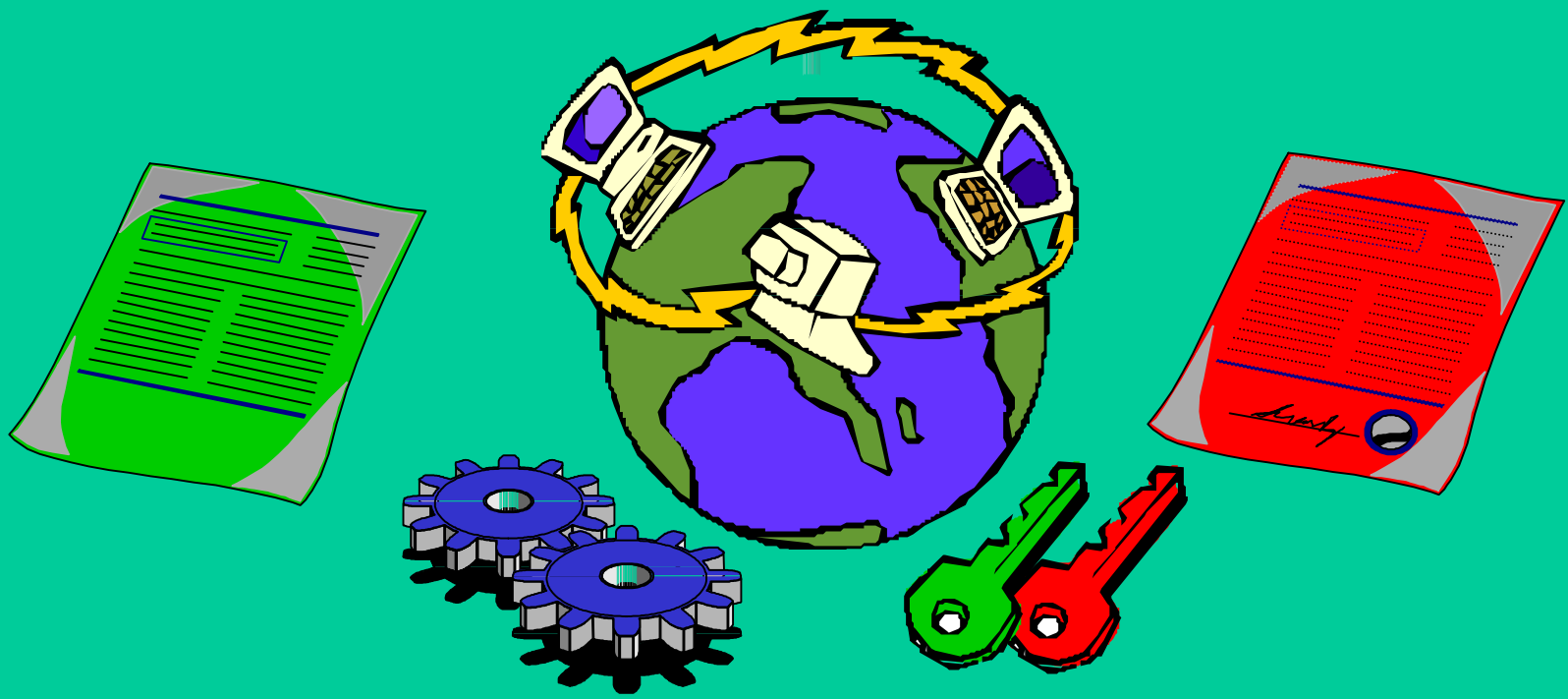
KRIPTOGRAFIA



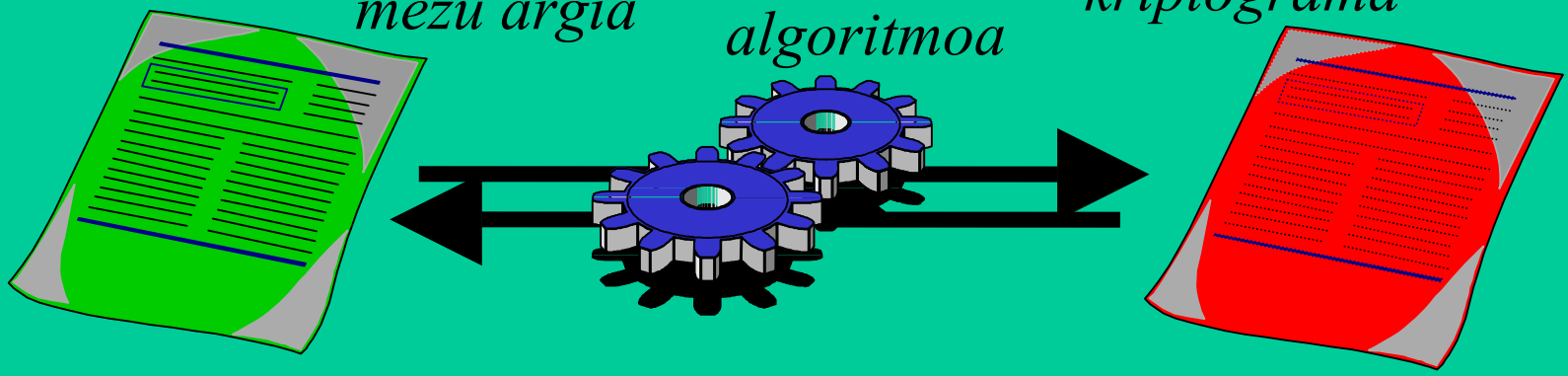
OINARRIAK

Liher Elgezabal

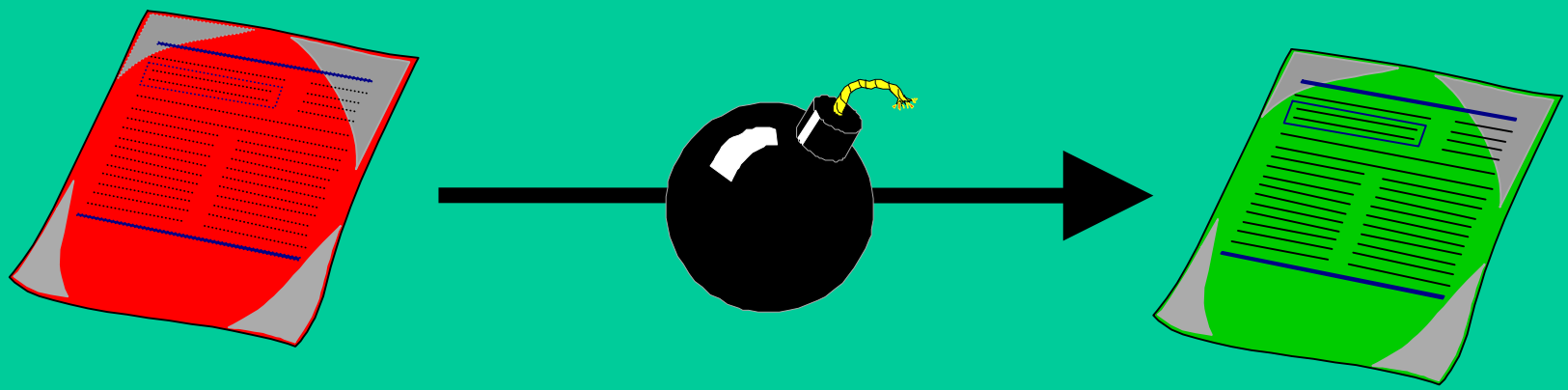
KRIPTOLOGIA

Kriptografia

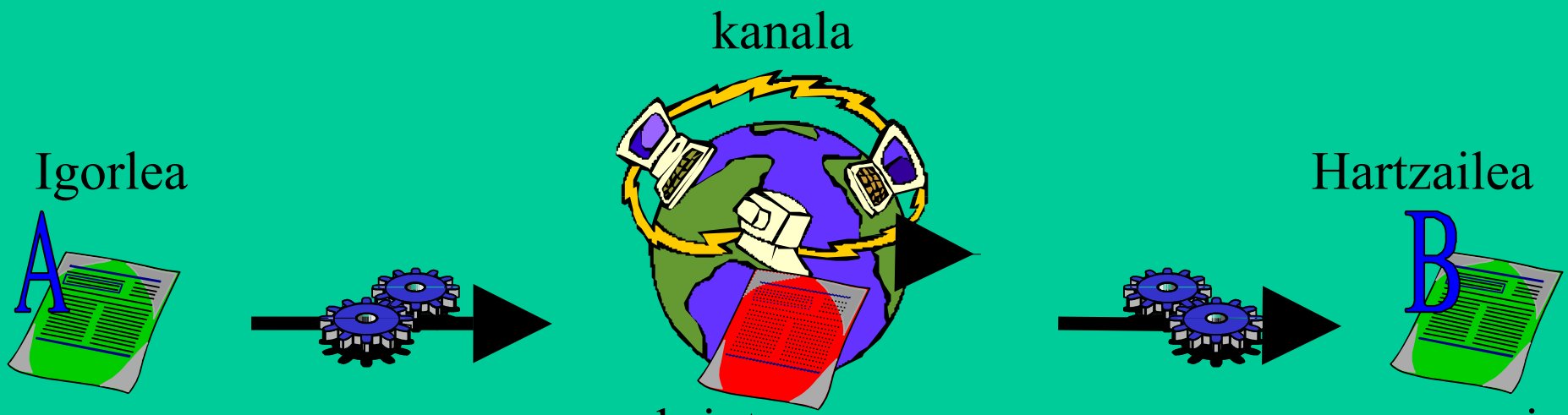
mezu argia *algoritmoa* *kriptograma*



Kriptoanalisia

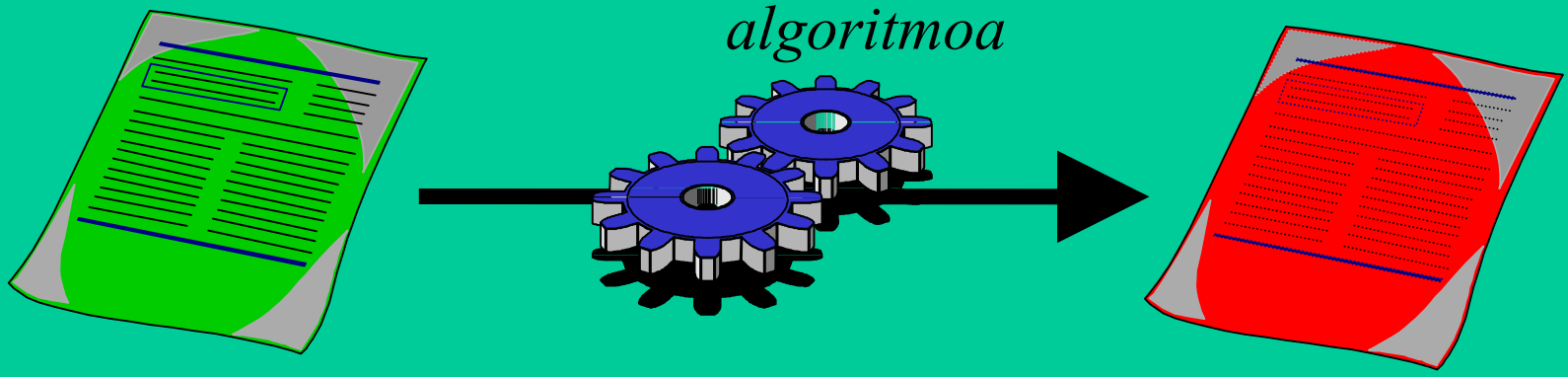


KRIPTOSISTEMA

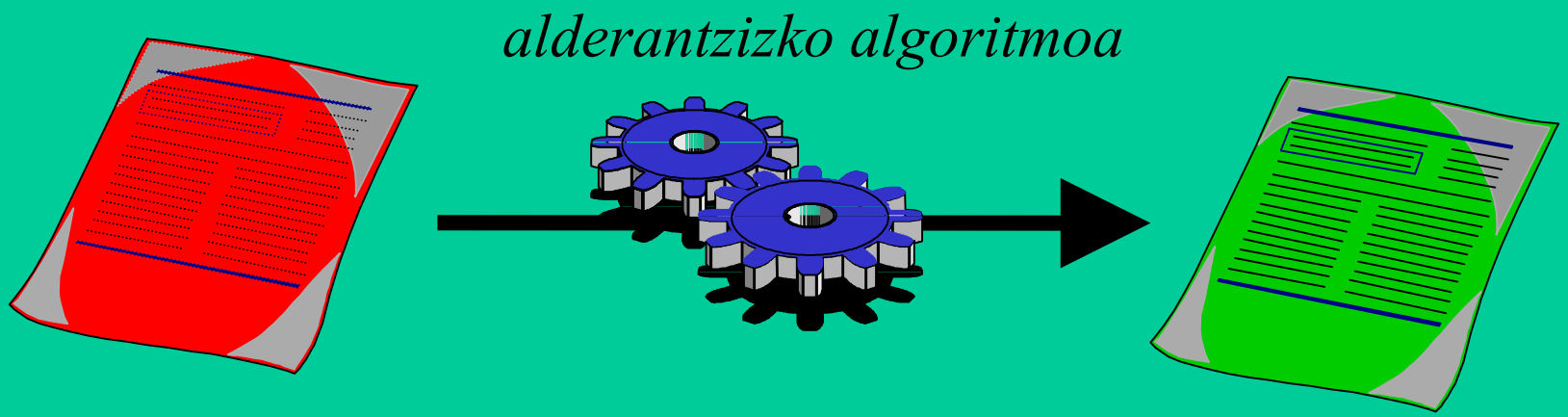


KRIPTOGRAFIA

Zifratzea



Deszifratzea



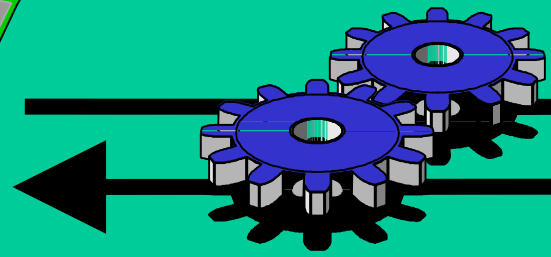
ZIFRATZE TEKNIKAK

Lekualdatzea

hedatzea

argia

kontrako ordena



aigra

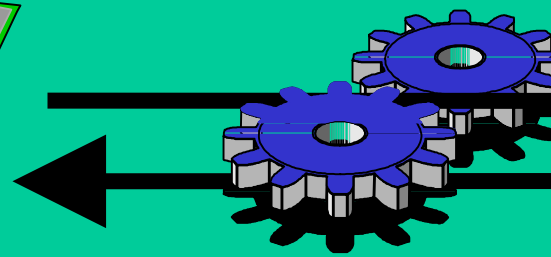
kontrako ordena

Ordezkatzea

nahastea

argia

+3

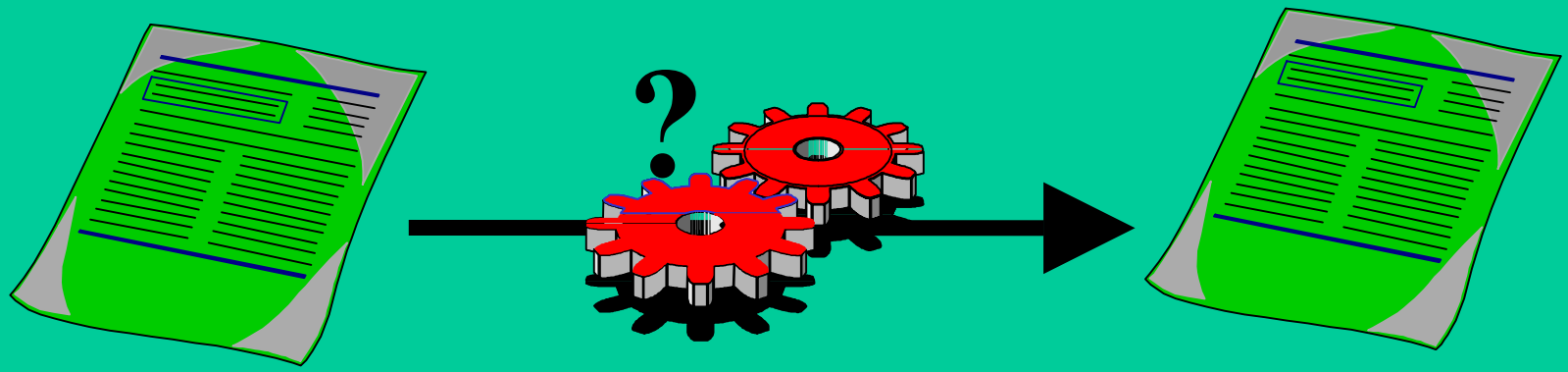


dujld

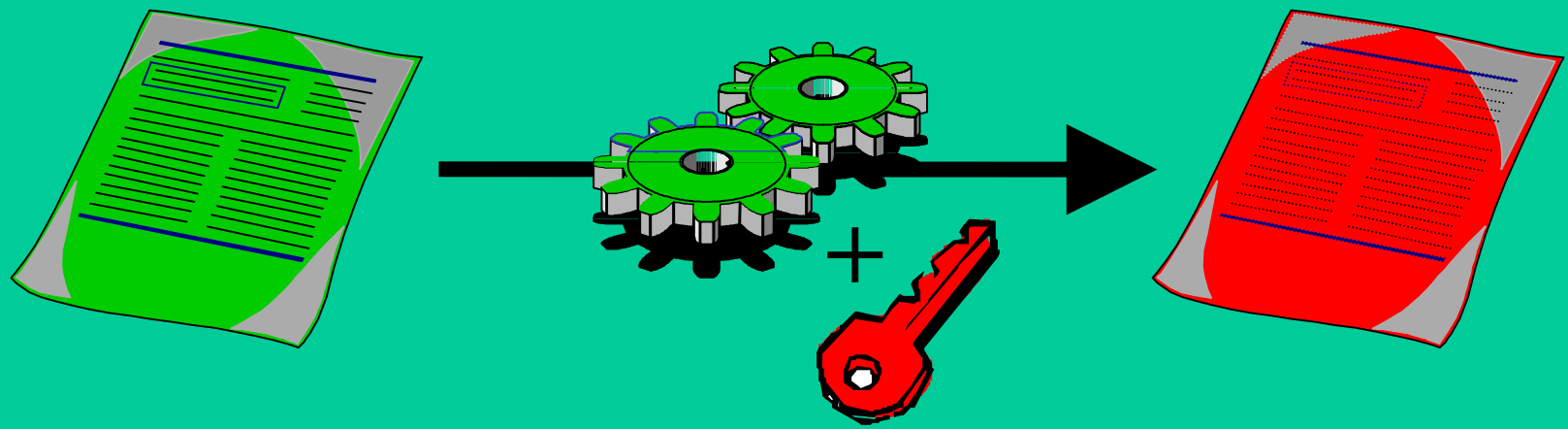
-3

ALGORITMO MOETAK

Algoritmo Sekretua

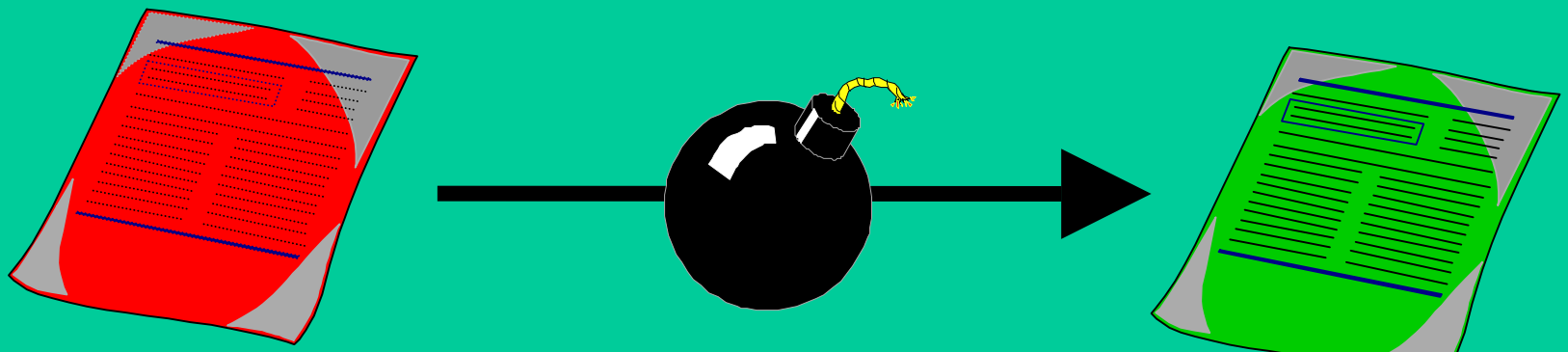


Algoritmo Publikoa
+ Gako Sekretua

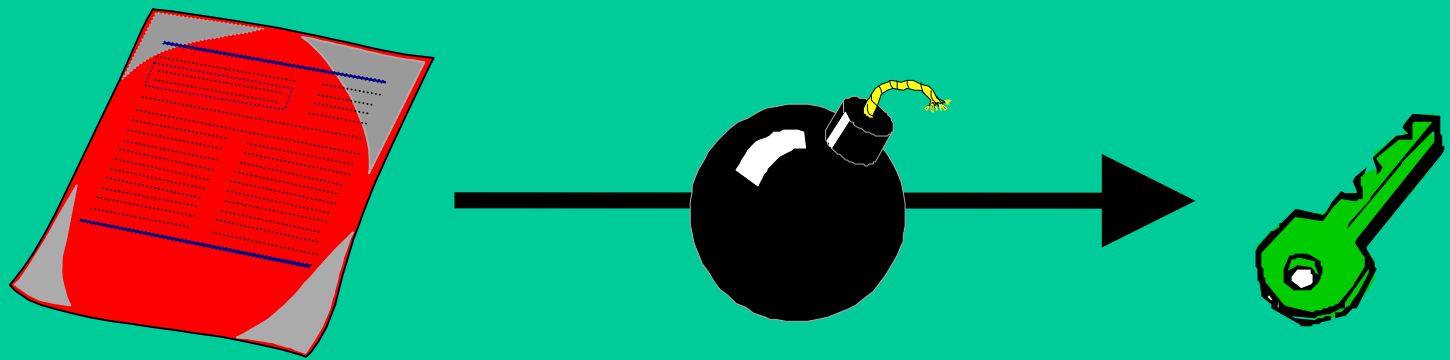


KRIPTOANALISIA

Kriptograma deszifratzea

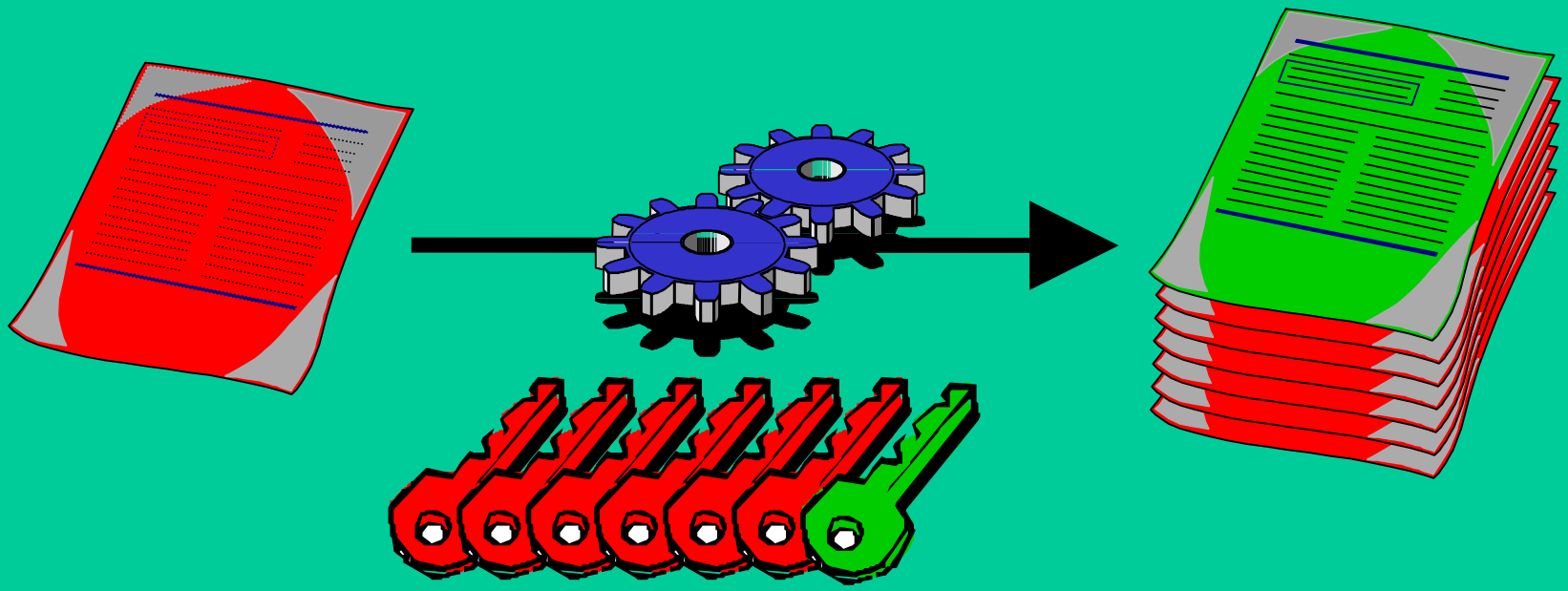


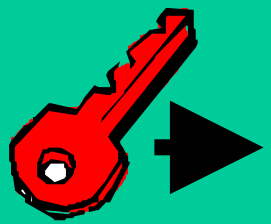
Gakoa asmatzea



KRIPTOANALISI TEKNIKAK

Indar gorria



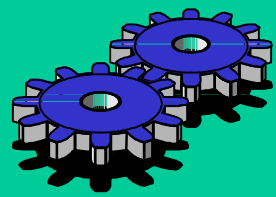


$2^{56}=7{,}2 \cdot 10^{16}$ gako

56 bit

1.000.000 saio/s

1.000.000.000.000 saio/s



1.142 urte

10 ordu

ONDORIOAK

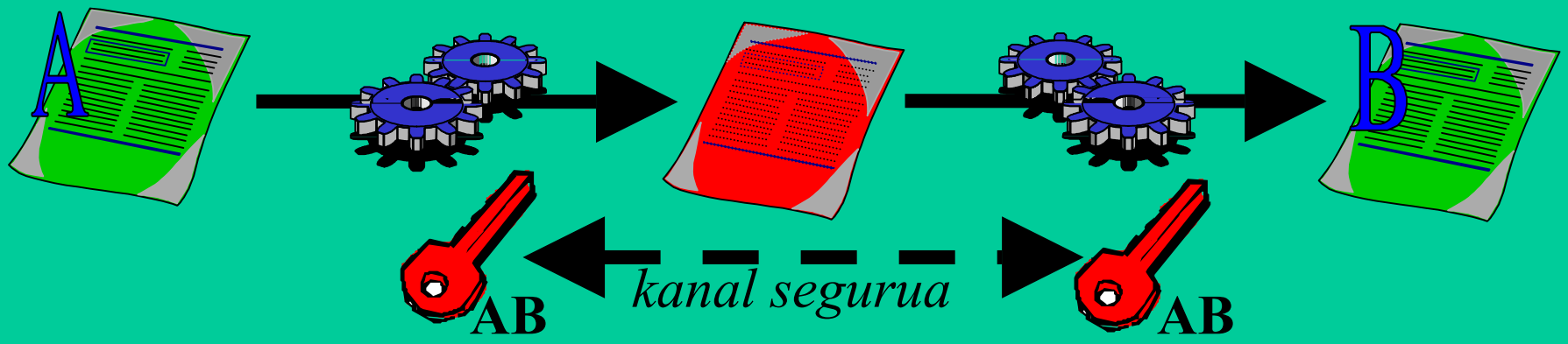
Ez da kriptosistema guztiz segururik existitzen.
Beti proba daitezke gako posible guztiak.

Beraz kriptosistema sendo batek bi baldintza hauek bete beharko ditu:

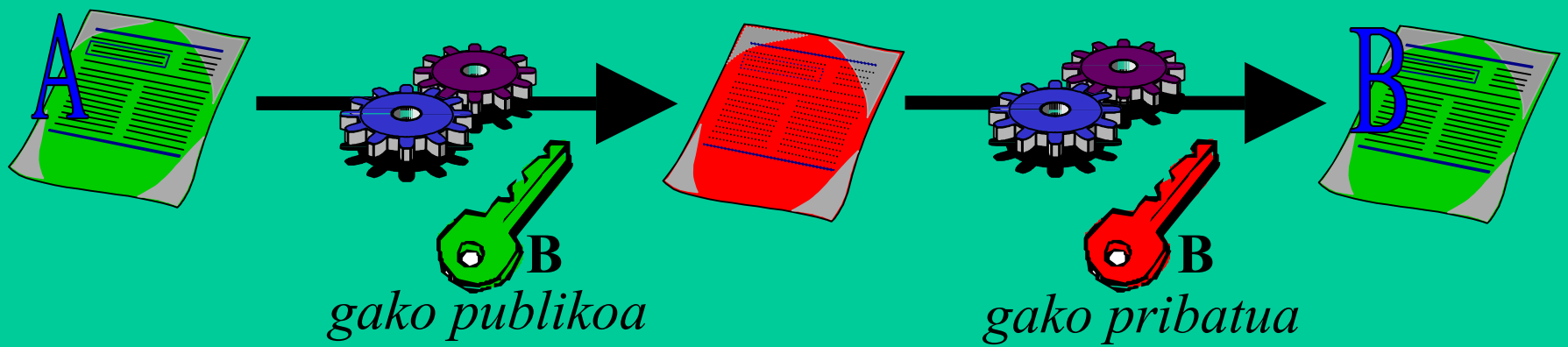
- kriptograma hausteko **prezioa** informazioaren balioa baino handiagoa izatea.
- kriptograma hausteko beharrezko **denbora** informazioaren balioa baino handiagoa izatea.

ALGORITMO MOETAK

Gako simetrikoak

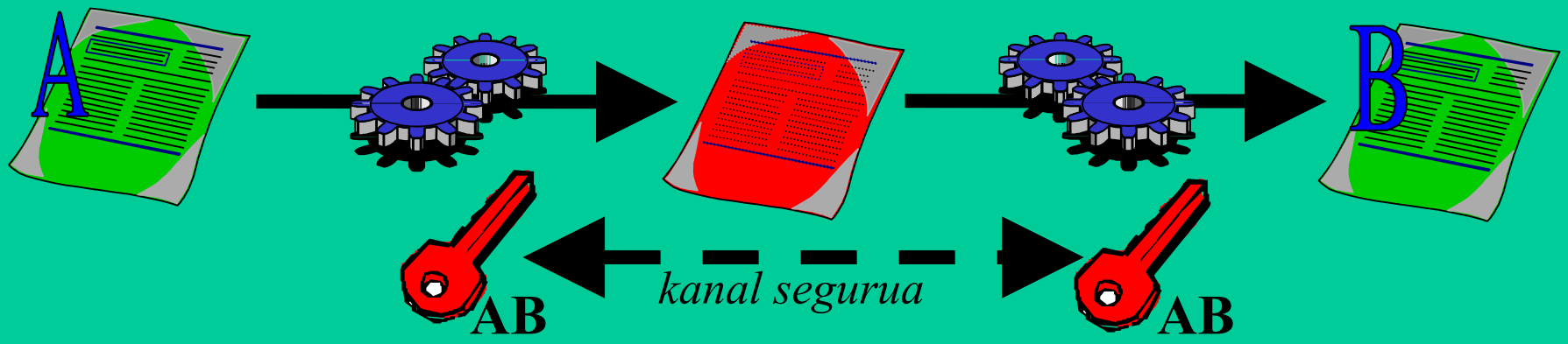


Gako asimetrikoak

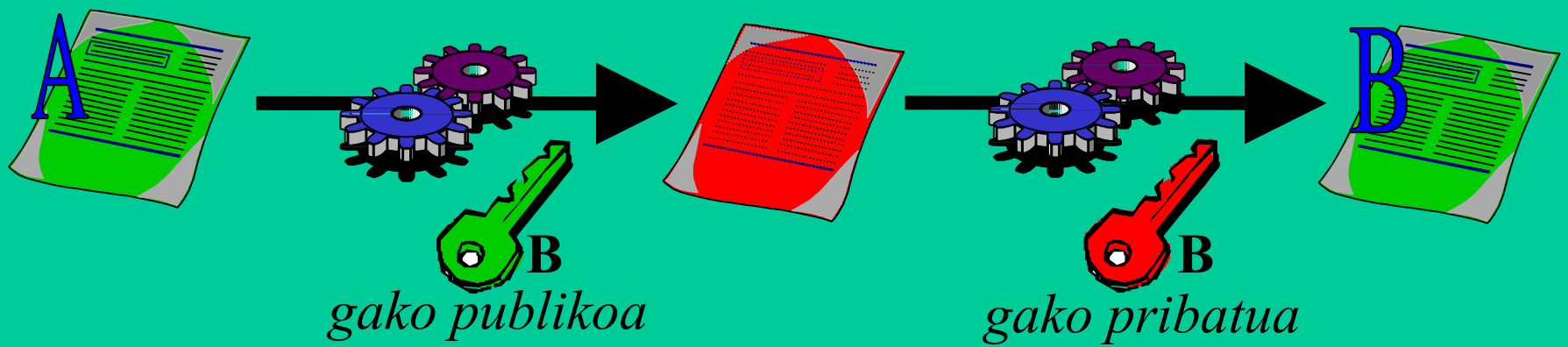


ALGORITMO MOETAK

Gako simetrikoak

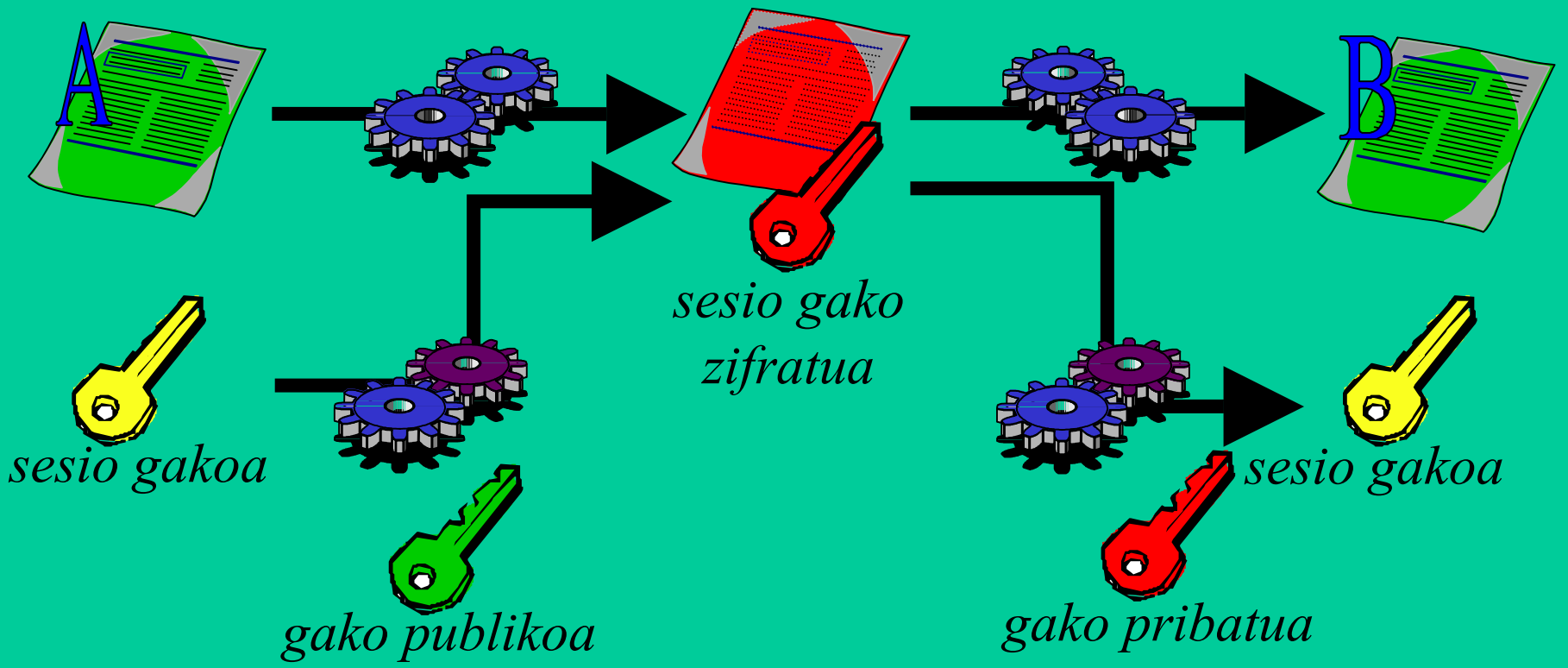


Gako asimetrikoak



SISTEMA HIBRIDOAK

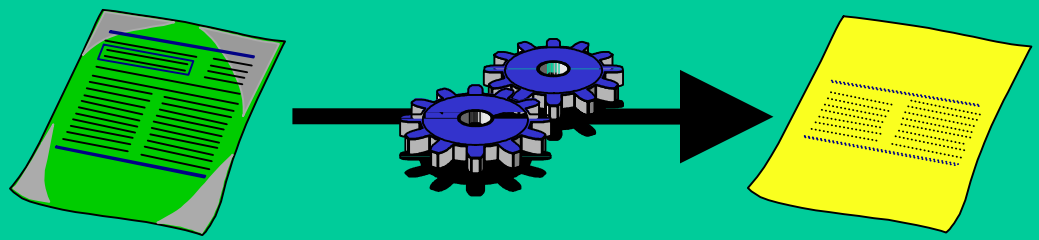
Gako simetriko + asimetrikoak



SAKABANATZE FUNTZIOAK

Sakabanatze funtzioa (hash)

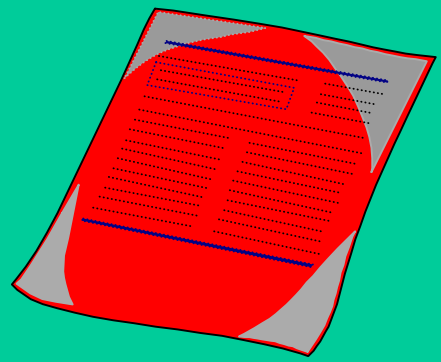
laburpen kriptografikoa



- algoritmo publikoa
- itzulezina
- tamaina finkoa

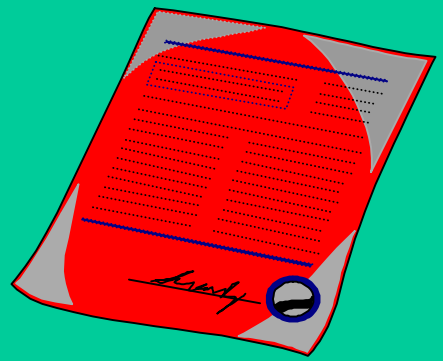
KRIPTOGRAFIAREN APLIKAZIOAK

Konfidentzialtasuna



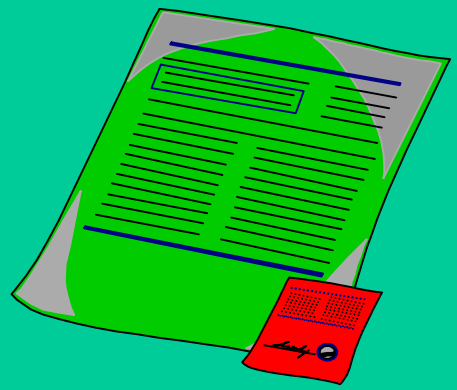
Atzitu arren informazioa ulertezina izango da.

Kautotzea



Informazio iturria egiazta daiteke

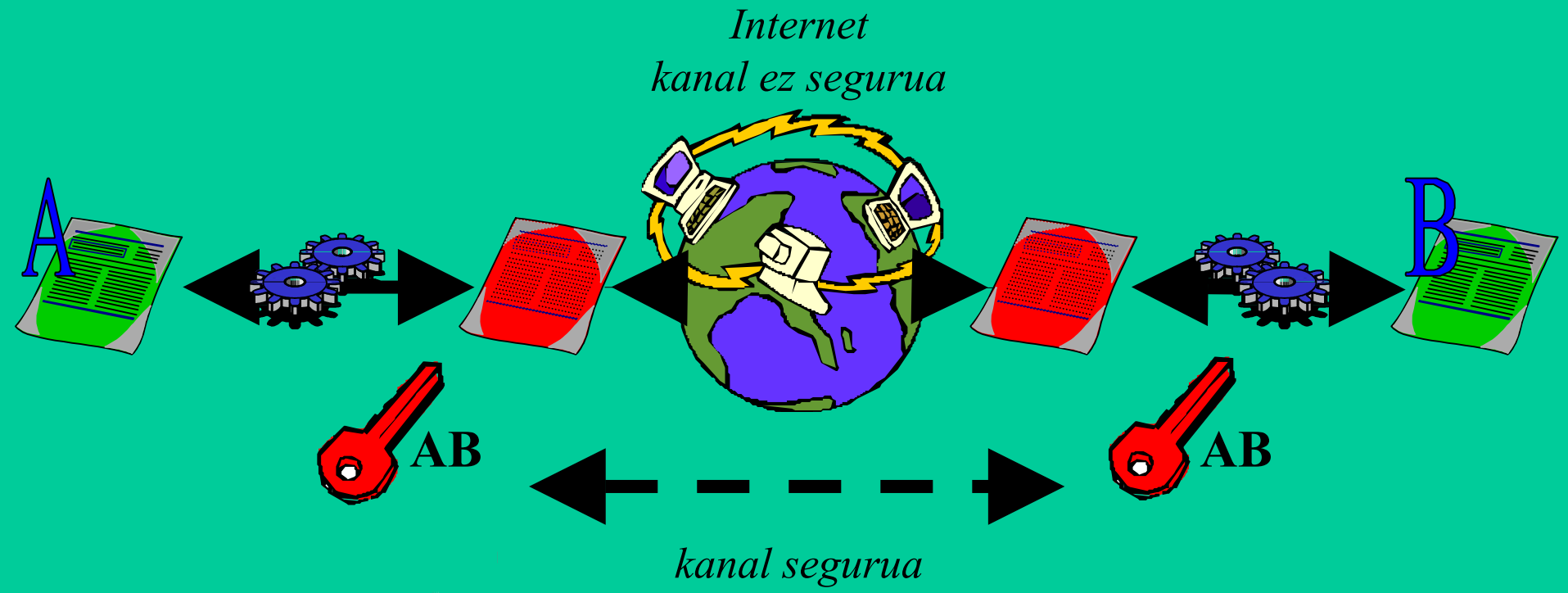
Osotasuna



Datuak bere osotasunean daudela ziurta daiteke

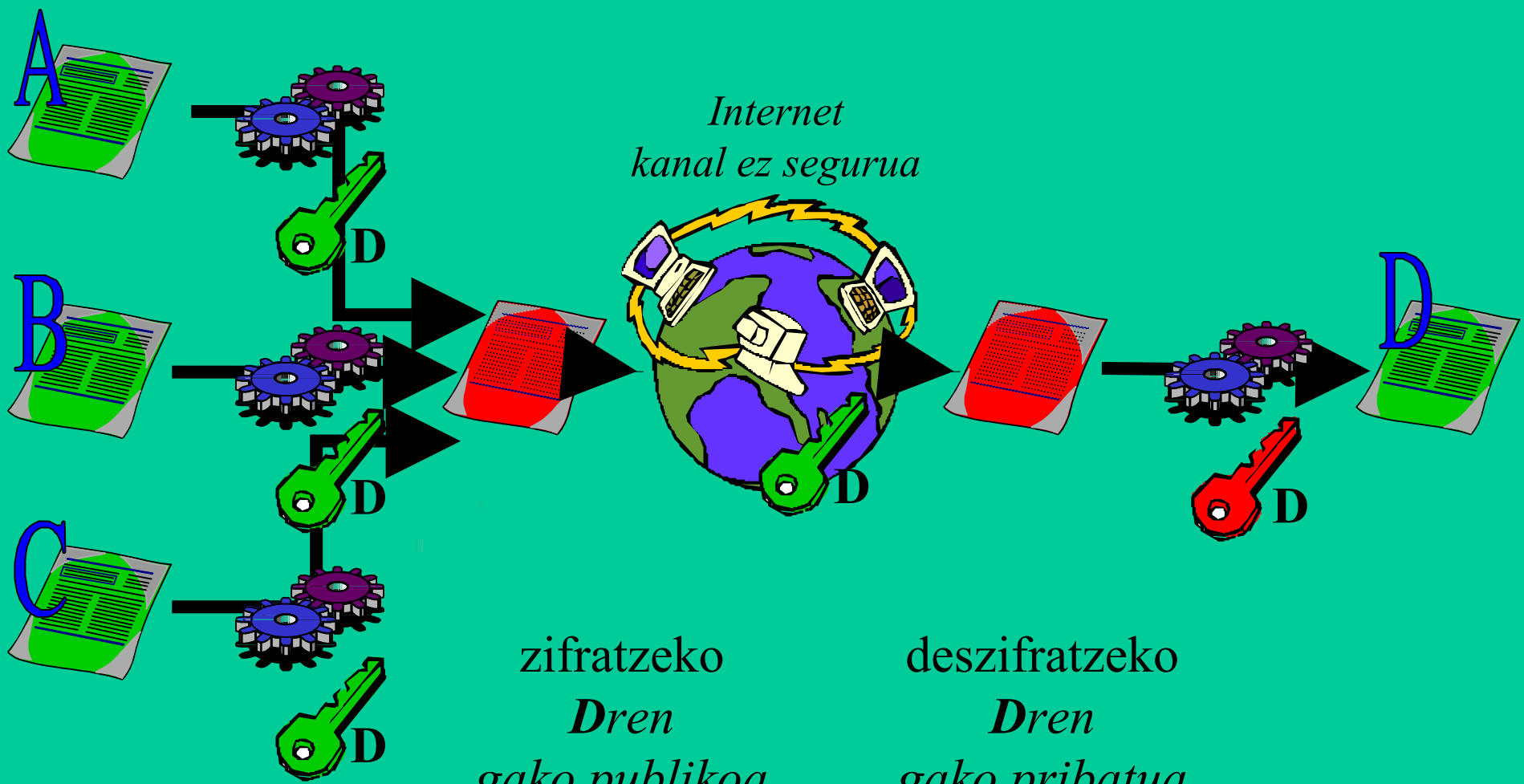
KONFIDENTZIALTASUNA

Kriptografia simetrikoa



KONFIDENTZIALTASUNA

Kriptografia asimetrikoa



zifratzeko
***D*ren**
gako publikoa

deszifratzeko
***D*ren**
gako pribatua

KAUTOTZEA

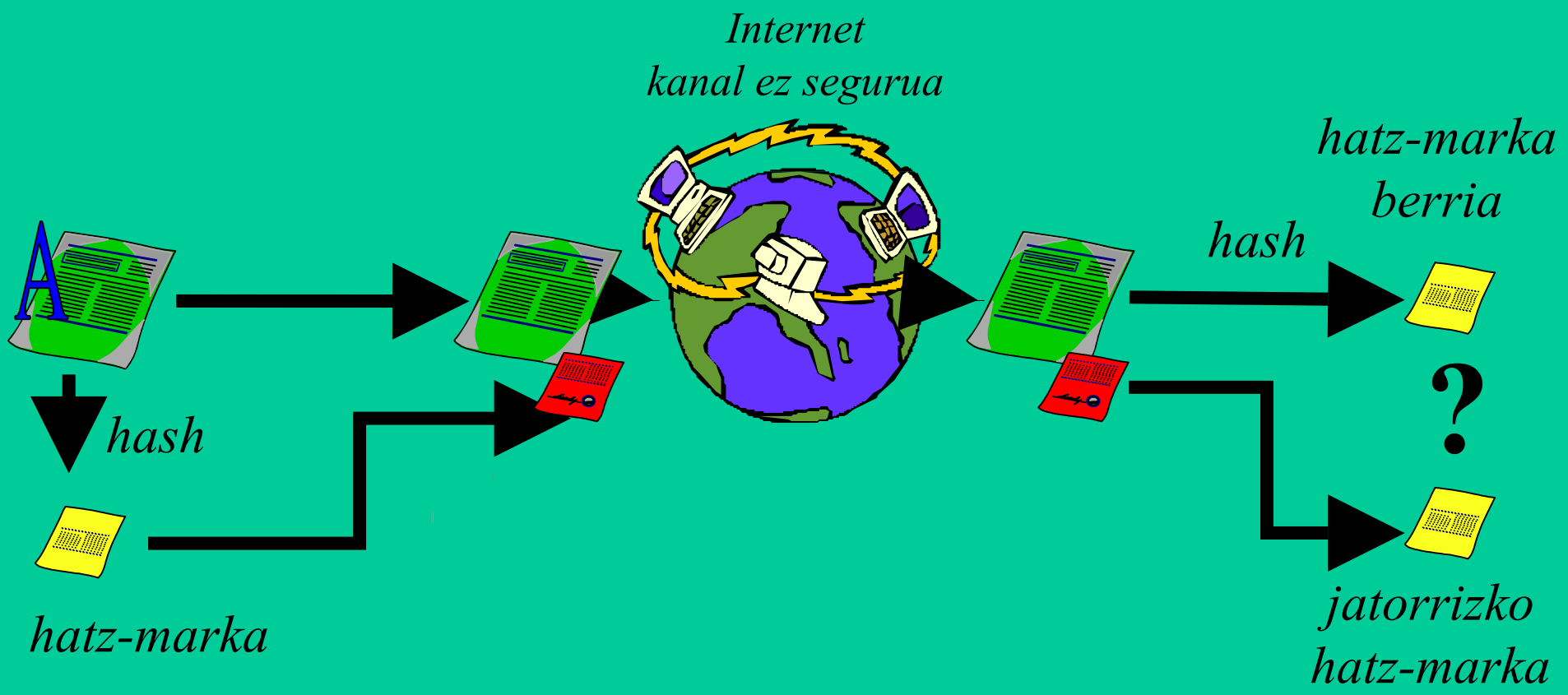
Kriptografia asimetrikoa

deszifratzeko
***D**ren*
gako publikoa

zifratzeko
Dren
gako pribatua

OSOTASUNA

Sakabanatze funtzioak (hash)



SINADURA DIGITALA

Kriptografia asimetrikoa + sakabanatze funtzioak