Welcome to

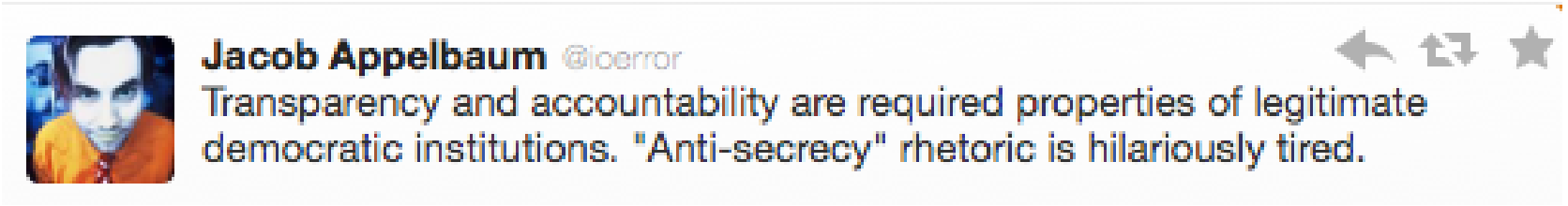
Sikker browsing, plugins og Tor project

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

http://www.solidonetworks.com

Key words: multiple browsers, crypto, Torproject and how to protect yourself

Formål: Hvorfor gør vi det her?



Et demokrati fordrer borgere med frihed som har evnen til at tage beslutninger uden konstant at være overvåget.

Et demokrati fordrer borgere som aktivt vælger hvornår de afgiver personlige data om deres liv og færden og **kryptografi er en fredelig protest mod indsamling at data.**

Indsamlede data vil altid blive misbrugt

Data som indsamles **bliver misbrugt** enten til kriminelle formål, kommercielle formål uanset oprindelige formål med indsamlingen - under dække af beskyttelse mod terror, ekstremisme, Al Qaeda, nazisme, misbrug af børn, ... Le mal du jour / dagens onde.

Derudover stalking, ekskærester, arbejdsgivere, forældre, ...

Du bestemmer - det er demokrati

Why think of security?

> Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world. A Cypherpunk's Manifesto by Eric Hughes, 1993

Copied from `https://cryptoparty.org/wiki/CryptoParty`

Security is not magic

.

Think security, it may seem like magic - but it is not

Follow news about security

Support communities, join and learn

Face reality

- Criminals sell your credit card information and identity theft
- Trade infected computers like a commodity
- Governments write laws that allows them to introduce back-doors - and use these
- Governments do blanket surveillance of their population
- Governments implement censorship, threaten citizens and journalist
- Governments will introduce back-doors in products we use
- Danish police and TAX authorities have the legals means, see *Rockerloven*

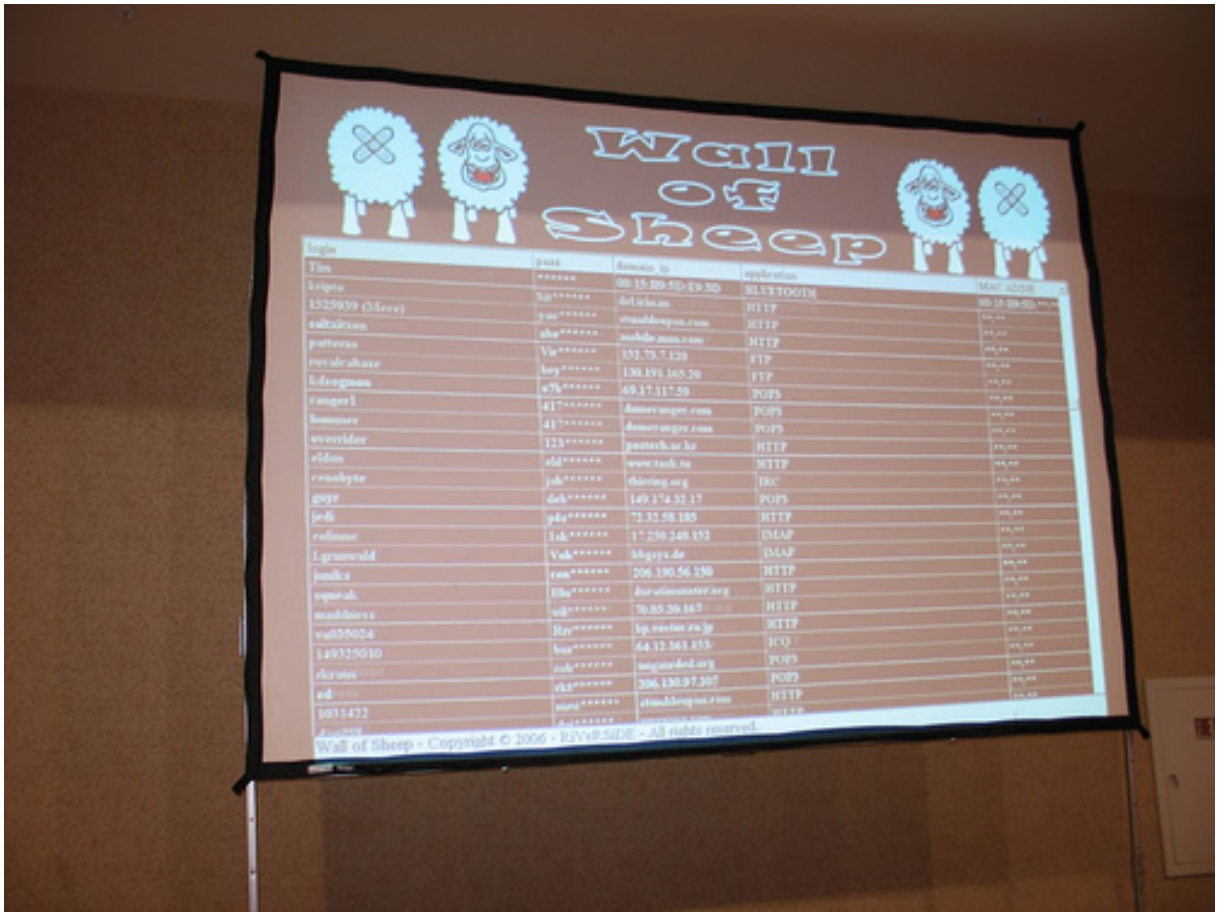
You are not paranoid when there are people actively attacking you!

Use protection - always

Hacking er ikke magi

Hacking kræver blot lidt ninja-træning

Wall of sheep



Defcon Wall of Sheep - play nice!

ER dit kodeord nemt at sniffe?

Hvordan bliver du sikker

Don’t Panic!

Lad være med at bruge een computer til alt
- en privat bærbar ER mere privat end en firmacomputer

Brug en sikker konfiguration, minimumskonfiguration

Brug sikre protokoller, kryptering:
SSH, IMAPS, POP3S, OpenPGP, HTTPS, Tor project

Opsætning af computere og netværk, hvordan?

Anbefalinger

- Låsekode på telefonen og computeren
- Opdater software og apps
- Brug ikke det samme kodeord overalt
- Pas på med at bruge åbne netværk
- Flere browsere: en til facebook, en til netbank
- Tænk på data du producerer, hvem ser dine (nøgne) SnapChat billeder?
  Måske pseudonymer og alias - brug ikke altid dit rigtige navn alle steder
- slå kryptering til: IMAP**S**, POP3**S**, HTTP**S**

First advice use the modern operating systems

Newer versions of Microsoft Windows, Mac OS X and Linux

- Buffer overflow protection
- Stack protection, non-executable stack
- Heap protection, non-executable heap
- *Randomization of parameters* stack gap m.v.

Note: these still have errors and bugs, but are better than older versions

Always try to make life worse and more costly for attackers

Flere browsere

- Flere browsere: en til facebook, en til netbank
- Sikre indstillinger og NoScripts til generel surfing
- Løsere indstillinger til Netflix, Facebook m.fl.
- Husk at installere gode plugins som HTTPS Everywhere, NoScript, CertPatrol m.fl.

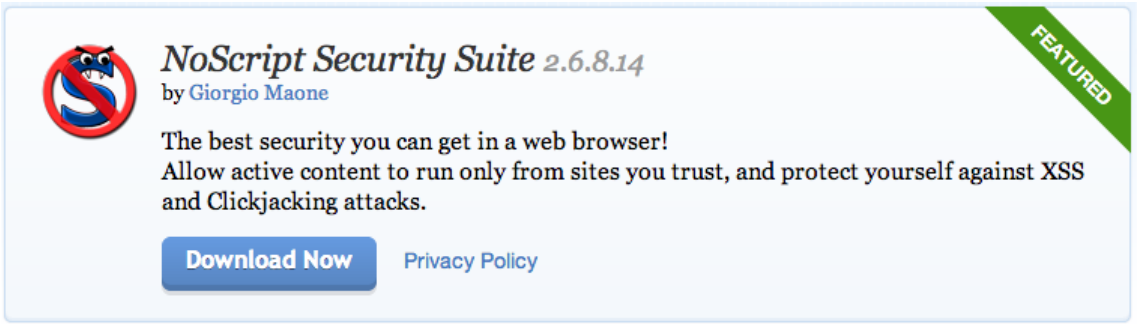
HTTPS Everywhere

HTTPS Everywhere is a Firefox extension produced as a collaboration between The Tor Project and the Electronic Frontier Foundation. It encrypts your communications with a number of major websites.

`http://www.eff.org/https-everywhere`

Also in Chrome web store!

NoScript and NotScripts



NotScripts for Chrome

> A clever extension that provides a high degree of 'NoScript' like control of javascript, iframes, and plugins on Google Chrome.

Du tillader kun scripts på de sider hvor det er nødvendigt.

Hint: du kan undgå mange reklamer, og måske springe foran i køsystemer ☺

CertPatrol - which site uses which certificate

An add-on formerly considered paranoid: CertPatrol implements ”pinning” for Firefox/Mozilla/SeaMonkey roughly as now recommended in the User Interface Guidelines of the World Wide Web Consortium (W3C).

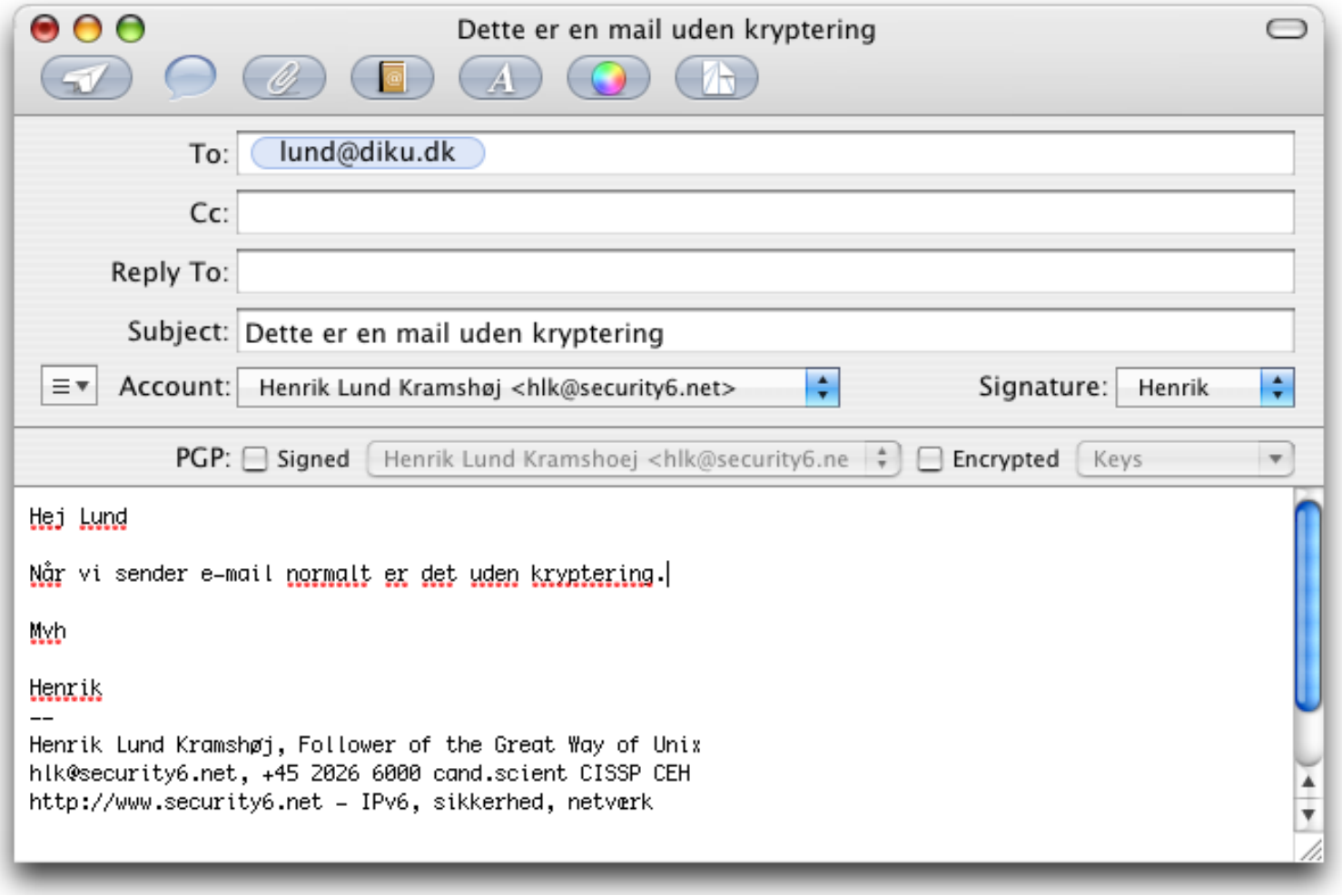
`http://patrol.psyced.org/`

Vi laver nu øvelsen

Installation af alternativ browser

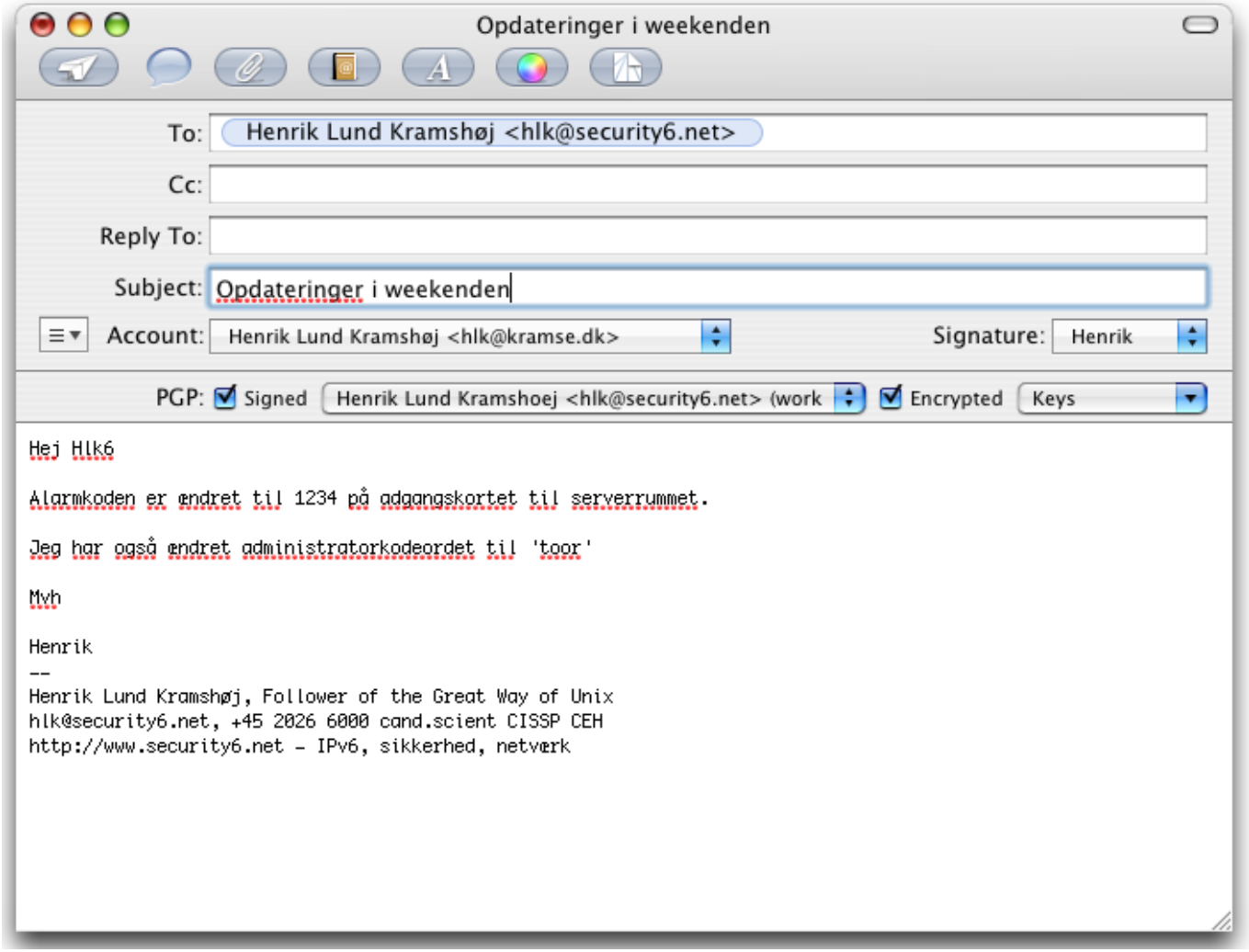
som er øvelse 1 fra øvelseshæftet.

Email er usikkert



Email uden kryptering - er som et postkort

Email med kryptering - afsendelse

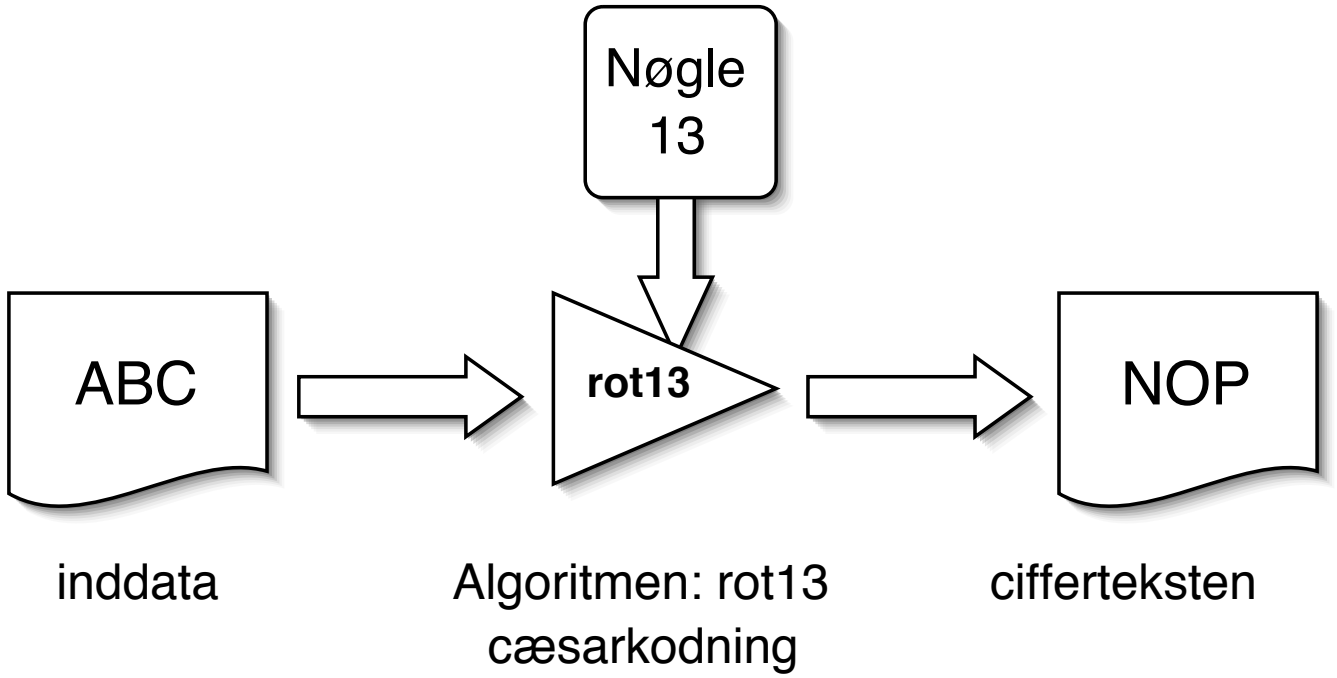


En sikker krypteret email er ikke sværere at sende

Krypteret Email under transporten

En sikker krypteret email er beskyttet undervejs

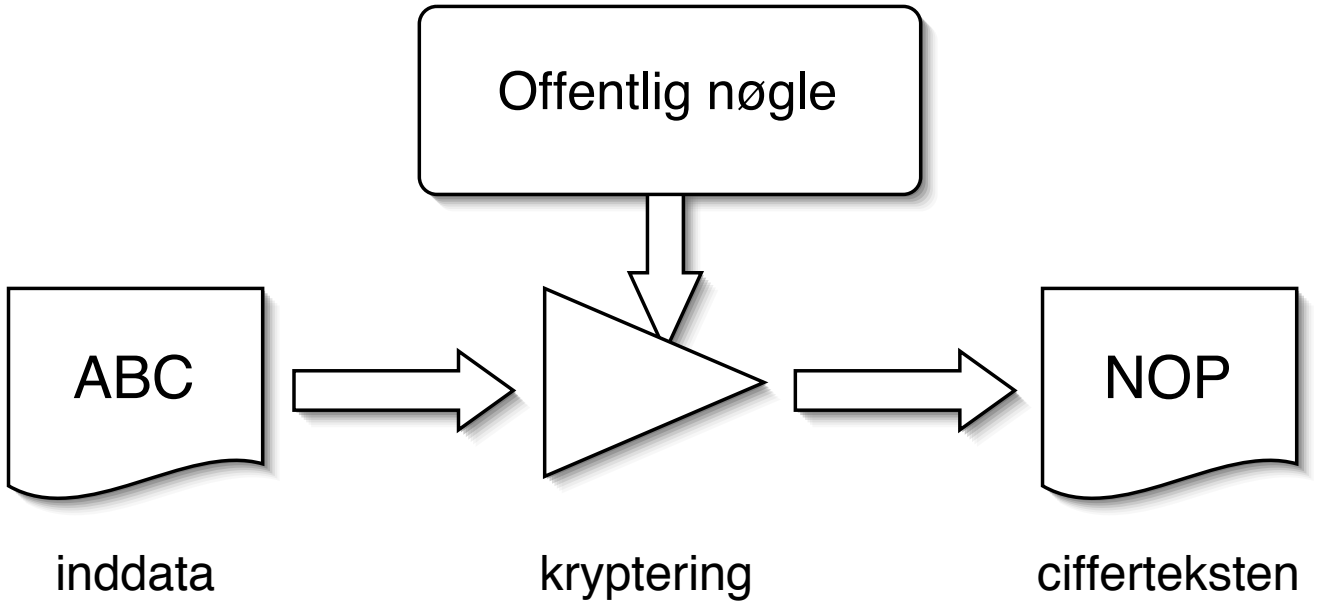
Kryptografi



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

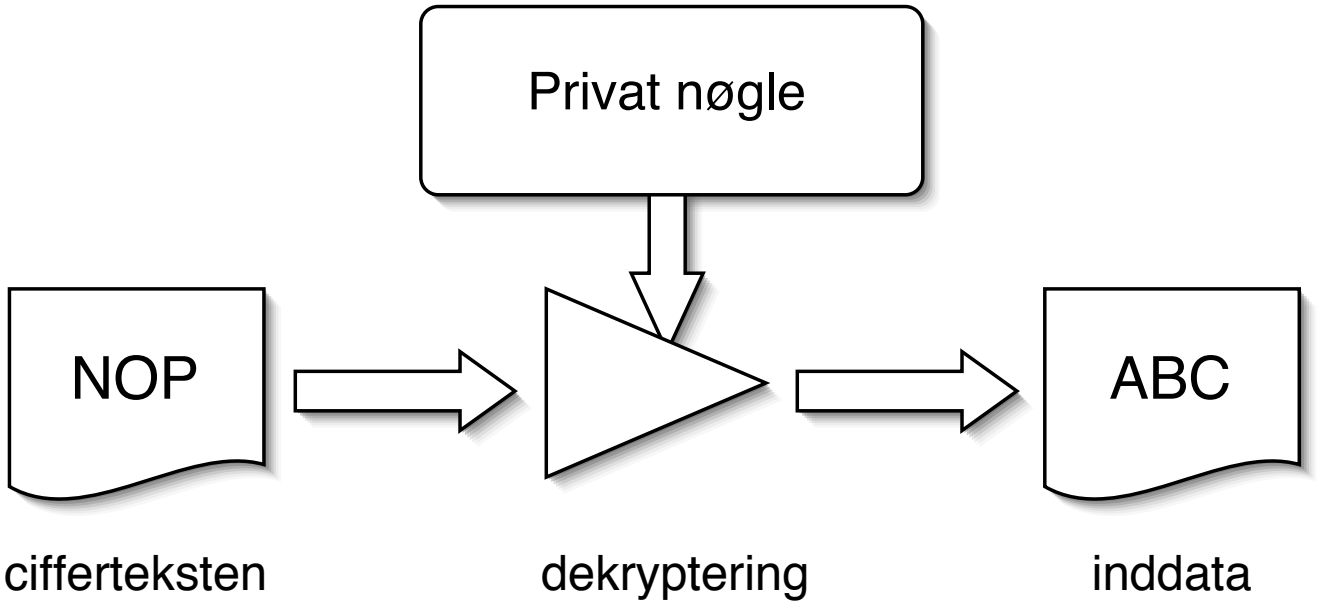
Public key kryptografi - 1



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

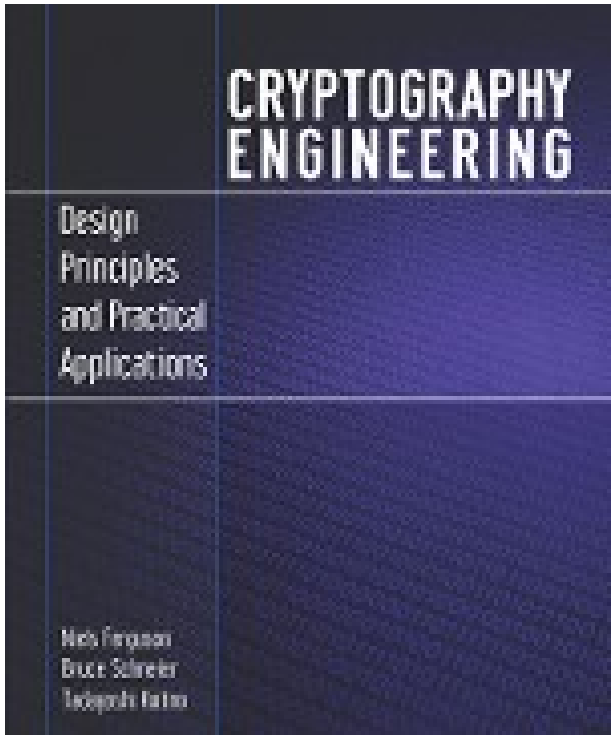
Public key kryptografi - 2



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

Vi laver nu øvelsen

Installation af Thunderbird

som er øvelse 2 fra øvelseshæftet.

SOLIDO NETWORKS

Vi laver nu øvelsen

Installation af GPG GNU Privacy Guard

som er øvelse 3 fra øvelseshæftet.

SOLIDO NETWORKS

Vi laver nu øvelsen

Lav en PGP-kompatibel nøgle

som er øvelse **5** fra øvelseshæftet.

SOLIDO NETWORKS

Vi laver nu øvelsen

Hent en nøgle fra en anden

som er øvelse 6 fra øvelseshæftet.

SOLIDO NETWORKS

Vi laver nu øvelsen

Send en krypteret mail

som er øvelse 7 fra øvelseshæftet.

Vi laver nu øvelsen

Signer en nøgle

som er øvelse 8 fra øvelseshæftet.

SOLIDO NETWORKS

Vi laver nu øvelsen

Installation af Truecrypt

som er øvelse 9 fra øvelseshæftet.

Filoverførsel - Do NOT USE FTP

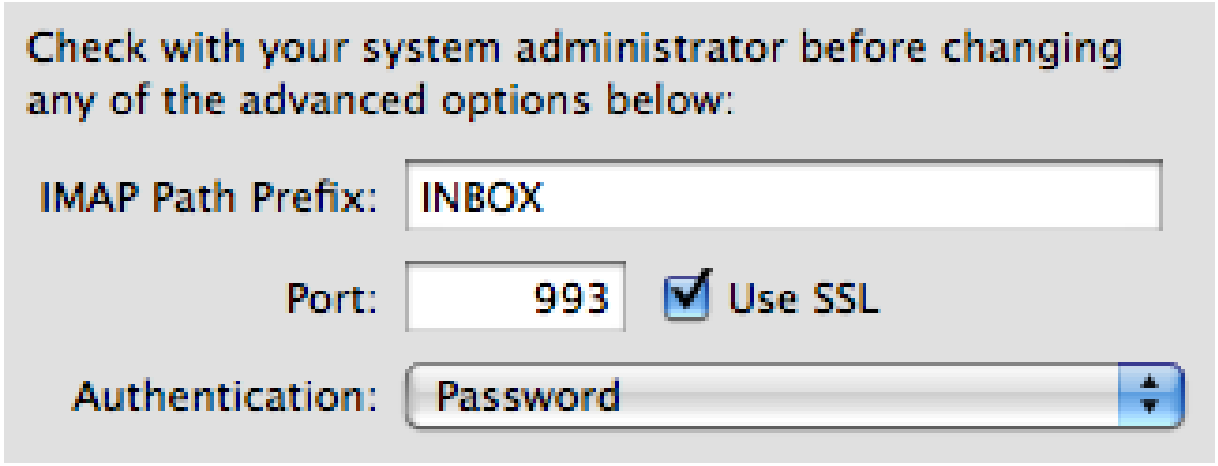
File Transfer Protocol - filoverførsler

FTP bruges især til:

- FTP - drivere, dokumenter, rettelser - Windows Update? er enten HTTP eller FTP
- Opdatering af websites
- Overførsel af data mellem virksomheder
- Serveren er indbygget i de fleste serveroperativsystemer

FTP sender i klartekst
USER brugernavn og
PASS hemmeligt-kodeord

SSL/TLS udgaver af protokoller



Mange protokoller findes i udgaver hvor der benyttes SSL

SSL er det samme som HTTPS - altså en sikker kommunikation

HTTPS vs HTTP, IMAPS, POP3S, osv.

Bemærk: nogle protokoller benytter to porte IMAP 143/tcp vs IMAPS 993/tcp

FileZilla - understøtter SFTP

FileZilla Features

Overview

FileZilla Client is a fast and reliable cross-platform FTP, FTPS and SFTP client with lots of useful features

Features

Among others, the features of FileZilla include the following:

- Easy to use
- Supports FTP, FTP over SSL/TLS (FTPS) and SSH File Transfer Protocol (SFTP)
- Cross-platform. Runs on Windows, Linux, *BSD, Mac OS X and more
- IPv6 support
- Available in many languages
- Supports resume and transfer of large files >4GB
- Tabbed user interface
- Powerful Site Manager and transfer queue
- Bookmarks
- Drag & drop support
- Configurable transfer speed limits

http://filezilla-project.org/

Vi laver nu øvelsen

Installation af FileZilla

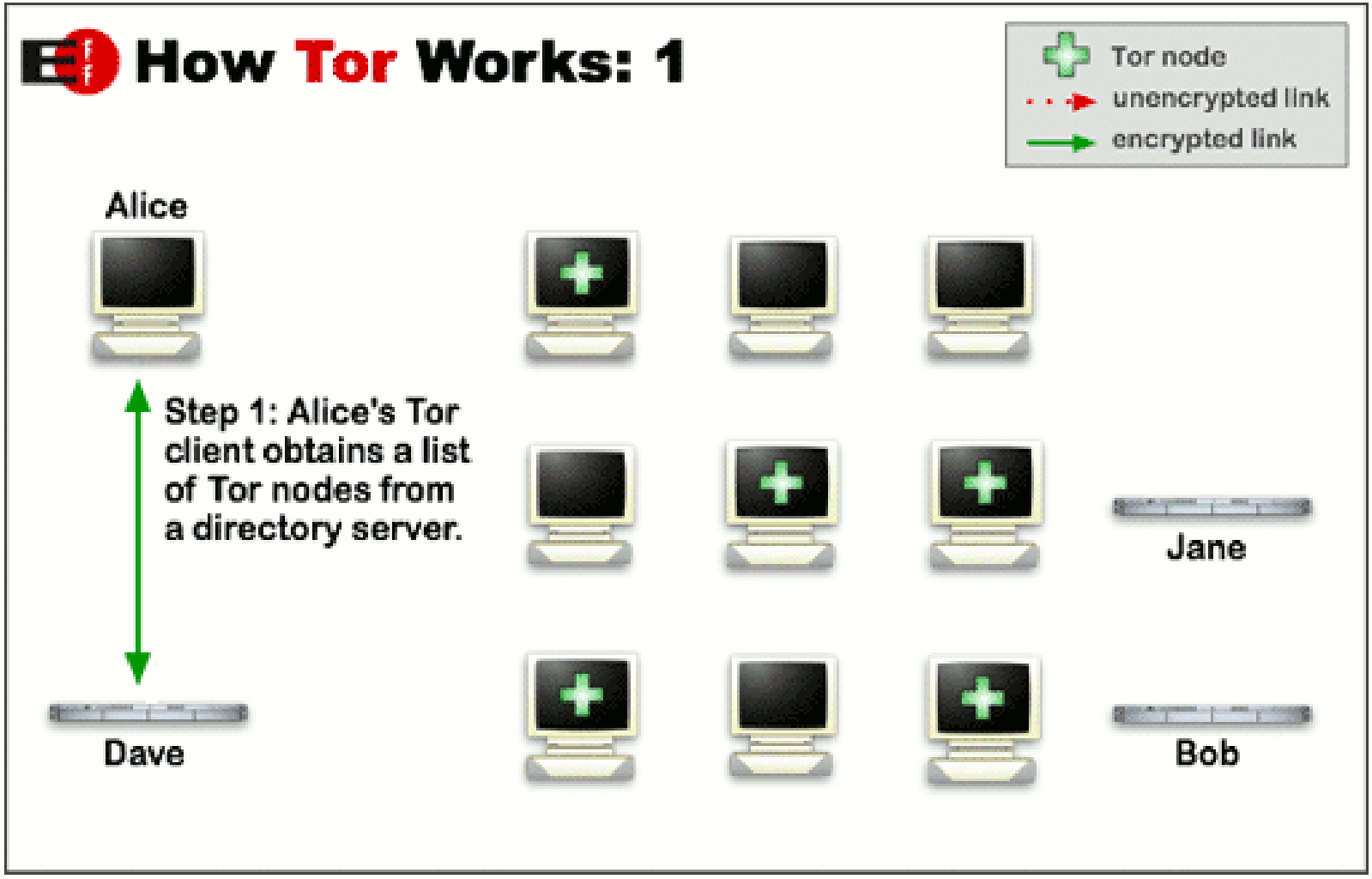
som er øvelse **10** fra øvelseshæftet.

Tor project anonym webbrowsing

`https://www.torproject.org/`

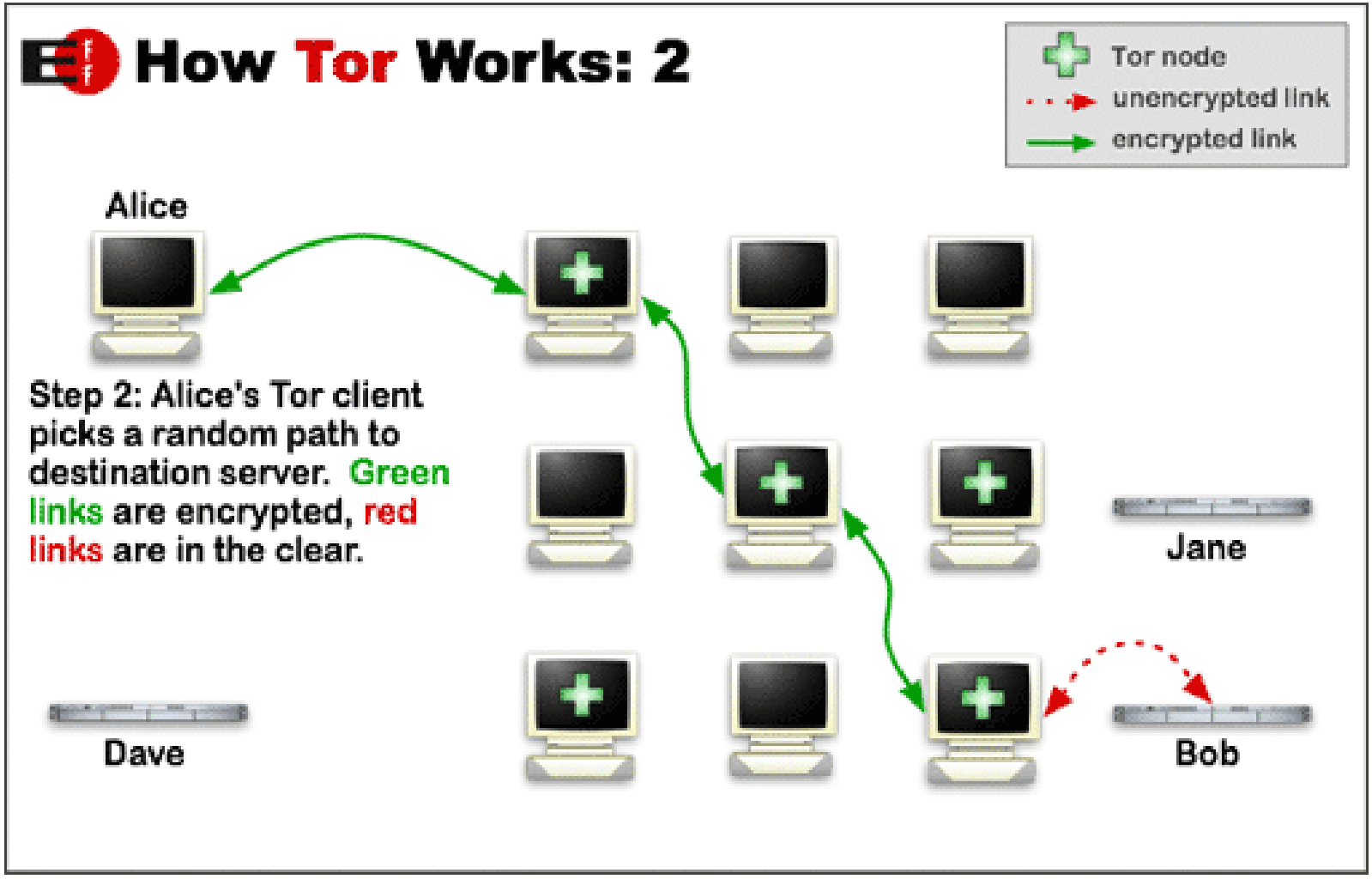
Der findes alternativer, men Tor er mest kendt

Tor project - how it works 1



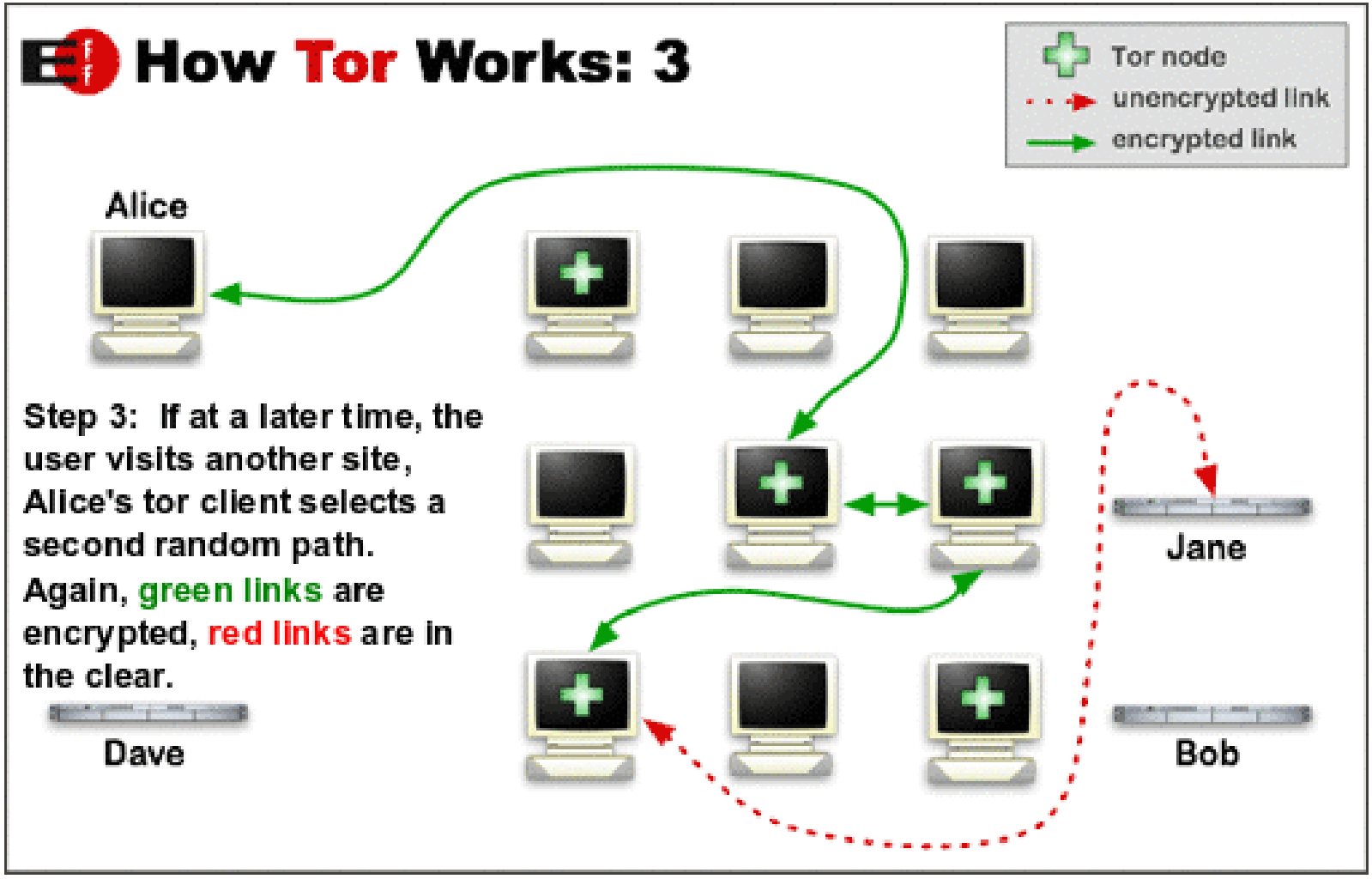
pictures from `https://www.torproject.org/about/overview.html.en`

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

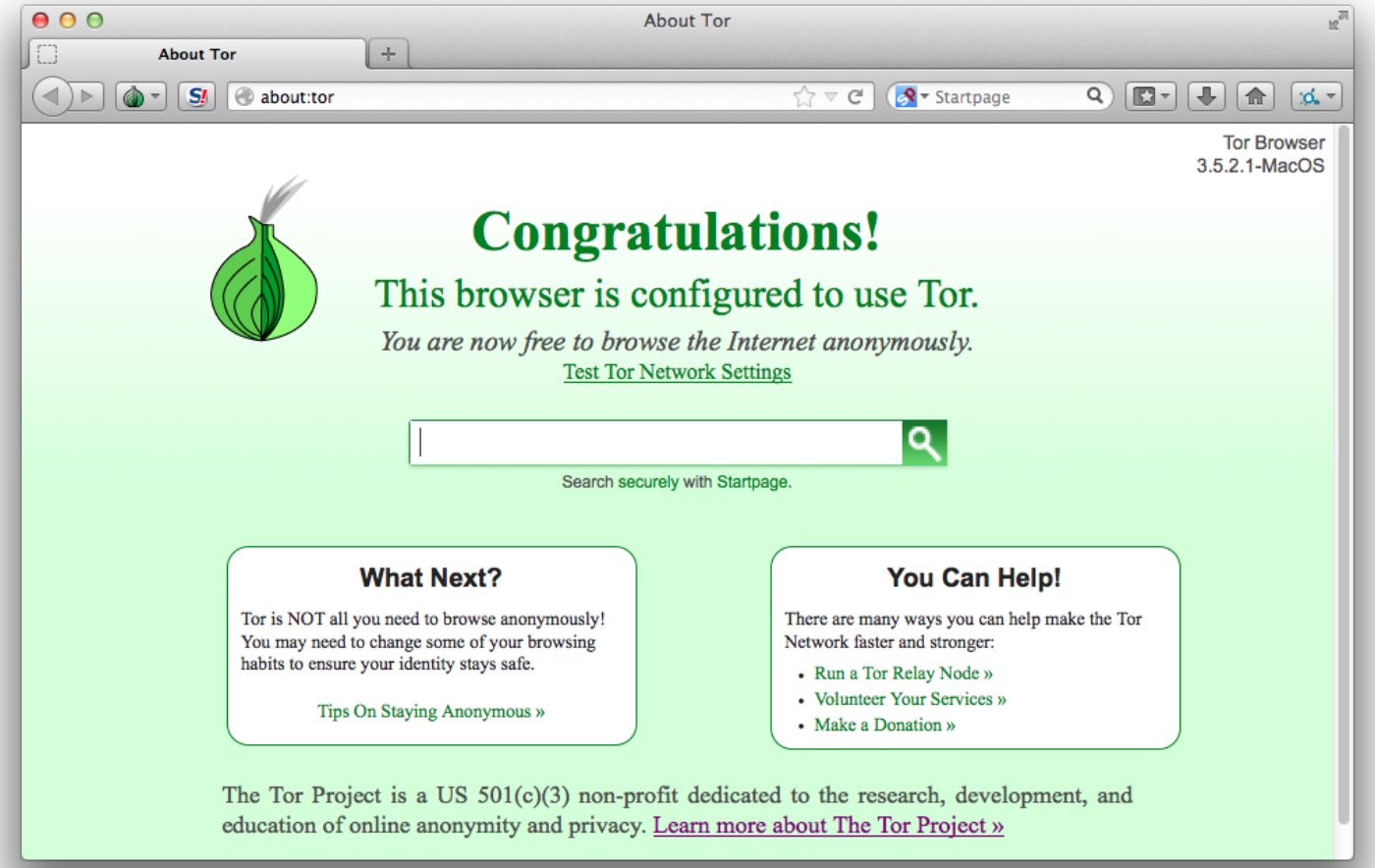
Der findes diverse tools til Tor, Torbutton on/off knap til Firefox osv.

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

Torbrowser - outdated

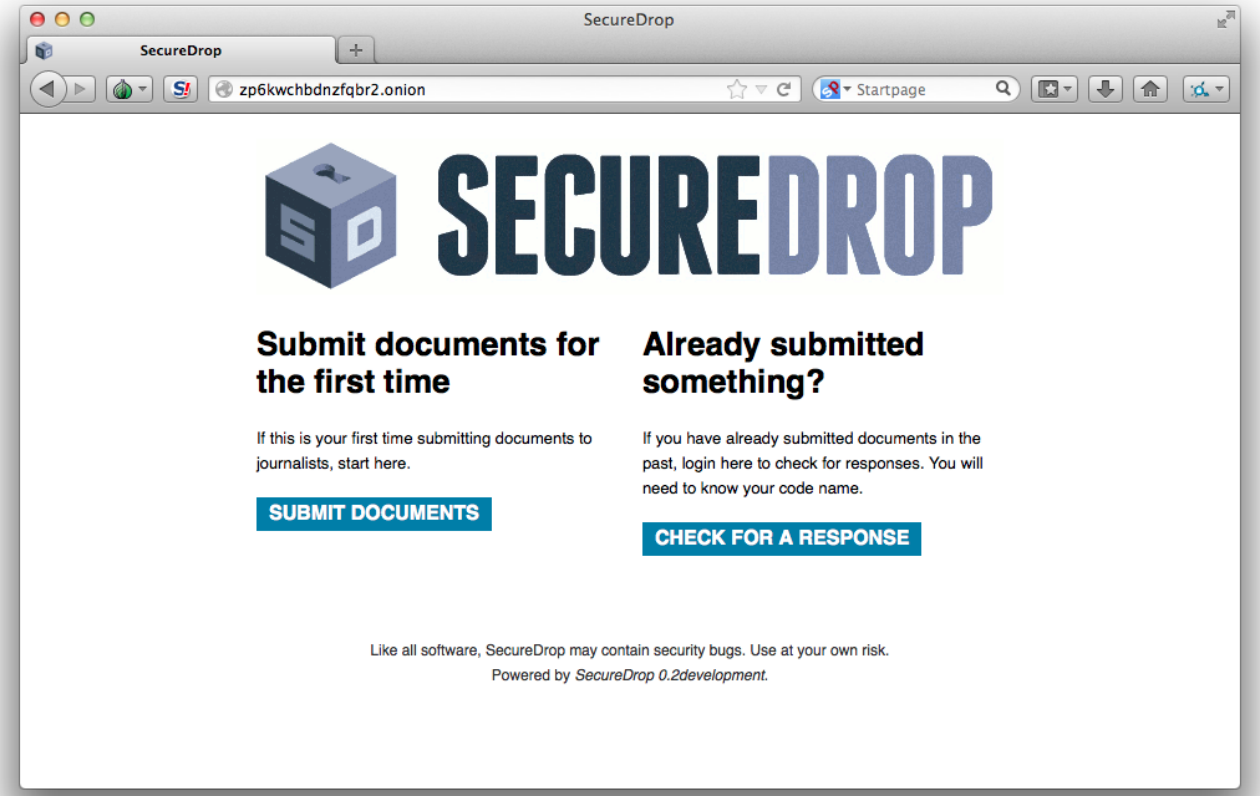
Hov den mangler opdatering!

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 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

Vi laver nu øvelsen

Installation af Torbrowser

som er øvelse 11 fra øvelseshæftet.

Hacker tools BackTrack and Kali

Hacking er sjovt, og du kan lære en masse

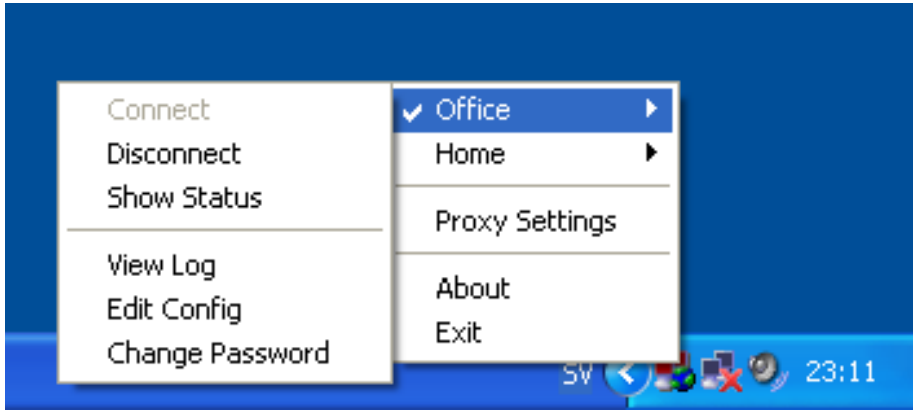
Husk at gøre det på dit eget netværk - egne systemer

Det anbefales at afvikle Kali i en virtuel maskine, på klient med VMware Player, Virtualbox eller tilsvarende

Kali Linux `http://www.kali.org/` denne version anbefales

(Gamle version BackTrack Linux `http://www.backtrack-linux.org/`)

VPN



Virtual Private Networks are useful - or even required when traveling

VPN `http://en.wikipedia.org/wiki/Virtual_private_network`

SSL/TLS VPN - Multiple incompatible vendors: OpenVPN, Cisco, Juniper, F5 Big IP

DNS censur i Danmark

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:

- ns1.censurfridns.dk / 89.233.43.71 / 2002:d596:2a92:1:71:53::
- ns2.censurfridns.dk / 89.104.194.142 / 2002:5968:c28e::53

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

Det er uacceptabelt at pille ved DNS - punktum!

DNSSEC trigger

Der findes mange DNSSEC programmer, blandt andet DNSSEC-trigger som er en navneserver til din lokale PC

- DNSSEC Validator for firefox
  `https://addons.mozilla.org/en-us/firefox/addon/dnssec-validator/`
- OARC tools `https://www.dns-oarc.net/oarc/services/odvr`
- `http://www.nlnetlabs.nl/projects/dnssec-trigger/`

Følg med Twitter news

Twitter has become an important new resource for lots of stuff

Twitter has replaced RSS for me

Checklisten

- BIOS kodeord, pin-kode til telefon
- Firewall - specielt på laptops
- Installer anti-virus og anti-spyware hvis det er på Windows
- Brug to browsere med forskellige indstillinger
- Brug evt. OpenPGP til mailkryptering
- Brug Password Safe, Keychain Access (OSX) eller tilsvarende
- Overvej at bruge harddisk eller filkryptering Trucrypt `http://www.truecrypt.org/`
- Opdatere alle programmer jævnligt
- **Backup af vigtige data - harddiske i bærbare kan også dø**
- Husk: sikker sletning af harddiske, medier osv.

Work together

Team up!

We need to share security information freely

We often face the same threats, so we can work on solving these together

PROSA CTF

PROSA afholdte CTF konkurrence 2013 29. - 30. november

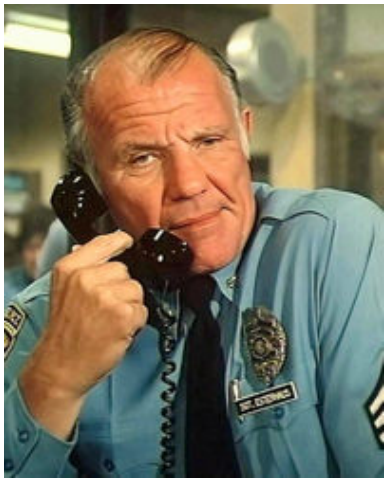
Capture the Flag er en mulighed for at afprøve sine hackerskillz

Distribueret CTF med hold Sjovt og lærerigt

Kilde: `http://ctf2013.the-playground.dk/`

Get ready! Lær debuggere, perl, java at kende, start på at hacke

Be careful - questions?



Hey, Lets be careful out there!

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

Source: Michael Conrad `http://www.hillstreetblues.tv/`