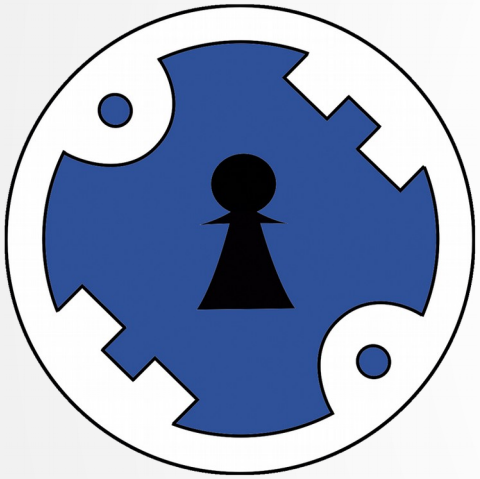
Presentación de la asociación



CRÍPTICA

Campus Nord, UPC
07/10/2015

Antes de comenzar...

- ¿Alguna vez has hecho algún comentario desafortunado?
- ¿Alguna vez has hecho algo de lo que te avergüences?
- ¿Recuerdas que es lo que colgabas en internet hace cuatro o cinco años?

Lo que subes a la red...

- ...se queda en la red

Cuando lo privado es público

Ejercicio:

- ¿Que es lo que se puede encontrar buscando vuestro nombre en google?
- … y vuestros nicks?
- … y vuestros emails?
- ¿Que encontrará alguien que busque en el histórico de vuestras publicaciones en redes sociales?

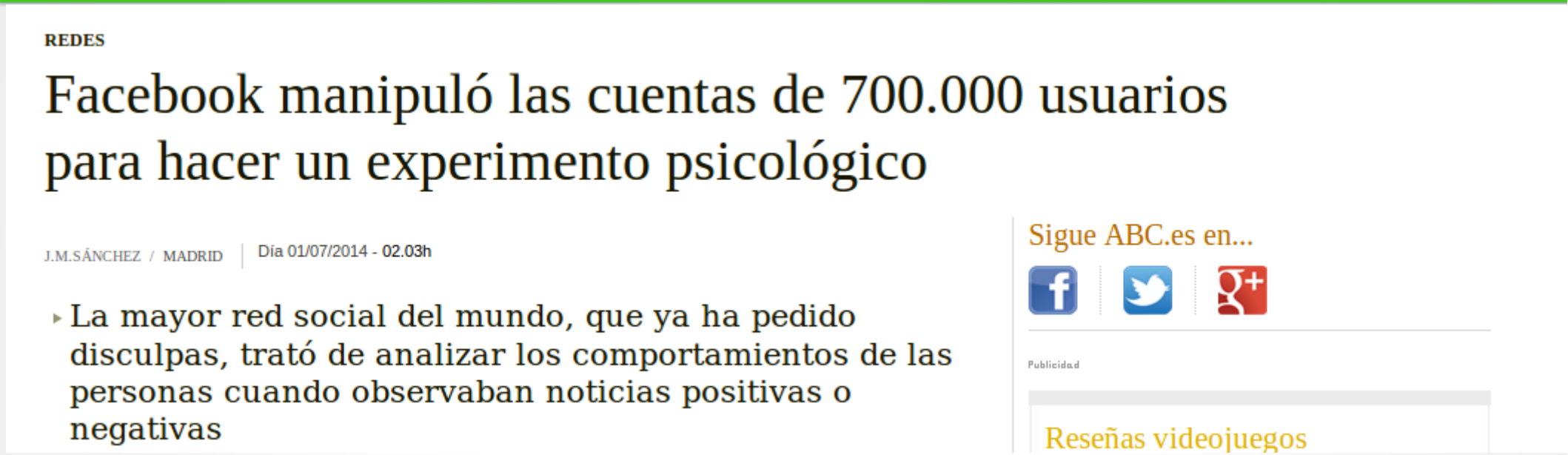
Te imaginas...

- ¿Que cuando vas por la calle alguien te fuera siguiendo, registrando todo lo que haces?
- ...que se leyese tu correo, escuchase tus conversaciones, tuviese acceso a tus documentos...
- ...supiese cuáles son tus intereses, quiénes son tus amigos, cuales son tus ideas, en que lugares en todo momento...

No hace falta mucha imaginación

- Google utiliza tus correos, tus búsquedas, las páginas que visitas, las apps que descargas, etc. para crear un perfil asociado a tu identidad.
- Facebook hace lo mismo con tus publicaciones, likes, chats, amigos e interacciones... y las páginas que visitas también.
- Apple sabe cuales son los lugares que más frecuentas y cuando los frecuentas gracias a tu iPhone.

El experimento social de Facebook



REDES

Facebook manipuló las cuentas de 700.000 usuarios para hacer un experimento psicológico

J.M.SÁNCHEZ / MADRID | Día 01/07/2014 - 02.03h

▸ La mayor red social del mundo, que ya ha pedido disculpas, trató de analizar los comportamientos de las personas cuando observaban noticias positivas o negativas

Sigue ABC.es en...

Publicidad

Reseñas videojuegos

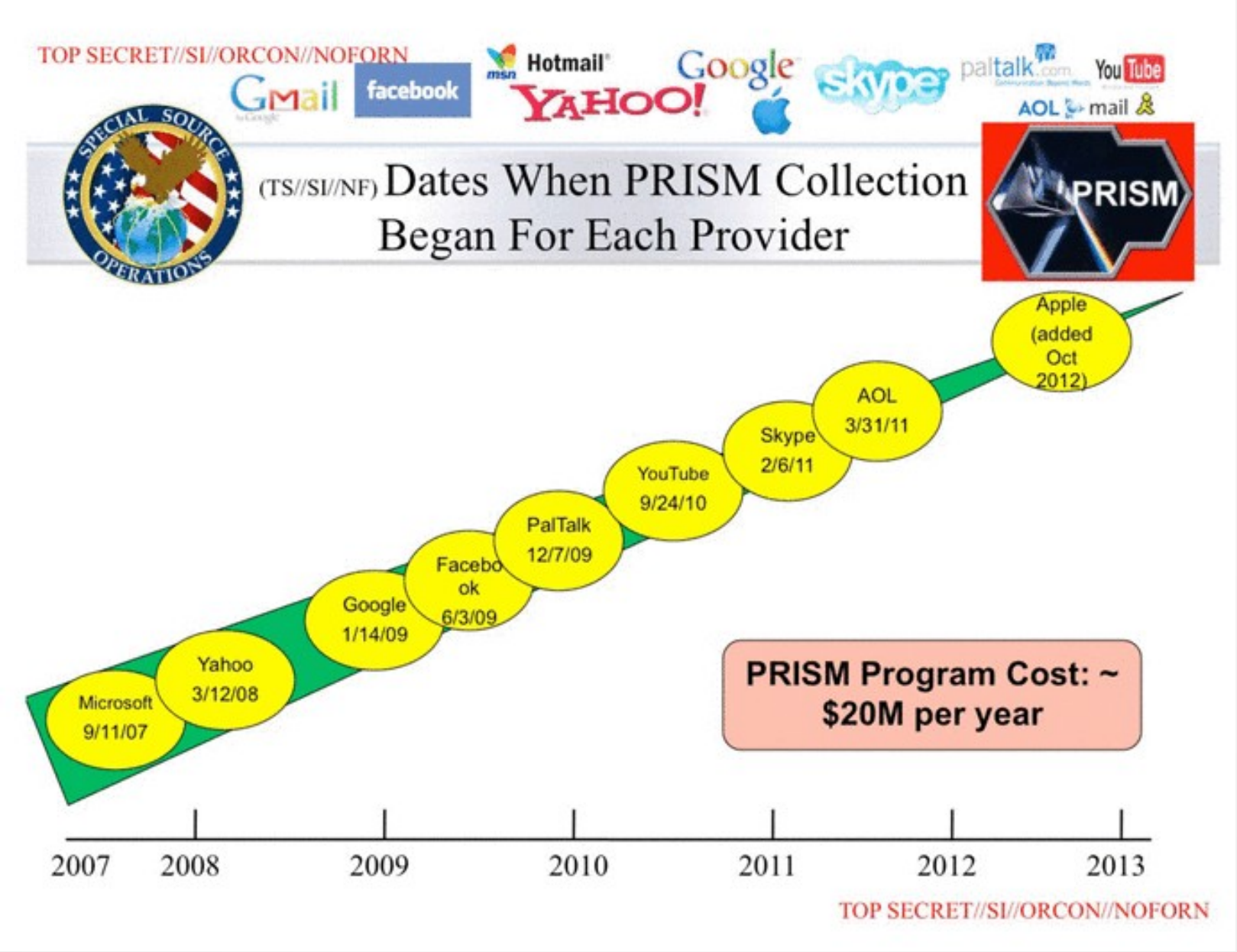
- Facebook demostró que podía influir masivamente en el estado de ánimo de sus usuarios usando filtros selectivos de contenido

Esto abre otras cuestiones

- ¿Tiene Facebook la capacidad de promover revoluciones en un país enemigo de EEUU, promocionando el descontento?
- ¿Tiene la capacidad de promover a un candidato a unas elecciones, por encima de otro?

Edward Snowden

PRISM


TOP SECRET//SI//ORCON//NOFORN
Gmail
facebook
Hotmail
YAHOO!
Google
skype
paltalk.com
YouTube
AOL mail
SPECIAL SOURCE OPERATIONS
(TS//SI//NF) Dates When PRISM Collection Began For Each Provider
PRISM
Microsoft 9/11/07
Yahoo 3/12/08
Google 1/14/09
Facebook 6/3/09
PalTalk 12/7/09
YouTube 9/24/10
Skype 2/6/11
AOL 3/31/11
Apple (added Oct 2012)
PRISM Program Cost: ~ $20M per year
2007
2008
2009
2010
2011
2012
2013
TOP SECRET//SI//ORCON//NOFORN

Nada a esconder

- “No tengo nada que esconder”
  - Idea errónea: Solo los “malos” tienen cosas que esconder
  - Idea escondida: Si eres complaciente con los poderosos, no tienes nada que esconder
  - Periodistas, activistas y disidentes tienen motivos legítimos para esconder información.
  - Incluso si no eres uno de ellos, no sabes qué serás mañana

La privacidad: Sentido clásico

- ¿Por que usas un pestillo en el baño?
- ¿Vivirías en una casa de cristal?
- ¿Me dejarías conocer tus problemas familiares?
- ¿Me dejarías leer todos tus correos?

Art. 12 de la Declaración Universal de los Derechos Humanos
Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra y su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Una visión actual de la privacidad

- Privacidad de la persona
- Privacidad de comportamiento y acción
- Privacidad de comunicaciones
- Privacidad de datos e imagen
- Privacidad de pensamientos y sentimientos
- Privacidad de localización y espacio
- Privacidad de asociación

¿De dónde sale Críptica?

Objetivos y medios

- Promover hábitos y herramientas que protejan la confidencialidad y el anonimato
  - Talleres, manuales, artículos
- Concienciar a la sociedad sobre la importancia de la privacidad
  - Charlas, artículos, campañas
- Crear una comunidad activa que pueda aportar al campo de la privacidad en las TIC
  - Contribuir a proyectos, crear nuevos...

Eines i criteri

- Open source
  - Ens permet estudiar el funcionament del programari per a assegurar-nos que no hi ha funcionalitats malicioses.
- Us de la criptografia
  - Permet protegir la informació usant claus i contrassenyes. S'usen algorismes publics i estandards que han estat verificats per la comunitat durant anys.
- Comunicacions: xifrat punt a punt
  - Els missatges es xifren abans de sortir del dispositiu del remitent i es desxifren al arribar al dispositiu del destinatari: els servidors intermitjos no poden veure res.
- Punts positius:
  - Sistemes descentralitzats: són més robustos a atacs i no depenen de servidors que podrien ser d'una companyia amb interessos econòmics incompatibles amb la llibertat de l'usuari.

Llista d'eines

Comunicación

- Cryptocat
- Tox
- Ricochet
- Pond
- OTR (Pidgin)

Móvil

- TextSecure / Signal
- RedPhone
- ChatSecure

Anonimato / Redes distribuidas anónimas

- Tor / Tor Browser
- FreeNet
- I2P
- RetroShare

Cifrado

- LUKS
- VeraCrypt
- GnuPG

Gestión Passwords

- KeePassX

Plugins navegador

- HTTPS-Everywhere
- Privacy Badger
- uBlock

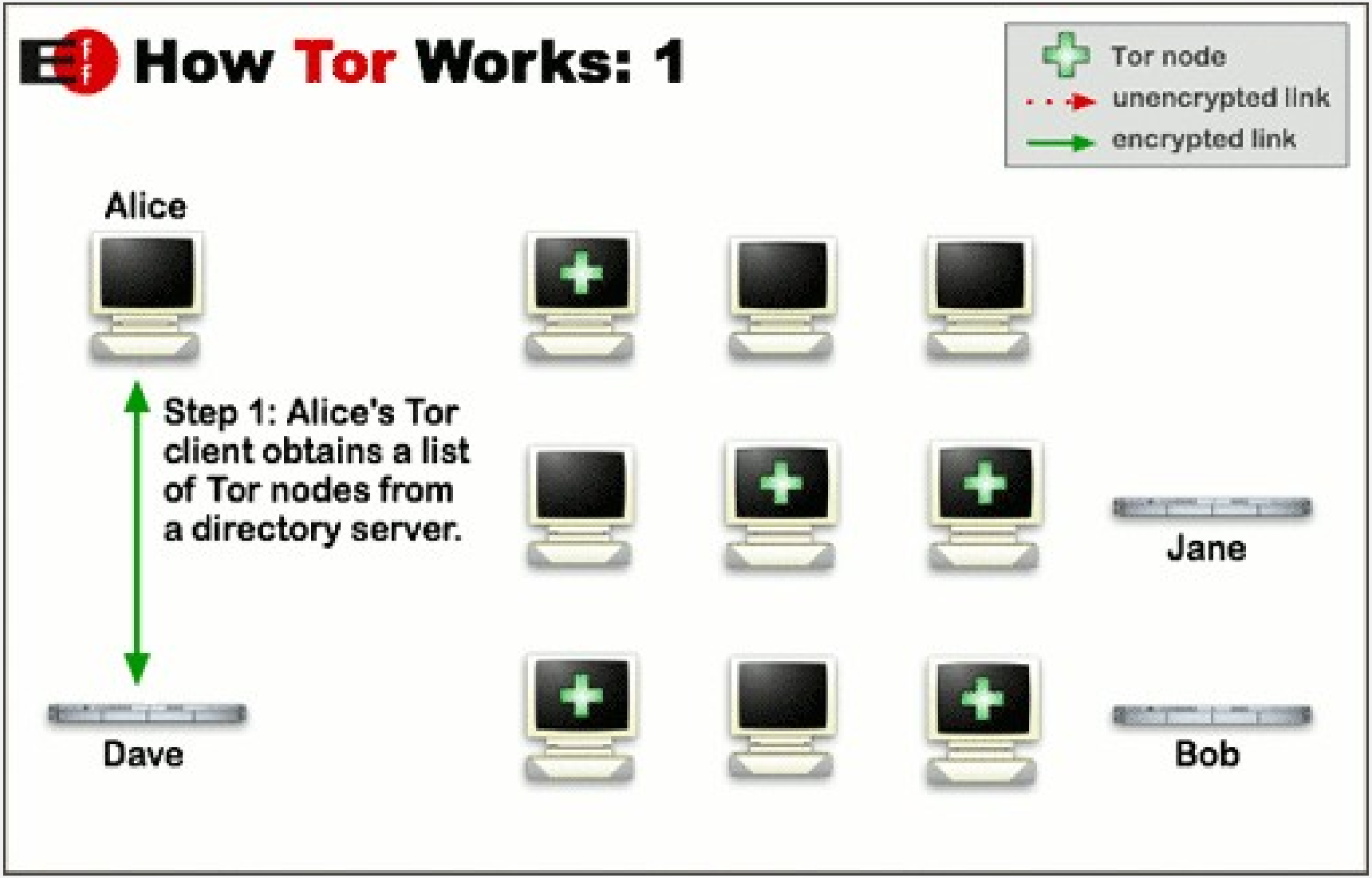
Otros

- Tails

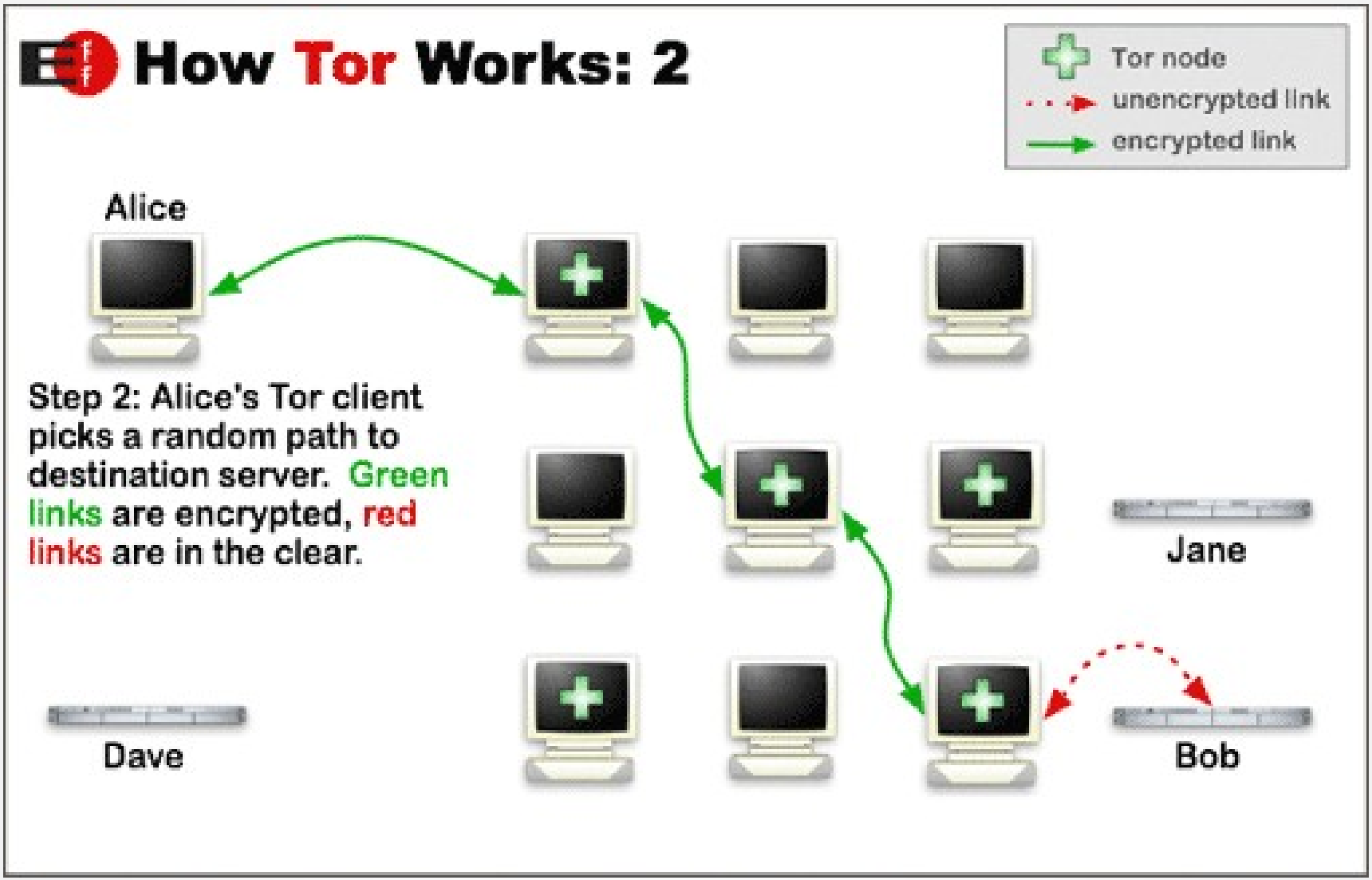
Tor

- Navegar per internet sense ser vigilat (anònimament)
  - Mantenir control sobre la privacitat.
- Eludir bloquejos d'Internet
  - Derrotar la censura.
- TorBrowser: Navegació web anònima; evita seguiment.
- Cap node de la red pot relacionar l'usuari (IP) amb el destí de la comunicació
  - Privacitat per disseny.
- Els criminals que volen saltar-se la llei tenen eines més eficients.
- Per a activistes, periodistes, residents en paisos amb censura, usuaris que desitjen privacitat, etc.

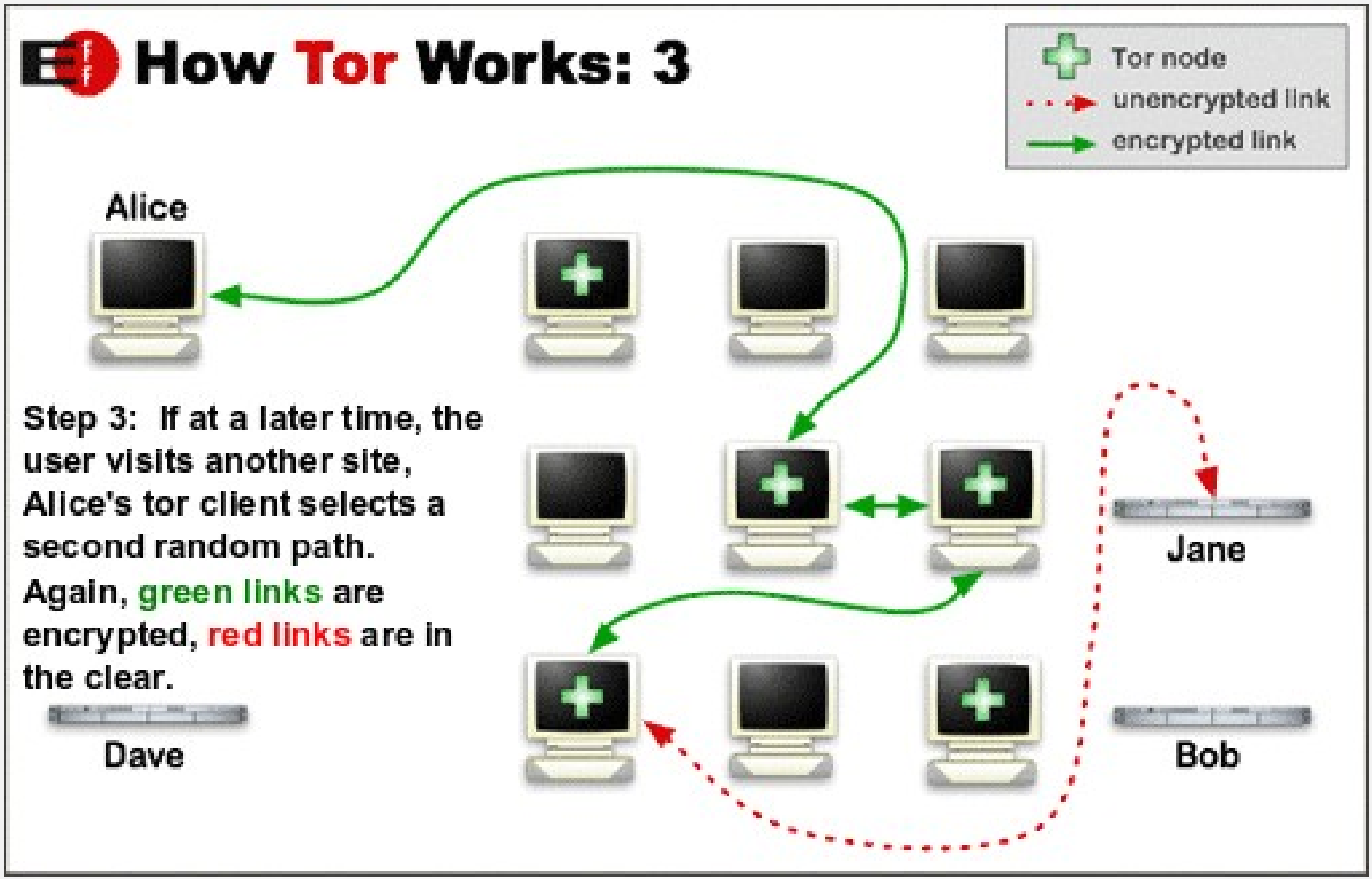
Tor - Funcionament



Tor - Funcionament



Tor - Funcionament



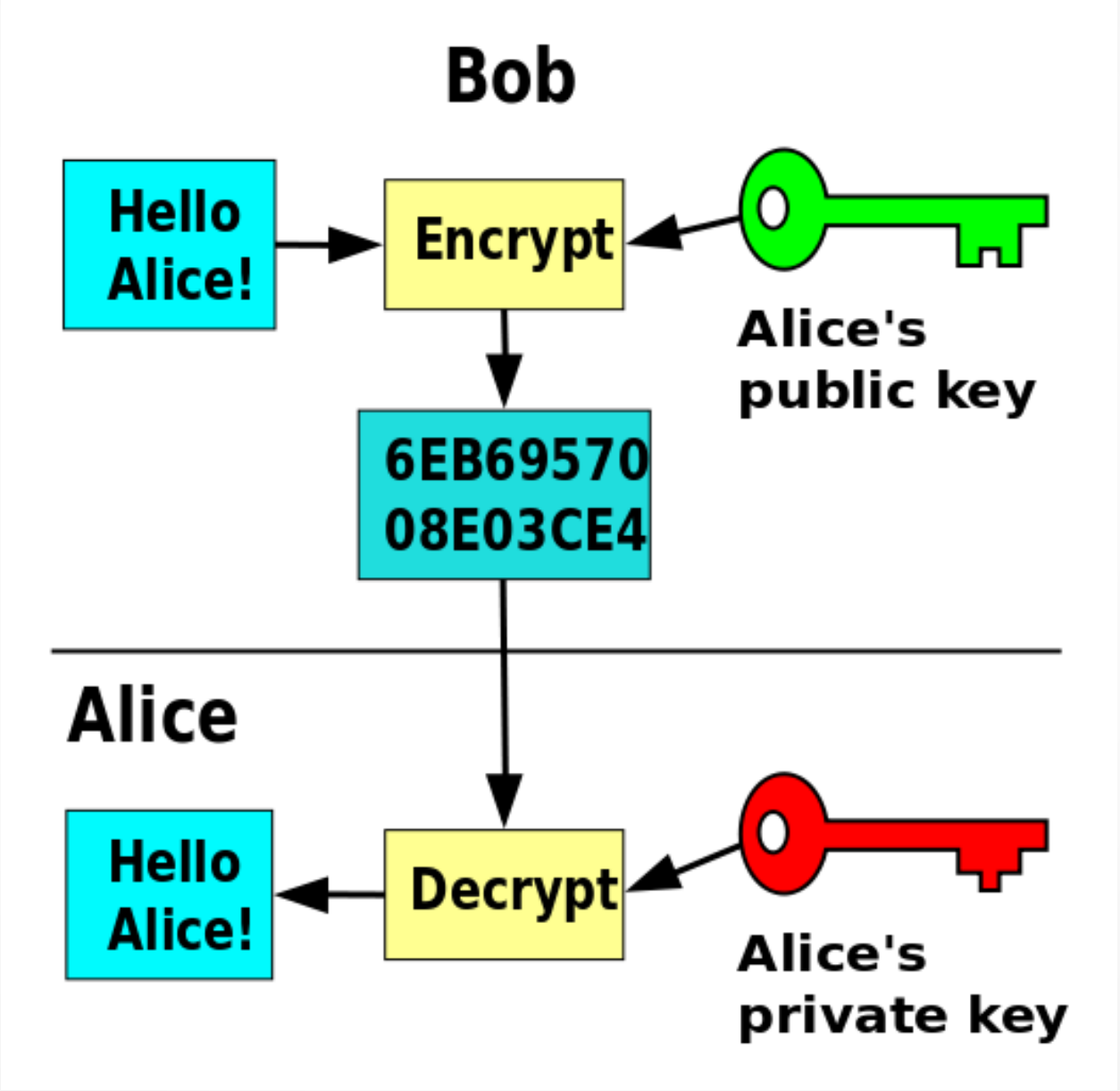
Tor - enllaços

- https://www.torproject.org/
- https://www.torproject.org/about/overview.html.en
- https://www.torproject.org/docs/hidden-services.html.en
- https://people.torproject.org/~karsten/tor-brochure/tor-brochure-es.pdf

GnuPG

- Tots els teus correus electrònics poden ser llegits pel teu proveidor de correu i per les agències de vigilància.
- GnuPG et permet xifrar els correus per a que només el destinatari els pugui llegir.
- GnuPG et permet firmar els correus per a que no puguin ser modificats.
- Us de criptografia asimètrica: parells de claus (pública i privada).
- Funciona amb qualsevol proveidor de correu.

GnuPG – clau assimètrica



GnuPG

- L'Alicia es crea un parell de claus: pública i privada.
- L'Alicia es guarda la clau privada i dona la clau pública als seus amics (Bob)
- En Bob pot enviar correus a l'Alicia usant la clau pública que ha obtingut

- Un cop el correu està xifrat, només l'Alicia el podrà desxifrar.
- Si en Bob es crea un parell de claus, pot firmar el correu perquè l'Alicia pugui garantir que el correu ve d'en Bob.

GnuPG - enllaços

- https://gnupg.org/
- https://ssd.eff.org/en/module/introduction-public-key-cryptography-and-pgp

Projectes

- (31 Octubre) Taller de seguretat avançat al Free Culture Forum: Fòrum per l'accés a la cultura i el coneixement.

  http://fcforum.net

- Traducció de la documentacio de Tails al castellà i al català

  https://tails.boum.org/doc/index.en.html

- Recopilacio i creacio de material en una wiki oberta, entra i col·labora!

  https://inno.criptica.org/wiki

Funcionament de l'associació

- Newsletter
- Llista de correu (comunicació dins l'associació)
- Trobades setmanals al Omega per a provar aplicacions i aprendre entre tots.
- 1 soci, 1 vot
- Quota a discutir al febrer, quan farem una assamblea general.

Gràcies!

- Carlos Fernández <cfernandez@openmailbox.org>

  F0C5 39F9 A4C7 B0E0 08EA

  2F0E E3FA D394 0341 FB74

- Eduard Sanou <eduardsanou@openmailbox.org>

  9BC4 8EF8 08DB 91DD 158D

  559D 4FA4 57A1 8514 CC63