

Velkommen til

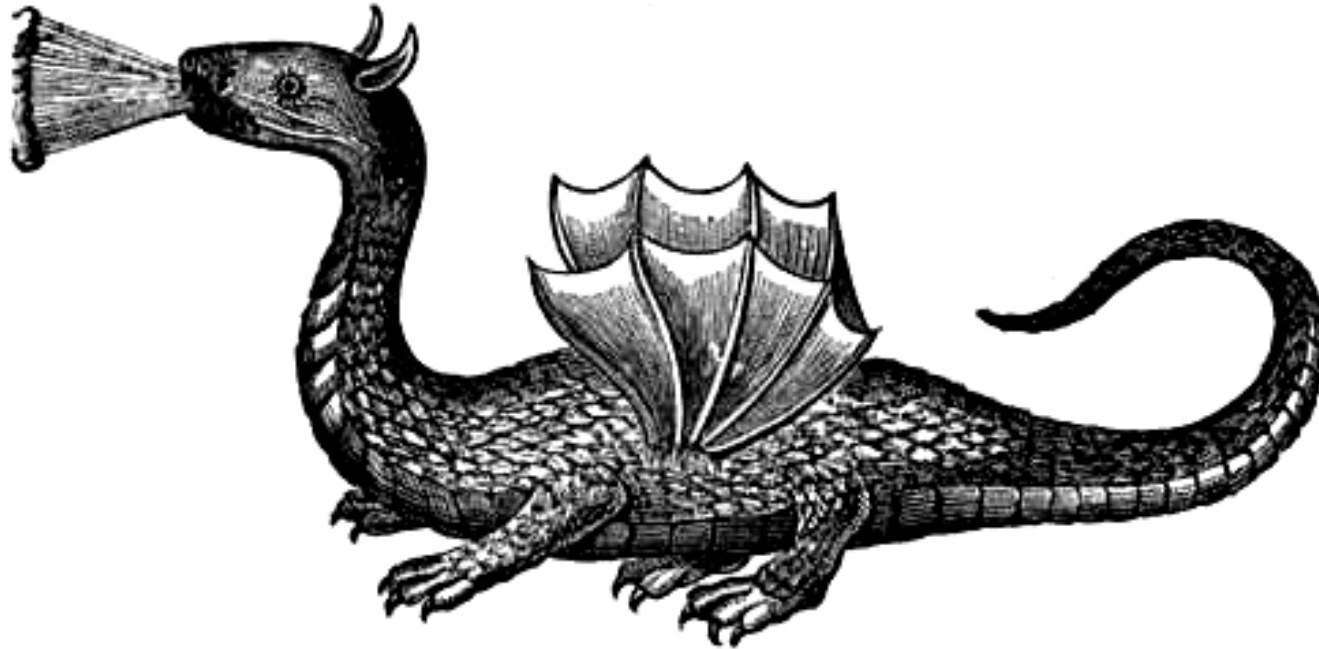
Cryptoworkshop

Henrik Lund Kramshøj hlik@kramse.org



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

Warning

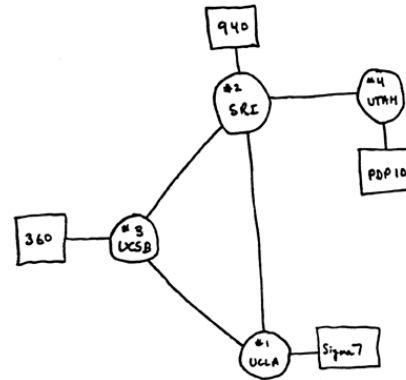


This is just a taste of crypto - introduction

Dont feel secure until you have experience and understand the programs better.

BUT learn the tools before you need them

Internet: A very short story



1969: ARPANET 4 nodes

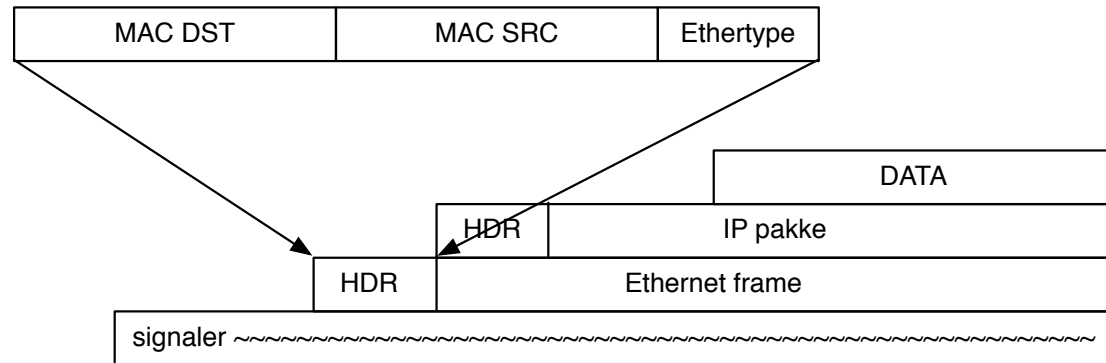
World wide network - of networks!

No owner, no single entity responsible

International, cross border, spans the world

Now 50.000 ASNs announced, and 80.000 allocated

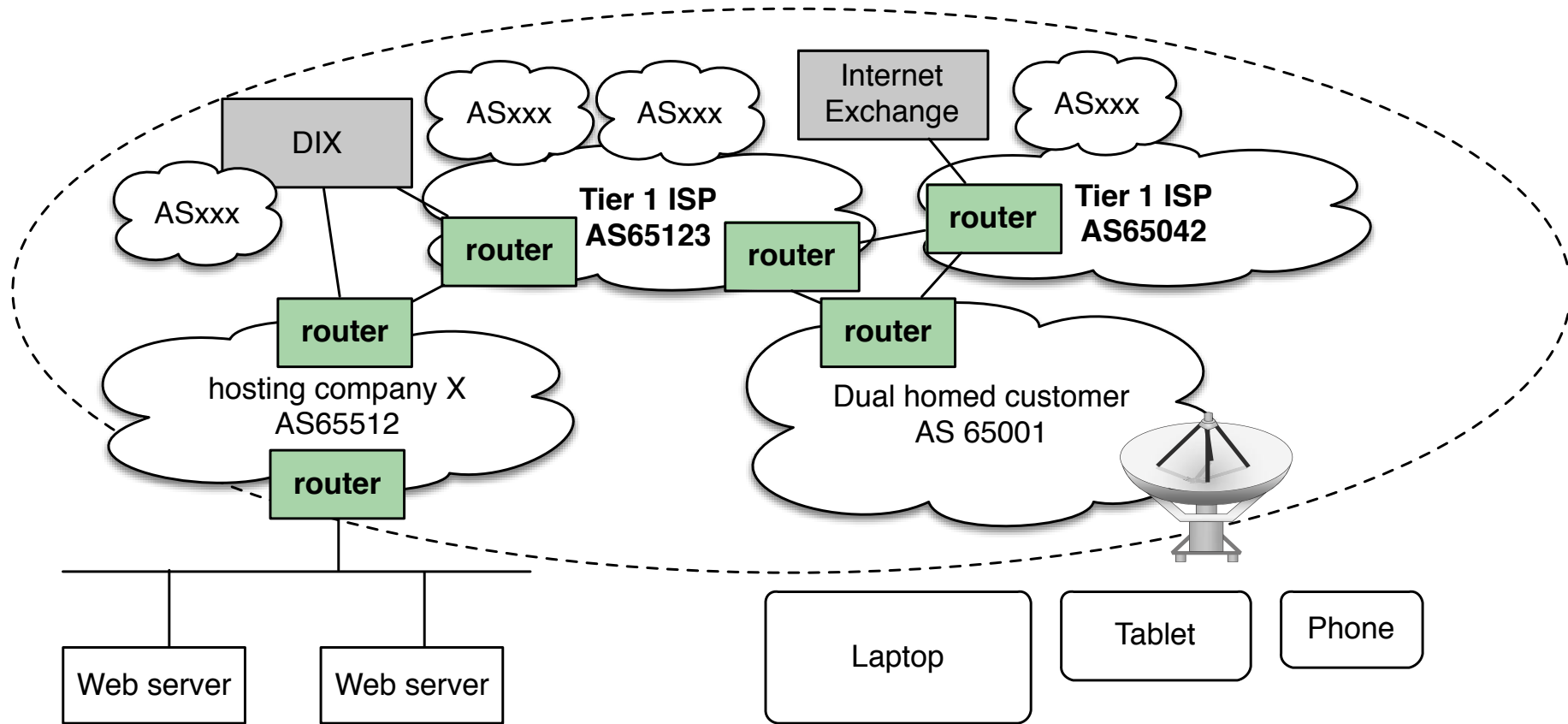
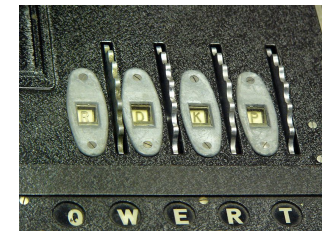
Now 515.000 prefixes - reach 550.000 routes/prefixes in 2015?



Example Internet Datagram Header

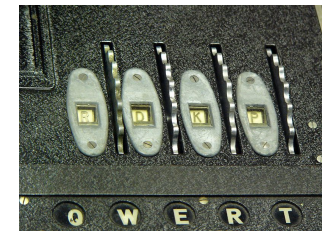
© copyright 2015 Creative Commons CC Zero - public domain

Internet core today networks approx = AS numbers



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

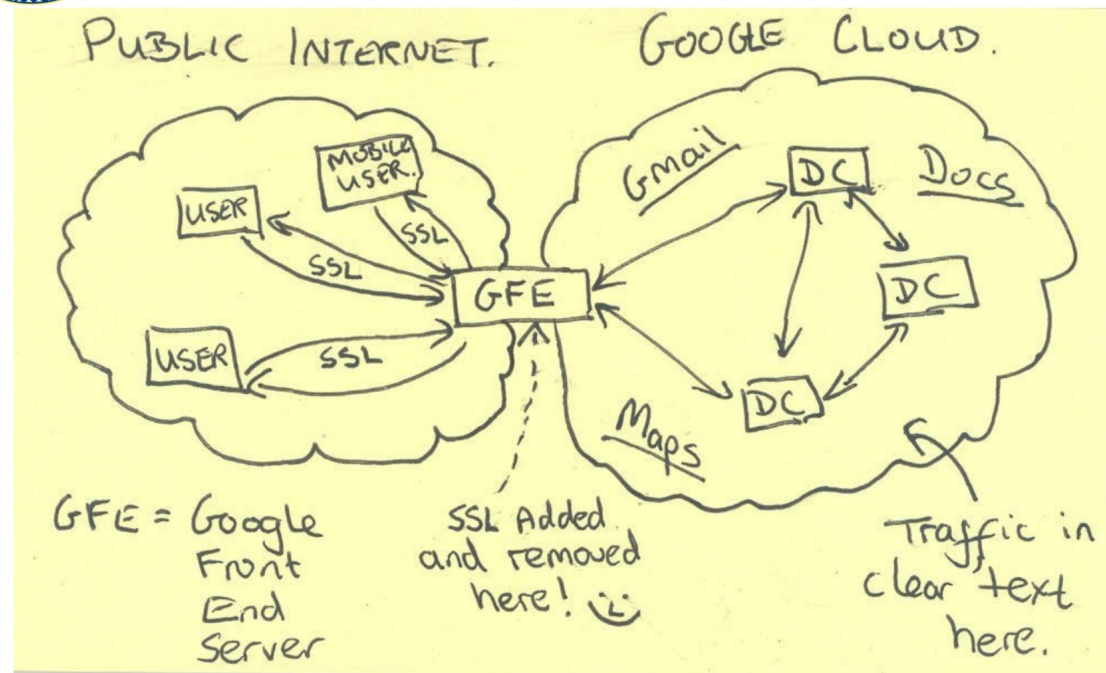
<http://oldwww.dknog.dk/dknog3/agenda>



TOP SECRET//SI//NOFORN



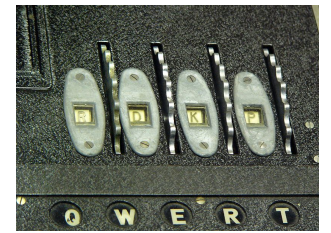
Current Efforts - Google



TOP SECRET//SI//NOFORN

SSL (encryption) added and removed here

Solidaritetskryptering



Hvorfor skal vi kryptere?

Køn

Seksualitet

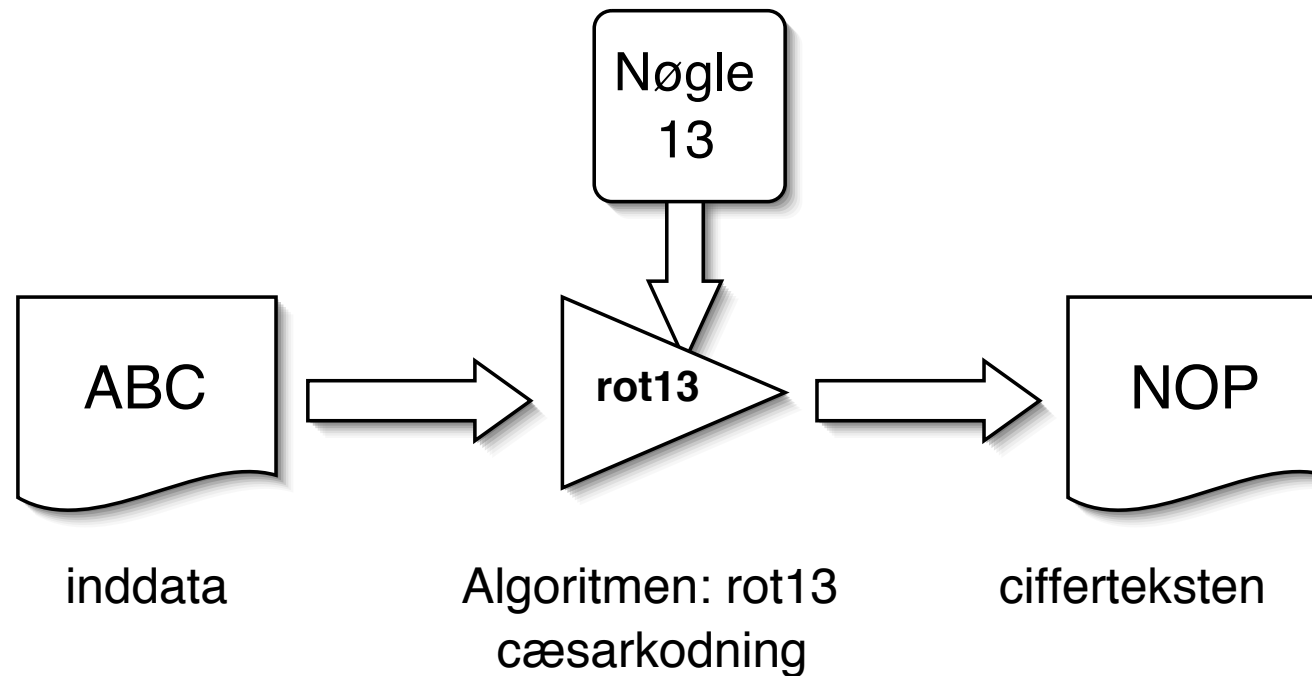
Tro religion hatecrimes

Politisk overbevisning, eller blot aktiv

Whistleblowers soldater diplomater

Du bestemmer ikke hvem der diskrimineres eller trues i andre lande

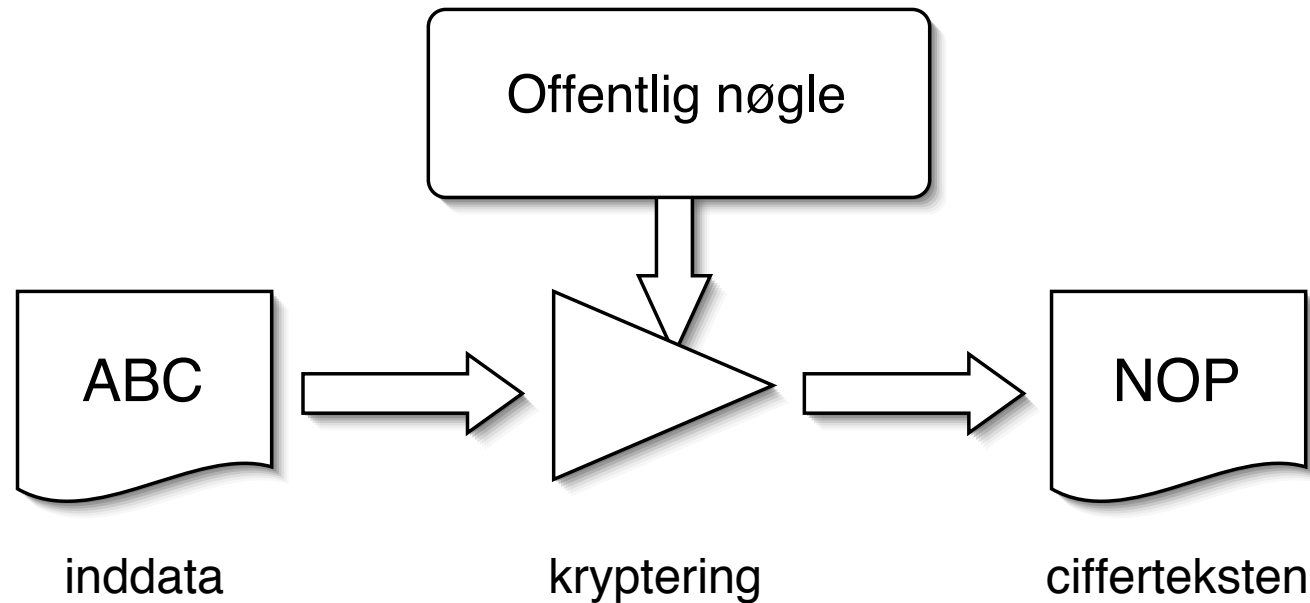
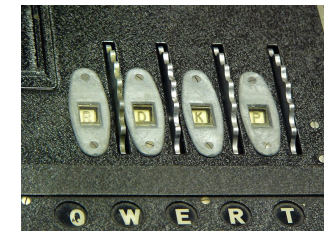
Når vi krypterer hjælper vi andre! **Solidaritetskryptering**



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

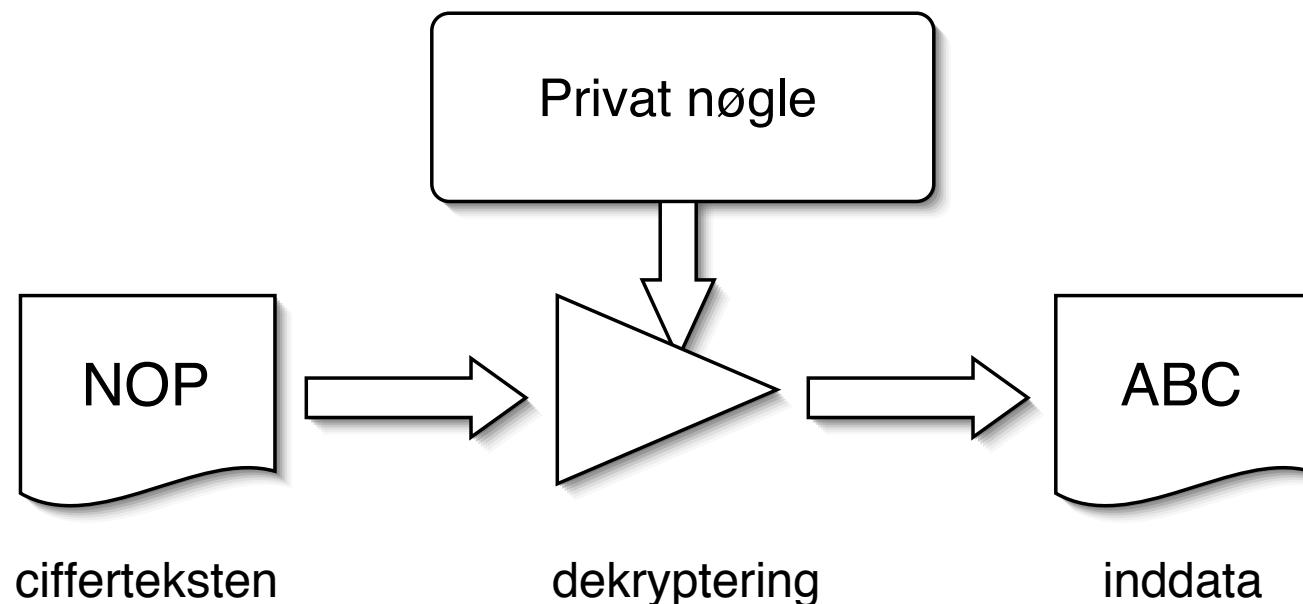
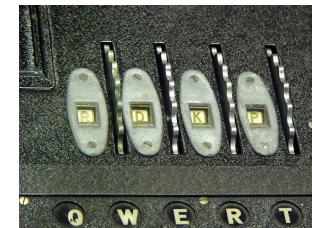
Public key kryptografi - 1



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


NB: Kryptering alene sikrer ikke anonymitet

Tor project anonym web browsing



Anonymity Online

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

[Download Tor](#)

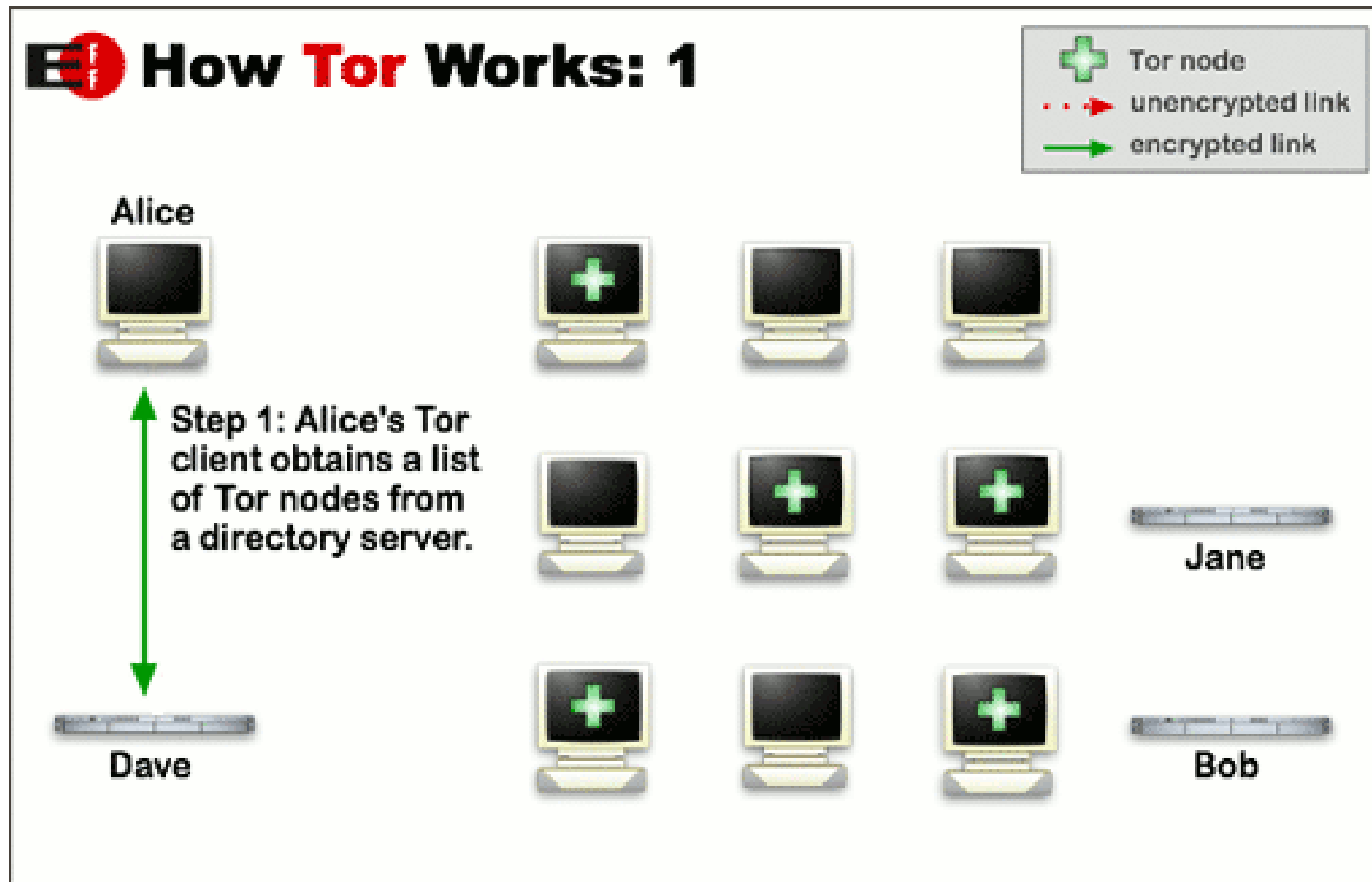
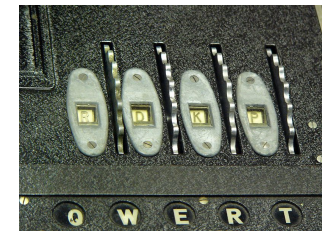
- Tor prevents anyone from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, remote logins, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android

Der findes alternativer, men Tor er mest kendt

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

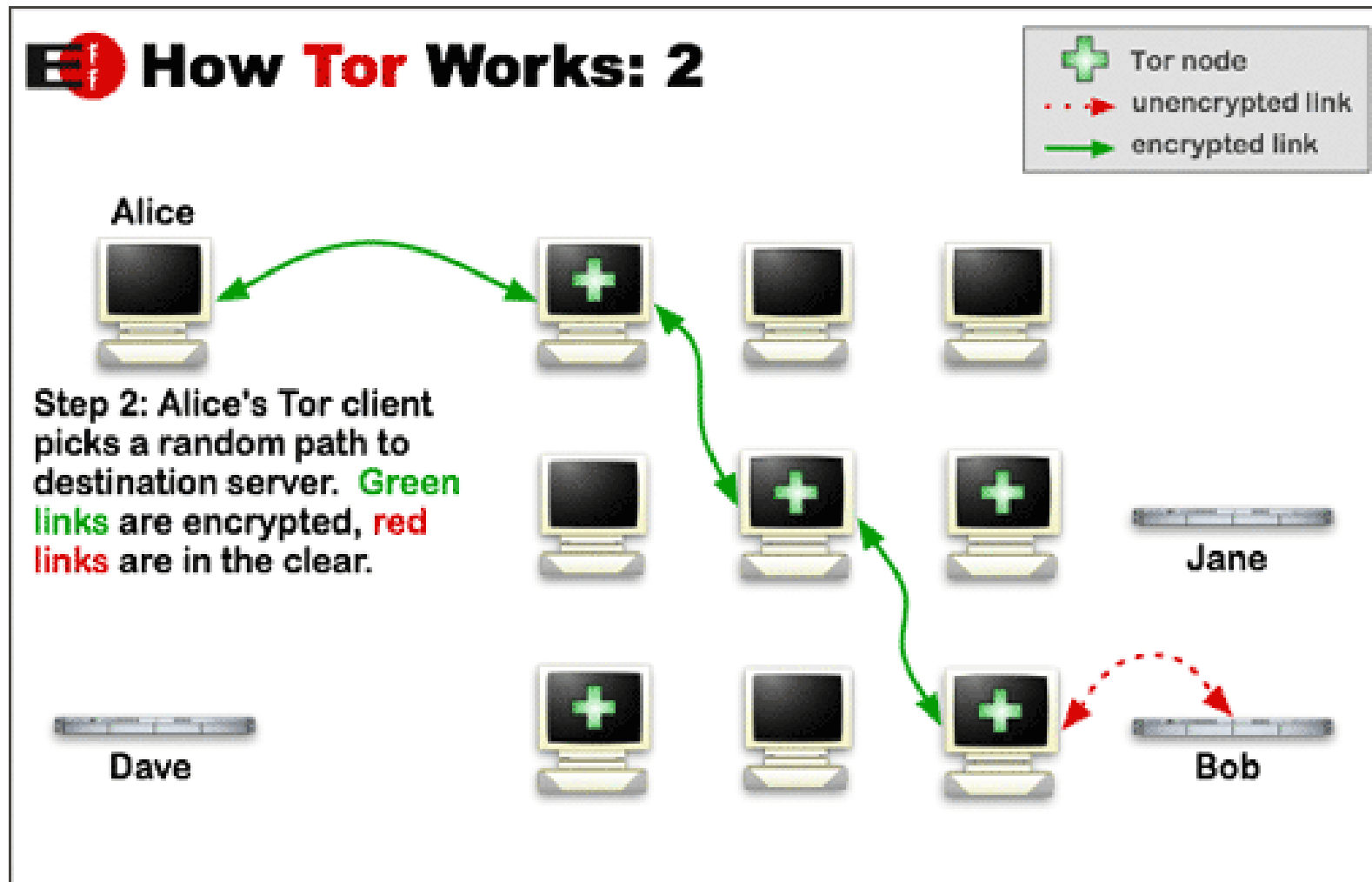
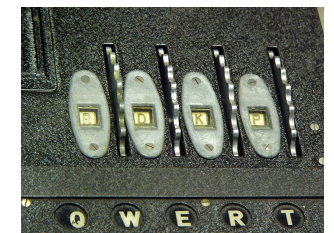
Det anbefales at bruge Torbrowser bundles fra <https://www.torproject.org/>

Tor project - how it works 1



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

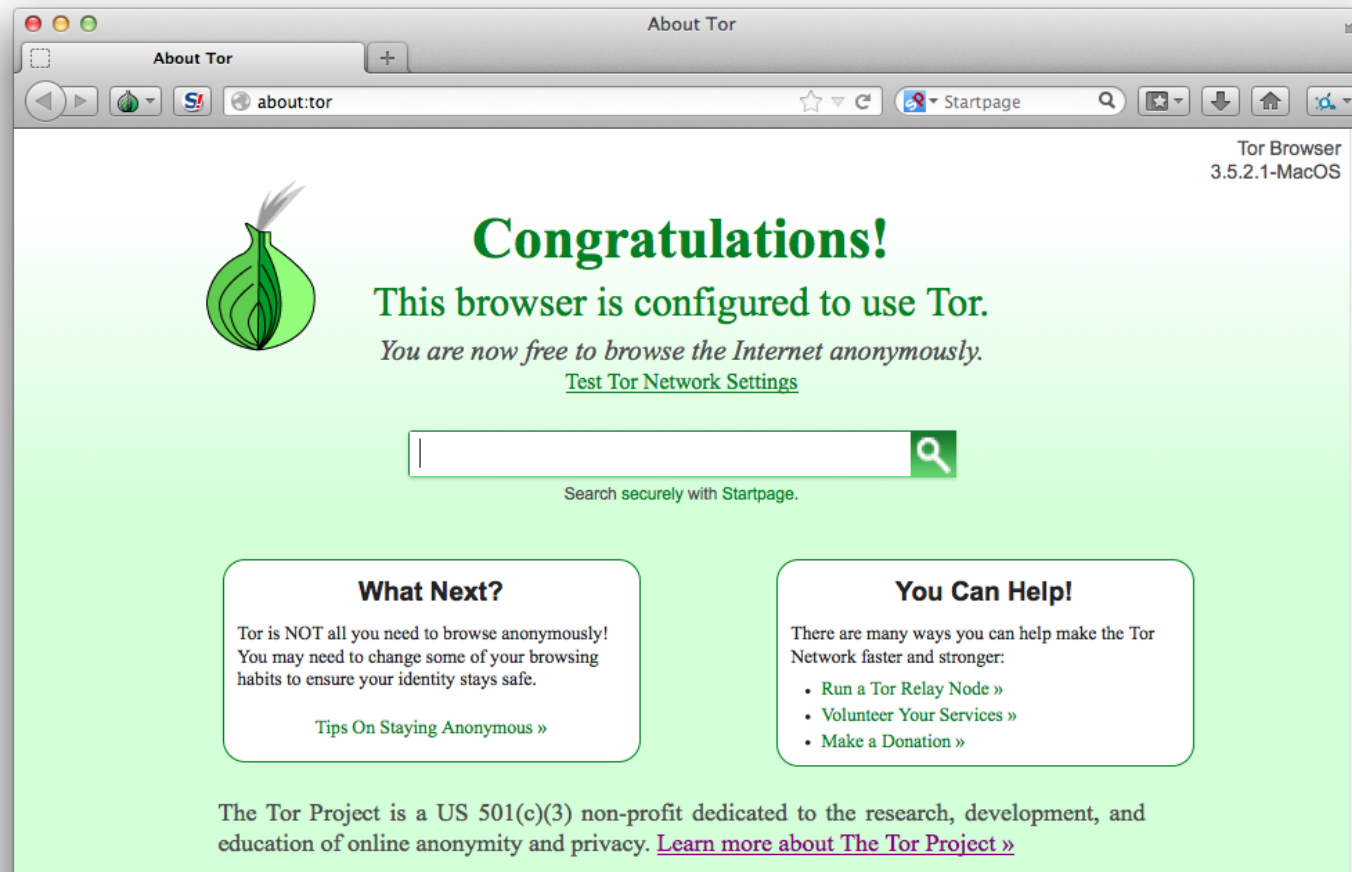
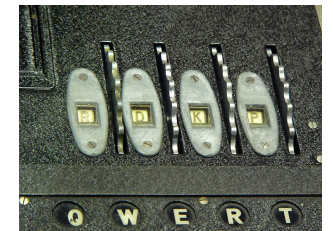
Tor project - how it works 2



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

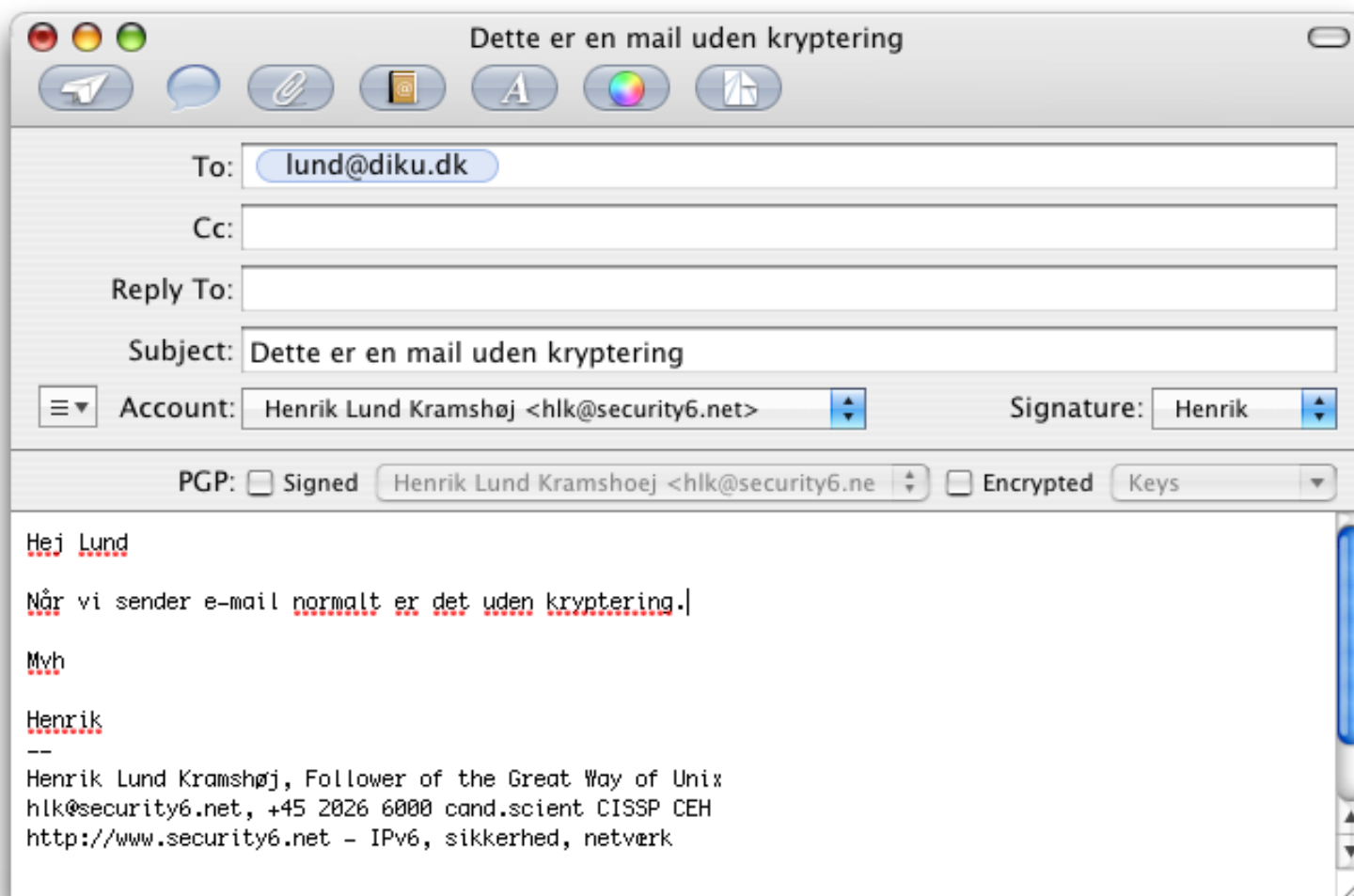
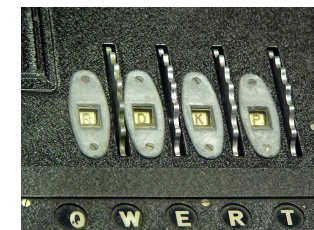


Torbrowser - anonym browser



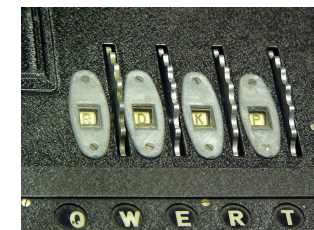
Mere anonym browser - Firefox i forklædning

Email er usikkert



Email uden kryptering - er som et postkort

Email med kryptering - afsendelse



Opdateringer i weekenden

To: Henrik Lund Kramshøj <hlk@security6.net>

Cc:

Reply To:

Subject: Opdateringer i weekenden

Account: Henrik Lund Kramshøj <hlk@kramse.dk> Signature: Henrik

PGP: ☒ Signed Henrik Lund Kramshøj <hlk@security6.net> (work) ☒ Encrypted Keys

Hej Hlk6

Alarmkoden er ændret til 1234 på adgangskortet til serverrummet.

Jeg har også ændret administratorkodeordet til 'toor'

Mvh

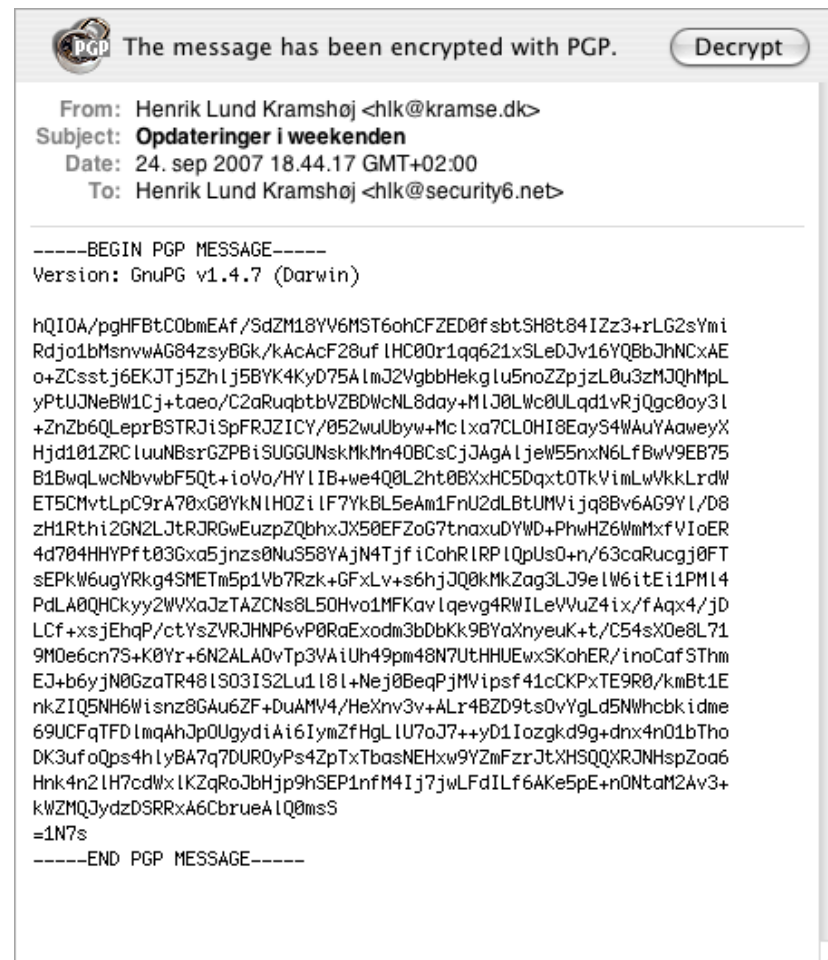
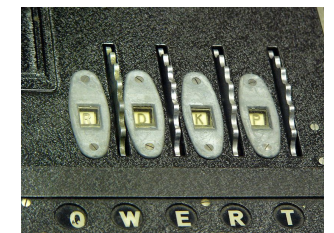
Henrik

--

Henrik Lund Kramshøj, Follower of the Great Way of Unix
hlk@security6.net, +45 2026 6000 cand.scient CISSP CEH
<http://www.security6.net> - IPv6, sikkerhed, netværk

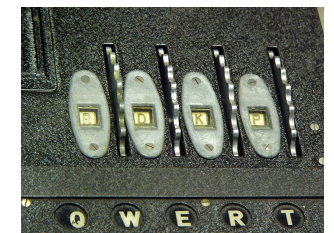
En sikker krypteret email er ikke sværere at sende

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

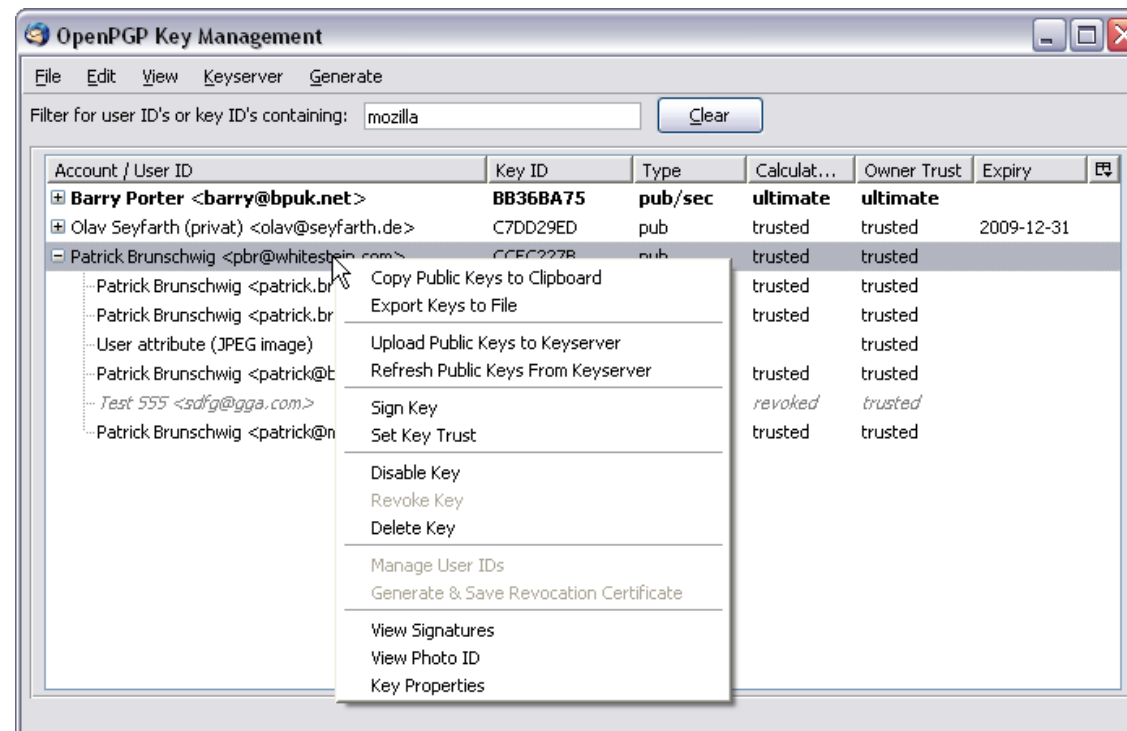
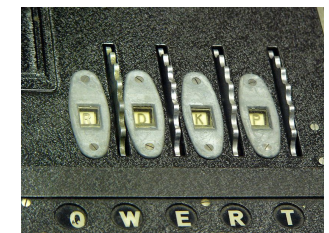
Enigmail provides end to end security for Mozilla Thunderbird and SeaMonkey.

Enigmail automatically decrypts and verifies your Email

Enigmail er en udvidelse til Thunderbird email programmet

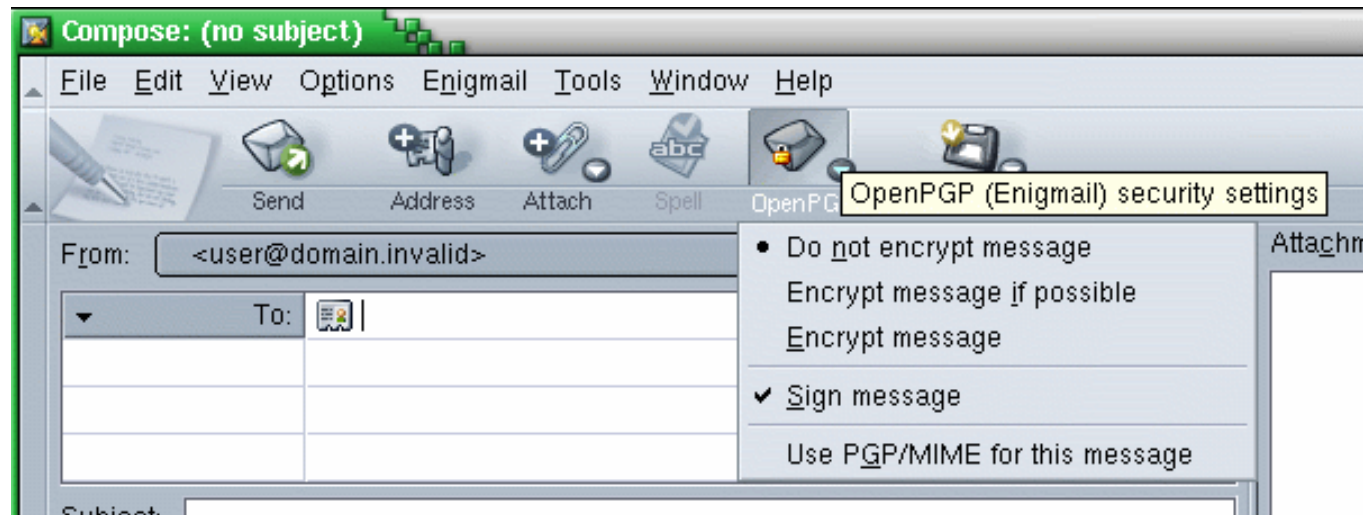
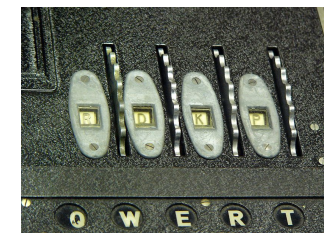
<https://www.enigmail.net>

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

Comments and questions



You are always welcome to send me questions later via email

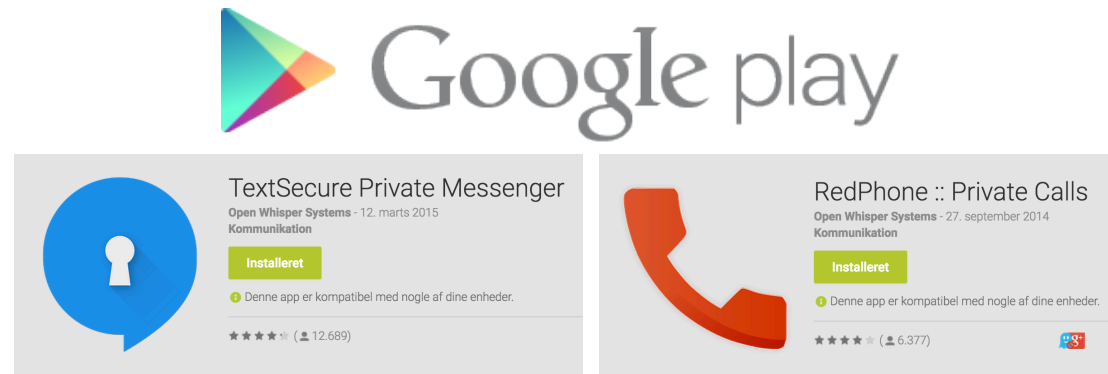
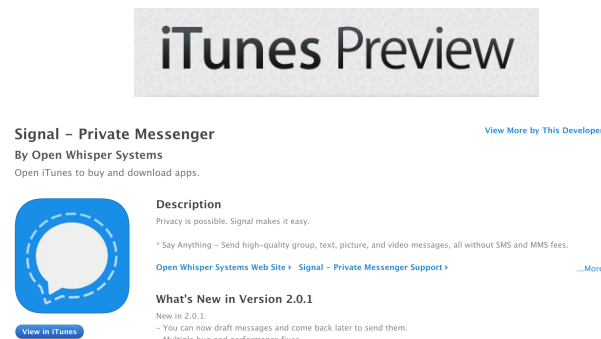
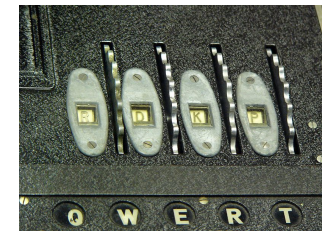
Henrik Lund Kramshøj hik@kramse.org

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 😊