

Privadesa i seguretat a Internet



UNIVERSITAT
ROVIRA I VIRGILI

Secundària i Batxillerat
Miquel Guiot Cusidó



Financiado por
la Unión Europea
NextGenerationEU



GOBIERNO
DE ESPAÑA

MINISTERIO
PARA LA TRANSFORMACIÓN DIGITAL
Y DE LA FUNCIÓN PÚBLICA

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN
E INTELIGENCIA ARTIFICIAL



Plan de
Recuperación,
Transformación
y Resiliencia



INSTITUTO NACIONAL DE CIBERSEGURIDAD

Projecte HERMES, finançiat per



- Recerca d'alt nivell en:
 - Seguretat i privadesa en l'aprenentatge automàtic
 - Seguretat i privadesa en entorns descentralitzats
 - Criptografia avançada
 - Ciberseguretat en entorns vehiculars i entorns IOT
 - Gestió de la identitat
 - Avaluació, compliment normatiu i certificació
- Valorització i transferència dels resultats a la societat
- Divulgació i disseminació envers la ciutadania

Et sents segur navegant per Internet?

Estafes amb phishing: falsos SMS i mails suplanten Correus i la DGT per robar dades bancàries

Les notificacions falses arriben als mòbils i correus de les víctimes i també a Facebook, on un suposat extreballador de Decathlon ofereix motxilles de marca a 2 euros

Català ▾

Aquest web utilitza galetes (cookies)

Utilitzem galetes pròpies i de tercers per millorar la teva experiència de navegació, analitzar el trànsit del web i personalitzar el contingut que es mostra. Pots acceptar-les, rebutjar-les totes o configurar-les.

[Més informació sobre l'ús de les galetes en aquest web.](#)

Analítica

Recullen informació anònima sobre l'ús del web, les pàgines que visites, els elements amb els quals interactues i com has arribat al web. Aquesta informació es fa servir per analitzar el comportament dels usuaris al web i millorar-ne l'experiència.

Accepta-les totes

Rebutja-les

[Desa els canvis](#)

Facebook pagarà 4.432 milions d'euros per l'escàndol de Cambridge Analytica

És la multa més alta posada mai pel regulador i respon a la filtració de dades d'usuaris

Què hi ha al darrere de tot això?

A vibrant illustration of a path lined with cherry blossom trees. The path is a light blue-grey color, winding through a lush green field. On both sides of the path, there are rows of trees with dark brown trunks and dense, bright pink blossoms. The sky is a clear, bright blue, and several pink petals are shown floating in the air. In the background, there are rolling green hills under a clear sky. The overall scene is peaceful and beautiful, capturing the essence of a spring day.

Què hi ha al darrere de tot això?



Què hi ha al darrere de tot això?



Les nostres dades

Què aprendrem avui?

Privadesa i seguretat a Internet

1. Per què les dades importen?

- Negoci a Internet
- Dades sensibles

1. Com puc navegar de manera segura?

- Polítiques de privadesa
- Permisos
- *Cookies*

1. Què és un protocol de seguretat?

- Criptografia
- Encriptació de missatges
- Signatures digitals

The background is a dark blue field filled with vertical lines of light in shades of blue, cyan, and white, creating a digital or data-like effect. In the foreground, there is a grid of small, out-of-focus dots in blue, orange, and white, suggesting a perspective view of a data space.

La importància de les dades

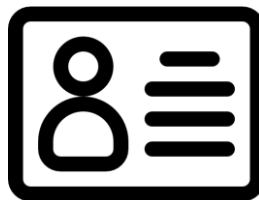
Què entenem per dades?

La importància de les dades: Definició

Qualsevol **informació** que es recopila, processa o emmagatzema sobre un **individu o usuari** durant la seva **interacció** amb un servei, aplicació, lloc web o plataforma.

Exemples

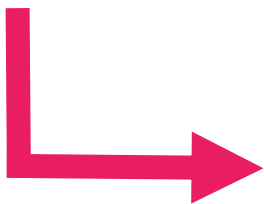
- Nom i cognoms
- Adreça
- empremta dactilar
- Publicacions a xarxes socials



La importància de les dades: Negoci a Internet

Monetització a Internet

- Comerç electrònic
- Subscripció
- Publicitat *online*
- Venda de dades a tercers



amazon

NETFLIX

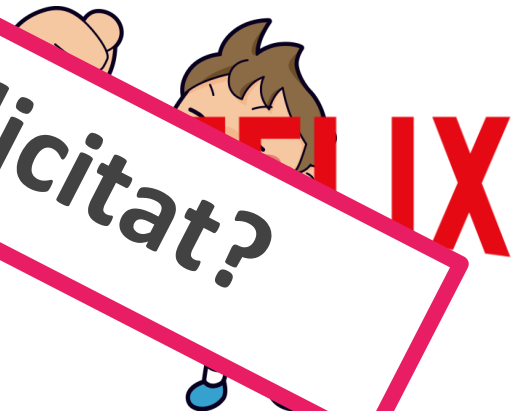


Google Ads

Importància de les dades: Publicitat *online*

- Els serveis són més **personalitzada**
- Les nostres dades **determinen** la publicitat que rebem
- La publicitat **p** més paga a un preu **més elevat**

amazon



Importància de les dades: Venda de dades a tercers

actuen com a **captadors d'usuaris**

es **venen** amb **fins comercials**

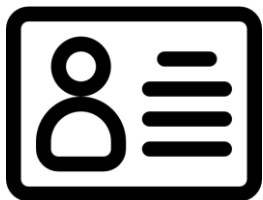
- Les d



Si el servei és gratuït, el producte ets tu

La importància de les dades: Dades sensibles

- Dades personals: nom, adreça, DNI
- Dades biomètriques: empremta, retina, cara
- Geolocalització
- Informació de salut i financera



La importància de les dades: Dades sensibles

Acomiadat de l'hotel on treballava per queixar-se a les xarxes socials amb l'uniforme posat

El jove, que treballava en un hotel de l'illa de Mallorca, va publicar un vídeo i, dos dies després, va ser cessat per «no superar el període de prova».



The background of the image is a dark blue field filled with a variety of colorful icons representing digital technology and communication. These include Wi-Fi symbols, speech bubbles, lightbulbs, gears, and various mobile devices. In the center, a large magnifying glass with a white handle and a dark blue frame is positioned. The lens of the magnifying glass is focused on a circular area that contains a very dense and colorful collection of these same digital icons, making it the central point of focus.

Navegació segura

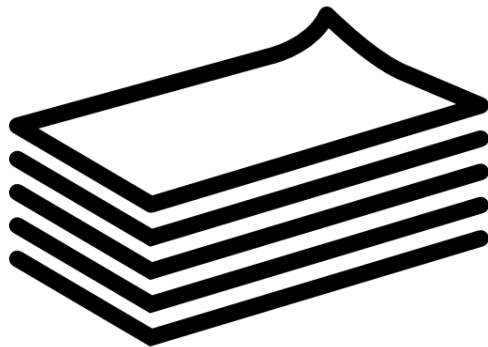
**Què entenem per polítiques de
privacitat?**

Navegació segura: Polítiques de privacitat

*Declaració **pública** i formalment documentada en què una **organització o administració pública** fa conèixer els principis i els criteris bàsics que determinen la manera **d'obtenir i tractar dades** de caràcter personal dels seus usuaris.*

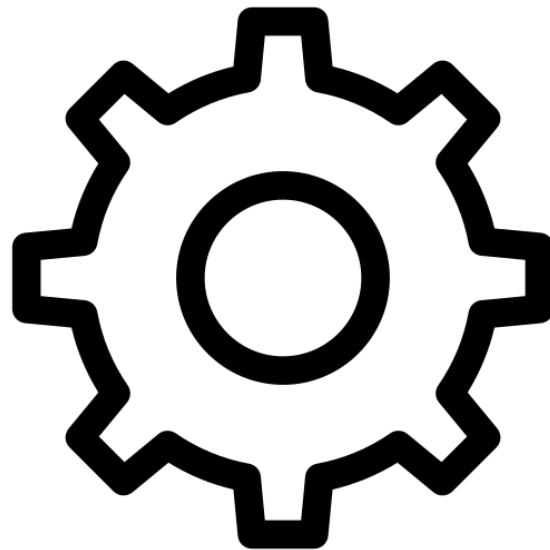
Navegació segura: Polítiques de privacitat

- Empren llenguatge **tècnic i jurídic**
- Sovint són d'una **extensió considerable**
- **Consell:** buscar **paraules clau** (compartir, tercers, publicitat)



Navegació segura: Permisos d'aplicacions

- Controlen **l'accés** de les aplicacions a les dades personals
- Es poden **modificar** en qualsevol moment



Navegació segura: Permisos d'aplicacions

Una aplicació gratuïta de llanterna per a Android va robar dades de localització per enviar-les als anunciant

Brightest Flashlight Free va tenir més de 50 milions de descàrregues, però els seus desenvolupadors van ser acusats per la FTC d'"enganyar els consumidors"

Què entenem per *cookies*?

Navegació segura: *Cookies*

*Petits **fitxers d'informació** que les **pàgines web** guarden al teu **navegador** per recordar dades i reconèixer-te quan hi tornes a accedir.*

Català ▾

Aquest web utilitza galetes (cookies)

Utilitzem galetes pròpies i de tercers per millorar la teva experiència de navegació, analitzar el trànsit del web i personalitzar el contingut que es mostra. Pots acceptar-les, rebutjar-les totes o configurar-les.

[Més informació sobre l'ús de les galetes en aquest web.](#)

Analítica

Recullen informació anònima sobre l'ús del web, les pàgines que visites, els elements amb els quals interactues i com has arribat al web. Aquesta informació es fa servir per analitzar el comportament dels usuaris al web i millorar-ne l'experiència.

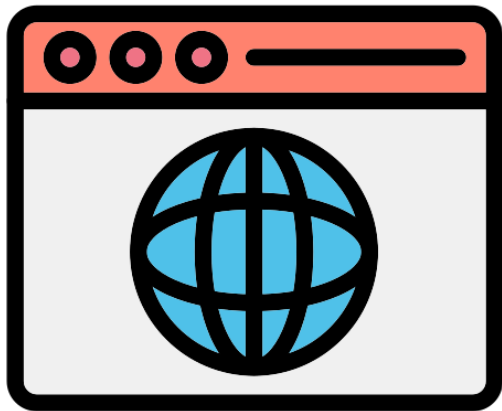


Accepta-les totes

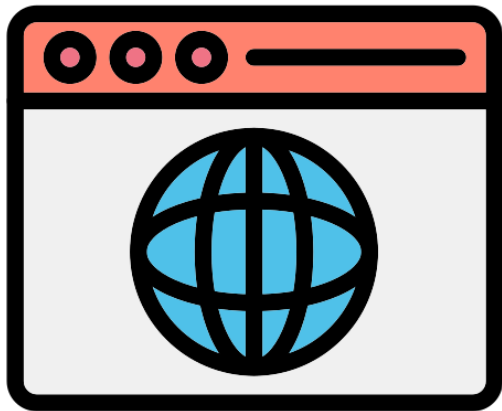
Rebutja-les

[Desa els canvis](#)

Navegació segura: *Cookies*



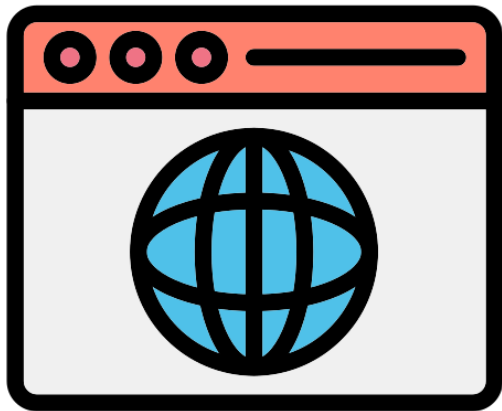
Navegació segura: *Cookies*



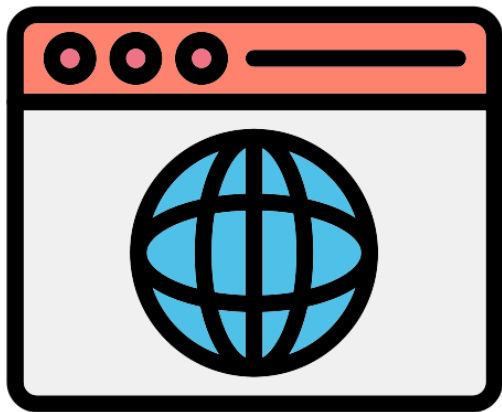
Ciutats



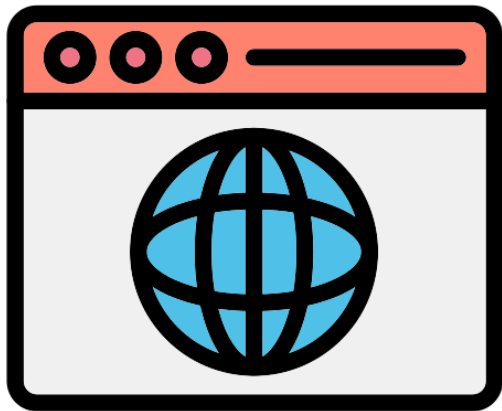
Navegació segura: *Cookies*



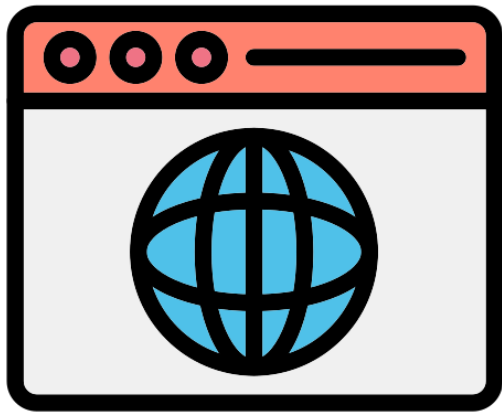
Navegació segura: *Cookies*



Navegació segura: *Cookies*



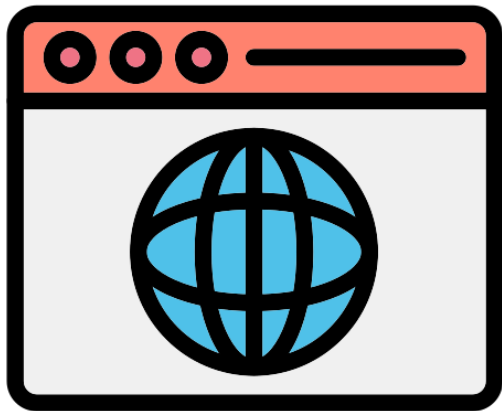
Navegació segura: *Cookies*



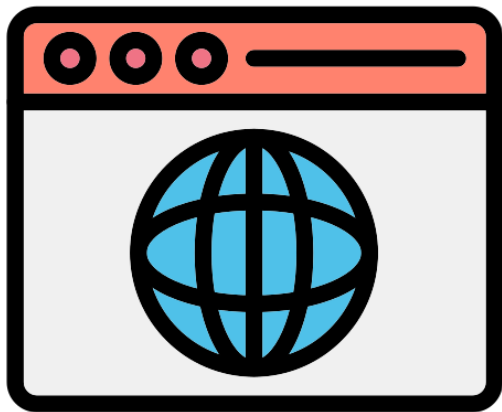
Futbol



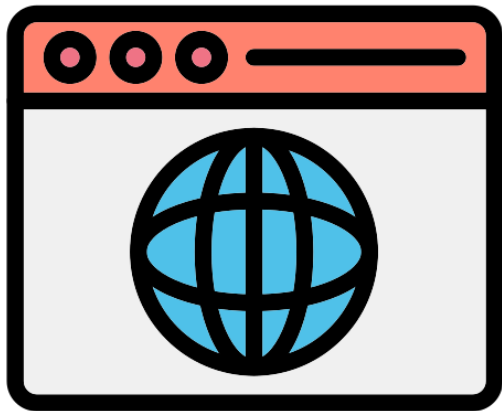
Navegació segura: *Cookies*



Navegació segura: *Cookies*



Navegació segura: *Cookies*



Navegació segura: *Cookies*

- Les *cookies* **funcionals milloren** l'experiència de navegació
- Les *cookies* **de tercers** tenen **fins comercials**
- Totes les pàgines **permeten triar** quines *cookies* volem
- Podem **esborrar** les cookies a través del navegador



Protocols de seguretat

Què entenem per criptografia?

Protocols de seguretat: Criptografia

Pràctica i estudi de tècniques de comunicació segura en presència de comportaments adversos

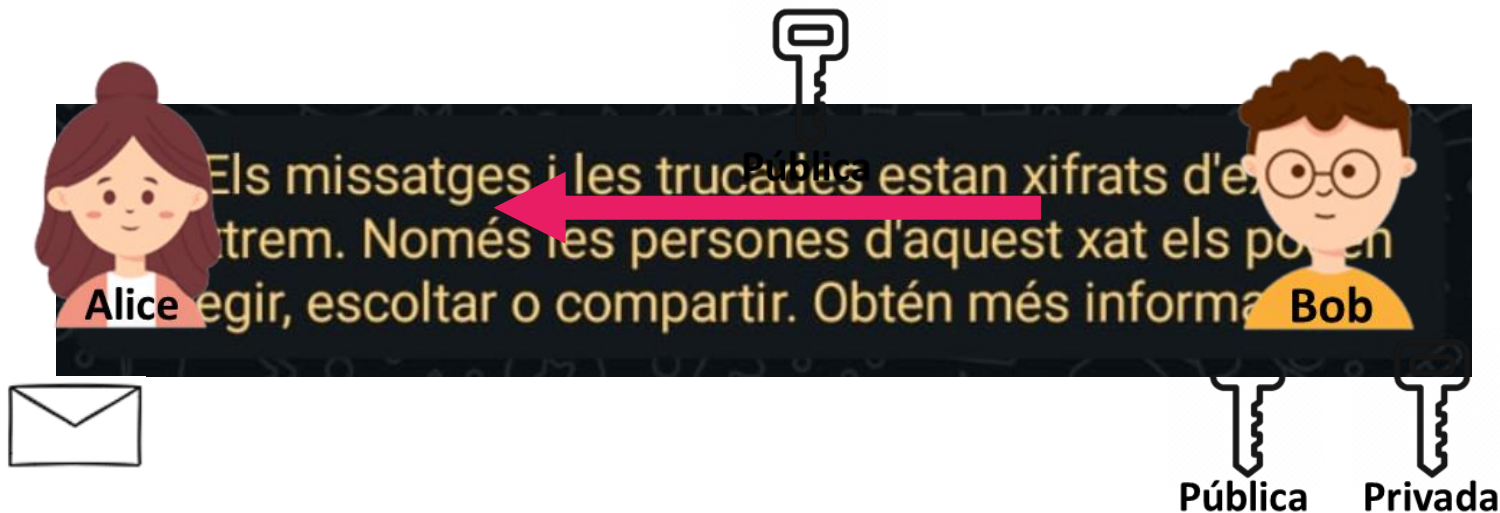
Objectius

- Privadesa
- Autenticació



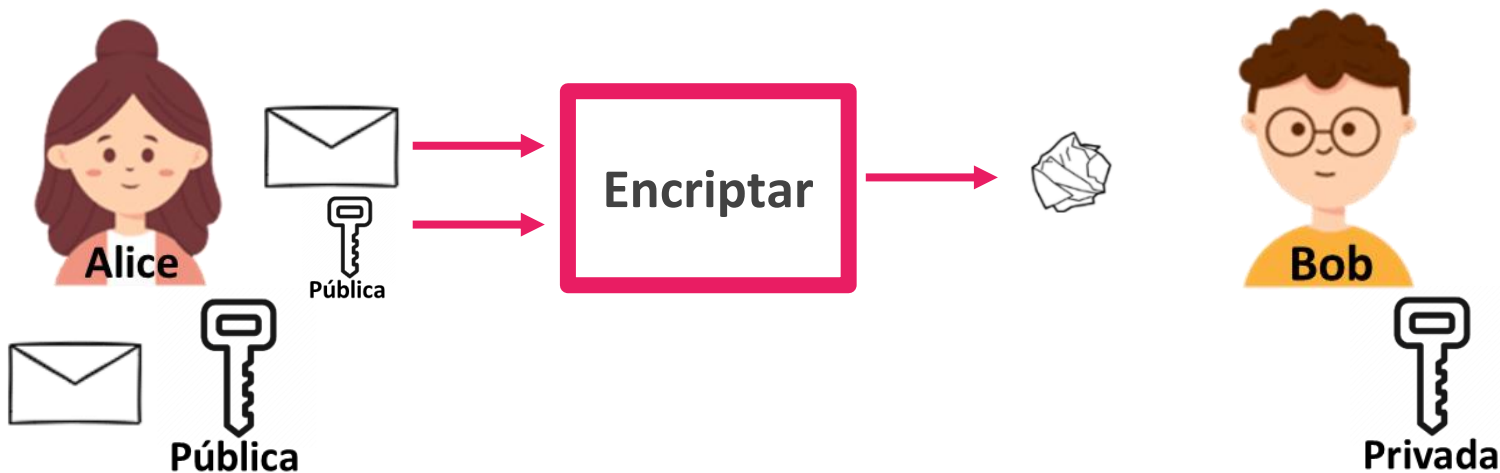
Protocols de seguretat: Encriptació de missatges

- **Objectiu:** enviar i rebre missatges de manera **privada**
- Aquests mecanismes estan basats en **problemes matemàtics**
- Cada usuari disposa d'una clau **pública** i d'una clau **privada**



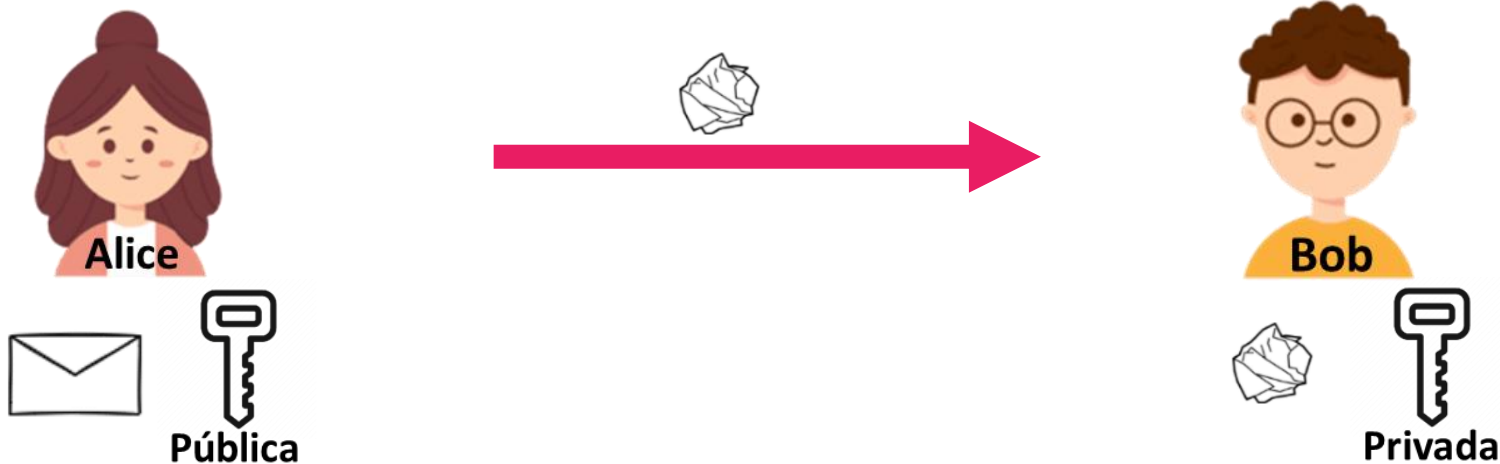
Protocols de seguretat: Encriptació de missatges

- **Objectiu:** enviar i rebre missatges de manera **privada**
- Aquests mecanismes estan basats en **problemes matemàtics**
- Cada usuari disposa d'una clau **pública** i d'una clau **privada**



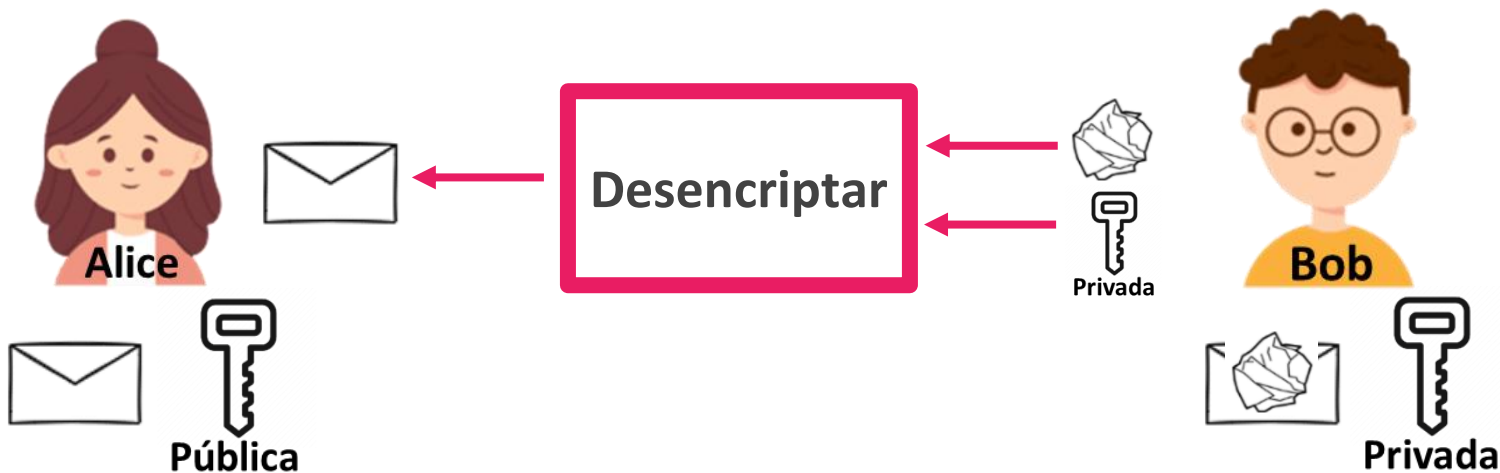
Protocols de seguretat: Encriptació de missatges

- **Objectiu:** enviar i rebre missatges de manera **privada**
- Aquests mecanismes estan basats en **problemes matemàtics**
- Cada usuari disposa d'una clau **pública** i d'una clau **privada**



Protocols de seguretat: Encriptació de missatges

- **Objectiu:** enviar i rebre missatges de manera **privada**
- Aquests mecanismes estan basats en **problemes matemàtics**
- Cada usuari disposa d'una clau **pública** i d'una clau **privada**



Protocols de seguretat: Encriptació de missatges

Experts criptogràfics fan unes eleccions hipersegures i ara no poden desxifrar-ne els resultats

L'Associació Internacional de Recerca Criptològica (IACR) repetirà les eleccions per escollir els representants de l'organització perquè han perdut una part de la clau per veure'n els resultats



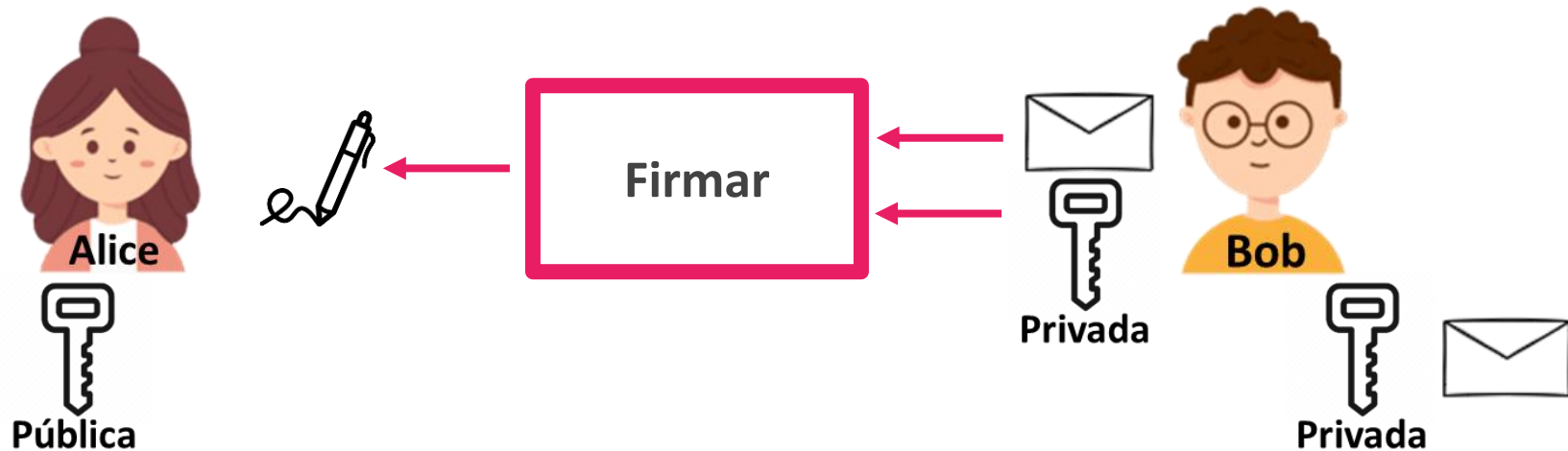
Protocols de seguretat: Signatures digitals

- **Objectiu:** garantir l'**autoria** d'un missatge digital
- També estan basades en **problemes matemàtics**
- Cada usuari disposa d'una clau **pública** i d'una clau **privada**



Protocols de seguretat: Signatures digitals

- **Objectiu:** garantir l'**autoria** d'un missatge digital
- També estan basades en **problemes matemàtics**
- Cada usuari disposa d'una clau **pública** i d'una clau **privada**



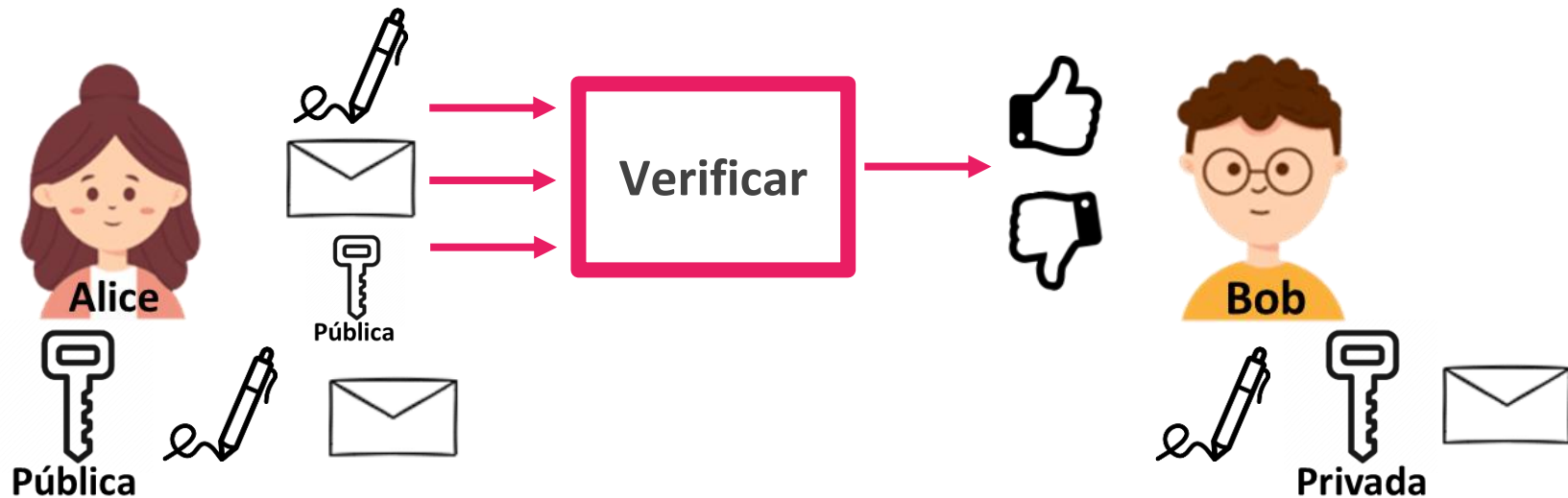
Protocols de seguretat: Signatures digitals

- **Objectiu:** garantir **l'autoria** d'un missatge digital
- També estan basades en **problemes matemàtics**
- Cada usuari disposa d'una clau **pública** i d'una clau **privada**



Protocols de seguretat: Signatures digitals

- **Objectiu:** garantir l'**autoria** d'un missatge digital
- També estan basades en **problemes matemàtics**
- Cada usuari disposa d'una clau **pública** i d'una clau **privada**



Conclusions

- Les nostres **dades** són **valuoses** per les empreses tecnològiques
- Cal **anar amb compte** al navegar per **Internet**
- La **criptografia** és la base de la **seguretat digital**

Criptografia + bones pràctiques = navegació segura

Privadesa i seguretat a Internet



CFA El Vendrell
Miquel Guiot Cusidó

