



# CryptoParty

@CryptoPartyBCN

#cryptopartybcn

CryptoParty.cat

Barcelona, 20 febrer 2016

# Qui som

- Part d'un moviment mundial (les CryptoParties) que vol ajudar a protegir millor la nostra privadesa
- Enginyers Informàtics preocupats per aquest tema
- Organitzant cursos i tallers des de 2013
- Ens podeu trobar a:
  - [www.CryptoParty.cat](http://www.CryptoParty.cat)
  - [@CryptoPartyBCN](https://twitter.com/CryptoPartyBCN)



# Per què ?



Font: Jordi Iparraguirre



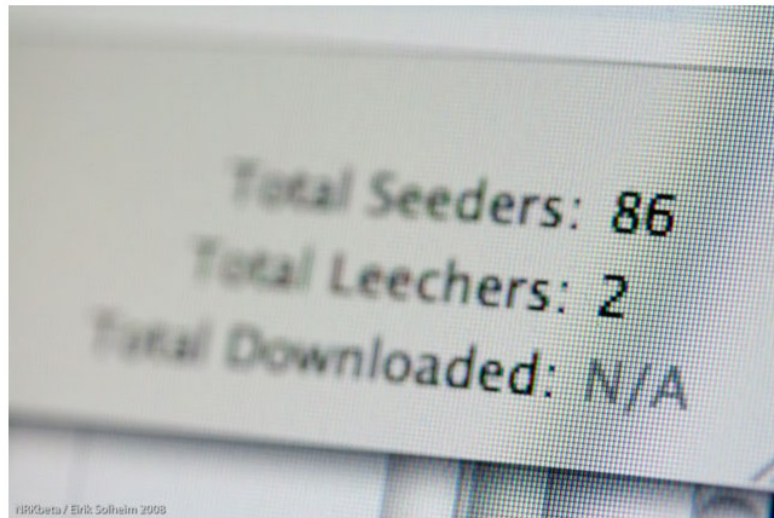
# Per què ?

## "Six strikes" system goes live this fall, appeals to cost \$35

"Trained professionals and automated processes" will identify illegal downloads.

by Cyrus Farivar - Oct 18, 2012 4:02 pm UTC

INTELLECTUAL PROPERTY 184



VR/beta / Erik Solheim 2008

mrkbeta

The Center for Copyright Information has revealed more details about its "six strikes" system, which it calls the Copyright Alert System (CAS). In a [blog post](#) published Thursday morning, the program's head, Jill Lesser, announced that the CAS "will begin in the coming weeks."

## TorrentFreak

Home About  
Contact

The place where **breaking news**, BitTorrent and copyright collide

Subscribe via RSS    @ Subscribe via Email    + Tip Us Off!

## French 3 Strikes: Court Fines First File-Sharer, Even Though He's Innocent

enigmax

September 13, 2012

182

hadopi

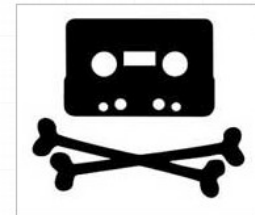
Print

It's been a long time coming but today the controversial French 'Hadopi' anti-piracy law has claimed its first scalp. After his account was connected to a series of previous infringements, a 40 year-old man was summoned to court today. Despite a third-party admitting that the music piracy in question was carried out by them and not the accused, the court still decided to fine the account holder.

For almost two years France has been running its controversial "3 strikes" mechanism to deal with the issue of online digital media piracy.

Alleged pirates are sent three warnings before being punished, giving them plenty of time to either mend their ways or take other measures to stop infringements being logged against their accounts.

Since October 2010, rightholders have identified a total of 3 million French IP addresses. Of these, Hadopi considered 1.15 million worthy of a "first strike" notice, 102,854 deserving of a second, and just 340 in line for a third.



# Per què ?

EN DIRECTO **hora 25** CADENA SER Login - Registrarse

Jueves, 6/6/2013 22:24

Inicio Programación Emisoras Noticias Deportes Gastro Blogs Podcast Vídeos Lo más

España Internacional Sociedad Tecnología Economía Cultura Gente TV y medios Deportes

## Google y Facebook rechazaron identificar a los convocantes del 25-S fuera de la Justicia

PILAR VELASCO 03-10-2012

La Audiencia Nacional solicitó los datos personales y los dispositivos desde donde se estaban utilizando los correos electrónicos habilitados para organizar la convocatoria del 25-S. Google y Facebook facilitaron a la Policía más de 50 IPs de ordenadores, es decir la clave numérica que identifica el dispositivo, además de un número de móvil asociado a uno de los correos.

EL PAÍS PORTADA INTERNACIONAL

## CATALUÑA

▶ ESTÁ PASANDO Consulta catalana 2014 Método 3 Hospital Sant Pau de Barcelona

## Los Mossos detienen a cinco anarquistas de Bandera Negra por terrorismo

- La Audiencia Nacional ordenó el registro de
- La policía acusa al grupo anarquista de acc

REBECA CARRANCO / FERNANDO J. PÉREZ | I

Italia y Grecia, lo que explicaría también que este caso lo coordine la Audiencia Nacional. Los cinco detenidos pasarán a disposición del magistrado Pedraz el viernes.

La Audiencia además es la competente en materia de terrorismo. Uno de los delitos que se les imputa es el enaltecimiento del mismo. Según Catalunya Ràdio, uno de los detenidos hizo comentarios violentos en su Facebook. También son habituales en este tipo de grupos la distribución de documentos donde se defiende la violencia como una forma legítima de combatir el capitalismo.



# Per què ?

EL PAÍS

PORTADA INTERNACIONAL POLÍ

SOCIEDAD

VIDA & ARTES EDUCACIÓN SALUD CIENCIA MEDIO AMBIENTE IGUALDAD CONSUMO

▶ ESTÁ PASANDO > Aborto Selectividad Caso Celador de Olot Pobreza Caso Maestro

## Jueces y fiscales progresistas cuestionan que la policía use troyanos

- Gallardón afirma que se trata de "propuestas" abiertas al "debate público"
- PSOE e IU califican de atropello la iniciativa que plantea el borrador
- [La propuesta](#)

MANUEL ALTOZANO / MÓNICA CEBERIO BELAZA | Madrid | 5 JUN 2013 - 00:04 CET





# Per què ?

Microservos

Ecología

Fotografía

Juegos

Ciencia


Internet

Aviones

Humor/WTF



microservos

Acerca de | Contactar | Archivos · Categorías · Buscar |  RSS | | ¡Salta!

[EXOPLANET, UN CATÁLOGO DE PLA](#)

## Código Penal Gallardón, criminalizando media Internet para proteger la propiedad intelectual

Por si la denostada [Ley Lassalle](#) nos parecía poco, el gobierno sigue adelante con su empeño de criminalizar los enlaces y cualquier dispositivo o software que permita saltarse un sistema anti copia, aunque sea para ejercer nuestro derecho a copia privada, derecho que ya queda enormemente restringido por la Ley Lassalle.



[www.CryptoParty.cat](http://www.CryptoParty.cat) @CryptoPartyBCN



# Per què ?

- Per protegir les nostres dades personals i dispositius en cas de pèrdua o robatori
- Per controlar una mica millor la nostra petjada digital
- Per a que siguem nosaltres qui controla els dispositius i no al revés
- Per decidir quan, què i com volem comunicar al món i fer-ho més conscientment
- *Your entire life is online and it might be used against you*
  - <https://www.youtube.com/watch?&v=F7pYHN9iC9I>





# Objectius

- Conèixer algunes de les eines que podem fer servir per protegir la nostra informació i la nostra intimitat a Internet
  - Conèixer la nostra petjada digital involuntària
  - Saber com protegir, una mica més, les nostres dades
- Instal·lar-les en el nostre dispositiu (ordinador, tauleta, mòbil)
- Aprendre a fer-les servir en el dia a dia
- Poder explicar-ho i ajudar a amics, coneguts i saludats
- Augmentarem la nostra privadesa, però no serem anònims
- No ens fem responsables del mal ús de les eines presentades



# Idees

- Això és un taller, no una presentació. Participeu i fem-ho plegats
- L'objectiu és aprendre, instal·lar i usar
- Pregunteu en cas de qualsevol dubte
- Ajudar els altres és la millor manera de comprovar si ho hem entès
  
- Atenció: La seguretat i privadesa canvien contínuament, el que hem escrit aquí pot ser obsolet quan ho llegiu



# Principis

- *Murphy* no dorm. Mai
- Que siguis paranoic no vol dir que no et segueixin
- Si no pagues pel servei, tu ets el producte
- *"There is no delete button on your digital identity"*  
- Eric Schmidt (Google)
- La seguretat total té cost infinit
- Podem intentar millorar la nostra intimitat a un cost raonable
- Veiem-ho!

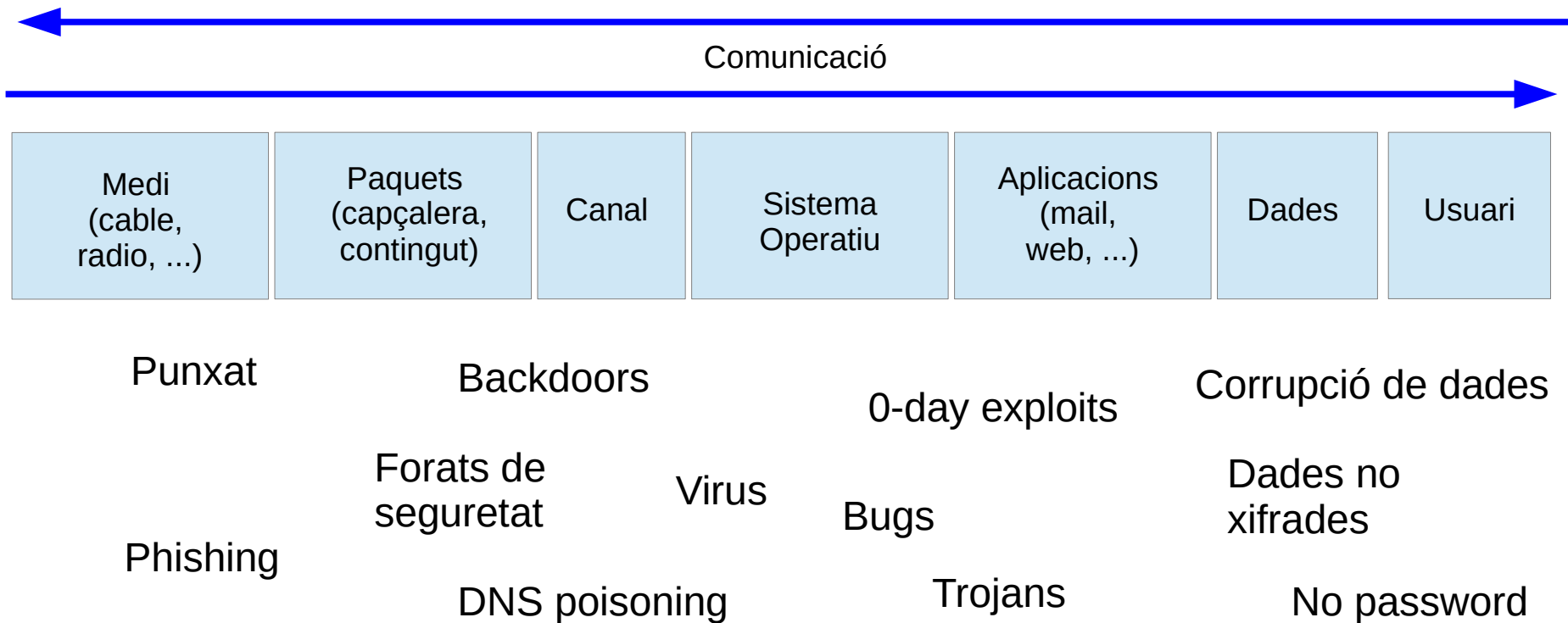


# Privadesa vs. Anonimat

- Privadesa:
  - La capacitat d'escollir què volem comunicar al món
- Anonimat:
  - La impossibilitat de que altres puguin saber qui som



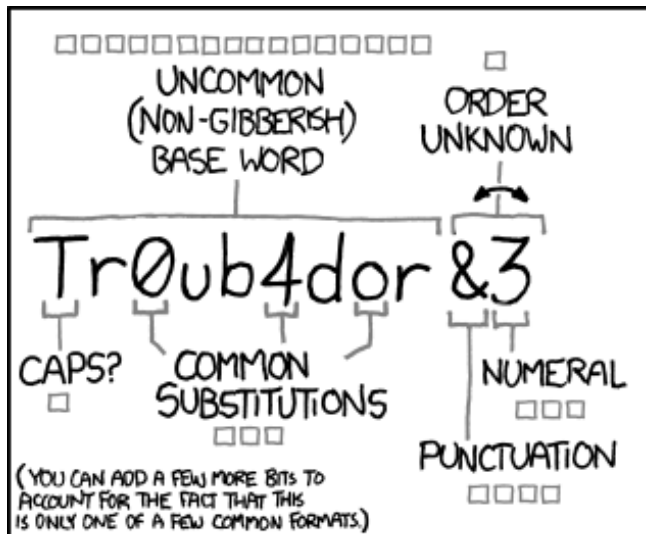
# Capes o cadena de bits a Internet



# Paraules de pas (passwords)

- Llargs (més de 15 o 20 caràcters)
  - Per exemple unint varies paraules o una frase sense sentit (amb faltes d'ortografia i altres complexitats)
- Únics (no els repetim mai)
- Secrets i no deduïbles (atenció al *doxing*)
  
- Keepass.info al rescat
  - Base de dades xifrada de users, passwords, url
  - Tingueu-ne una bona còpia de seguretat externa!





~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

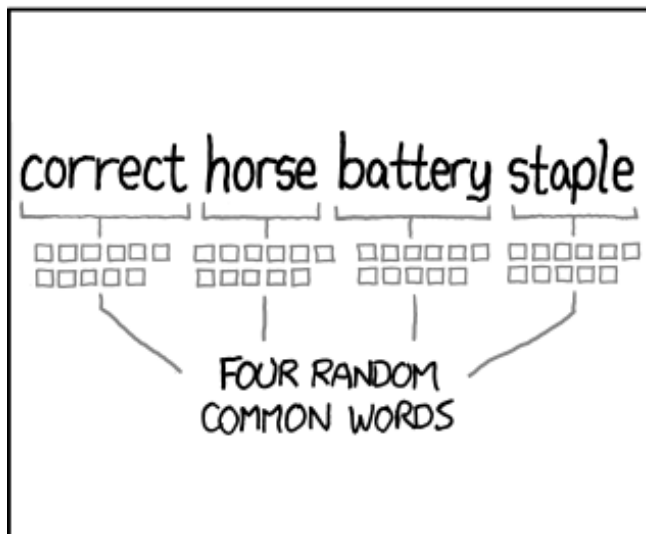
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

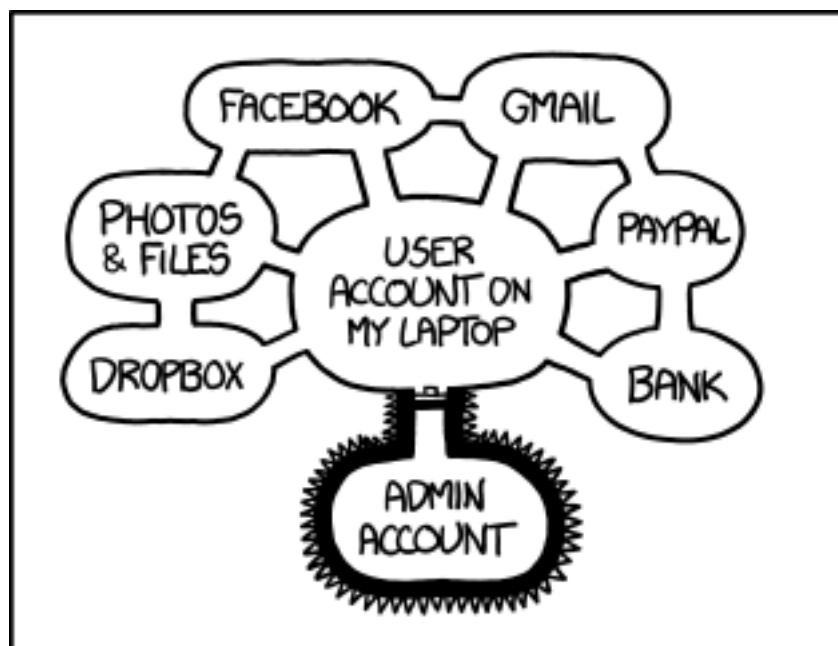
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

<http://xkcd.com/936/>





# Bloquegem pantalles si no hi ha activitat



IF SOMEONE STEALS MY LAPTOP WHILE I'M LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY MONEY, AND IMPERSONATE ME TO MY FRIENDS, BUT AT LEAST THEY CAN'T INSTALL DRIVERS WITHOUT MY PERMISSION.

<http://xkcd.com/1200>



# Sistemes operatius

- No podem saber què fa una caixa tancada
  - Win10 connecta uns 500 cops/h a 93 IPs (MS i altres)
  - Android no s'actualitza i té versions prehistòriques
- No serveix de res protegir-se i deixar la porta oberta amb un soft que controla el dispositiu i no saps que fa
- Sigui quin sigui però, cal actualitzar-lo regularment



# Sistemes operatius

- S.O. ha de ser programari lliure
  - GNU/Linux (Ubuntu, Mint, Debian, Fedora, etc, etc, ...)
  - Qubes (màquines virtuals per a cada aplicació)
    - <https://www.qubes-os.org/>
  - Tails: **The Amnesic Incognito Live System**
    - <https://tails.boum.org/>
  - Cyanogen (mòbils) <https://cyngn.com/>
  - UbuntuPhone



# Pèrdua del dispositiu

- FindMyPhone i similars
- Per exemple: [preyproject.com](http://preyproject.com) (codi obert)
- Programes residents que es «comuniquen» amb central
- Està per veure què podem fer un cop sabem on és
- Més tranquils si tot està ben xifrat i tenim còpies seguretat



# El meu mòbil

- És un dispositiu de seguiment (connexió a torres telecom)
  - metadades, geolocalització, sincronia
- Apaguem WiFi i Bluetooth si no els fem servir
- Esborrem aplicacions que no usem
- Verifiquem permisos d'apps en instal·lació i actualització
- Protegim accés amb codi, pin o password
- Xifrem memòria i tarja SD (o vigilar què hi tenim)
- Fem còpies de seguretat externes (xifrades?)



# El meu mòbil

- Tapar càmera (i micro ?)
- S.O: poques opcions i tancats; poques actualitzacions.
  - Ara Cyanogen --> <https://cyngn.com/> i UbuntuPhone
- Deshabilitar descàrrega de Stores desconegudes
- Firefox + els consells específics; Orbot (Tor per a mòbils)
- VPN – Xarxa Privada Virtual
- Signal
- Atenció amb el xifrat de Telegram i Whatsapp



# Fitxers xifrats

- Xifreu la partició d'usuari (Win,Mac,GNU/Linux)
  - Evitar accés a info en cas de robatori o pèrdua
- Xifrar USB, fitxers, disc al núvol, etc
- TrueCrypt 7.1a (<https://db.tt/qYSg0exJ>)
- VeraCrypt, però ...
- Plausible deniability
- No oblideu les claus!



fitxer.xyz

Partició  
xifrada

Partició  
oculta





# Usuari: rastre digital

- Profiling: obtenir perfil personal a partir de la petjada digital
- Doxing: recerca i comunicació d'info personal trobada a la xarxa
  - Xarxes “d'amics” i què diem o ens agrada FB, Twitter, LinkedIn, ...
  - Feu Egosurfing: cerqueu-vos per nom, cognom, DNI, escola, club, fotos, ...
  - Cookies, cross-scripting, sessions obertes, ... (on naveguem, què mirem)
  - Com ens mostren el que “creuen” que ens interessa <http://dontbubble.us/>
  - Atenció a seguiment 3G, telefonia, IP, ...  
Desactiveu WiFi i Bluetooth si no els feu servir
  - Tapeu les webcam (i micros) si no els feu servir
  - Useu un email diferent només per a recuperar comptes o pwds



# Navegadors - activitat

- Reduir el “profiling” i les dades que es passen entre les web
  - provem add-on LightBeam per a veure-ho
- Packets, cookies, sessions, https, user agent, adreça IP, DNS
- Llegim <http://dontbubble.us>
- Els navegadors deixen a cada web una petjada molt específica:
  - <https://panopticlick.eff.org/>
  - <http://ipcheck.info>



# Navegadors - cercadors

- Reduïm el “*profiling*” i les dades que es passen entre les webs
  - provem add-on LightBeam per a veure-ho
- Llegim <http://dontbubble.us>
- Hi ha cercadors que no són tan invasius
- StartPage.com DuckDuckGo.com Search.Disconnect.me

startpage



2εαrτcη bηvατeίλ ηsίng λoηc ταvοιτe 2εαrτcη eηgίηe·  
**DISCONNECT** 2εαrτcη



# Navegadors - eina

- Firefox (codi obert)
- Deshabilitem cookies de 3ers; no desem passwords (KeePass!)
- Desactivem Falsh i Java
- uBlock Origin – anuncis amb/i malware
- Ghostery – cookies, trackers, beamers
- NoScript – des/habilita execució automàtica de JavaScript
- https everywhere – força https sempre que es pugui
- Desactivar el REFERER (about:config)



# Antivirus i malware

- Antivirus actualitzats (també per a Mac i GNU/Linux)
  - <http://www.av-comparatives.org/dynamic-tests/>
  - <https://help.ubuntu.com/community/Antivirus>
- Desactivem Java i Flash al Navegador
  - I només donar-los permís quan ens interressi






# Tor - Orbot

- <https://torproject.com>
- 3en1: és un navegador, un encaminador (router) o un servei
- Navegador = Firefox més blindat. Activeu però NoScript
- Navegació passa, xifrada, per 3 nodes intermedis abans de sortir a Internet.
- Tor per-se NO et fa anònim però protegeix molt la teva navegació
- Opcionalment es pot navegar dins l'espai .onion
  - scihub22266oqcxt.onion
  - facebookcorewwi.onion
  - expvqqiv2z5ekf47.onion --> Decoded Legal (advocats)

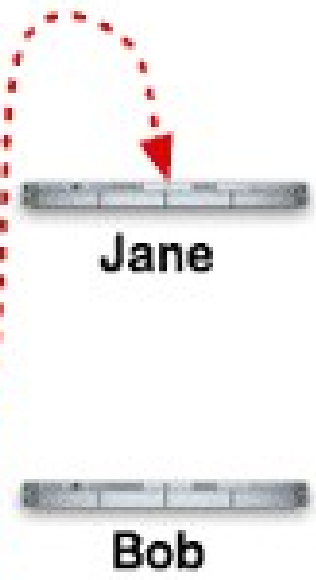
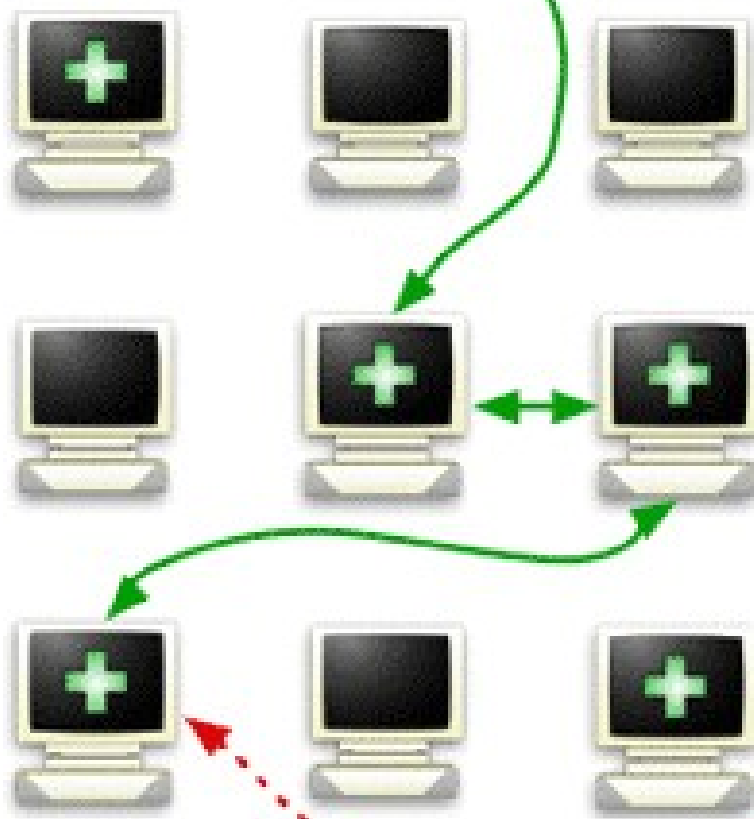


# How Tor Works: 3

-  Tor node
-  unencrypted link
-  encrypted link



Alice



Jane

Bob

Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, **green links** are encrypted, **red links** are in the clear.



Dave

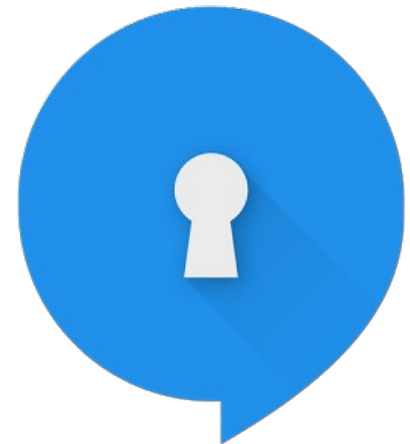
Font: Tor project





# Xat xifrat

- Signal - <https://whispersystems.org/>
- Crypto.cat - <https://crypto.cat>
- Tor messenger (beta)
- OTR – Off The Record



# Correu xifrat

- El correu-e és de fet una postal-e (no hi ha sobre!)
- El protegim amb xifrat de claus asimètriques
- Subject, From, To, CC, CCO, Data no es xifren
- Generem el parell clau pública, clau privada (4096 bits)
- Desem bé la clau privada, donem la clau pública
  - Key ID 0x05913335
  - B3F0 50EE CFD3 5132 45C5 CC11 8456 F4E0 0591 3335
  - És la clau (pública) de: abc@cryptoparty.cat

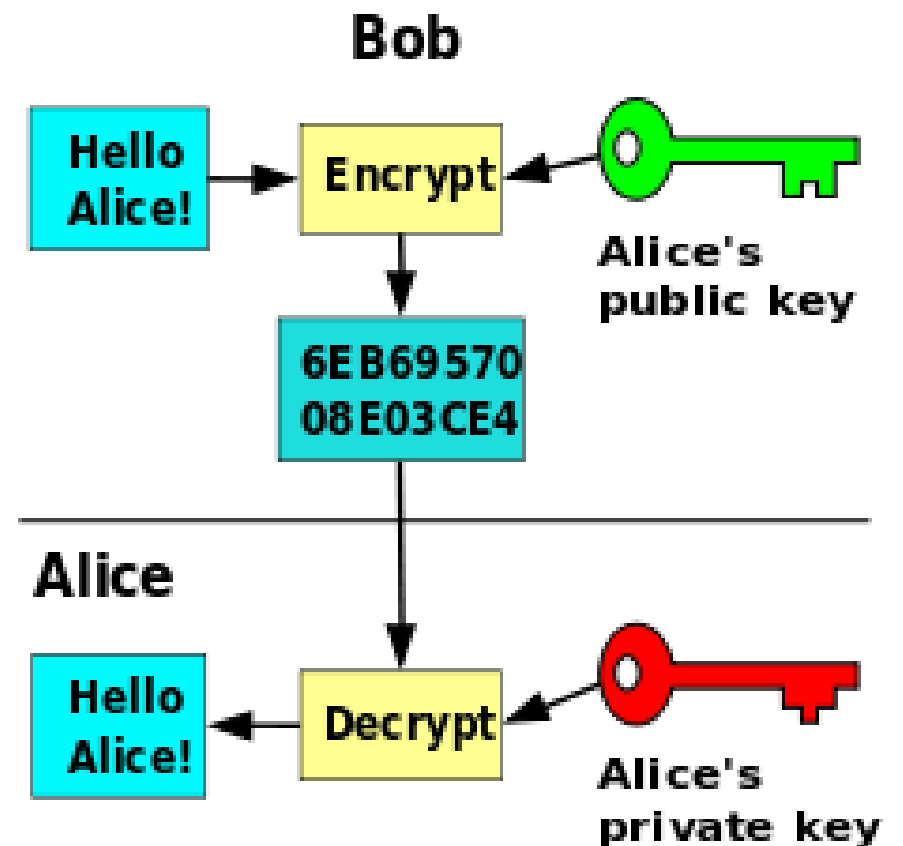
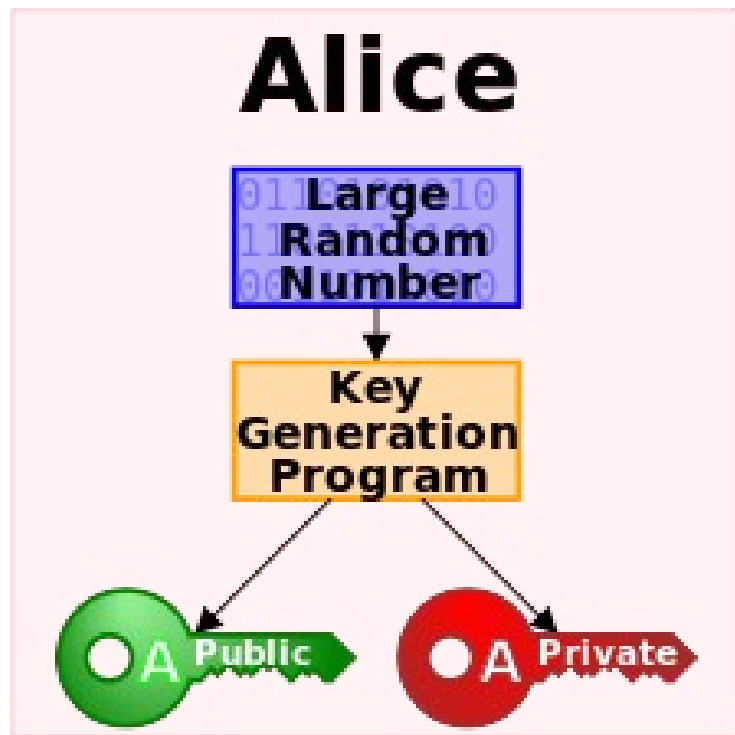


# Correu xifrat

- Generem parell (clau-pública, clau-privada)
- Desem bé la clau privada
- Generem la clau de revocació del parell public-privat
- Desem bé la clau de revocació
- Distribuïm la nostra clau pública
- Si volem signar ho fem amb la nostra clau privada
- Si volem xifrar ho fem amb la pública del destinatari
- Només es pot desxifrar amb la clau privada pròpia



# Correu xifrat



Font: Wikipedia



# Correu xifrat

- PGP, GPG, gpg4win.org (Windows)
- Thunderbird + EnigMail
- Webmail + Mailvelope
  
- Repartir la clau pública:
  - Repositoris de claus
  - Signatura al peu dels correus



# Sessió: Correu electrònic

- Es transmet sempre “en obert” !
  - El contingut pot ser llegit molt fàcilment
  - Es pot xifrar correu (text): Enigmail + Thunderbird
  - Però només xifra el text, no xifra To:, CC:, CCO:, ni Tema
- Mail efímers: protonmail.ch, riseup.net, ...
- Creeu un email per donar-vos d'alta a llocs de poca confiança
  - 10minutemail, guerrillamail, ...
  - No doneu dades personals, inventeu-vos-les!
  - Atenció no el feu servir de contacte per a recuperar mails



# DNS

- Resolvers DNS - conversió de domini a adreça IP
  - El teu DNS sap quines pàgines visites
  - Venen els ISP aquestes dades (agregades?) a 3rs?
- DNSSEC – resolució segura
  - L'ha d'oferir el titular del domini
  - Encripta la resolució del domini (trad. nom domini --> adreça IP)
  - Evita atacs de MiTM (man in the middle)



# DNS

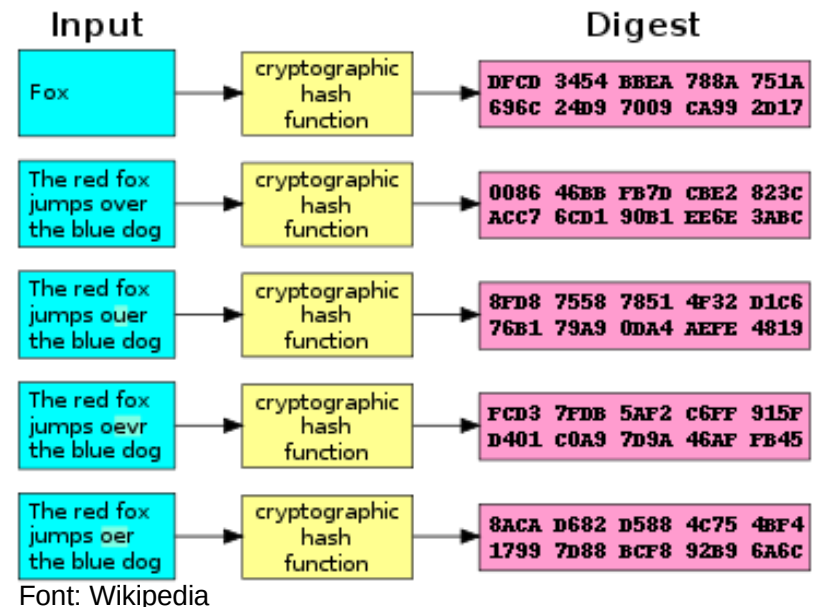
- Canvi de DNS
  - Canvi dels DNS del dispositiu o del router
  - Germany/Swiss Privacy Foundation 87.118.100.175, 94.75.228.29
  - Chaos Computer Club 213.73.91.35
  - Telecomix.org 91.191.136.152
  - El teu DNS: ex. Unbound DNS en una Raspi (eps, manteniment!)
  - DNS per a censurar continguts d'adults (control parental)
  - [https://wikileaks.org/wiki/Alternative\\_DNS](https://wikileaks.org/wiki/Alternative_DNS)





# Comprovar les descàrregues

- Signatures són els *hash* dels fitxers
  - irreversible, no-repetibles, sense col·lisions
  - map data of arbitrary size to data of fixed size.
- Serveixen per a comprovar que el que hem baixat no ha estat modificat
- Tipus: SHA1, MD5, gpg, ...



# Lectures i enllaços

- <http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm>
- <http://www.popsci.com/technology/article/2013-03/fbi-wants-watch-online-chats-they-happen>
- <http://arstechnica.com/security/2013/03/how-i-became-a-password-cracker/>
- <https://torrentfreak.com/free-access-to-dozens-of-anonymous-vpns-via-new-university-project-130324/>
- <http://www.wired.com/gadgetlab/2012/11/ff-mat-honan-password-hacker/all/>
- <http://www.cnn.com/2013/03/16/opinion/schneier-internet-surveillance/index.html>
- <http://www.elconfidencial.com/tecnologia/2013/04/15/el-trafico-de-datos-un-sector-en-auge-que-ya-mueve-millones-de-dolares-4651/>
- <http://www.elconfidencial.com/tecnologia/2013/04/08/blinda-tu-smartphone-robaran-tu-dispositivo-pero-no-tu-privacidad-4624/>
- <http://www.apd.cat/infantsijoves/>
- <http://www.crypt4you.com/>
- Youtube: "Mundo Hacker user: pvzzle"
- [Twitter.com/cryptopartybcn](https://twitter.com/cryptopartybcn)



# Conclusió

- No serem invulnerables però sí ho haurem posat més difícil
- Hem millorat la protecció de les nostres dades privades davant robatoris o intromissions
- Llegiu bé les instruccions de les aplicacions, no doneu res per evident
- Recordeu actualitzar les aplicacions i que tot pot fallar ;-)
- Esperem que pugueu replicar aquesta sessió a més persones i en altres llocs

Gràcies



# Dret de còpia i modificació

El material d'aquesta presentació és lliure i es pot fer servir sota les condicions de Creative Commons BY-NC-SA excepte els continguts trets d'altres fonts o titulars com:

- Els acudits de XKCD són del seu autor
- Les icones dels programes són dels seus autors
- Textos a articles i webs usades aquí com referència o exemple

Gràcies

