Certificats digitals: què són, perquè serveixen i com s'obtenen

Jaume Pujol

Professor retirat i

soci de la UES

7 de novembre de 2023

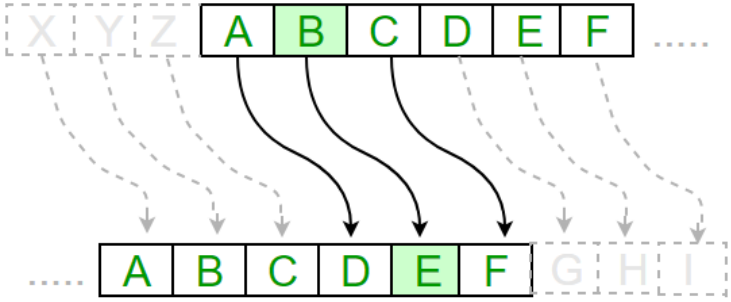
Certificat digital: document electrònic per verificar la identitat d'una persona o organització

Problema: com verificar la identitat d'una persona o organització?

Solució tradicional: DNI, empremta, notari, persona o organització de confiança.

Criptografia: ciència que estudia els mètodes per amagar la informació d'un missatge

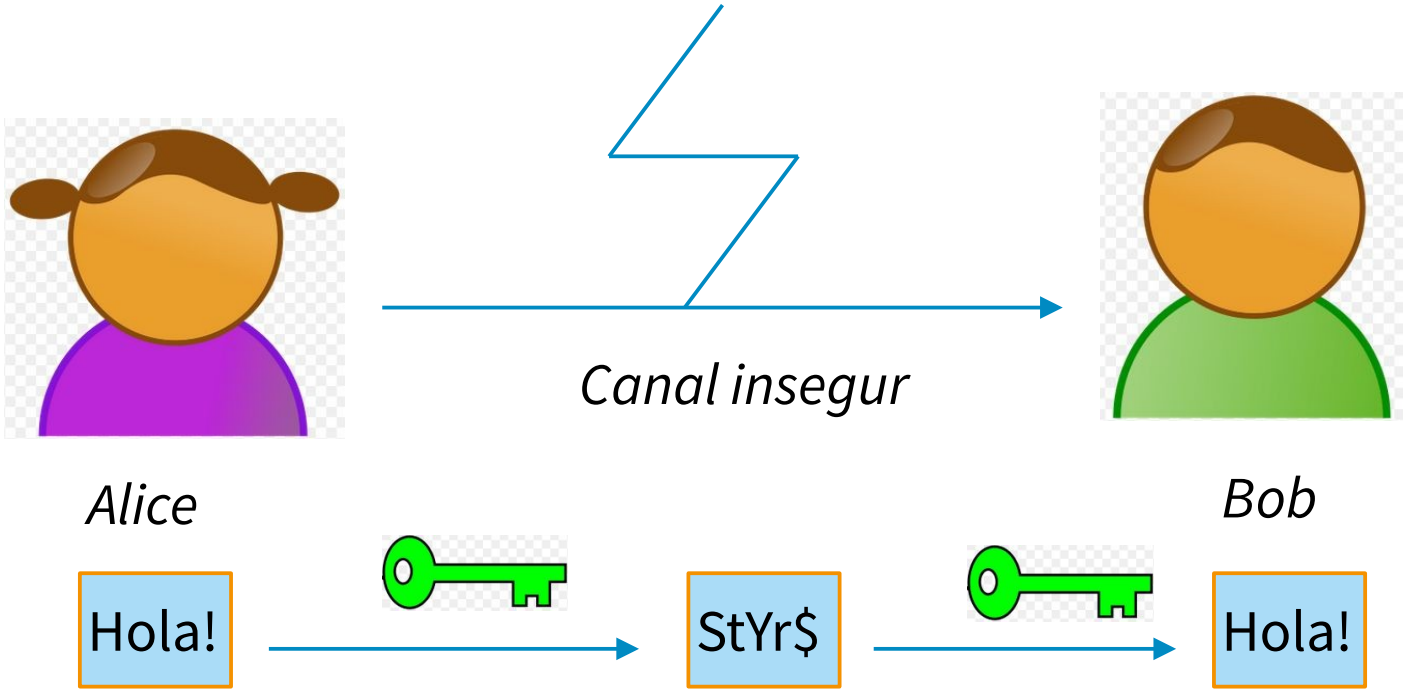
Escítala



Xifratge Caesar

p.e.: UES → XHV

Criptografia simètrica (1)



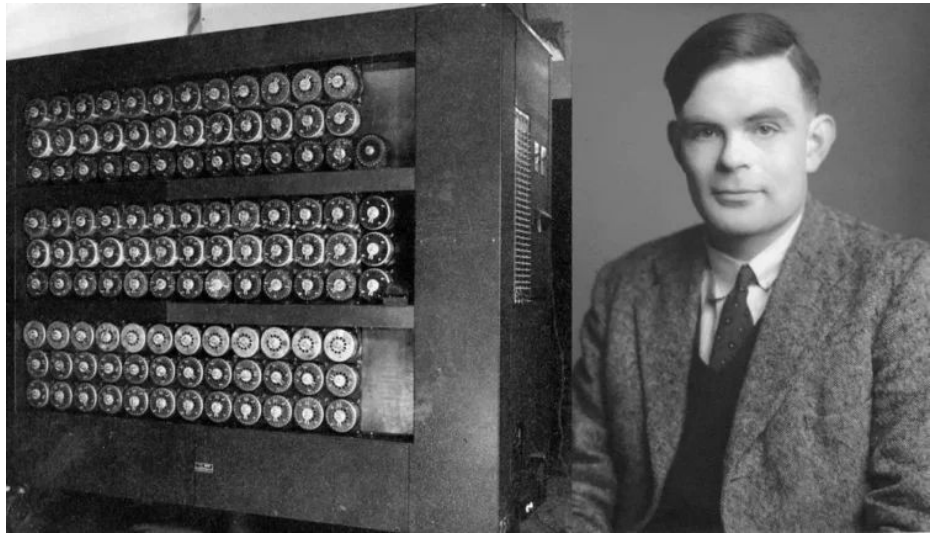
Segona Guerra Mundial (WW II)

La màquina Enigma

- Utilitzada per Alemanya.
- Consistia en una sèrie de rotors mecànics i connexions elèctriques.
- La configuració inicial dels rotors i les connexions elèctriques determinaven la clau.
- El nombre de combinacions superava els 159 quintillons.
- L'emissor i el receptor havien de tenir la mateixa configuració.
- Cada dia es canviava la configuració segons un llibre de claus.
- Criptoanalitzada per matemàtics polonesos i anglesos a Bletchley Park.

Segona Guerra Mundial (WW II)

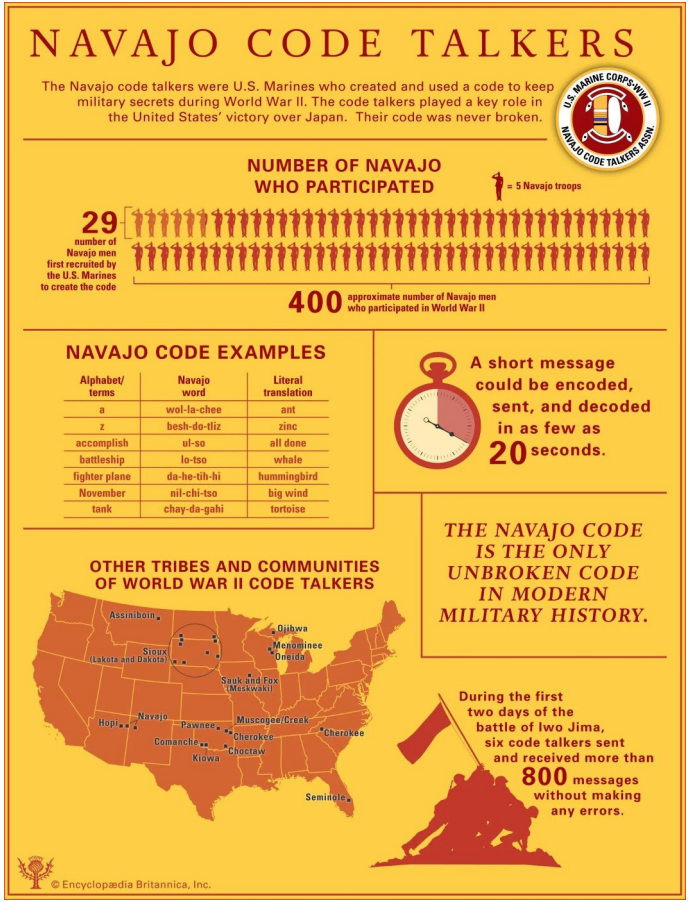
Alan Turing



- Matemàtic anglès que va participar en el criptoanàlisis de la màquina Enigma a Bletchley Park.
- Considerat el pare de la informàtica moderna.
- Condecorat amb l'ordre de l'imperi britànic.
- Condemnat per homosexualitat el 1952.
- Mort (possiblement suïcidat) el 1954 als 41 anys.
- Rehabilitat el 2009.
- La pel·lícula *The Imitation Game* (Prime Video, Netflix,...) està inspirada en la seva vida.
- El Premi Turing que atorga l'ACM cada any és l'equivalent al premi Nobel per als informàtics.

Segona Guerra Mundial (WW II)

El Pacífic



- JN-25 era el sistema utilitzat per l'armada japonesa en els atacs a Pearl Harbour i Midway.
- Els americans van poder desxifrar els missatges abans de l'atac a Midway.
- 400 indis Navajos van participar en la segona guerra mundial per xifrar les comunicacions.
- La pel·lícula *Windtalkers* (Prime Video, YouTube,...) està inspirada en aquests fets.

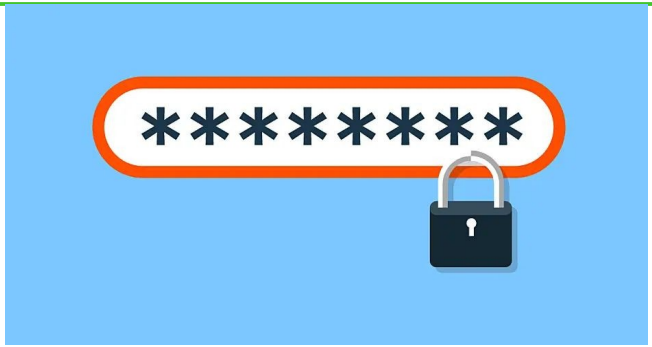
Criptografia simètrica (3)

Avantatges:

- Fàcil d'utilitzar.
- Ràpida de xifrar.
- Depèn d'una sola clau.
- Ideal per a xifratge de dades.

Inconvenients:

- La clau s'ha de compartir per un canal segur.
- Molt vulnerable als atacs estadístics.
- Difícil de manipular les claus si n'hi ha moltes.



Aplicacions: autenticació, wifi, targetes de crèdit, xifratge punt-a-punt (Whats App, Zoom...).

Identificació, autenticació i verificació

Identificació

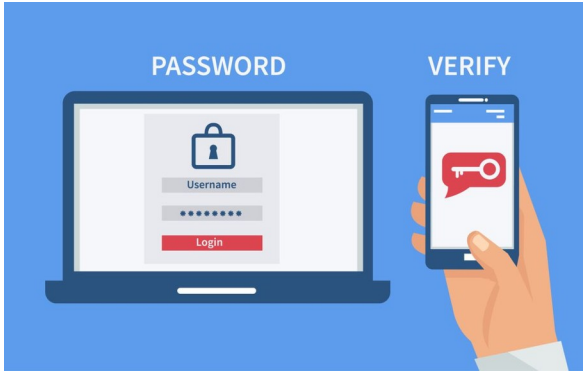
- Objecte que identifica l'entitat: nom, número DNI, adreça de mail,...

Autenticació

- Objecte que legitima l'entitat: *password*, biometria, doble autenticació (2FA),...

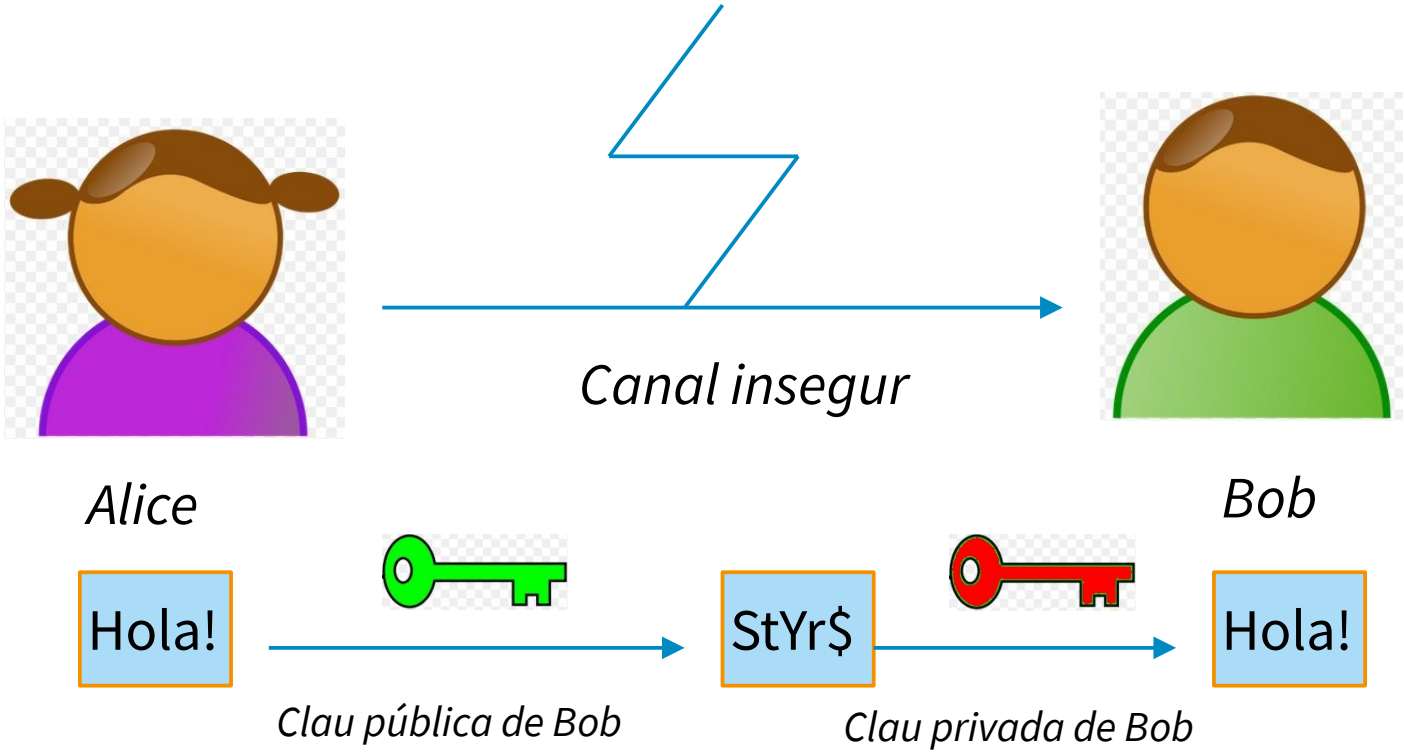
Verificació

- Procés per verificar l'autenticitat d'un usuari: foto, document, dades bancàries,...



Exemple: Wikiloc

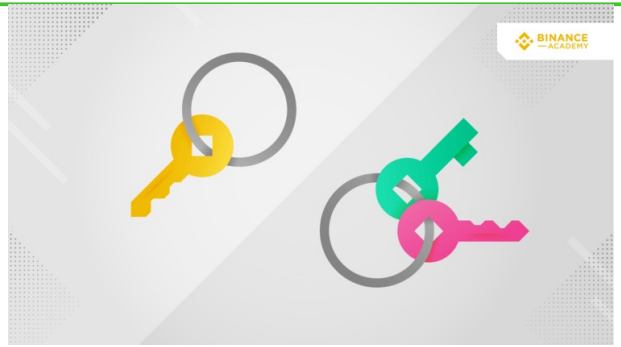
Criptografia asimètrica (1)



Criptografia asimètrica (2)

Avantatges:

- No necessita compartir claus.
- Permet la transmissió secreta.
- Permet l'intercanvi de claus.
- Permet la signatura electrònica.



Inconvenients:

- Necessita més temps de processament que la simètrica.
- Les claus tenen una mida més gran.
- No adequada per a xifratge de dades, ja que el missatge xifrat pot ocupar més espai que l'original.

Aplicacions: signatura de documents, certificats digitals, identitat digital,...

Identitat digital

Identitat: conjunt de propietats d'una persona que la diferencien de la resta. P.e. DNI

Identitat digital: conjunt de propietats d'una persona o organització en el món digital: P.e. Certificats digitals

Identitat Digital Europea

Certificats digitals

Document electrònic que serveix per verificar la identitat d'un usuari o una organització.

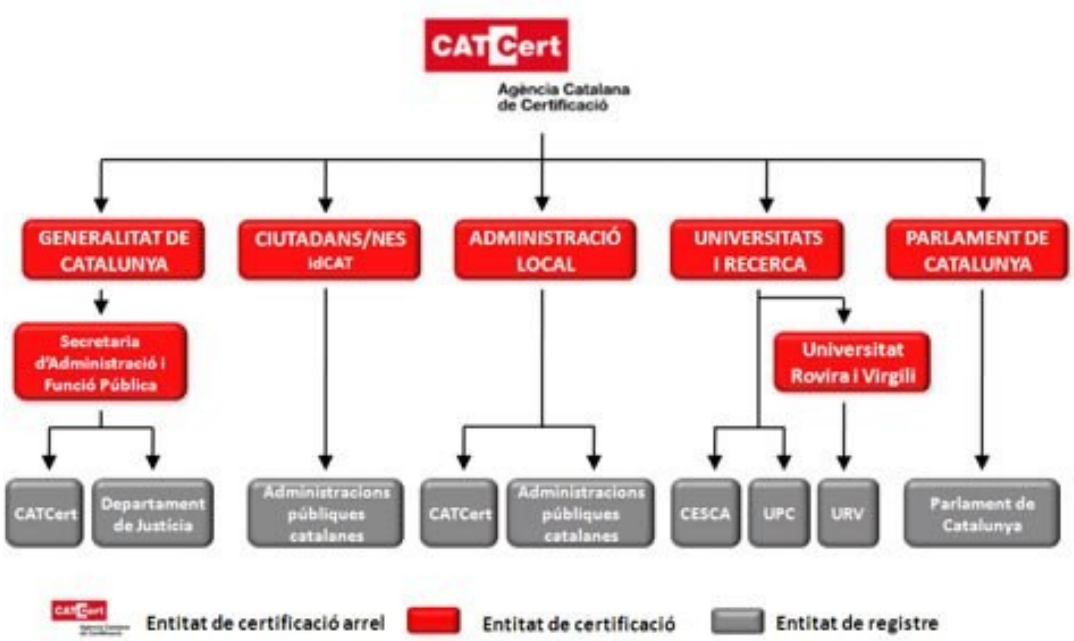
Exemple: Certificat SSL, UES

Característiques:

- Basat en criptografia asimètrica.
- La veracitat de les dades està garantida per una autoritat certificadora: CatCert, FNMT,...
- Permet confidencialitat, integritat i no repudi.
- Permet la signatura digital.
- Permet els tràmits amb administracions públiques a través d'internet, principalment.

Autoritats de certificació

Entitat dedicada a l'emissió i gestió posterior de certificats digitals, incloent-hi la renovació, l'expiració, la suspensió, l'habilitació i la revocació de certificats, a petició de l'autoritat de registre



Obtenció de certificats (1)

El Consorci Administració Oberta de Catalunya és l'ens que promou la transformació digital de l'administració pública catalana (AOC)

idCAT mòbil

idCAT

Altres accions:

- Renovar
- Revocar
- Modificar

Obtenció de certificats (2)

CERES és l'entitat pública de certificació espanyola.

Certificado Electrónico de Ciudadano: Obtenció certificat

Cl@ve Identificació Electrònica

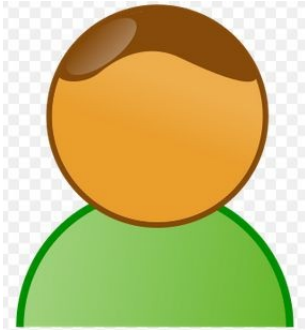
Altres accions:

- Verificació.
- Revocació.
- Anul·lació.

Aplicacions (1)

- Ajuntament de Sabadell
- Generalitat de Catalunya
- Servei Català de Trànsit
- Agència Tributària de Catalunya
- Agencia Tributaria
- Seguridad Social
- Catastro
- La meva Salut
- Consells Comarcals

Signatura electrònica (1)



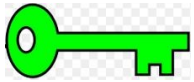
Hola!

Alice signa el document

Clau privada d'Alice

Hola! shy

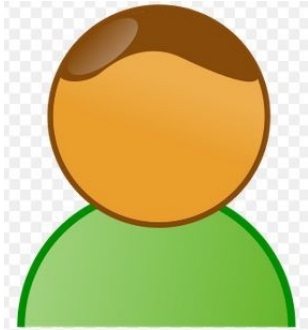
Bob verifica la signatura

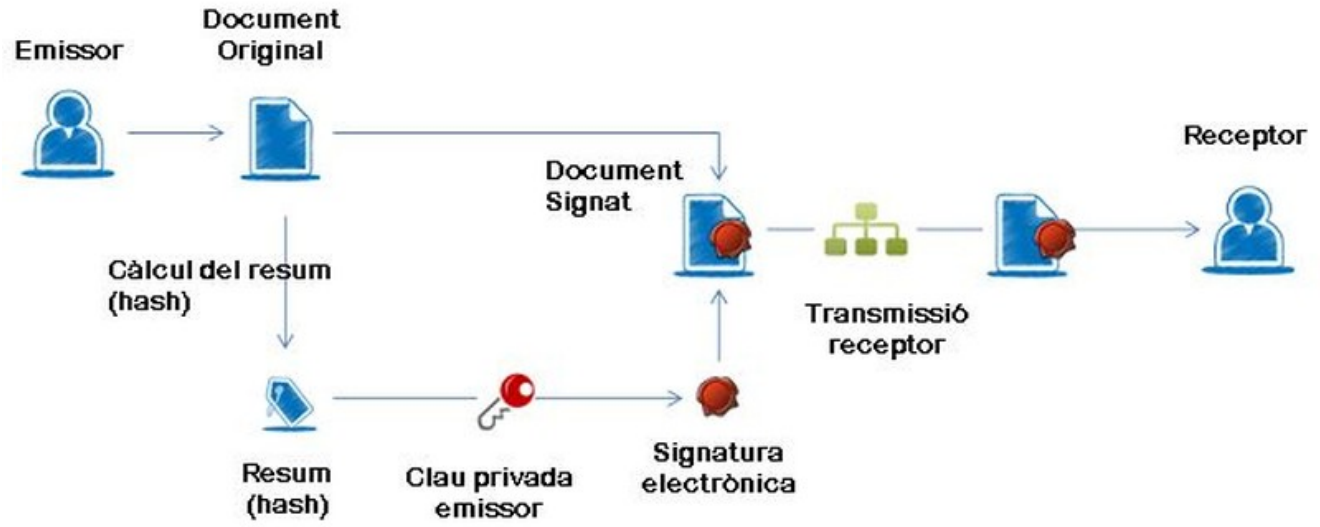


Clau pública d'Alice

Hola!

Signatura electrònica (2)





Aplicacions (2)

- Autofirma
- VALIDe
- DocuSign

- PDF
- Document Word
- Document LibreOffice

Certificats digitals: què són, perquè serveixen i com s'obtenen

Jaume Pujol

Professor retirat i

soci de la UES

7 de novembre de 2023

Gràcies per la seva atenció!