

Velkommen til

# Cryptoworkshop hvad er det?

Henrik Lund Kramshøj [hlik@kramse.org](mailto:hlik@kramse.org)



PDF available [kramshoej@Github: crypto-workshop-journo-2015](https://github.com/kramshoej/crypto-workshop-journo-2015)

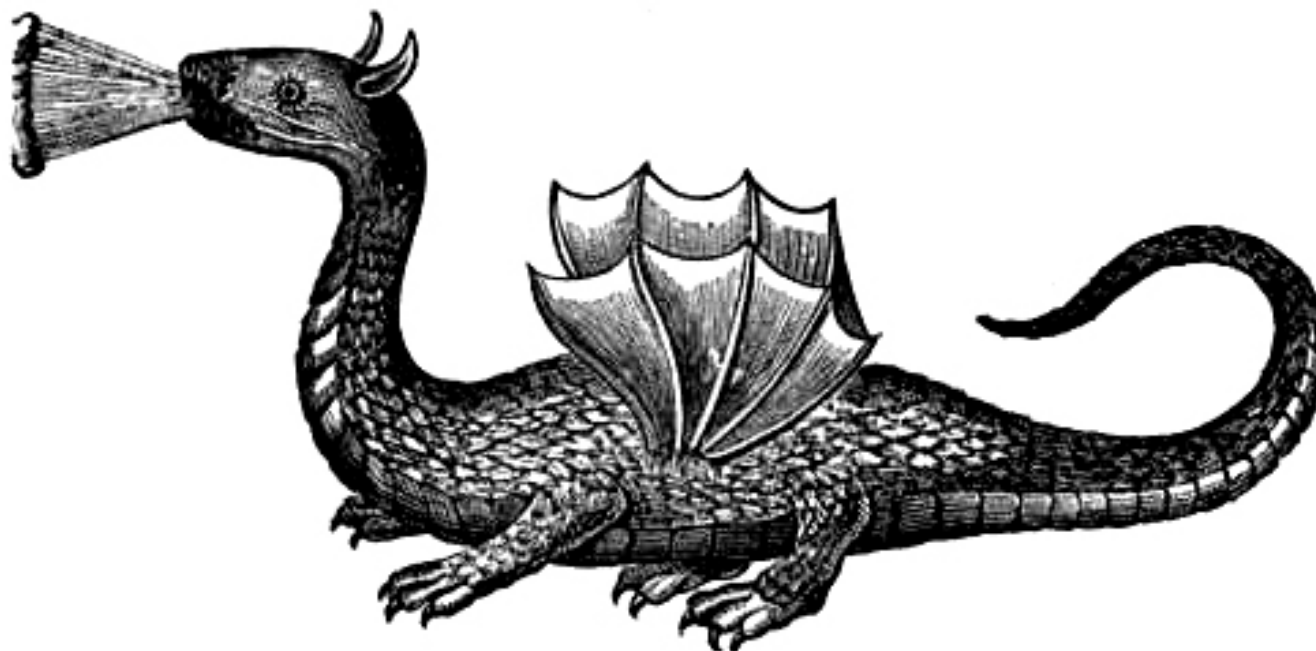
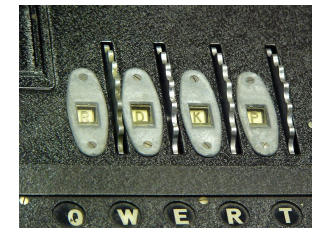
# agenda



## Planen for Cryptoworkshop 20:10 - 21:50

- Introduktion Peter Kofoed - optakten
- Kort introduktion cryptoworkshop - denne præsentation
- Minicryptoworkshop 10min Textsecure, Red Phone og Whispersystems Signal
- Anonymiseringsværktøjet Tor
- Minicryptoworkshop 10min Torbrowser install
- Sikker email med OpenPGP - PGP/GPG/GPGTools
- Minicryptoworkshop 30min PGP install

Tak for praktiske hjælp fra <https://bitbureauet.dk/> Twitter: @bitbureauet

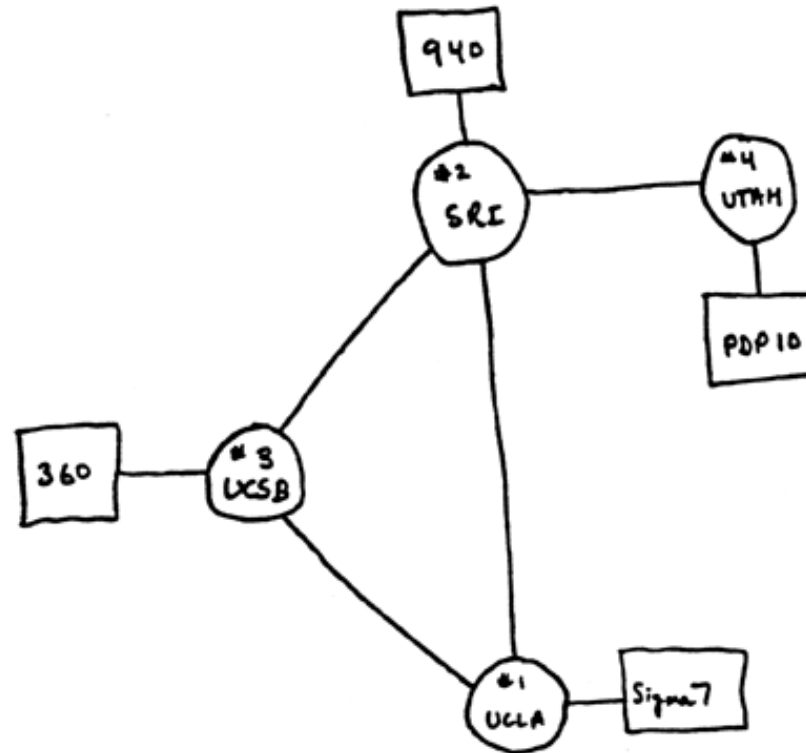


Denne aften er en smagsprøve - introduktion

Du skal ikke føle dig sikker før du forstår programmerne bedre.

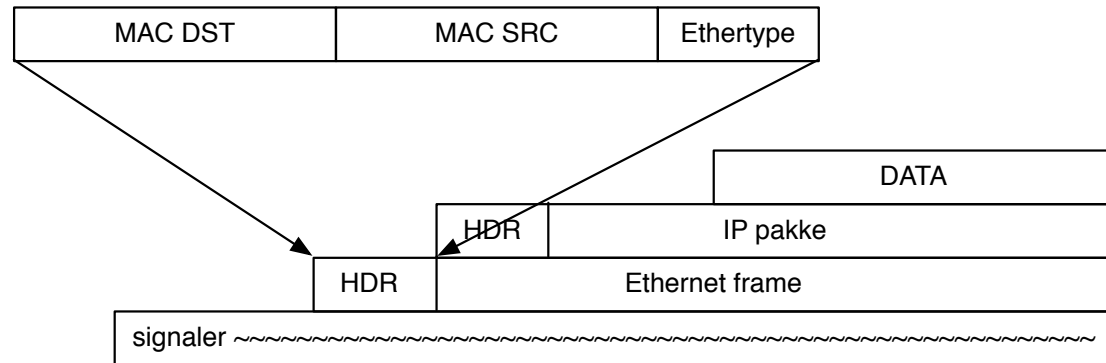
Brug, læs og lær - det er vigtigt at lære det at kende før man skal bruge det.

# Internet Internals: A short story



1969: ARPANET 4 nodes

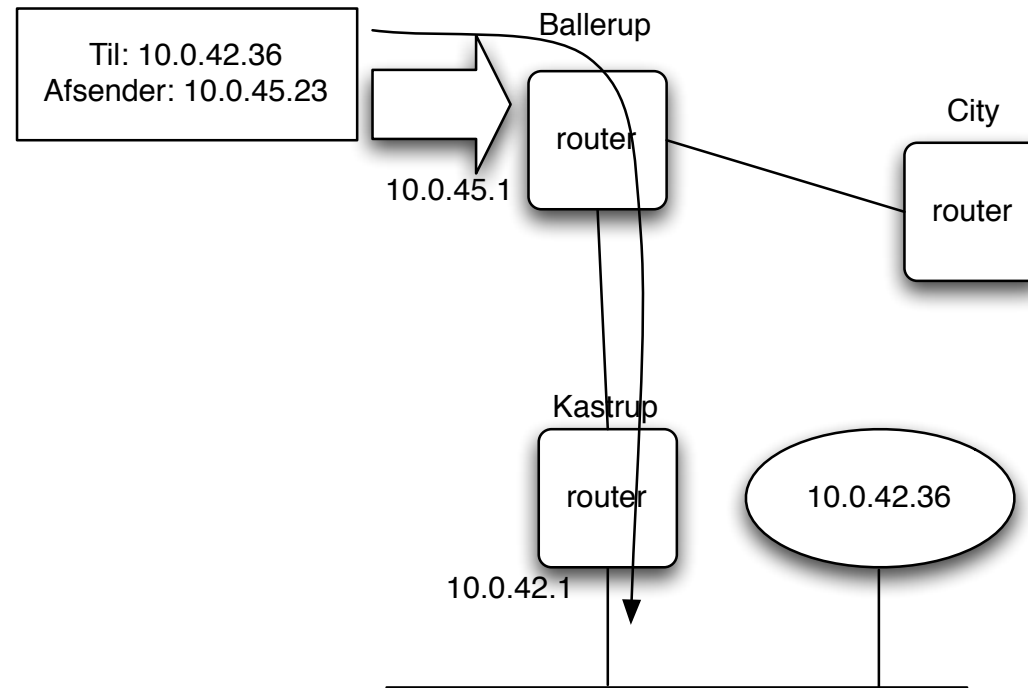
Present some internet internals, what is it?



### Example Internet Datagram Header

© copyright 2015 Creative Commons CC Zero - public domain

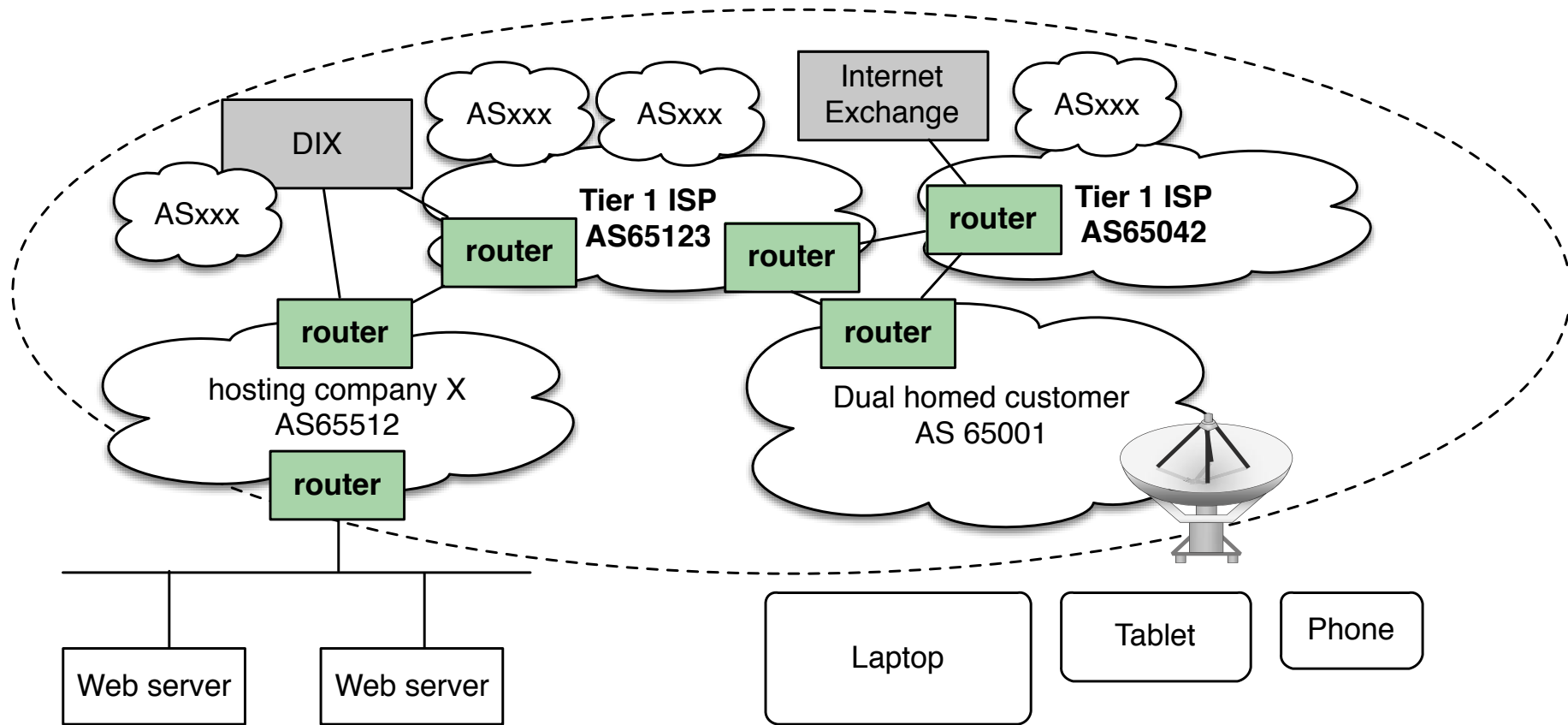
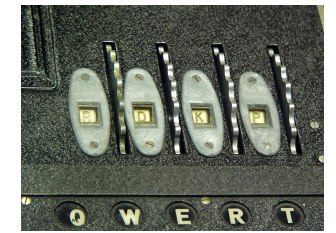
# Routing



Soo simple 😊

Dont forget IP routing is based on longest match in the routing table

# Internet core today AS numbers



Also pretty pictures in *Intercountry BGP As Topology* Martin J. Levy

<http://oldwww.dknog.dk/dknog3/agenda>



# BGP changes



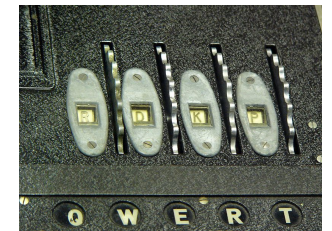
A good analogy for the development of the Internet is that of constantly renewing the individual streets and buildings of a city, rather than razing the city and rebuilding it. The architectural principles therefore aim to provide a framework for creating cooperation and standards, as a small "spanning set" of rules that generates a large, varied and evolving space of technology.

Source: RFC-1958

- Constant change
- Now 50.000 ASNs announced, and 80.000 allocated
- Now 515.000 prefixes - reach 550.000 routes/prefixes in 2015?

Movietime <https://stat.ripe.net/94.126.176.0/21#tabId=routing>  
Lots of data to be found at <http://bgp.potaroo.net/>

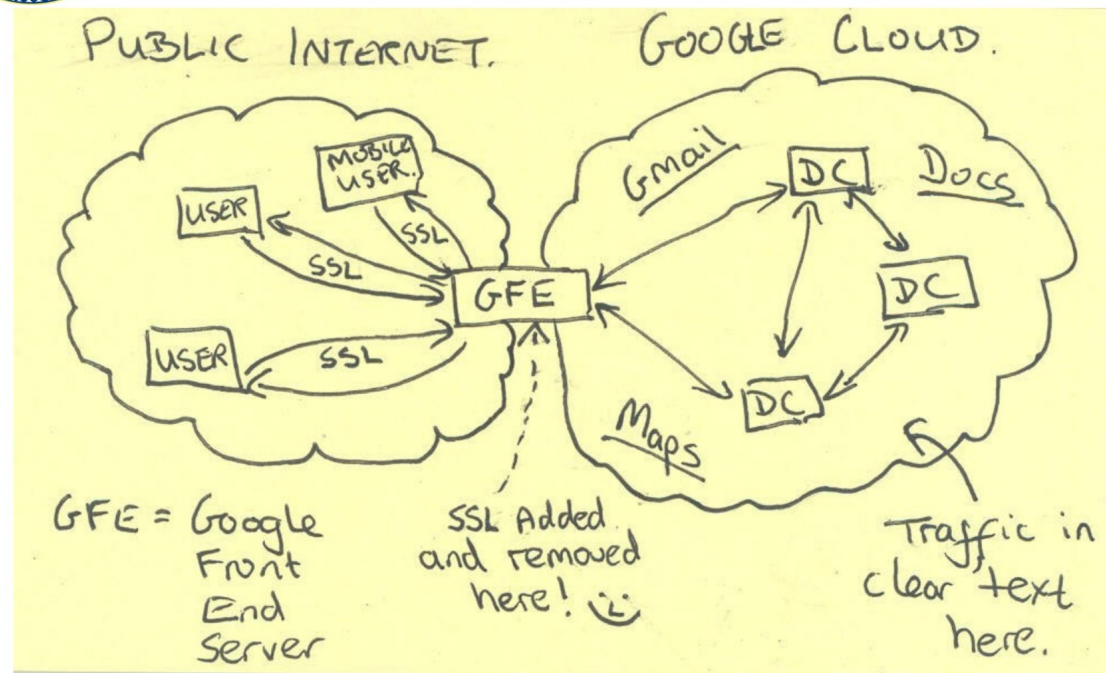




TOP SECRET//SI//NOFORN



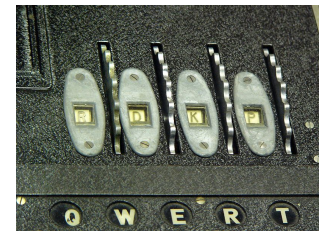
## Current Efforts - Google



TOP SECRET//SI//NOFORN

SSL (encryption) added and removed here

# Solidaritetskryptering



Hvorfor skal vi kryptere?

Køn

Seksualitet

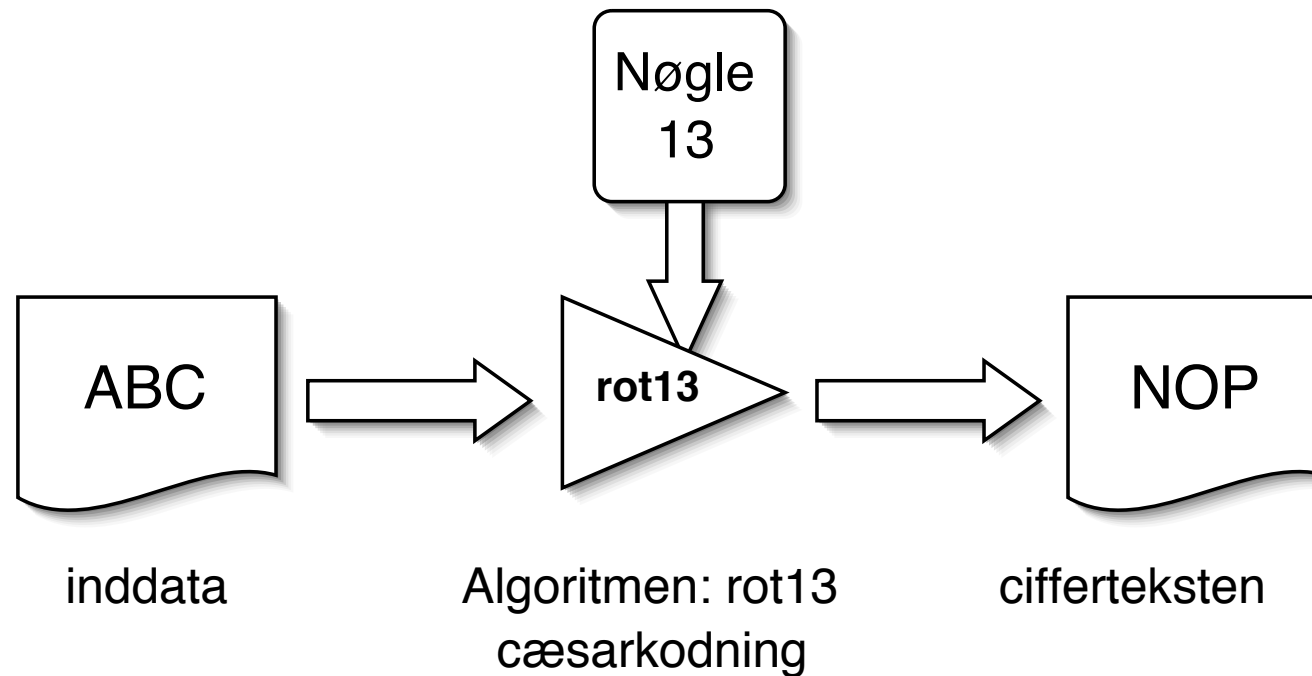
Tro religion hatecrimes

Politisk overbevisning, eller blot aktiv

Whistleblowers soldater diplomater

Du bestemmer ikke hvem der diskrimineres eller trues i andre lande

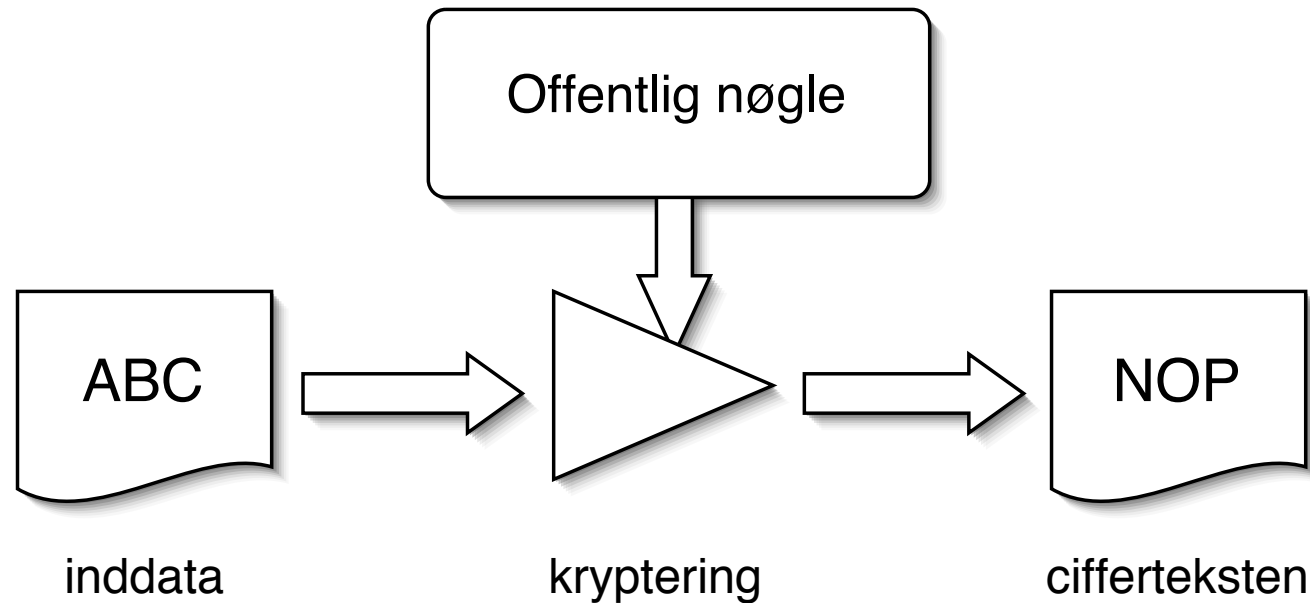
Når vi krypterer hjælper vi andre! **Solidaritetskryptering**



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

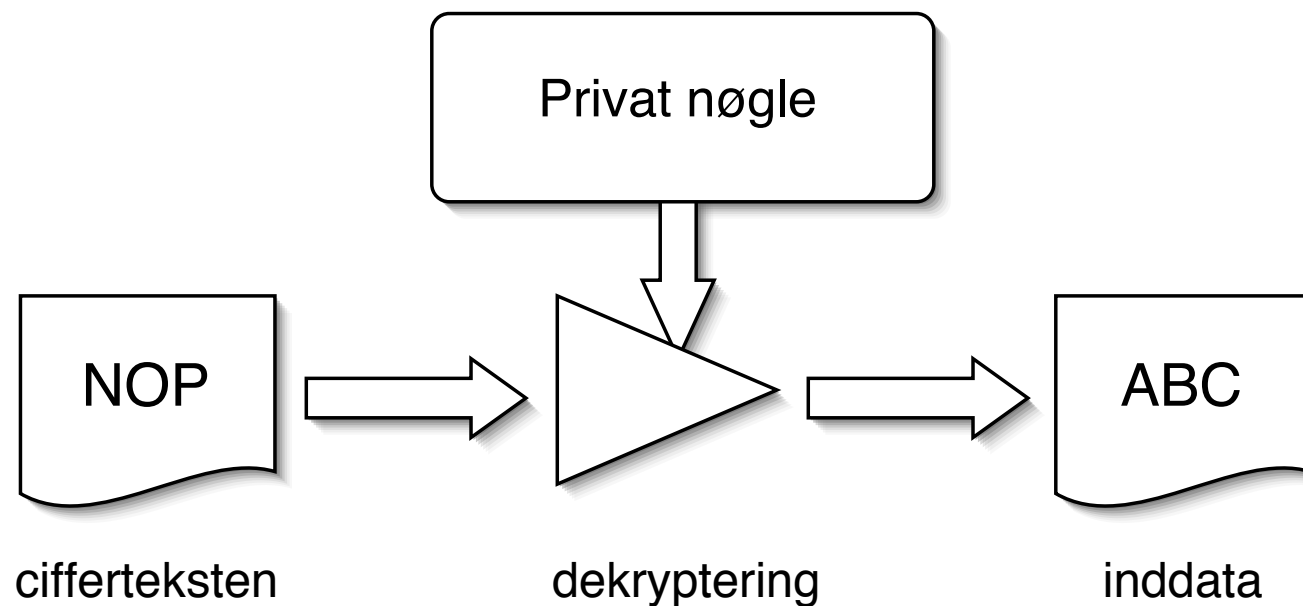
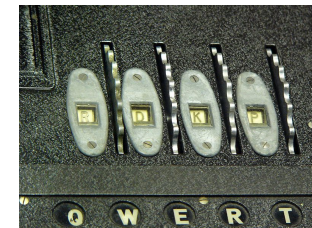
# Public key kryptografi - 1



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

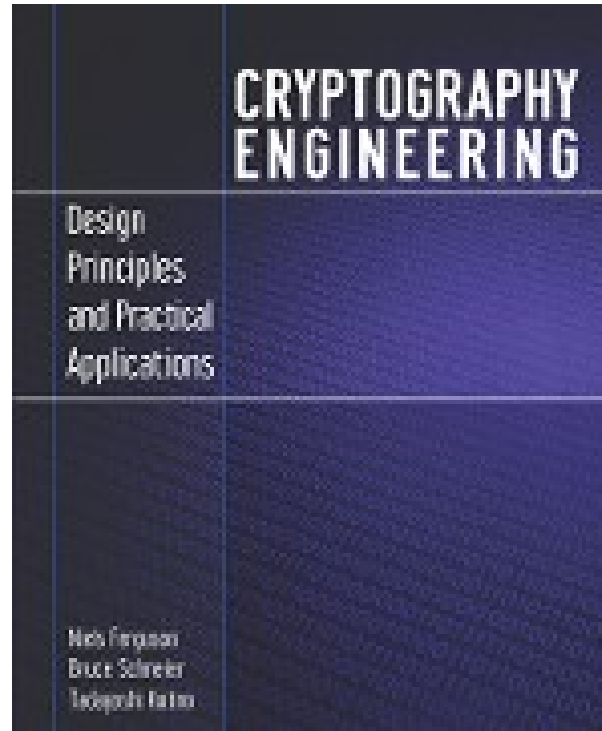


offentlig-nøgle kryptografi (eksempelvis RSA) bruger den private nøgle til at dekryptere

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

- som så verificeres med den offentlige nøgle

# Kryptering: Cryptography Engineering

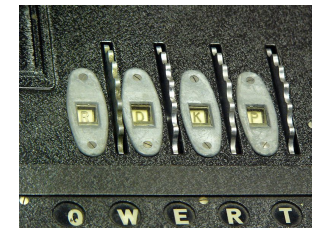


*Cryptography Engineering* by Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno

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

Kryptering sikrer fortrolighed og integritet af beskederne

# Hvad er cryptoworkshop



Udspringer af CryptoParty bevægelsen som afholder kryptofester

<https://en.wikipedia.org/wiki/CryptoParty>

Iaften vil vi fokusere på disse:

- Android: TextSecure og Redphone
- iPhone IOS installer Signal
- Torproject - Tor Browser Bundle
- OpenPGP - PGP/GPG Thunderbird Enigmail eller Mac OS X GPGtools

Note: følg også <https://cryptoparty.dk/>

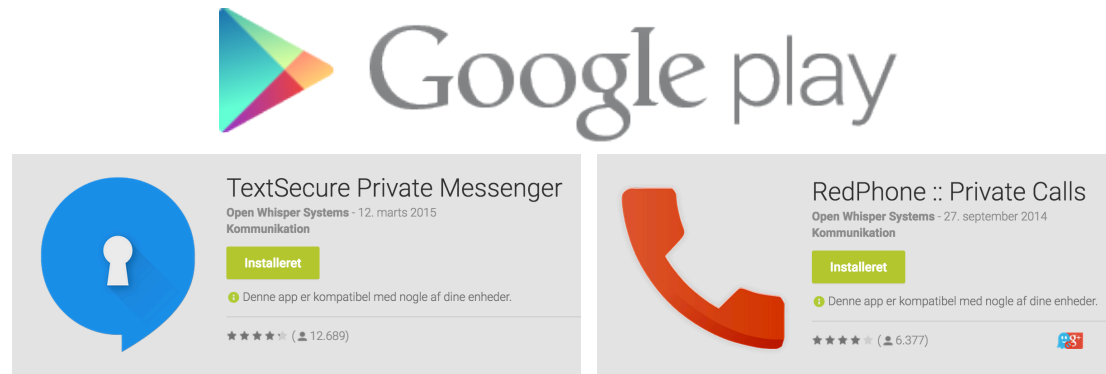
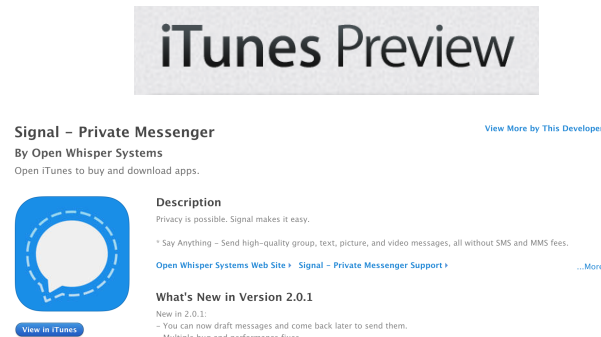
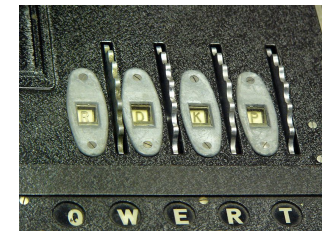


# Andre kilder til tools



- Surveillance Self-Defense EFF guide <https://ssd.eff.org/>
- The Guardian Project Mobile Apps and Code You Can Trust  
<https://guardianproject.info/>
- 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 cryptoworkshop



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 sig YEAH!

og brug så krypteret SMS fremover 😊

# Tor project anonym web browsing



## Anonymity Online

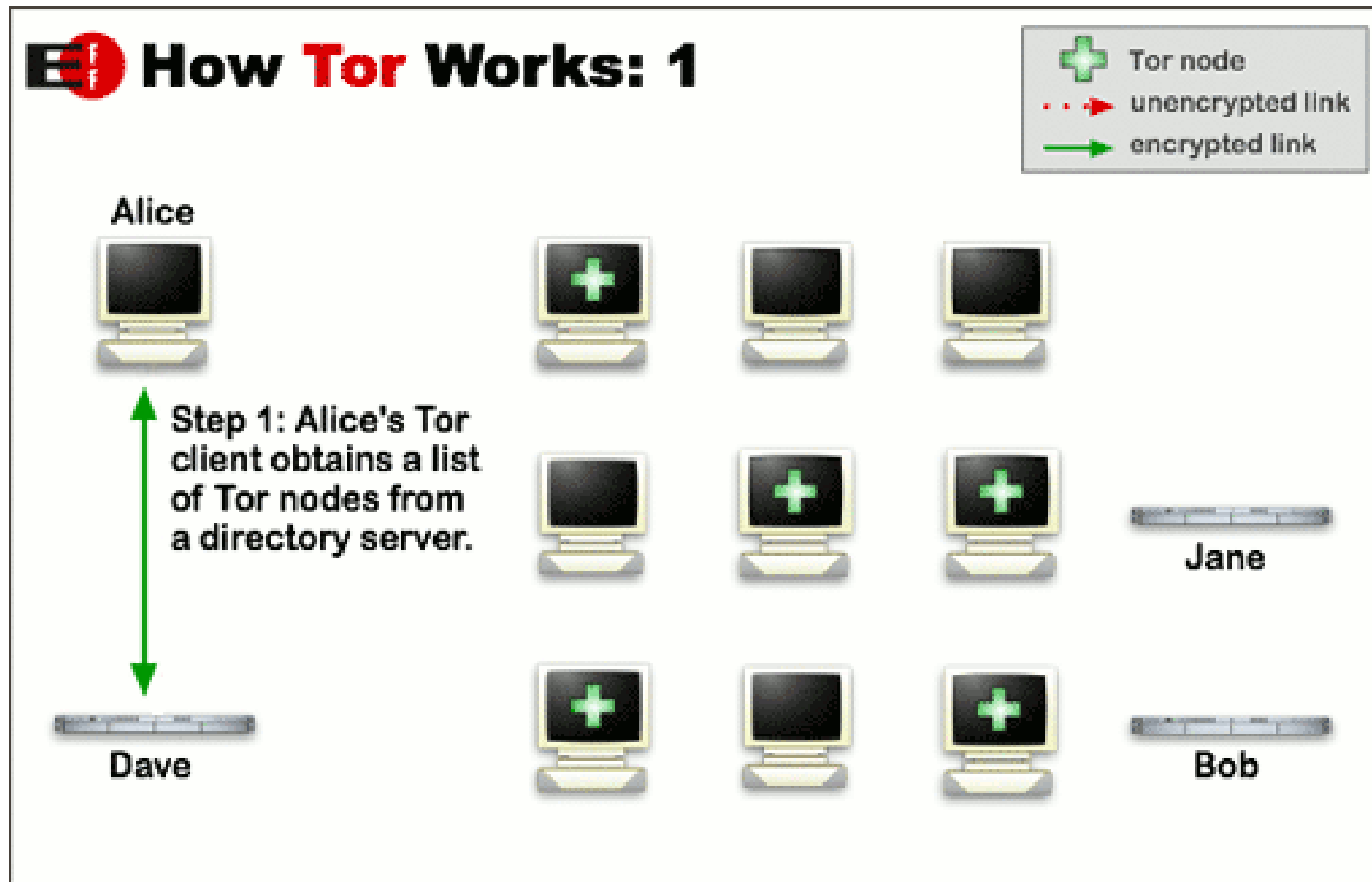
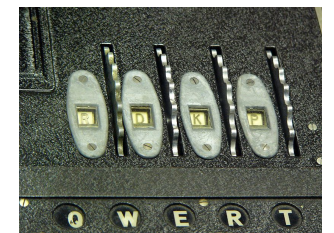
Protect your privacy. Defend yourself against network surveillance and traffic analysis.

[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

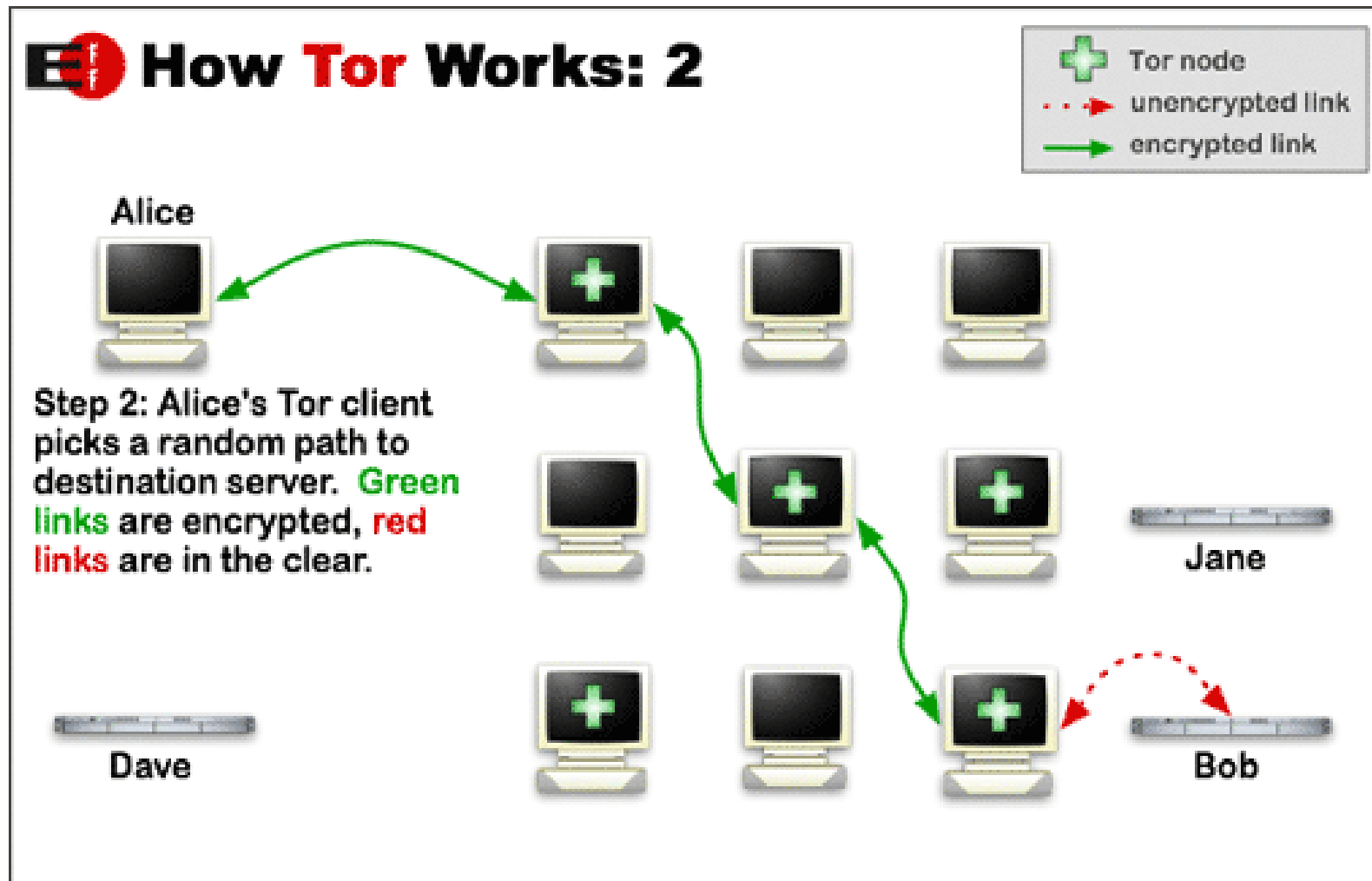
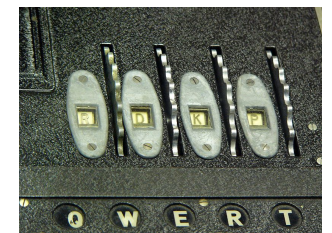
<https://www.torproject.org/>  
Der findes alternativer, men Tor er mest kendt

# Tor project - how it works 1



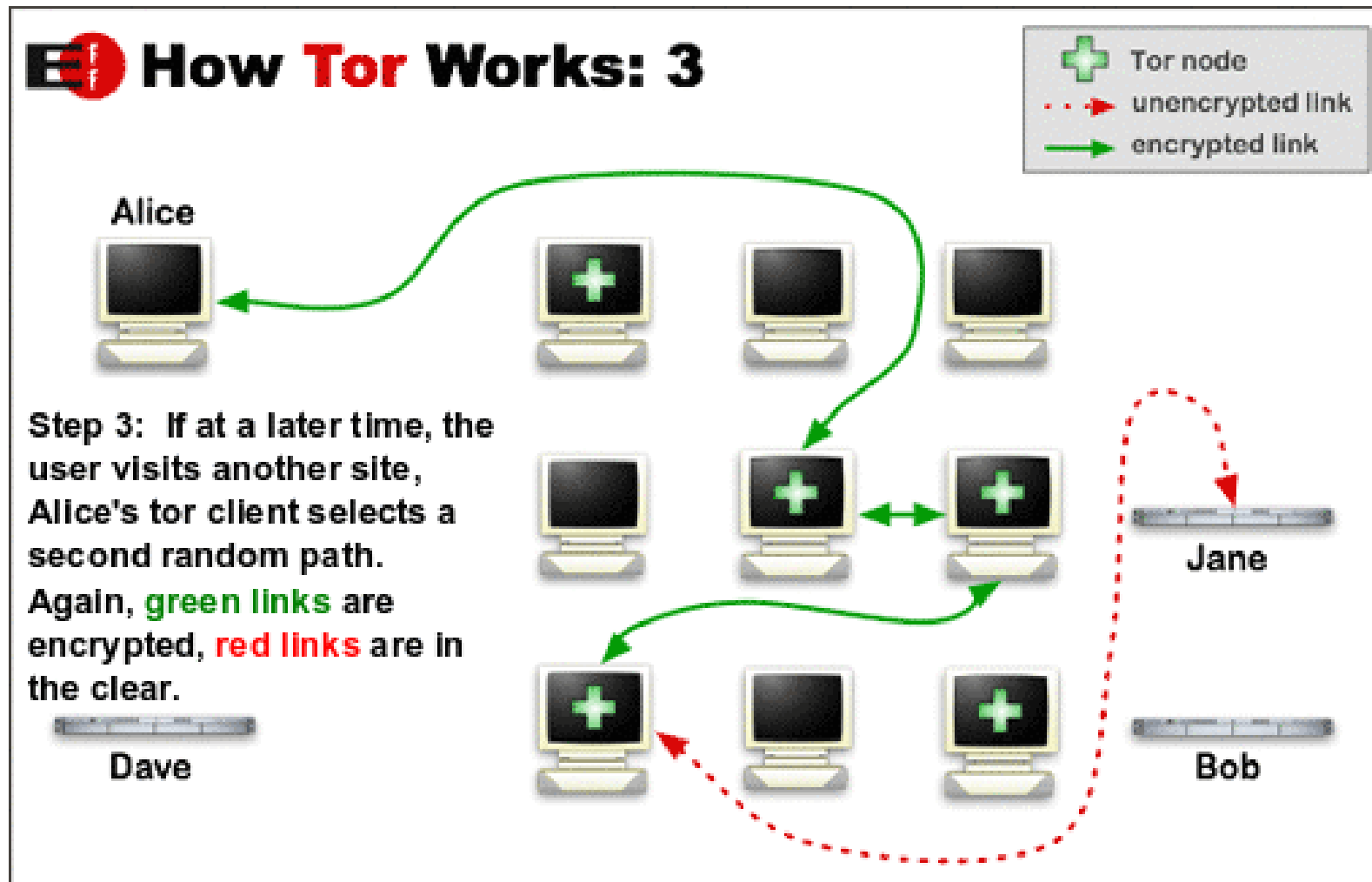
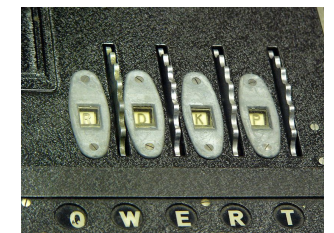
pictures from <https://www.torproject.org/about/overview.html.en>

# Tor project - how it works 2



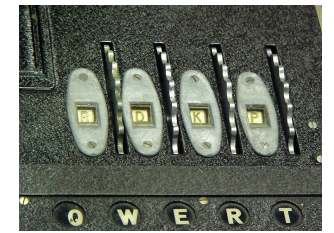
pictures from <https://www.torproject.org/about/overview.html.en>

# 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](#)

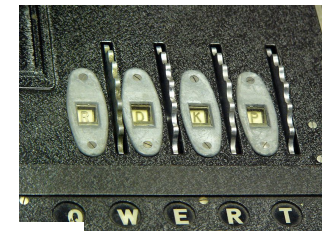
- Tor prevents anyone from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, remote logins, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android

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

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

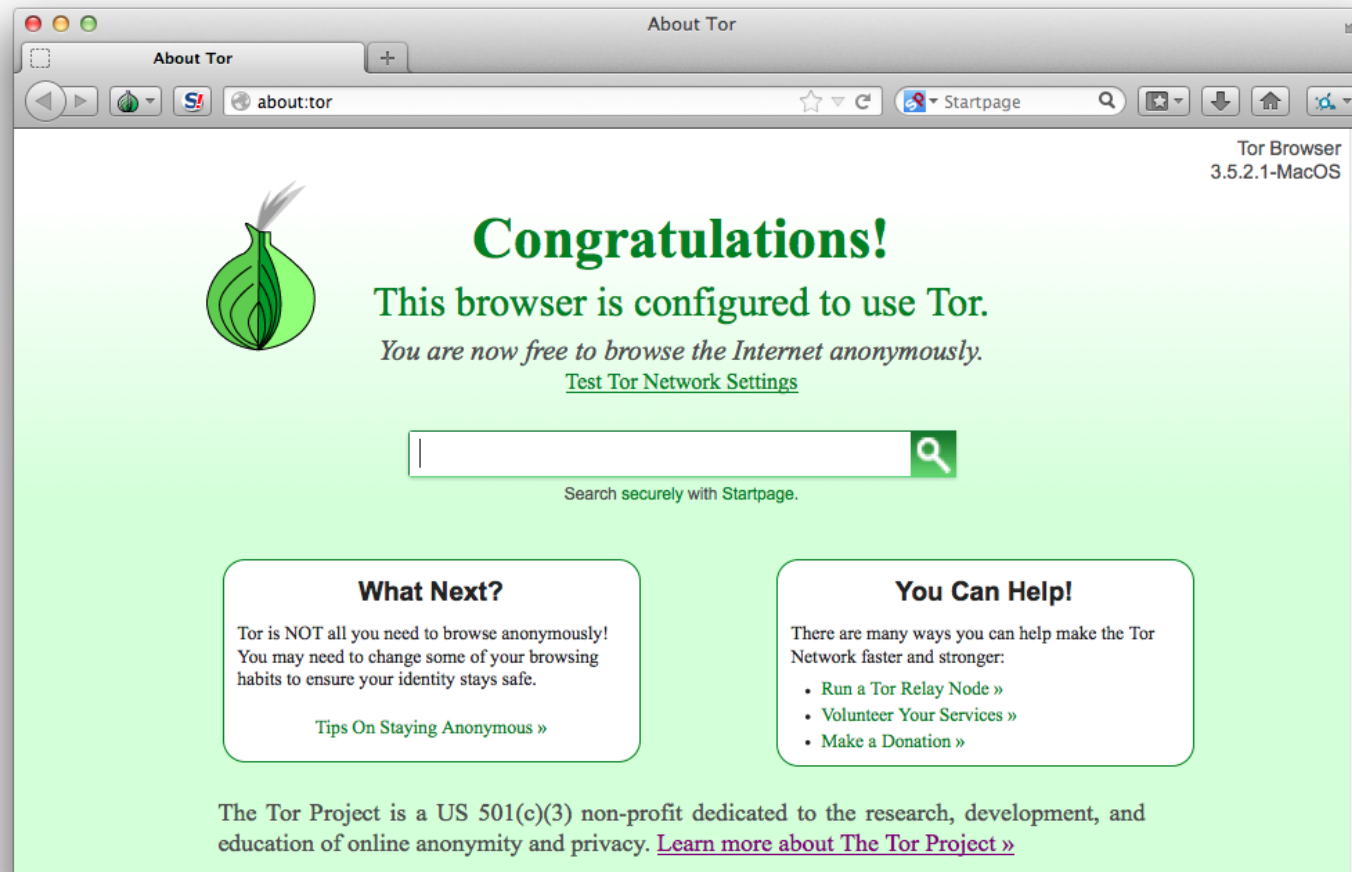


# Torbrowser - outdated



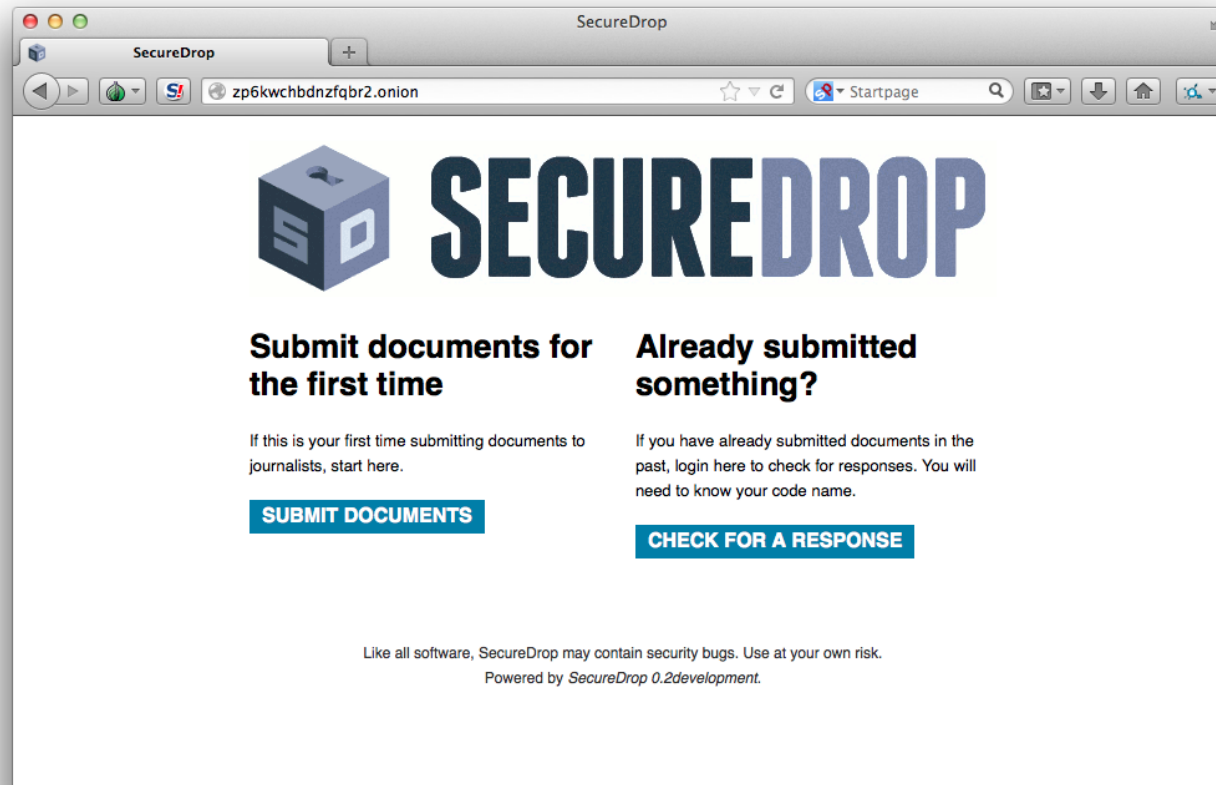
Hov den mangler opdatering!

# Torbrowser - anonym browser



Mere anonym browser - Firefox i forklædning

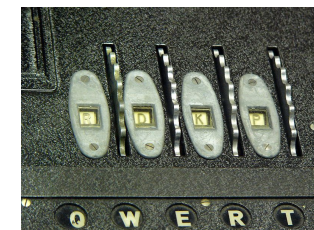
# Torbrowser - hidden service web site



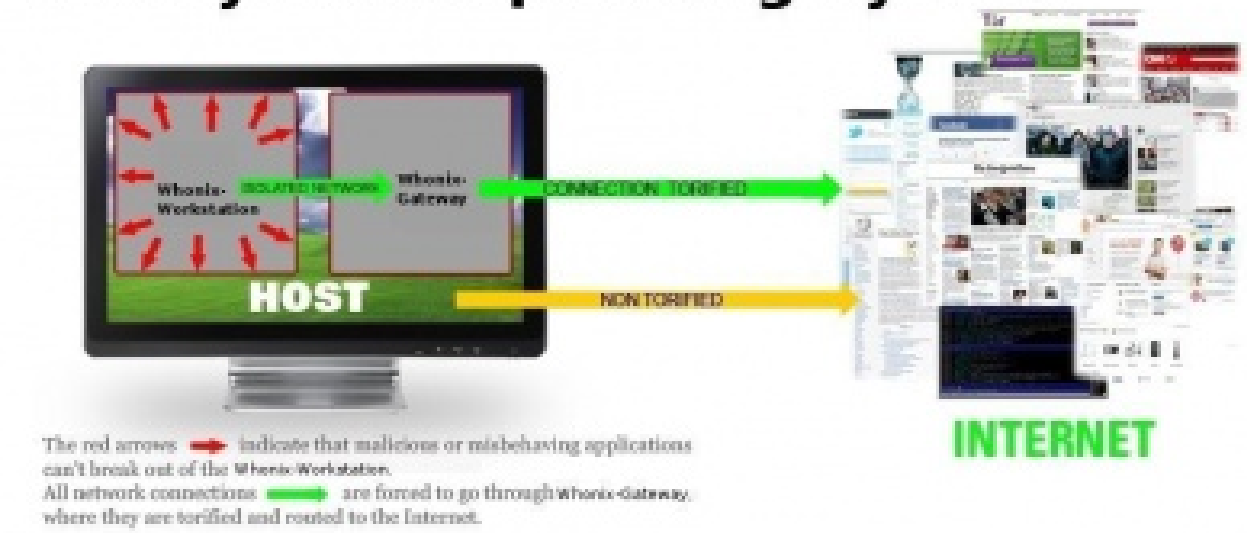
.onion er Tor adresser - hidden sites

<http://www.radio24syv.dk/dig-og-radio24syv/securedrop/>

# Whonix - Tor to the max!



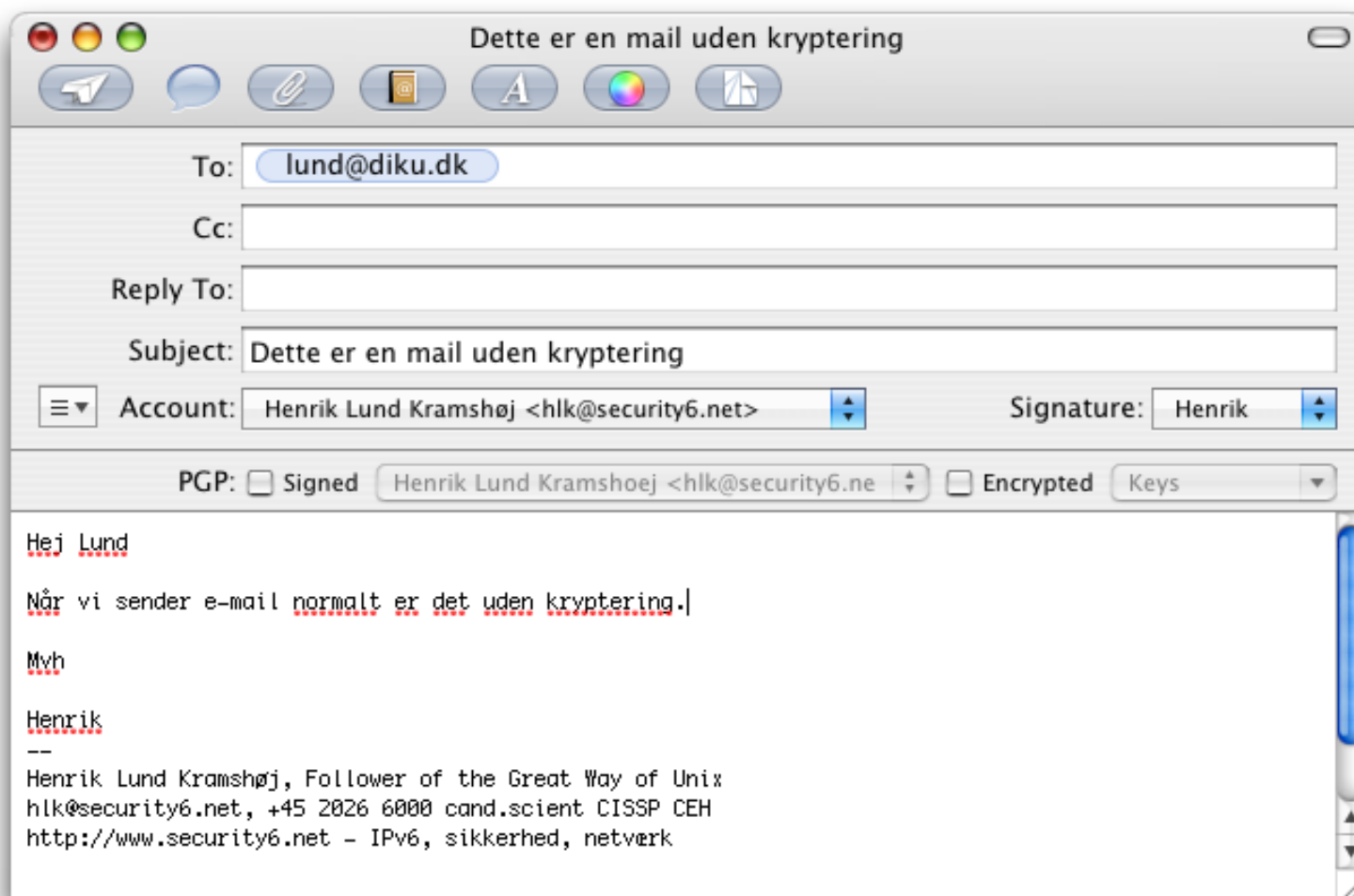
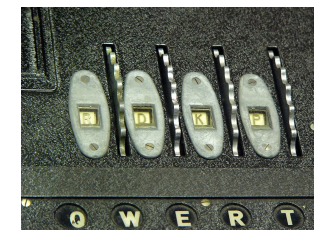
## Whonix Anonymous Operating System



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/>

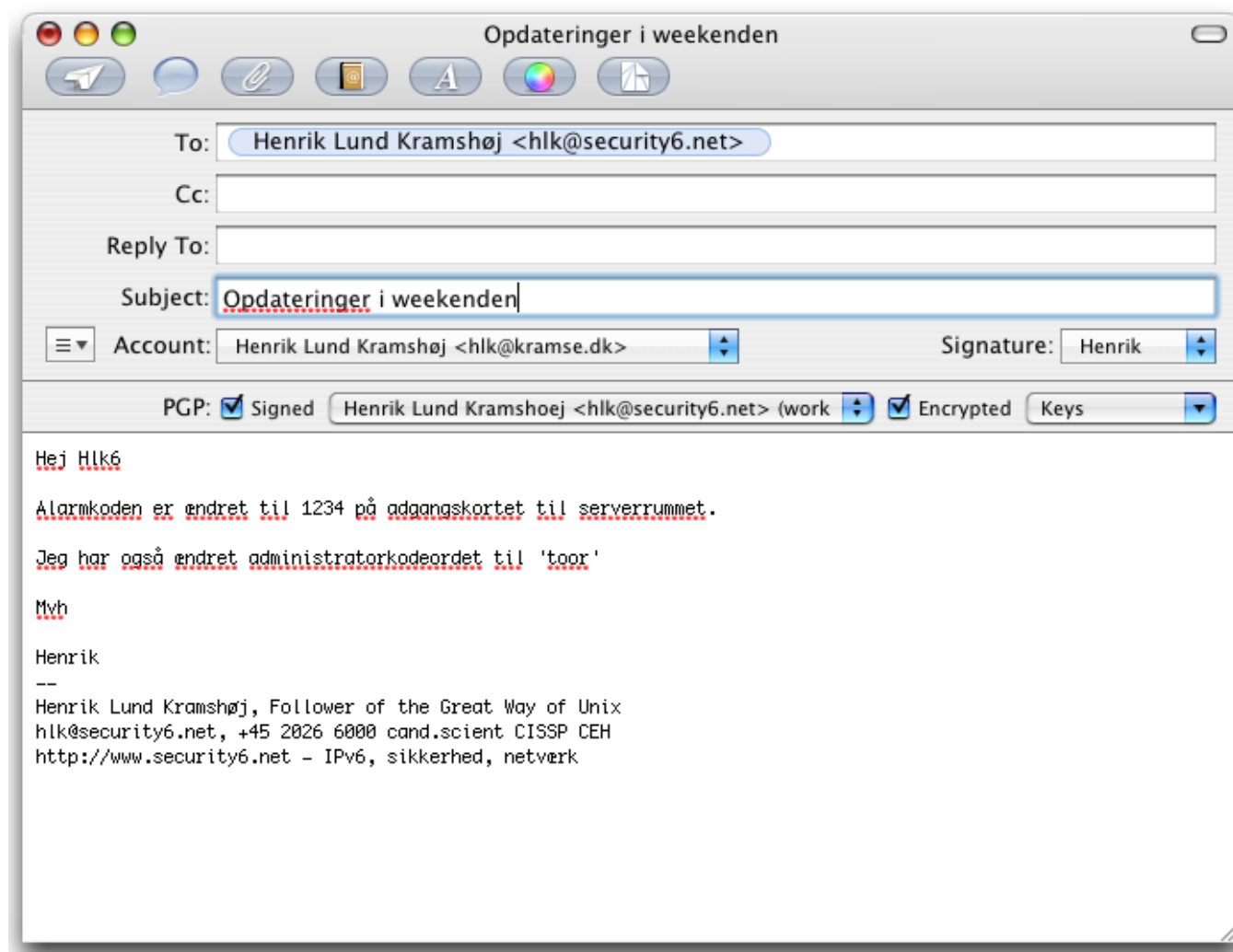
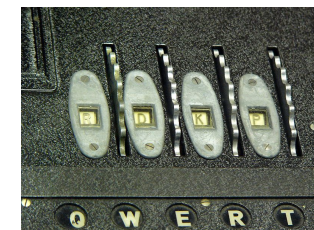
Torbrowser er godt, Whonix giver lidt ekstra sikkerhed

# Email er usikkert



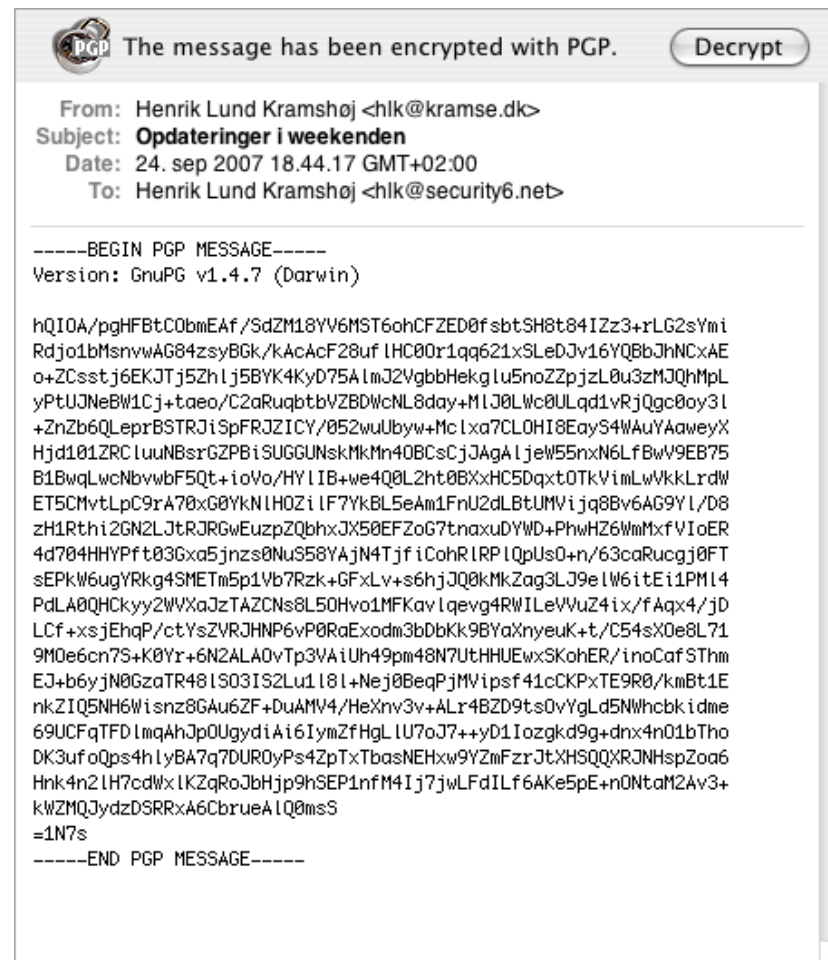
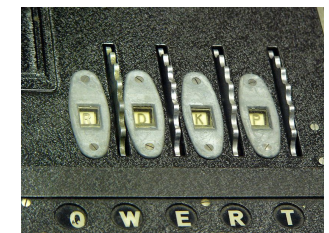
Email uden kryptering - er som et postkort

# Email med kryptering - afsendelse



En sikker krypteret email er ikke sværere at sende

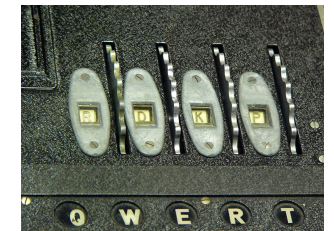
# Krypteret Email under transporten



En sikker krypteret email er beskyttet undervejs



# Thunderbird Enigmail



**THE ENIGMAIL PROJECT**  
OPENPGP EMAIL SECURITY FOR MOZILLA APPLICATIONS

[Home](#) [Download](#) [Documentation](#) [Support](#) [News](#) [Links](#)

## A simple interface for OpenPGP email security

### Download

[v1.6 for Mac OS X on Thunderbird 24.0](#)

### Announcements

[Enigmail has a new home](#)

### About Enigmail

- [Features](#)
- [Screenshots](#)
- [FAQ](#)
- [Quick start guide](#)

### What is this all about?

Enigmail is a security extension to Mozilla Thunderbird and Seamonkey. It enables you to write and receive email messages signed and/or encrypted with the OpenPGP standard.

Sending and receiving encrypted and digitally signed email is simple using Enigmail.

When starting it for the first time, you are guided through the basic setup. We also prepared a new users' guide that explains how to use OpenPGP.

Welcome to Enigmail

**OpenPGP** Good signature from Patrick Brunschwig <pat> [Details](#)

From: Patrick Brunschwig ★

Subject: **Welcome to Enigmail** 18:33

To: Patrick Brunschwig ★ [Other Actions](#)

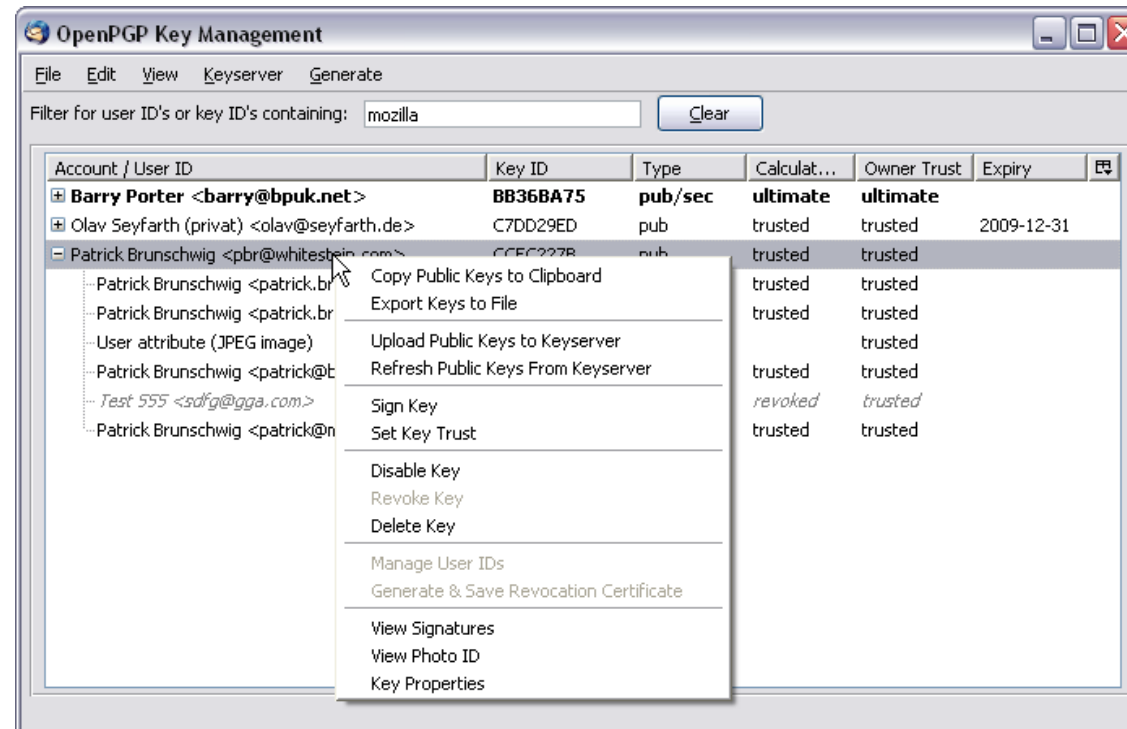
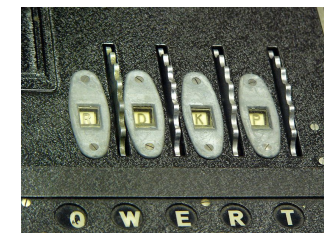
Enigmail provides end to end security for Mozilla Thunderbird and SeaMonkey.

Enigmail automatically decrypts and verifies your Email

Enigmail er en udvidelse til Thunderbird email programmet

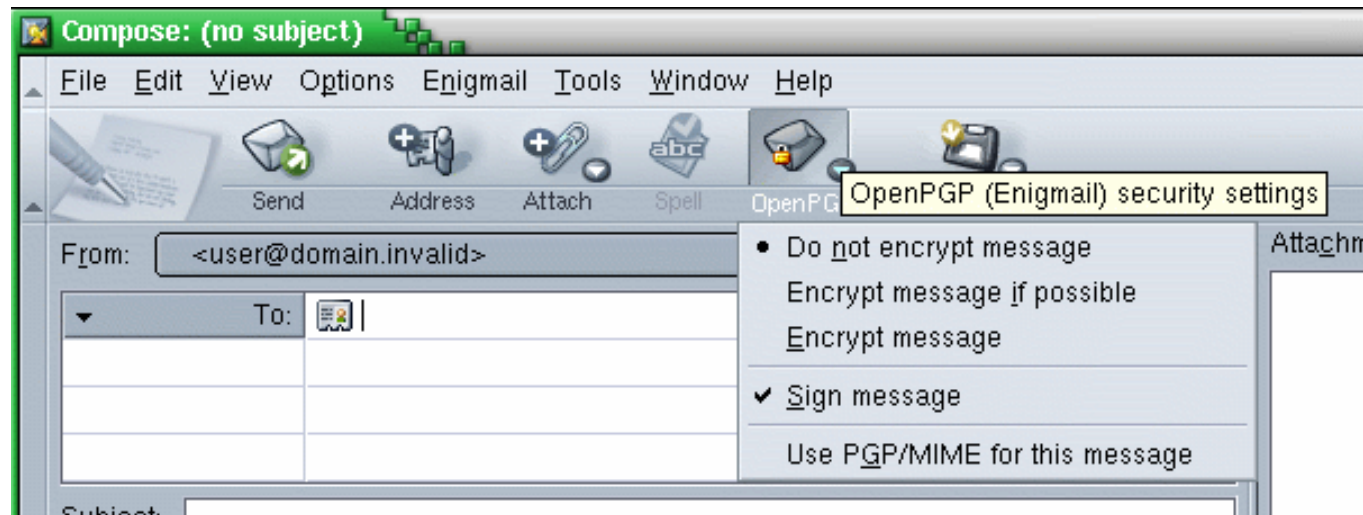
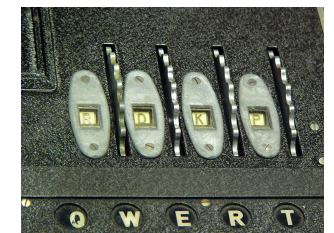
<https://www.enigmail.net>

# Thunderbird Enigmail: Key management



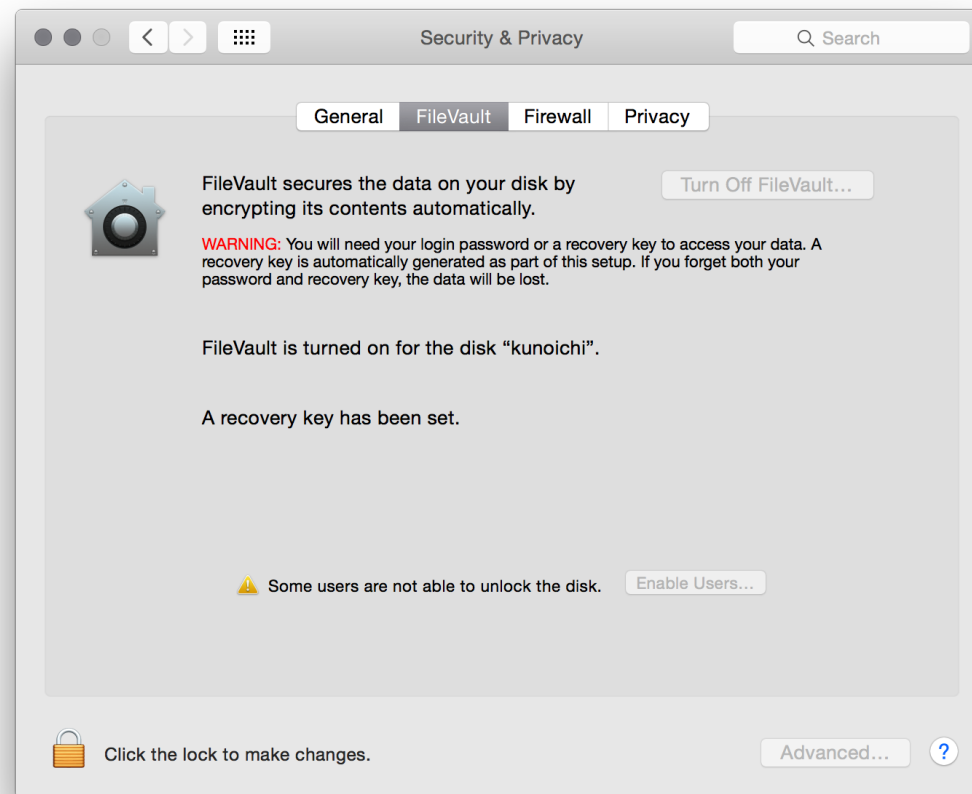
- Indbygget i Enigmail er funktionalitet til at generere nøgler
- følg den *wizard* som kommer frem.
- **Lav din første nøgle med 1 års levetid** - du ved mere om et år ☺

# Thunderbird Enigmail: Compose email



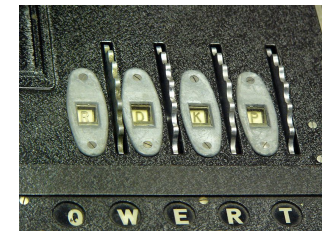
Når du sender vælger du om der skal krypteres og signeres

# Bonus: Full Disk Encryption Mac OS X



Indbygget, gratis, stærk - slå det til når I kommer hjem

## Bonus: DNS censur i Danmark



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

- `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](http://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](mailto:hik@kramse.org)