

Velkommen til

Cryptoparty hvad er det?

Henrik Lund Kramshøj hlik@kramse.org

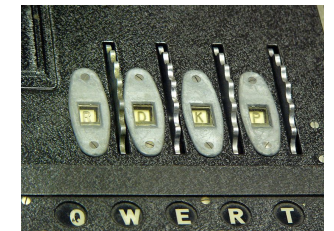


agenda



Planen for Cryptoparty 16:30 - 19:00

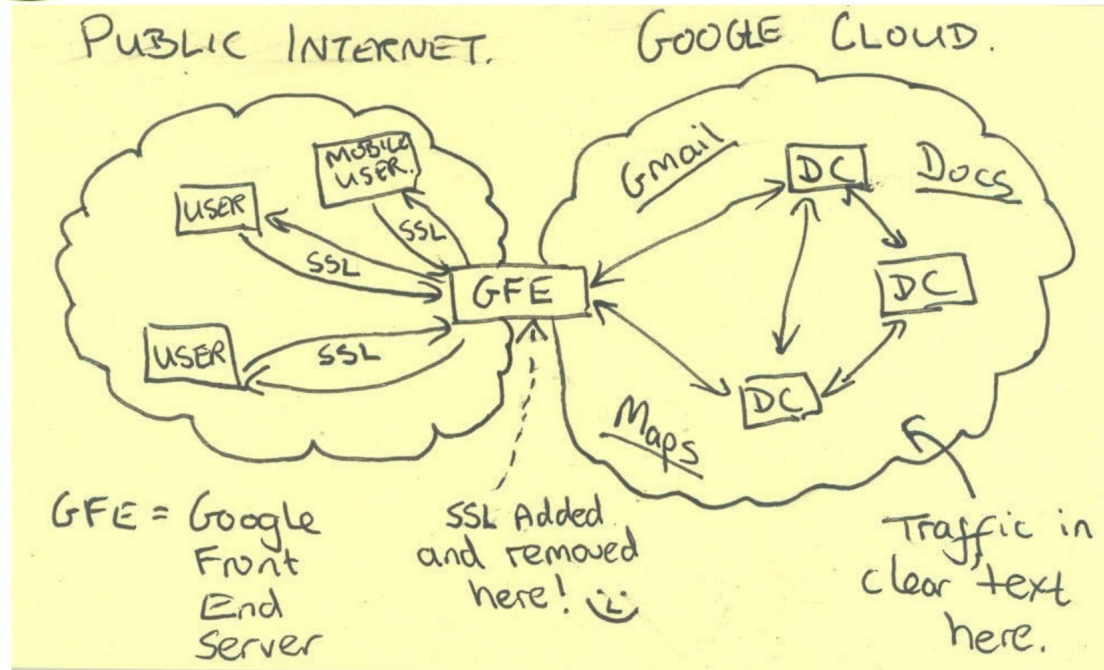
- Introduktion Peter Kofoed
- Kort introduktion cryptoparty - denne præsentation
- Minicryptoparty 10min Textsecure, Red Phone og Whispersystems Signal
- Cryptoparty opdeling i grupper, Tor, PGP



TOP SECRET//SI//NOFORN



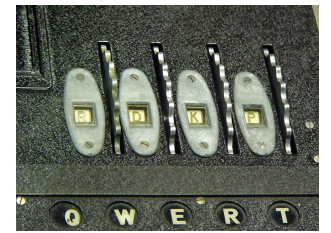
Current Efforts - Google



TOP SECRET//SI//NOFORN

SSL (encryption) added and removed here

Solidaritetskryptering



Hvorfor skal vi kryptere?

Køn

Seksualitet

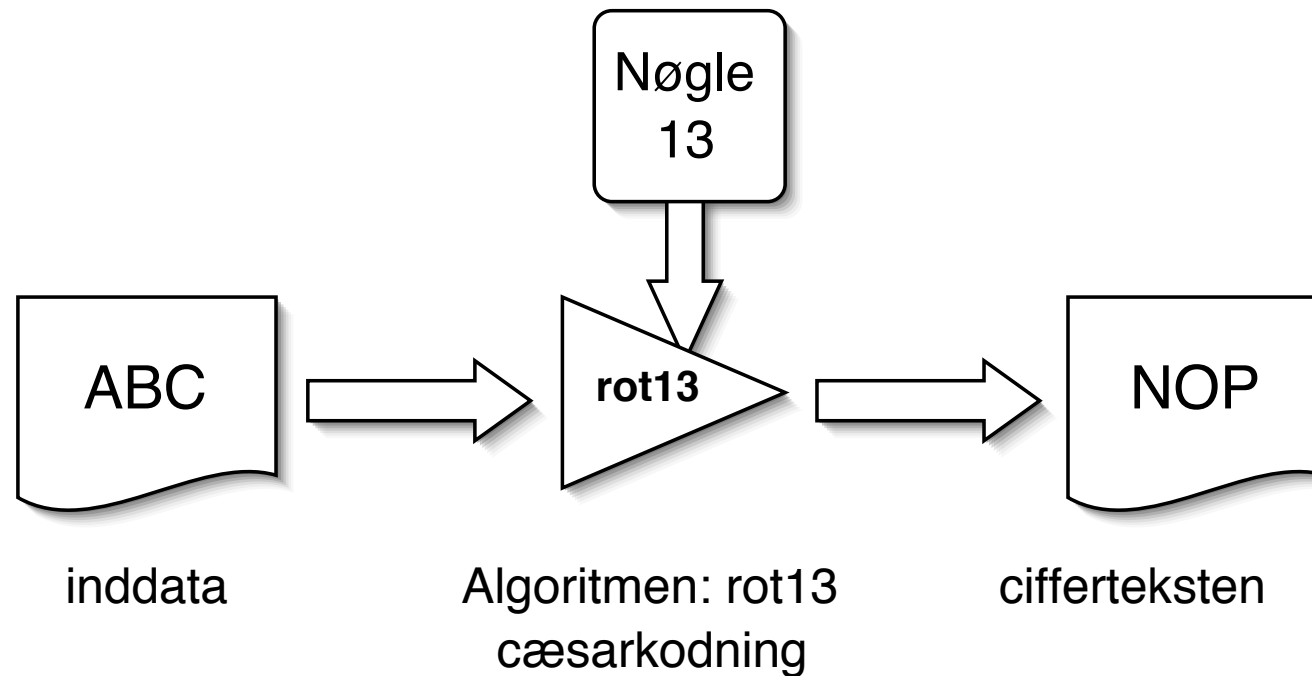
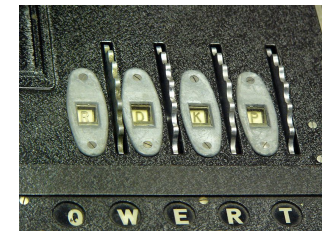
Tro religion hatecrimes

Politisk overbevisning, eller blot aktiv

Whistleblowers soldater diplomater

Du bestemmer ikke hvem der diskrimineres eller trues i andre lande

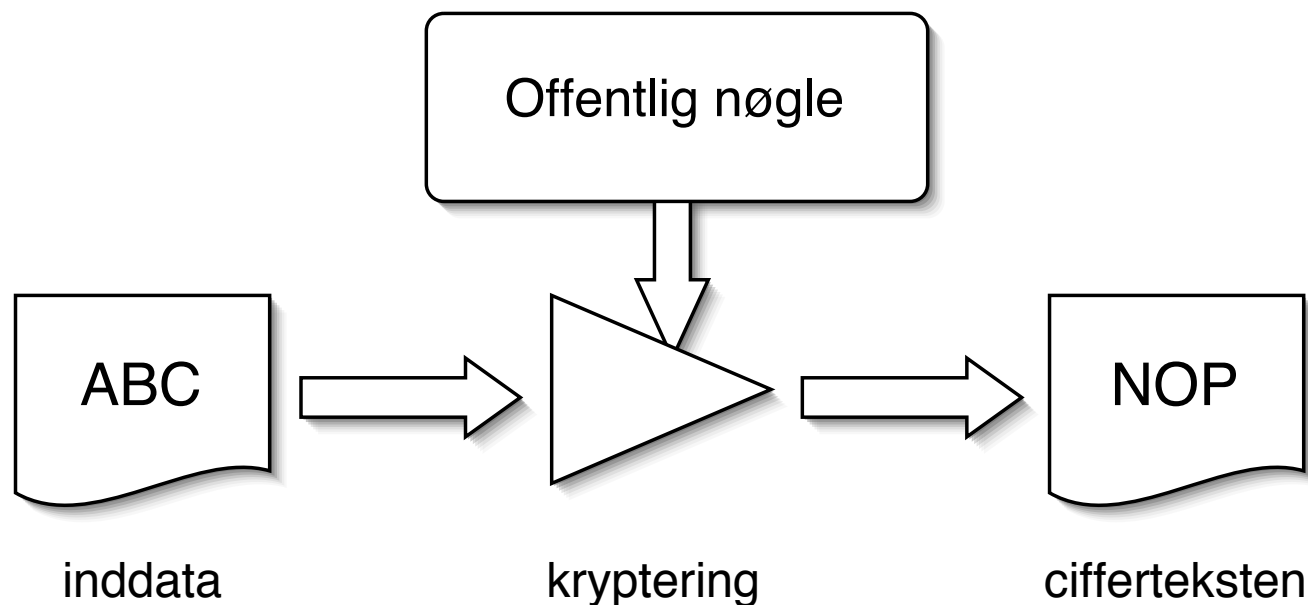
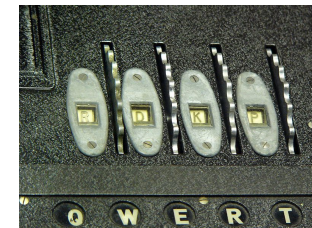
Når vi krypterer hjælper vi andre! **Solidaritetskryptering**



Kryptografi er læren om, hvordan man kan kryptere data

Kryptografi benytter algoritmer som sammen med nøgler giver en ciffertekst - der kun kan læses ved hjælp af den tilhørende nøgle

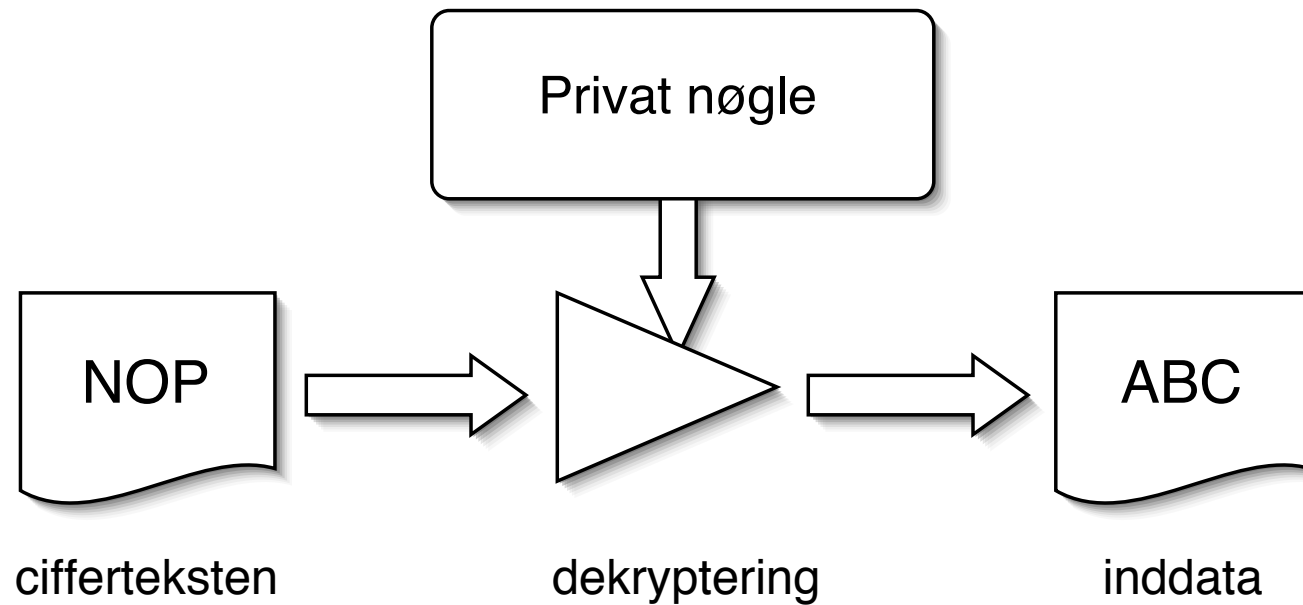
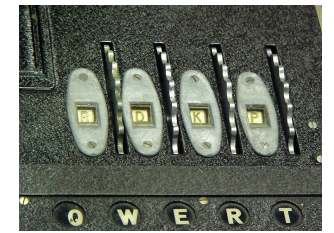
Public key kryptografi - 1



privat-nøgle kryptografi (eksempelvis AES) benyttes den samme nøgle til kryptering og dekryptering

offentlig-nøgle kryptografi (eksempelvis RSA) benytter to separate nøgler til kryptering og dekryptering

Public key kryptografi - 2

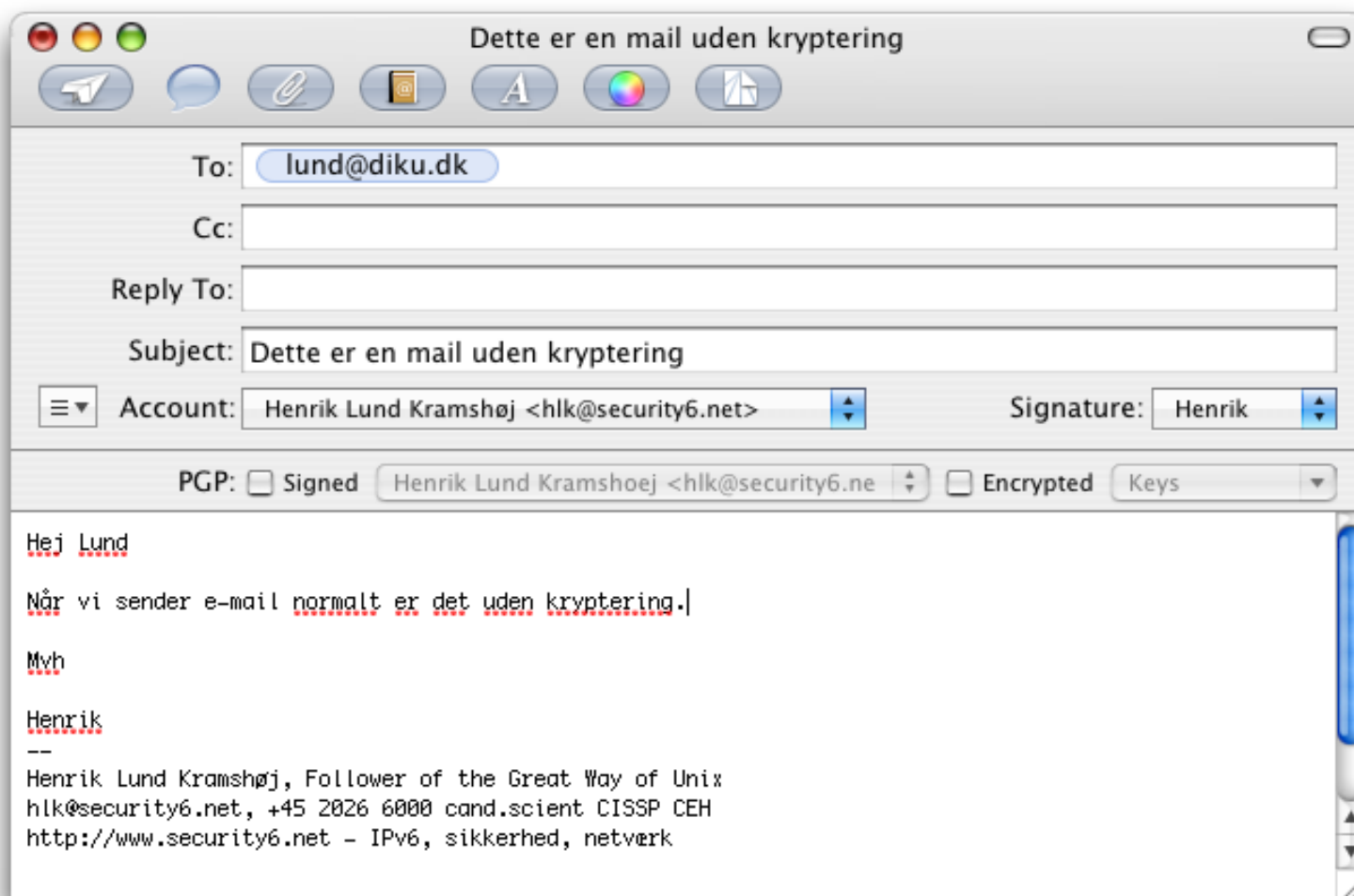
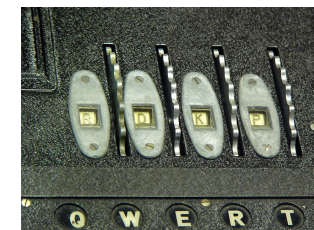


offentlig-nøgle kryptografi (eksempelvis RSA) bruger den private nøgle til at dekryptere

man kan ligeledes bruge offentlig-nøgle kryptografi til at signere dokumenter

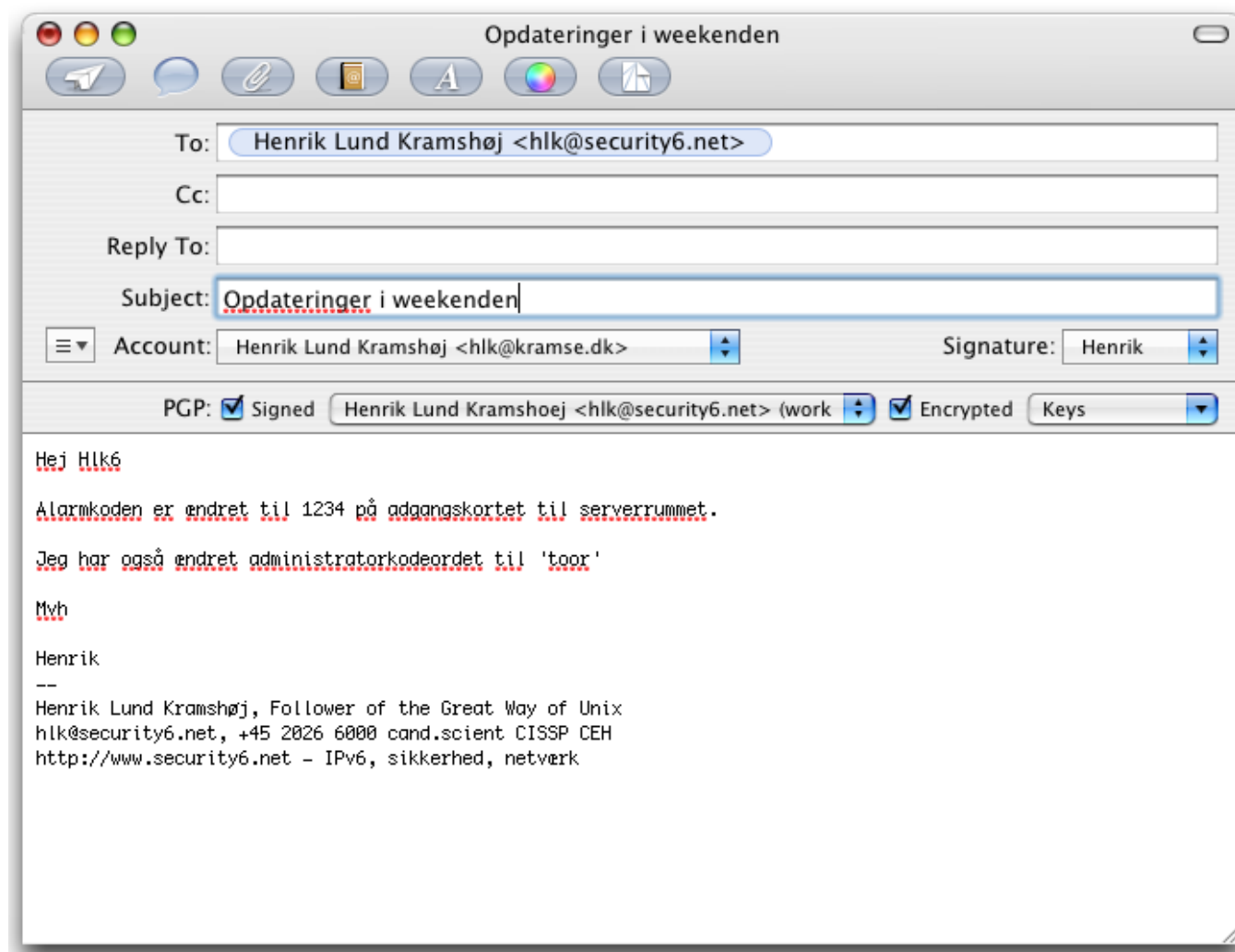
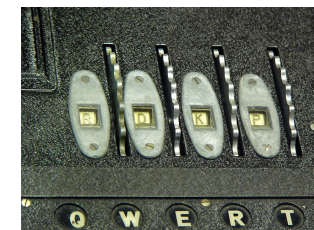
- som så verificeres med den offentlige nøgle

Email er usikkert



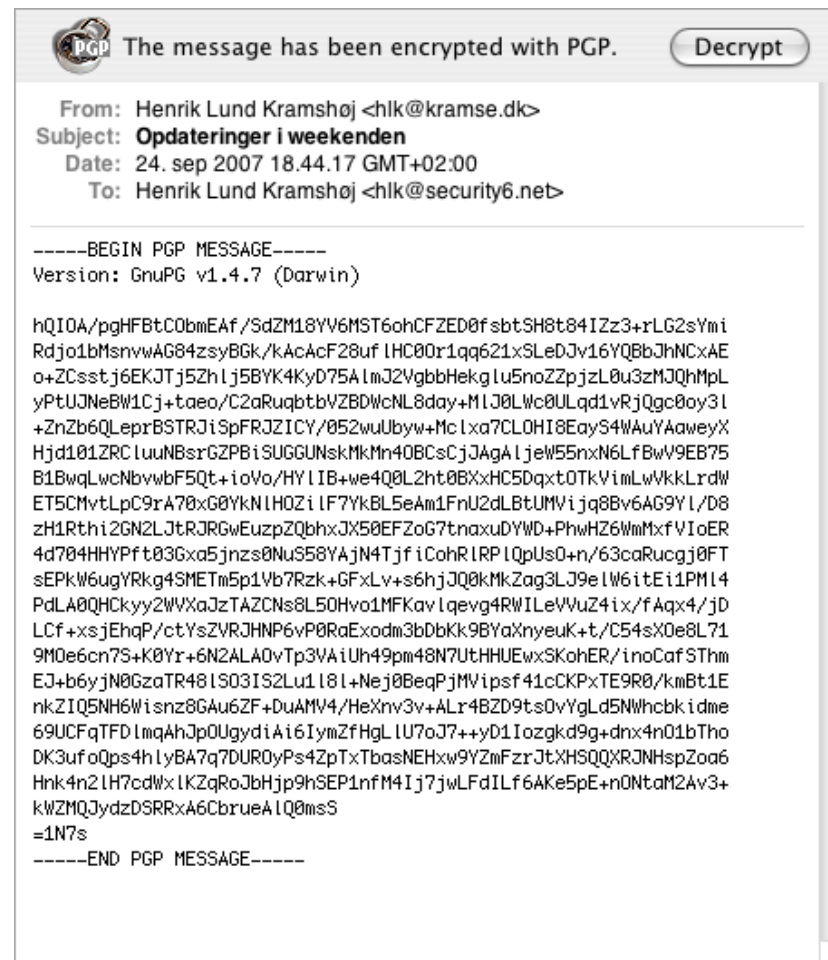
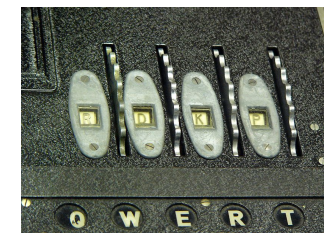
Email uden kryptering - er som et postkort

Email med kryptering - afsendelse



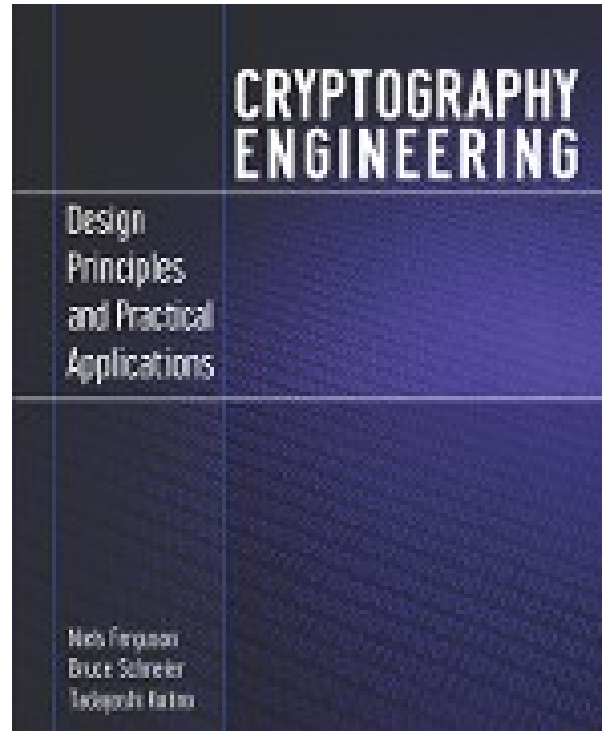
En sikker krypteret email er ikke sværere at sende

Krypteret Email under transporten



En sikker krypteret email er beskyttet undervejs

Kryptering: Cryptography Engineering

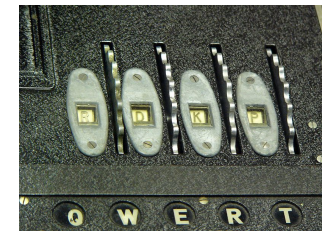


Cryptography Engineering by Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno

<https://www.schneier.com/book-ce.html>

Kryptering sikrer fortrolighed og integritet af beskederne

Tor project anonym web browsing



Anonymity Online

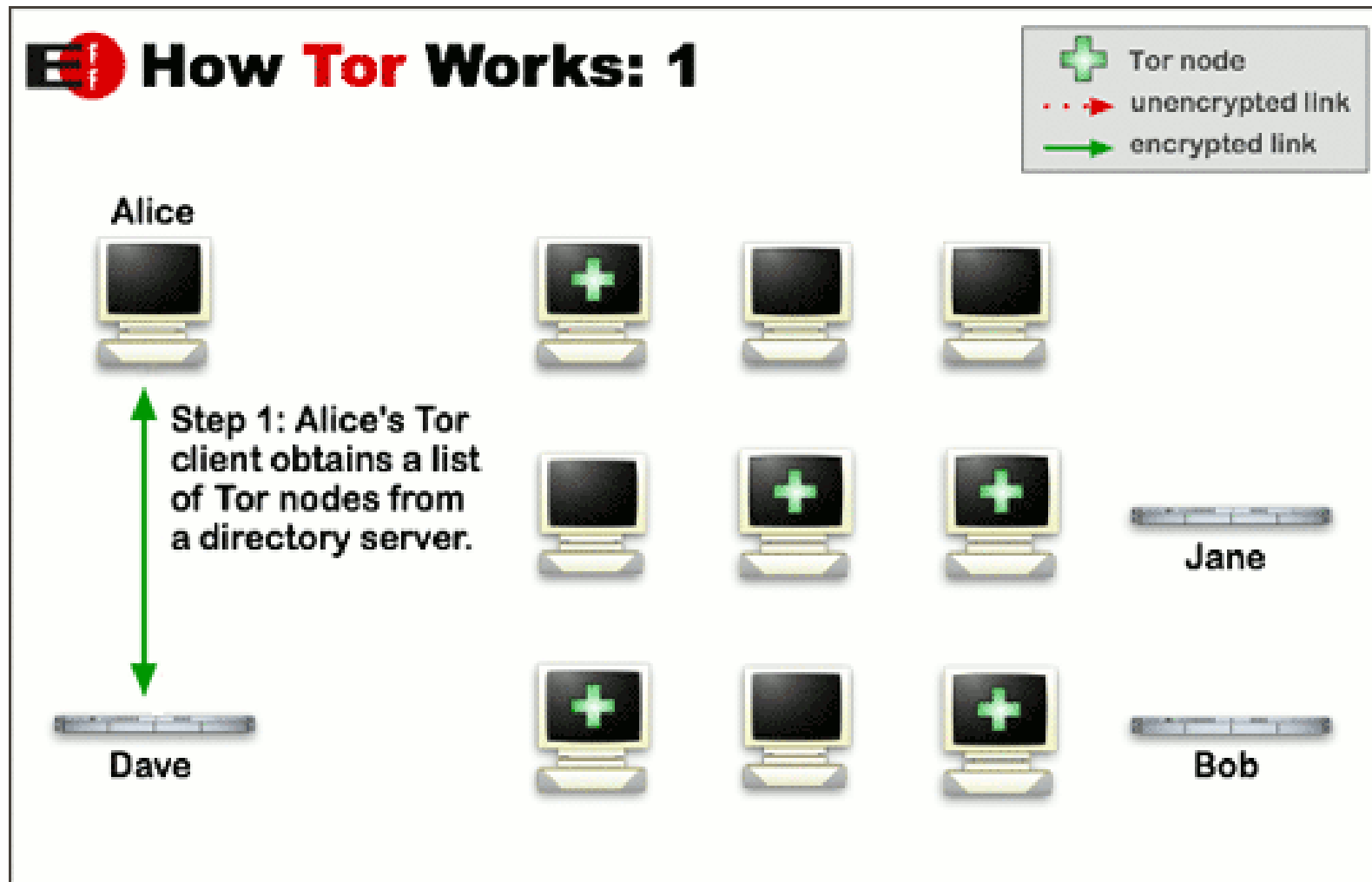
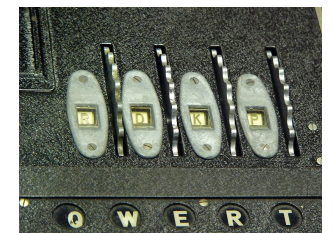
Protect your privacy. Defend yourself against network surveillance and traffic analysis.

[Download Tor](#)

- ➔ Tor prevents anyone from learning your location or browsing habits.
- ➔ Tor is for web browsers, instant messaging clients, remote logins, and more.
- ➔ Tor is free and open source for Windows, Mac, Linux/Unix, and Android

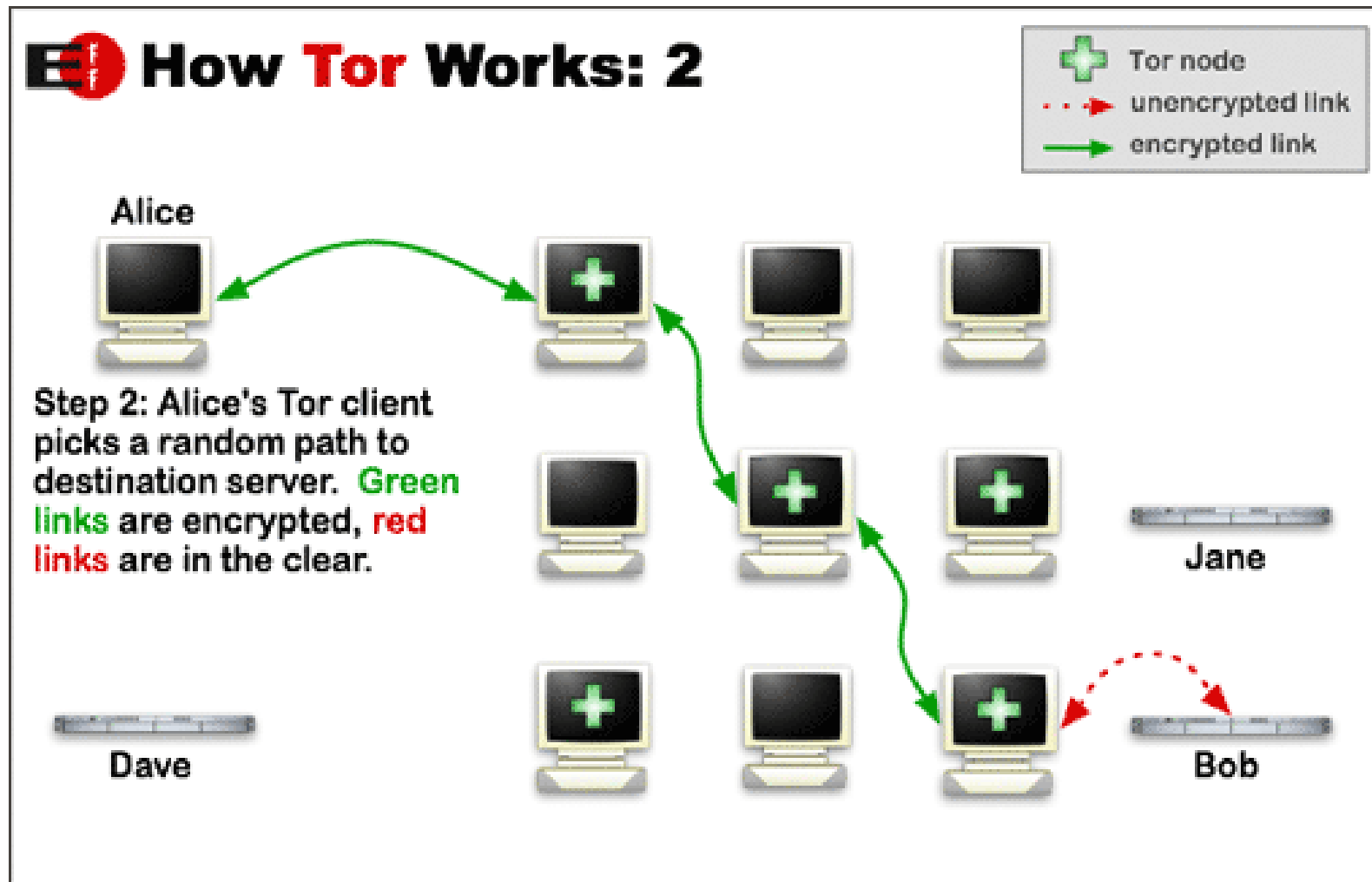
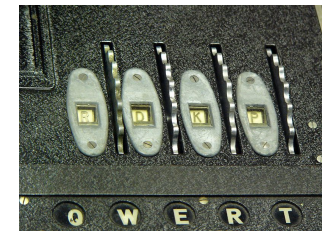
<https://www.torproject.org/>
Der findes alternativer, men Tor er mest kendt

Tor project - how it works 1



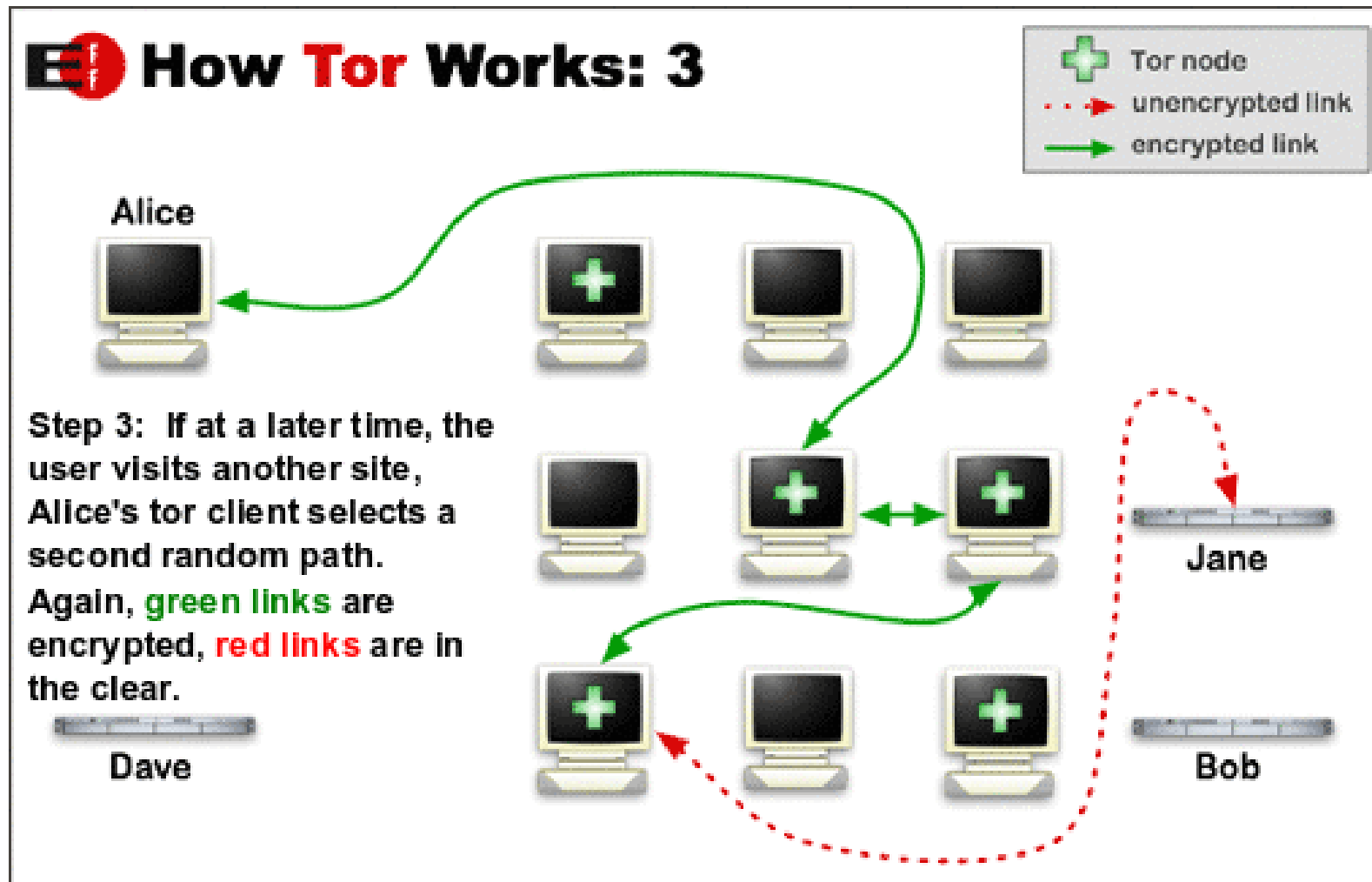
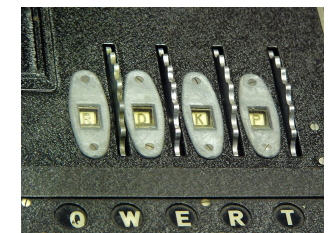
pictures from <https://www.torproject.org/about/overview.html.en>

Tor project - how it works 2



pictures from <https://www.torproject.org/about/overview.html.en>

Tor project - how it works 3




pictures from <https://www.torproject.org/about/overview.html.en>

Tor project install



Anonymity Online

Protect your privacy. Defend yourself against network surveillance and traffic analysis.

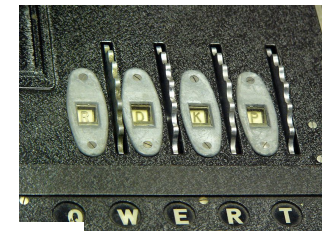
[Download Tor](#)

- Tor prevents anyone from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, remote logins, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android

Der findes diverse tools til Tor, Torbutton on/off knap til Firefox osv.

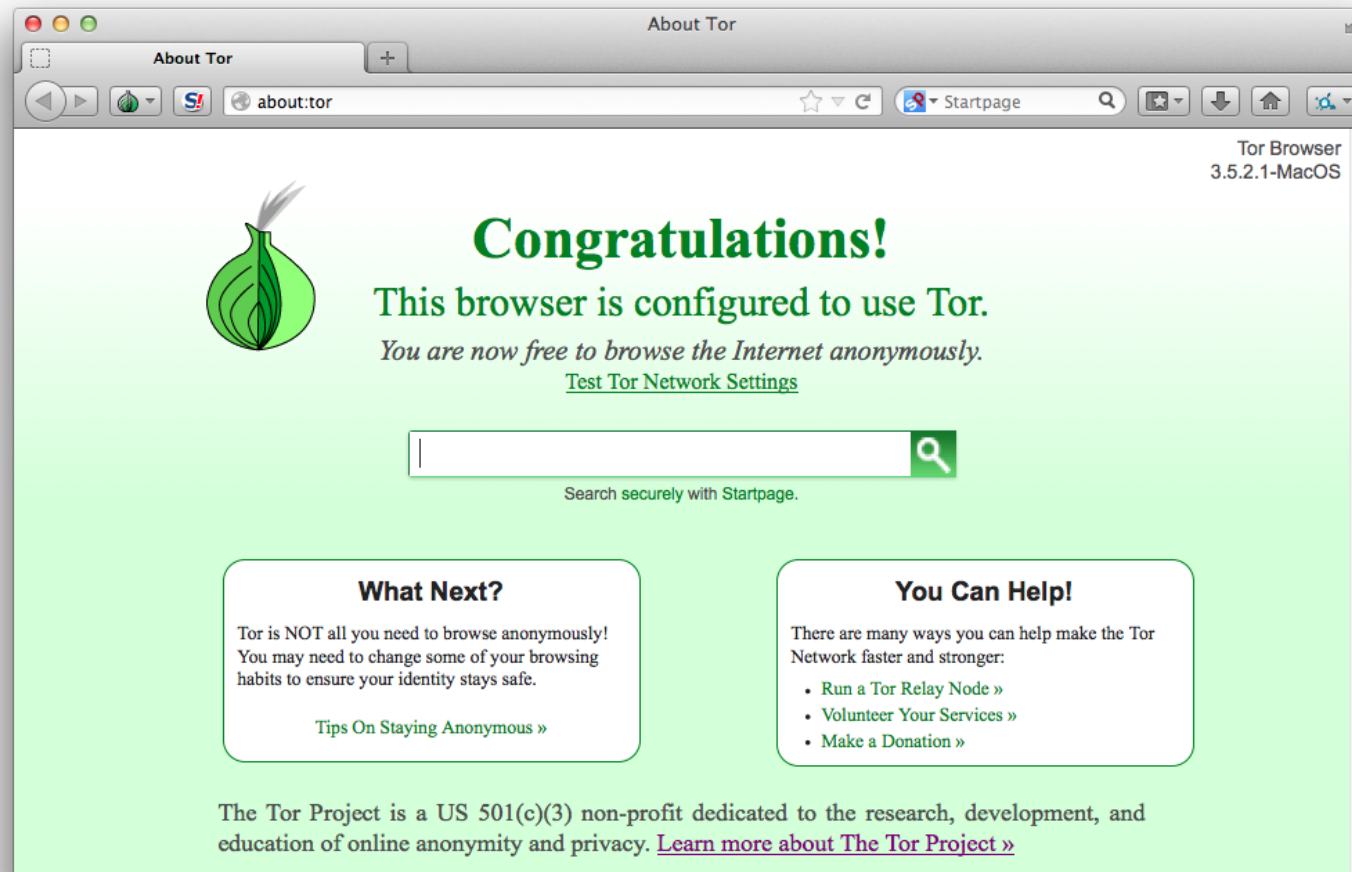
Det anbefales at bruge Torbrowser bundles fra <https://www.torproject.org/>

Torbrowser - outdated



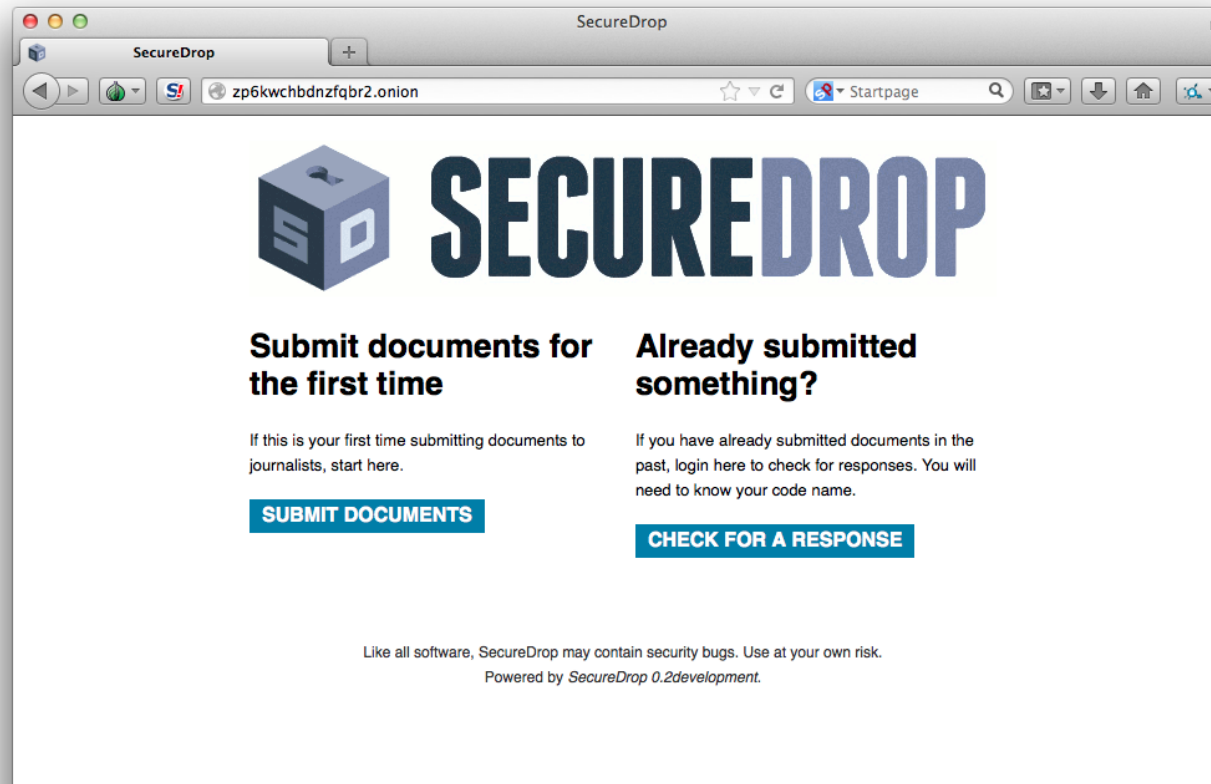
Hov den mangler opdatering!

Torbrowser - anonym browser



Mere anonym browser - Firefox i forklædning

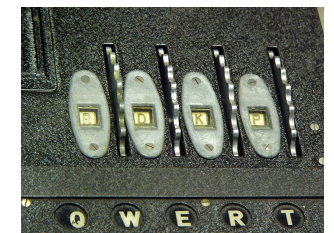
Torbrowser - sample site



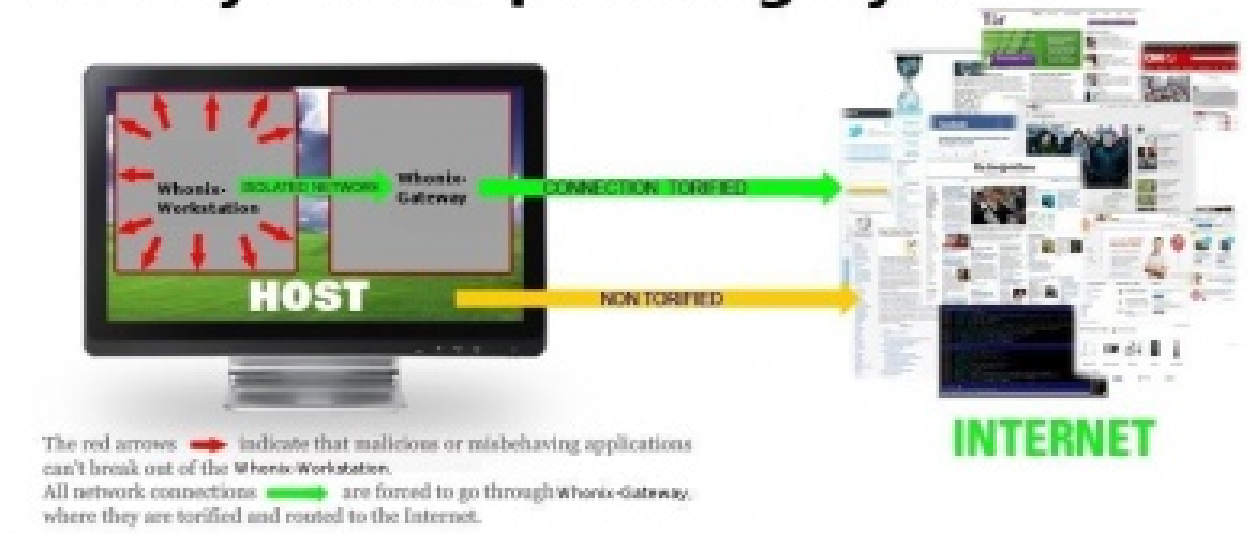
.onion er Tor adresser - hidden sites

Den viste side er SecureDrop hos Radio24syv <http://www.radio24syv.dk/dig-og-radio24syv/securedrop/>

Whonix - Tor to the max!



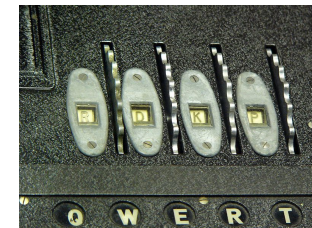
Whonix Anonymous Operating System



Whonix is an operating system focused on anonymity, privacy and security. It's based on the Tor anonymity network[5], Debian GNU/Linux[6] and security by isolation. DNS leaks are impossible, and not even malware with root privileges can find out the user's real IP. <https://www.whonix.org/>

Torbrowser er godt, Whonix giver lidt ekstra sikkerhed

Hvad er et cryptoparty



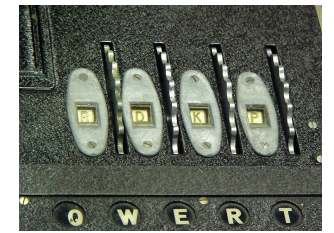
Iaften vil vi fokusere på disse:

- OTR Off-the-record Adium eller Pidgin, brug server cloak.dk
- Torproject - Tor Browser Bundle
- OpenPGP - PGP/GPG Thunderbird Enigmail eller GPGmail Mac

Andre kilder til tools:

- Surveillance Self-Defense EFF guide <https://ssd.eff.org/>
- Se citizenfour filmen - fik velfortjent Oscar!
<http://www.wired.com/2014/10/laura-poitras-crypto-tools-made-snowden-film-possible/>
- Information Security for Journalists
<http://www.tcij.org/resources/handbooks/infosec>

10minute cryptoparty



iTunes Preview

Signal – Private Messenger

By Open Whisper Systems

Open iTunes to buy and download apps.



View in iTunes

Description

Privacy is possible. Signal makes it easy.

* Say Anything – Send high-quality group, text, picture, and video messages, all without SMS and MMS fees.

[Open Whisper Systems Web Site](#) • [Signal – Private Messenger Support](#) •

...More

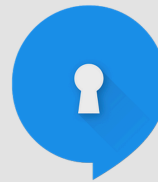
What's New in Version 2.0.1

New in 2.0.1:

- You can now draft messages and come back later to send them.
- Multiple bug and performance fixes.



Google play



TextSecure Private Messenger

Open Whisper Systems - 12. marts 2015
Kommunikation

Installeret

Denne app er kompatibel med nogle af dine enheder.

★★★★★ (12.689)



RedPhone :: Private Calls

Open Whisper Systems - 27. september 2014
Kommunikation

Installeret

Denne app er kompatibel med nogle af dine enheder.

★★★★★ (6.377)



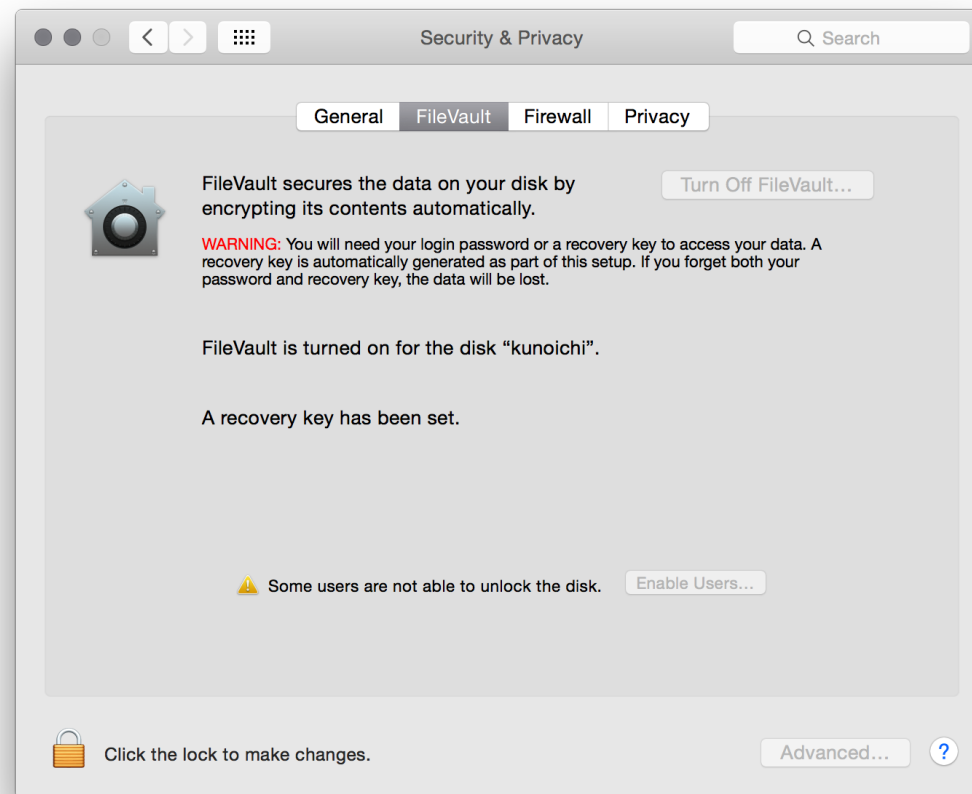
Forsøg, hvor mange kan kommunikere sikkert indenfor 10min?

- Android installer TextSecure og Redphone
- iPhone IOS installer Signal

Send krypteret SMS til en anden herinde

og brug så krypteret SMS fremover ☺

Full Disk Encryption Mac OS X



Indbygget, gratis, stærk - når I kommer hjem

DNS censur i Danmark



CENSORED

Hvis du er træt af den danske censur på DNS, så kan du skifte til at bruge: Censurfridns.dk UncensoredDNS

Du udskifter blot dine DNS indstillinger på din PC til:

- anycast.censurfridns.dk / 91.239.100.100 / 2001:67c:28a4::
- ns1.censurfridns.dk / 89.233.43.71 / 2002:d596:2a92:1:71:53::

Se også <http://www.censurfridns.dk> og blog.censurfridns.dk for mere info.

Det er uacceptabelt at pille ved DNS - punktum!

Comments and questions



You are always welcome to send me questions later via email

Henrik Lund Kramshøj hik@kramse.org