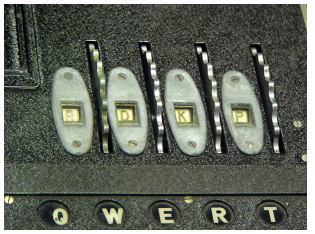


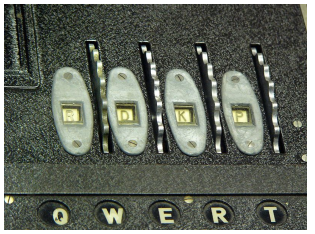
Welcome to

Fuld Disk Kryptering

Henrik Lund Kramshøj hlk@kramse.org

PDF available kramshoej@Github

Fuld Disk Kryptering



Data skal beskyttes, men hvor er data?

Vi benytter begreberne:

- Data in transit - undervejs
- Data at rest - i hvile

Det er nemt at flytte en harddisk fra en computer til en anden

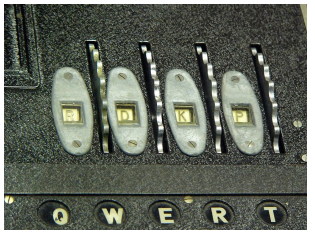
Fuld Disk Kryptering sikrer data-at-rest

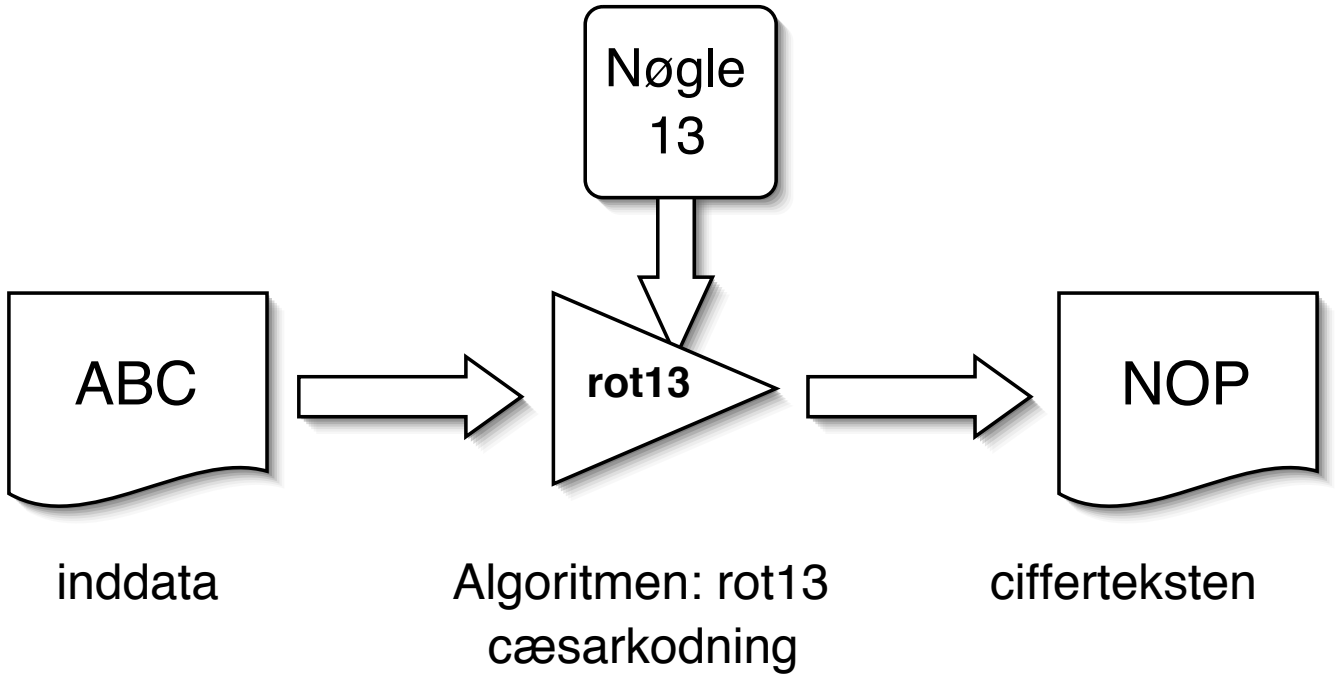
Anbefales fremfor løsninger der kun krypterer dele af harddisken/enkeltdokumenter

NB: for optimal sikkerhed skal disken krypteres FØR der opbevares fortrolige data

Kilder:
https://en.wikipedia.org/wiki/Data_at_rest
https://en.wikipedia.org/wiki/Data_in_transit

Kryptografi

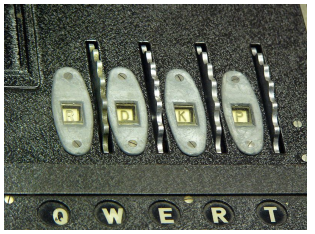


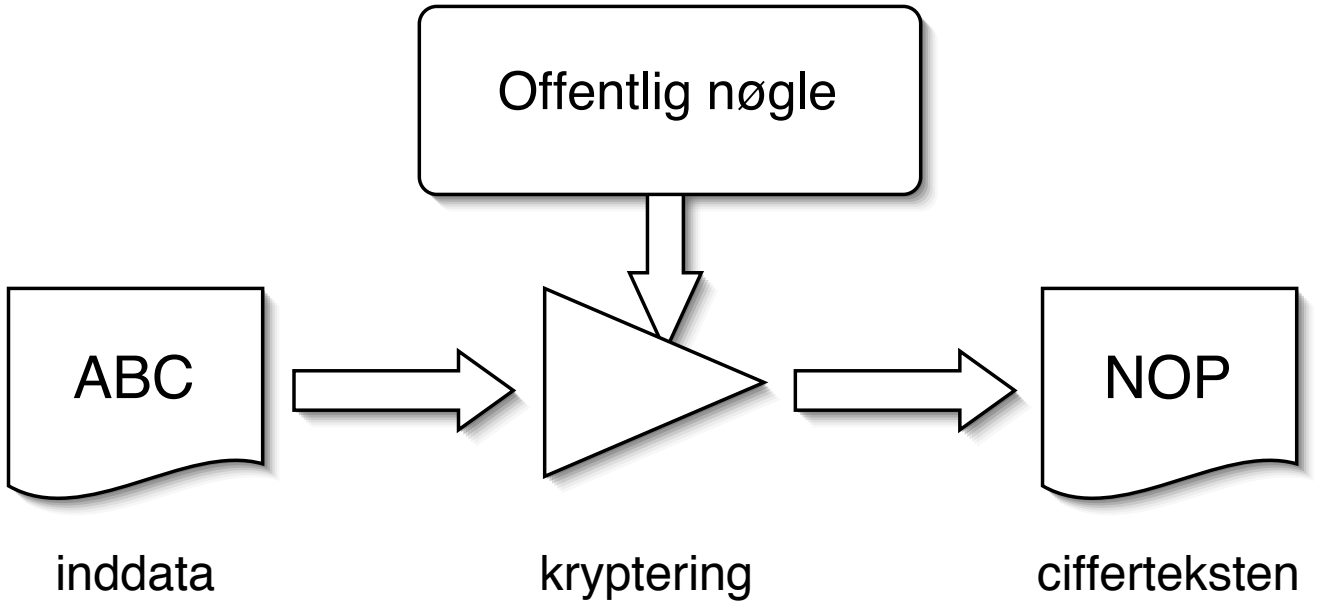


Kryptografi er læren om, hvordan man kan kryptere data

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

Public key kryptografi - 1

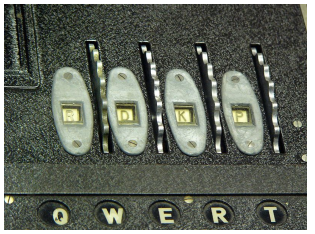


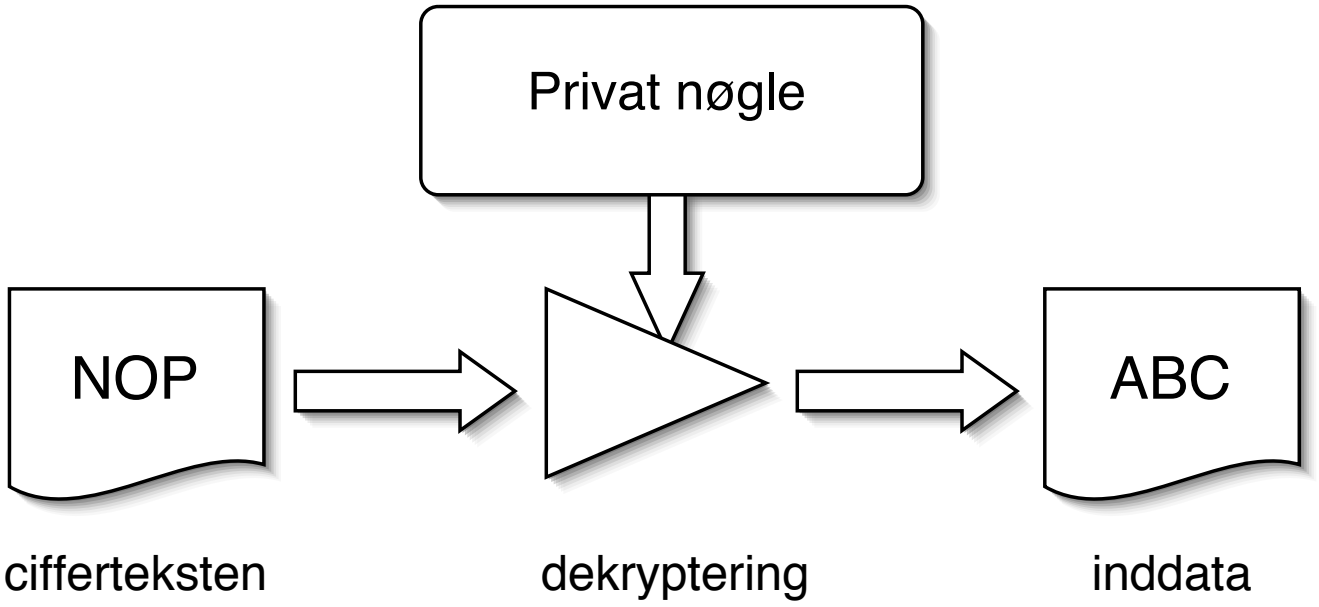


privat-nøgle kryptografi (eksempelvis AES) benyttes den samme nøgle til kryptering og dekryptering

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

Public key kryptografi - 2

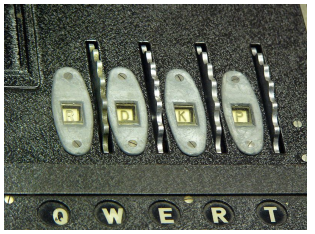




offentlig-nøgle kryptografi (eksempelvis RSA) bruger den private nøgle til at dekryptere

man kan ligeledes bruge offentlig-nøgle kryptografi til at signere dokumenter
- som så verificeres med den offentlige nøgle

Fuld Disk Kryptering: Bitlocker

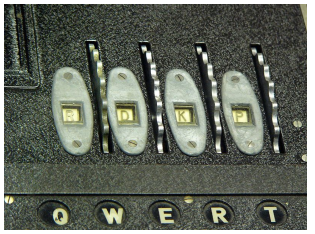


- Microsoft tilbyder Bitlocker fuld disk kryptering
- Åbnes med dit Windows kodeord
- Meget transparent - data krypteres når det skrives ned
- Nedsætter ikke hastigheden mærkbart, ofte forbedres den endda
- Genetableringsnøgle - er slået til på FT computere
  Giver mulighed for at IT-afd kan åbne din computer hvis du glemmer koden
- Fungerer på både roterende diske og SSD,
  men pas på SSD kan have data fra før kryptering slået til

Kilde: mere information om Bitlocker

`http://windows.microsoft.com/en-us/windows-vista/bitlocker-drive-encryption-overview`

Bitlocker



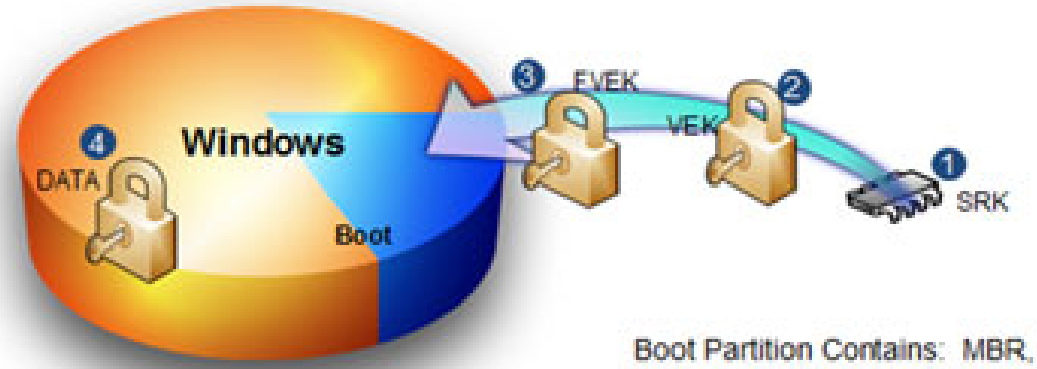
Disk Layout & Key Storage

Windows Partition Contains

- Encrypted OS
- Encrypted Page File
- Encrypted Temp Files
- Encrypted Data
- Encrypted Hibernation File

Where's the Encryption Key?

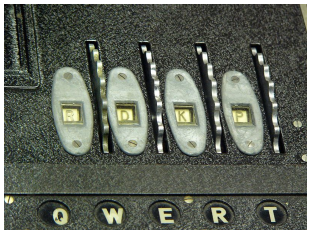
1. *SRK* (Storage Root Key) contained in TPM
2. *SRK* encrypts *VEK* (Volume Encryption Key) may also by PIN/Startup key
3. *VEK* stored (encrypted by *SRK*) in volume metadata
4. *VEK* encrypts an internal key *(FVEK)* used to encrypt the data. *FVEK* is stored in the volume metadata.



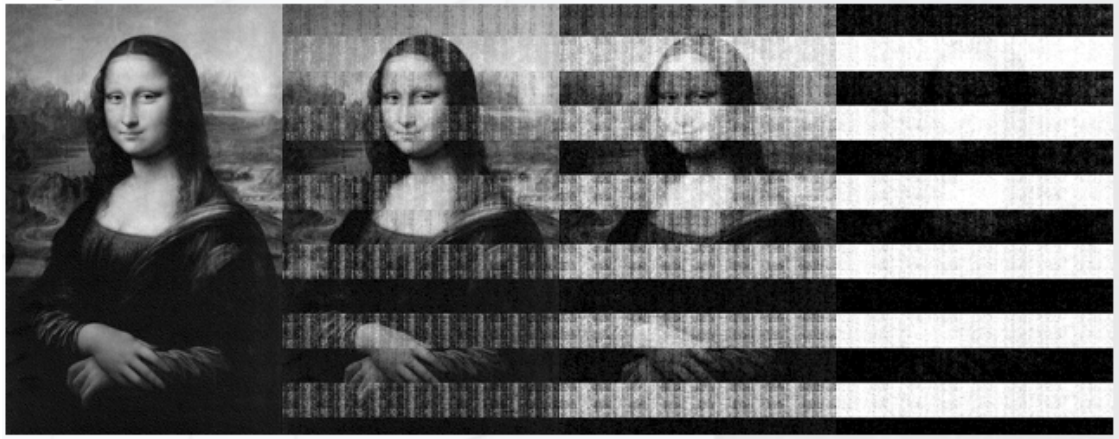
Boot Partition Contains: MBR, Loader, Boot Utilities (Unencrypted, small)

Kilde: https://technet.microsoft.com/en-us/library/cc512654.aspx

Angreb mod disk kryptering



Images



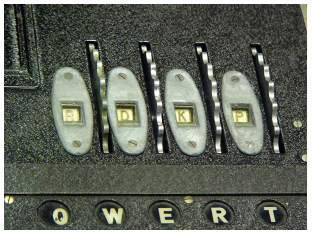
We loaded an image into memory, then cut power for varying lengths of time. After 5 seconds (left), the image is indistinguishable from the original. It becomes gradually more degraded, as shown after 30 seconds, 60 seconds, and 5 minutes. The horizontal bars result from the design of this memory chip, which represents some "1" bits by the presence of charge and some by the absence of charge.

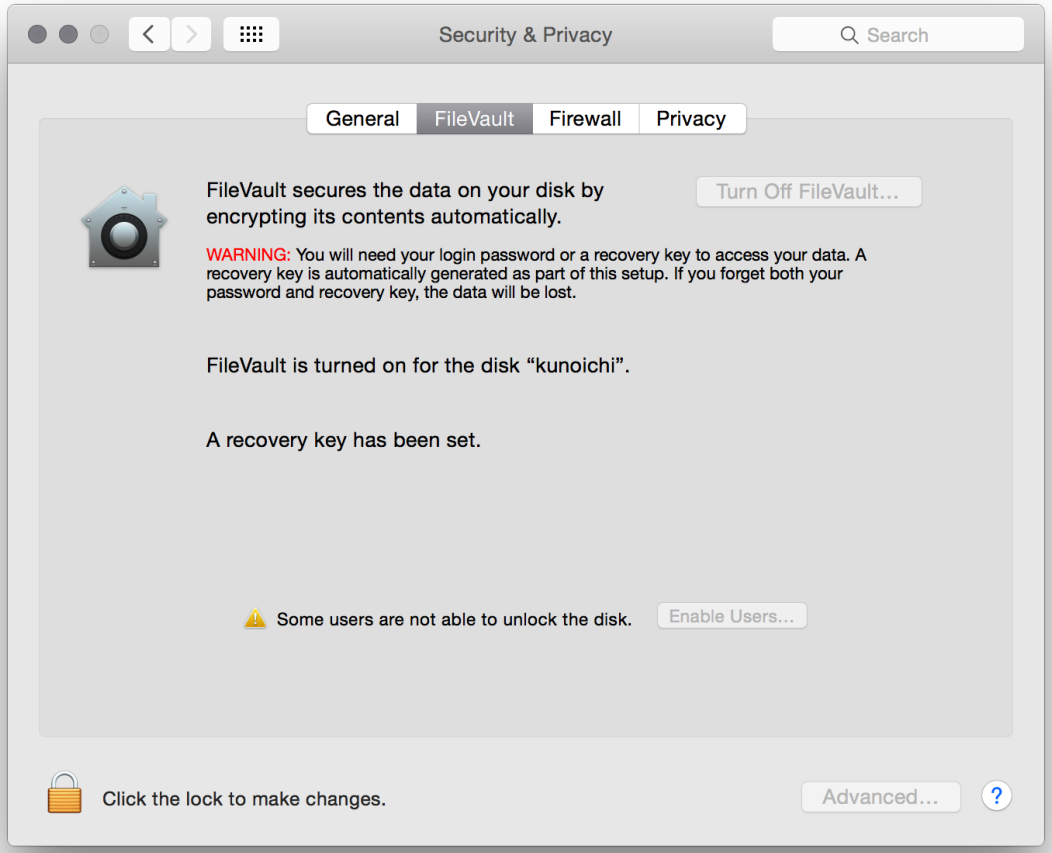
Fælles for mange angreb er at Computeren skal være tændt eller i dvale,
så er nøglen er i hukommelsen og kan måske fiskes ud

Det anbefales derfor at du lukker computeren helt ned, hvis den forlades i længere tid

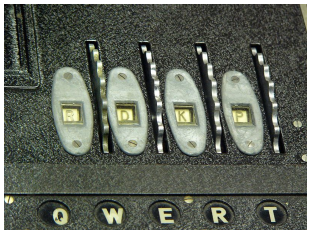
Kilde: `https://citp.princeton.edu/research/memory/`

Bonus: Full Disk Encryption Mac OS X





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

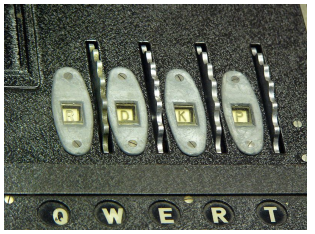


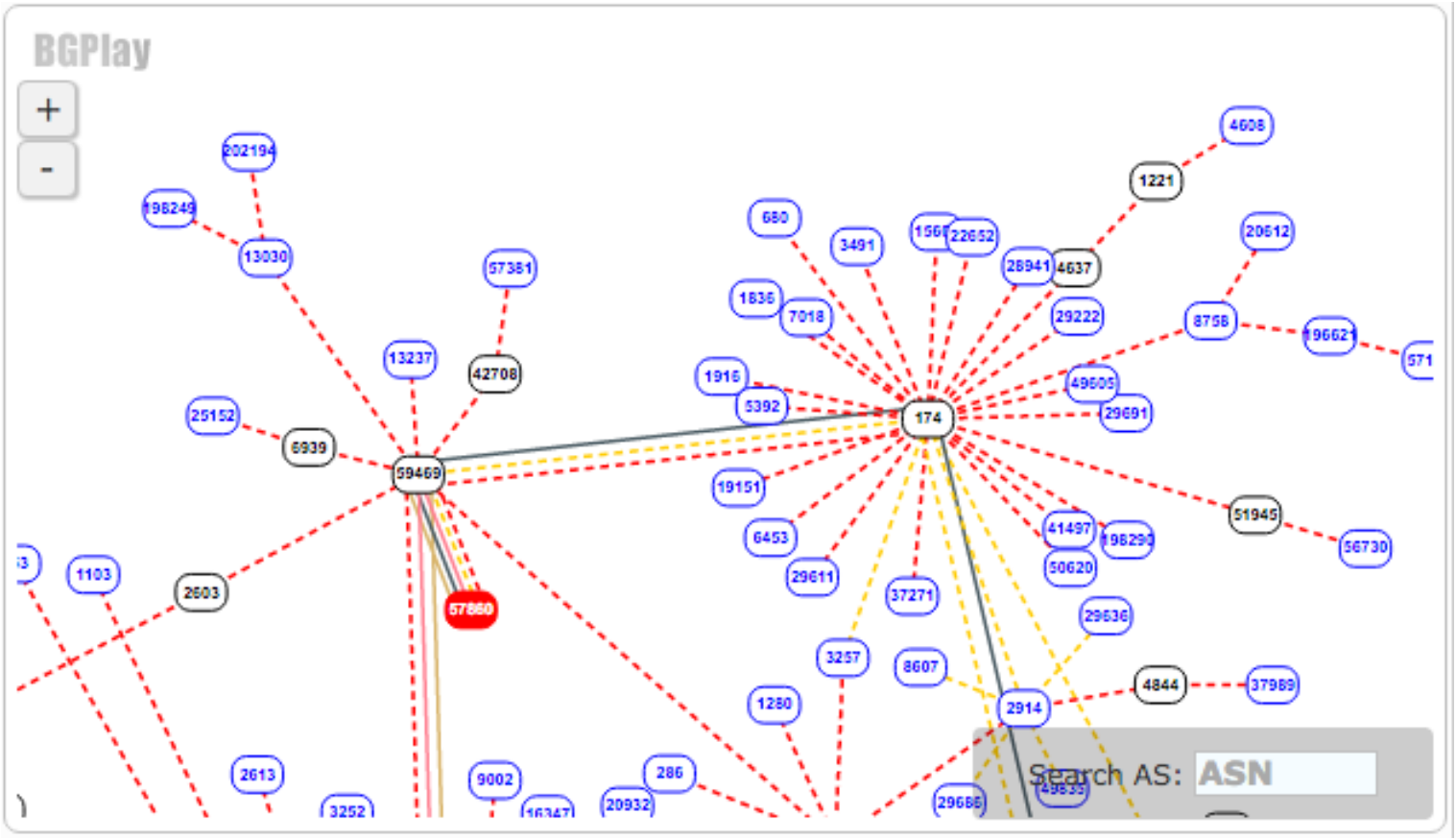
Welcome to

Sikker på nettet

Henrik Lund Kramshøj hlk@kramse.org

Internet set fra Zencurity AS57860

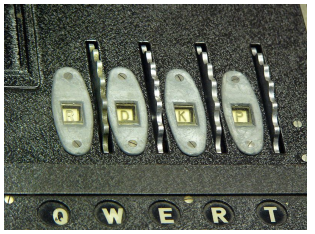




Small excerpt from:

https://stat.ripe.net/185.129.62.0/22#tabId=routing

Drive-by-download



Drive-by download

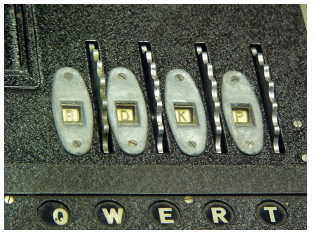
From Wikipedia, the free encyclopedia

Drive-by download means three things, each concerning the unintended download of computer software from the Internet:

1. Downloads which a person authorized but without understanding the consequences (e.g. downloads which install an unknown or counterfeit executable program, ActiveX component, or Java applet). This is usually caused by poor security design[*clarification needed*]. The user should not be frequently asked to accept security-critical decisions, often with very limited knowledge and within limited time.
2. Any download that happens without a person's knowledge.
3. Download of spyware, a computer virus or any kind of malware that happens without a person's knowledge.

Kilde: Wikipedia

Brug flere browsere



Firefox chrome Tor

TorProject.org

Allow active content to run only from sites you trust

ScriptBlock 1.0

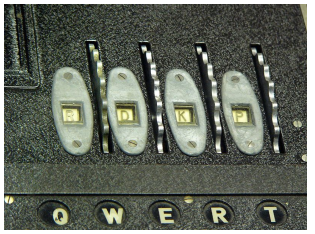
A smart extension that controls javascript, iframes, and plugins

HTTPS Everywhere

whonix

PRIVACY & ANONYMITY OS

Fordele ved flere browsere



Flere browsere giver højere sikkerhed

Data kan ikke flyde mellem flere browsere, cookies m.m.

Mit forslag:

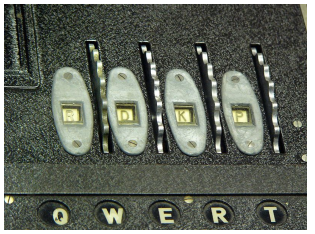
- En browser til *sikre sites* banken, intranet
- En browser til generel internet surfing
- En browser med alle mulige plugins, web udvikling eksempelvis

Installer gerne plugins til højere sikkerhed i allesammen:
HTTPS Everywhere, NoScript/ScriptBlock m.fl.

Det anbefales at disse installeres og vedligeholdes fra IT-afdelingen

Alle browsere har mange fejl!

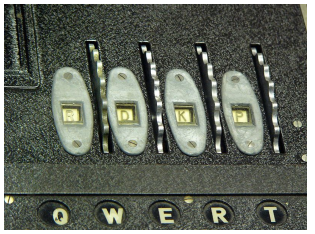
Safari på Mac eller Internet Explorer Windows

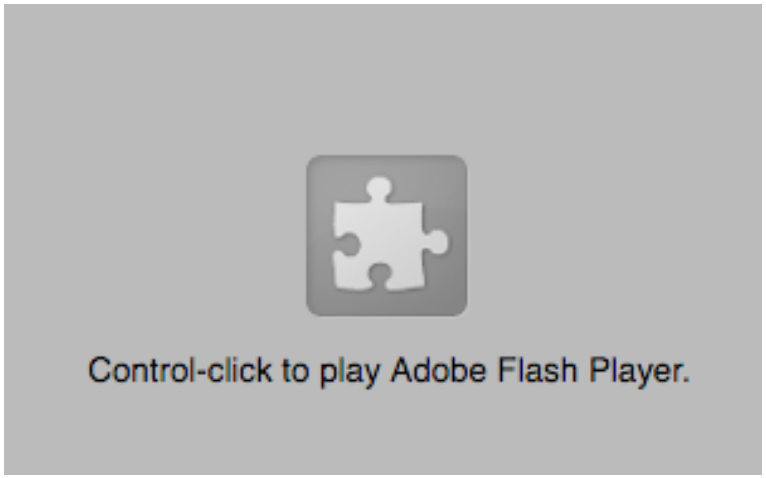


Browser	TastSelv Erhverv	skat.dk	TastSelv Borger og eIndkomst
IE 11	X	X	X
IE 10		X	X
IE 9		X	X
Firefox 31	X		
Firefox 14		X	X
Chrome 33	X		

- Den indbyggede browser testes af banker, skat, m.fl.
- Disse sites kræver oftest javascript, cookies, Flash og tidligere endda Java
- **Java** benyttes stadig visse steder - **højrisiko**
- Kan vise video og andet aktivt indhold, eksempelvis Netflix

Chrome en rimeligt sikker browser





Generelt er internet browsing en risikofyldt aktivitet

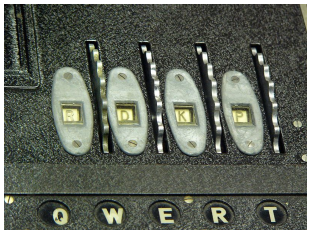
Drive-by-download hacking er reel trussel

Opdaterer sig selv løbende

Egen Sand-box til Flash

Denne browser kan indstilles rimeligt sikkert

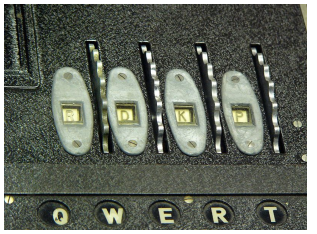
Firefox



- Firefox er en god generel browser med mange plugins
- Plugins kan indeholde mange fejl, læs indeholder mange fejl
- Firefox er et godt værktøj til webudvikling og andre formål

Jeg anbefaler derfor Firefox til de opgaver hvor du skal bruge mange plugins

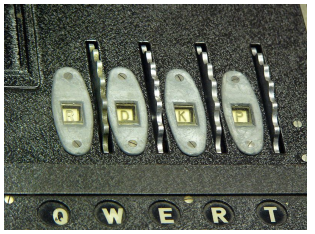
Generelt indstillinger for browsere

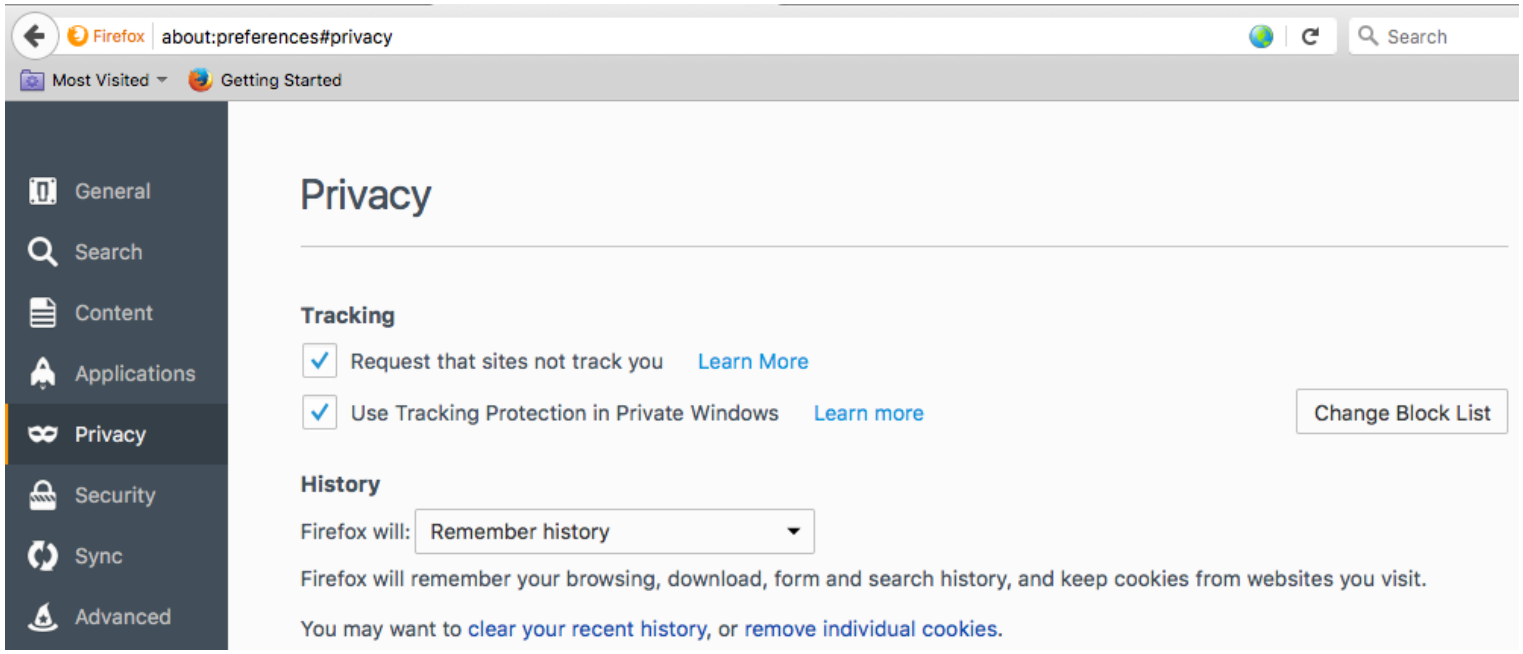


Skal være indstillet på den sikre browser til generel surf

- Slå JavaScript fra generelt med NoScript/ScriptBlock
- Slå click-to-play til for aktivt indhold
- Slå ”Do Not Track” til
- Slå Java helt fra, afinstaller evt. Java helt fra computeren
- Installer en AdBlocker - jeg bruger AdBlock
  Vigtigt: servere der viser reklamer er ofte mål for hacking

Hvor ændrer man indstillingerne



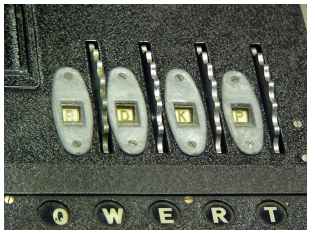


De fleste findes under:

- Chrome `chrome://settings/` og `chrome://extensions/`
- Firefox Indstillingerne og for enkelte ting: `about:config`

Kig også gerne på Safari eller Internet Explorer indstillingerne

HTTPS Everywhere

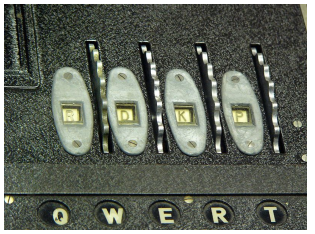


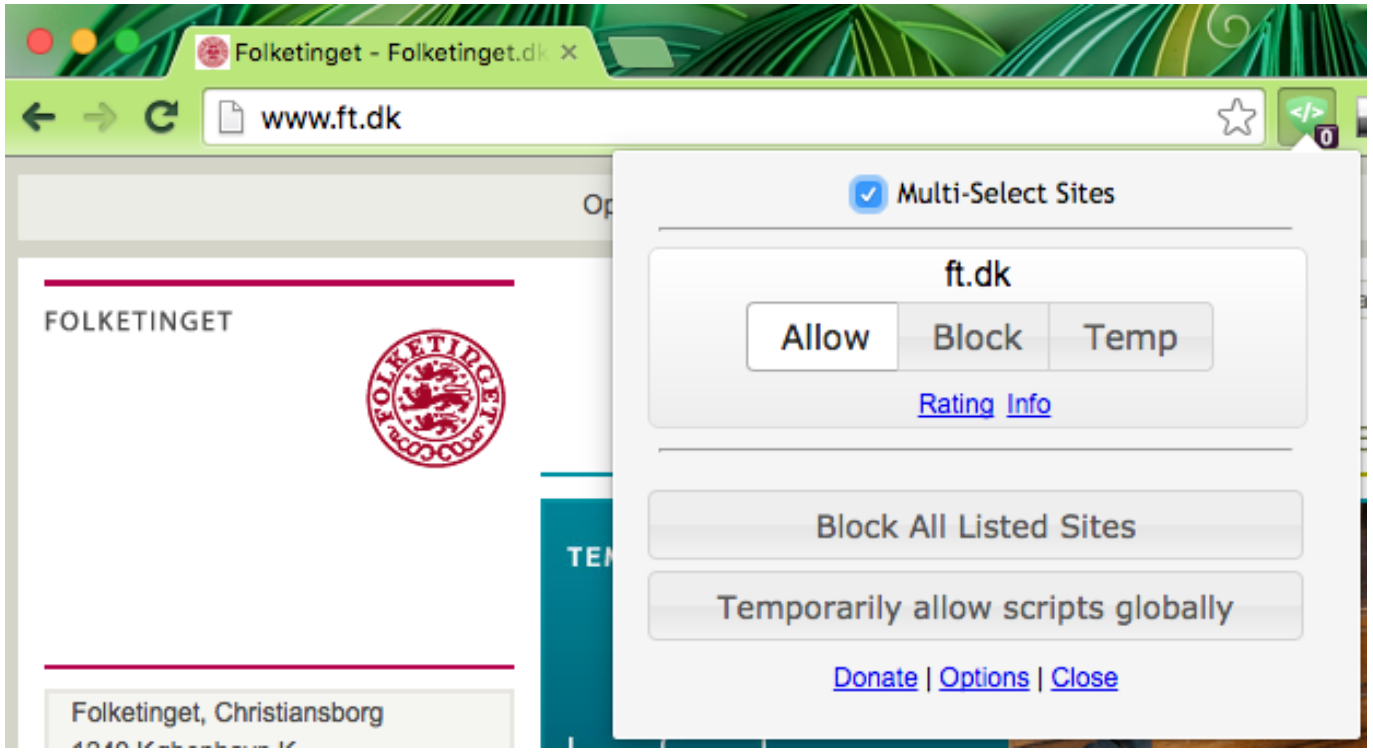
HTTPS Everywhere is a Firefox extension produced as a collaboration between The Tor Project and the Electronic Frontier Foundation. It encrypts your communications with a number of major websites.

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

Also in Chrome web store!

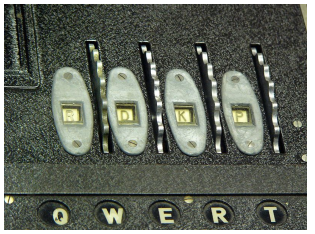
NoScript Firefox and ScriptBlock Chrome





NoScripts for Firefox eller ScriptBlock for Chrome
Tillader kun JavaScript på sider hvor det er OK

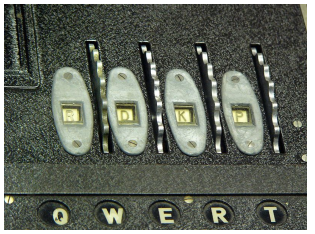
Tor project anonym webbrowsing

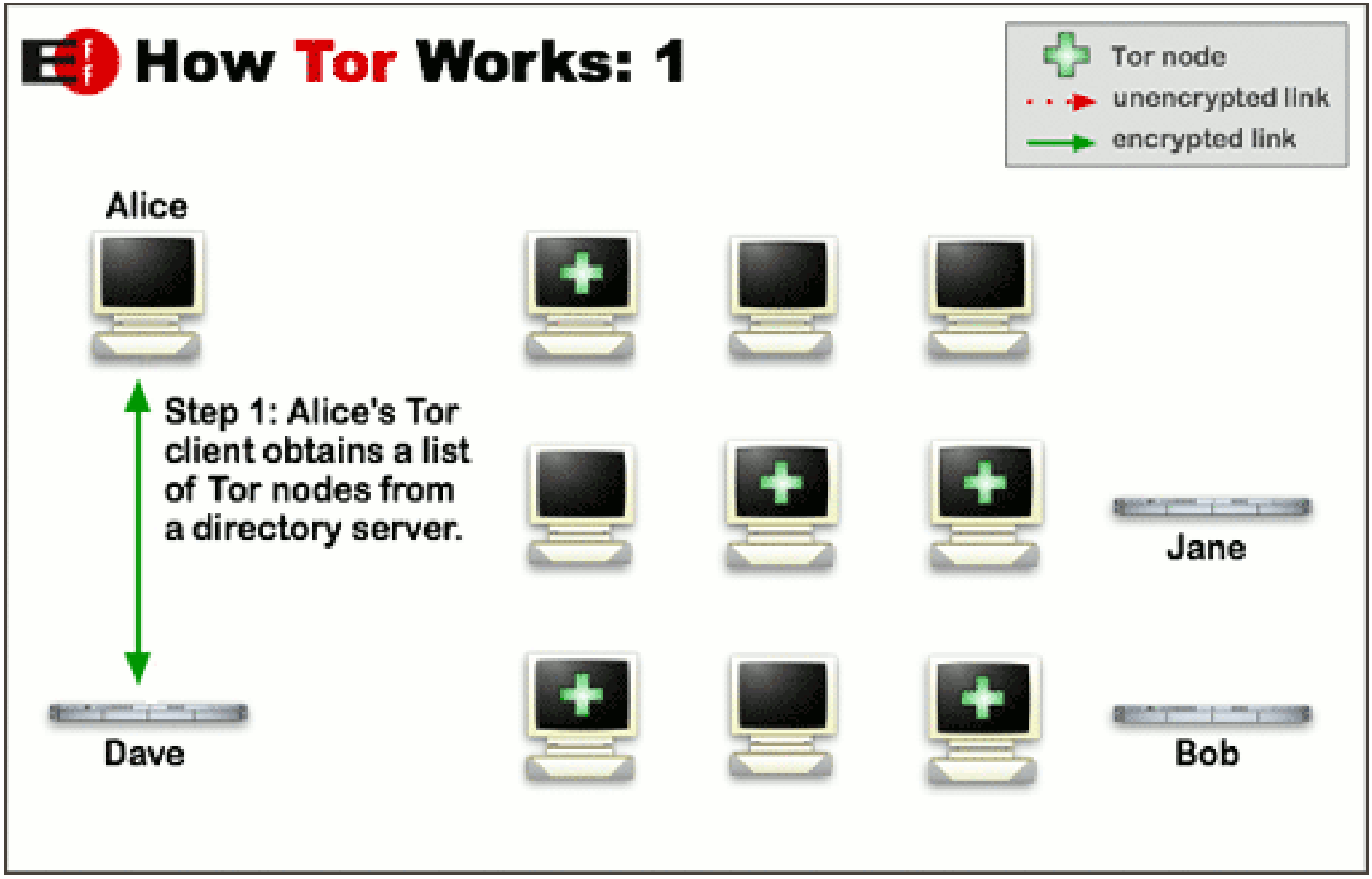


https://www.torproject.org/

Der findes alternativer, men Tor er mest kendt

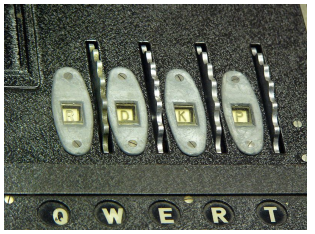
Tor project - how it works 1

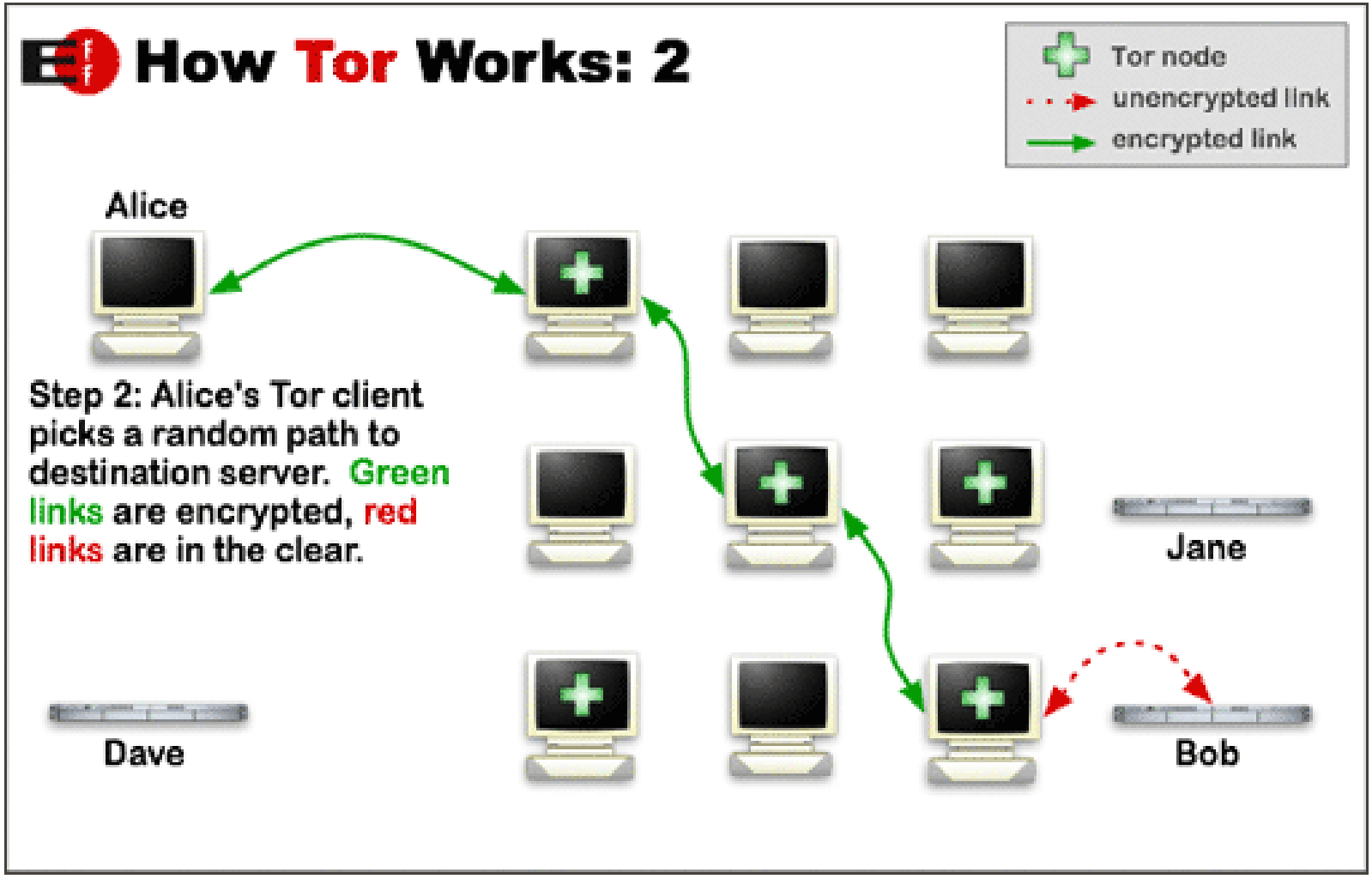




pictures from https://www.torproject.org/about/overview.html.en

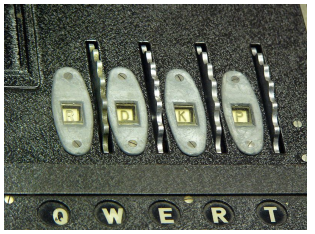
Tor project - how it works 2

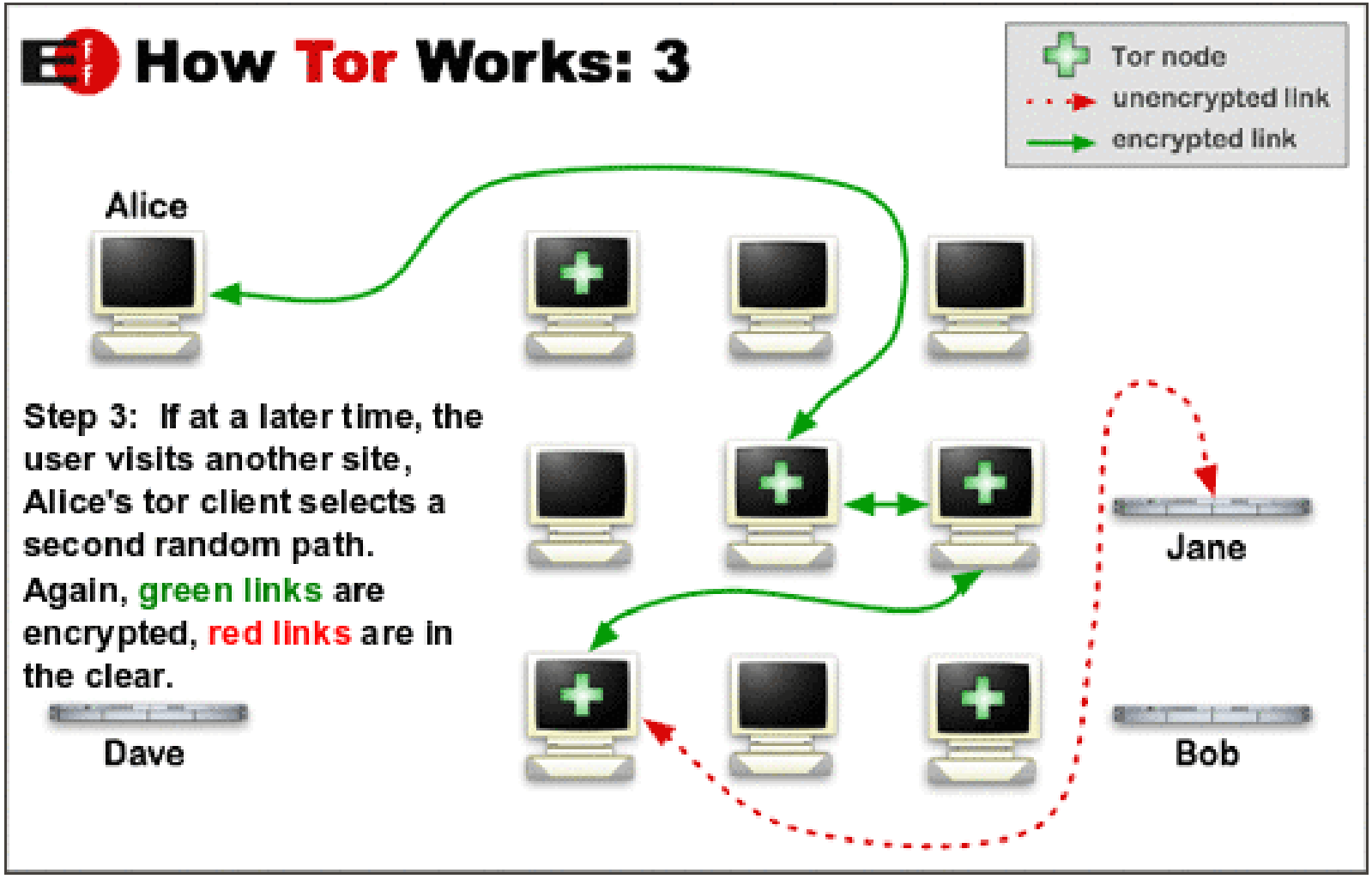




pictures from https://www.torproject.org/about/overview.html.en

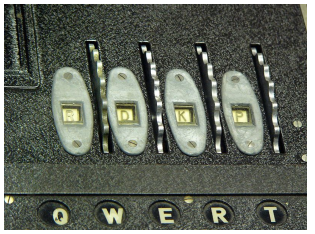
Tor project - how it works 3

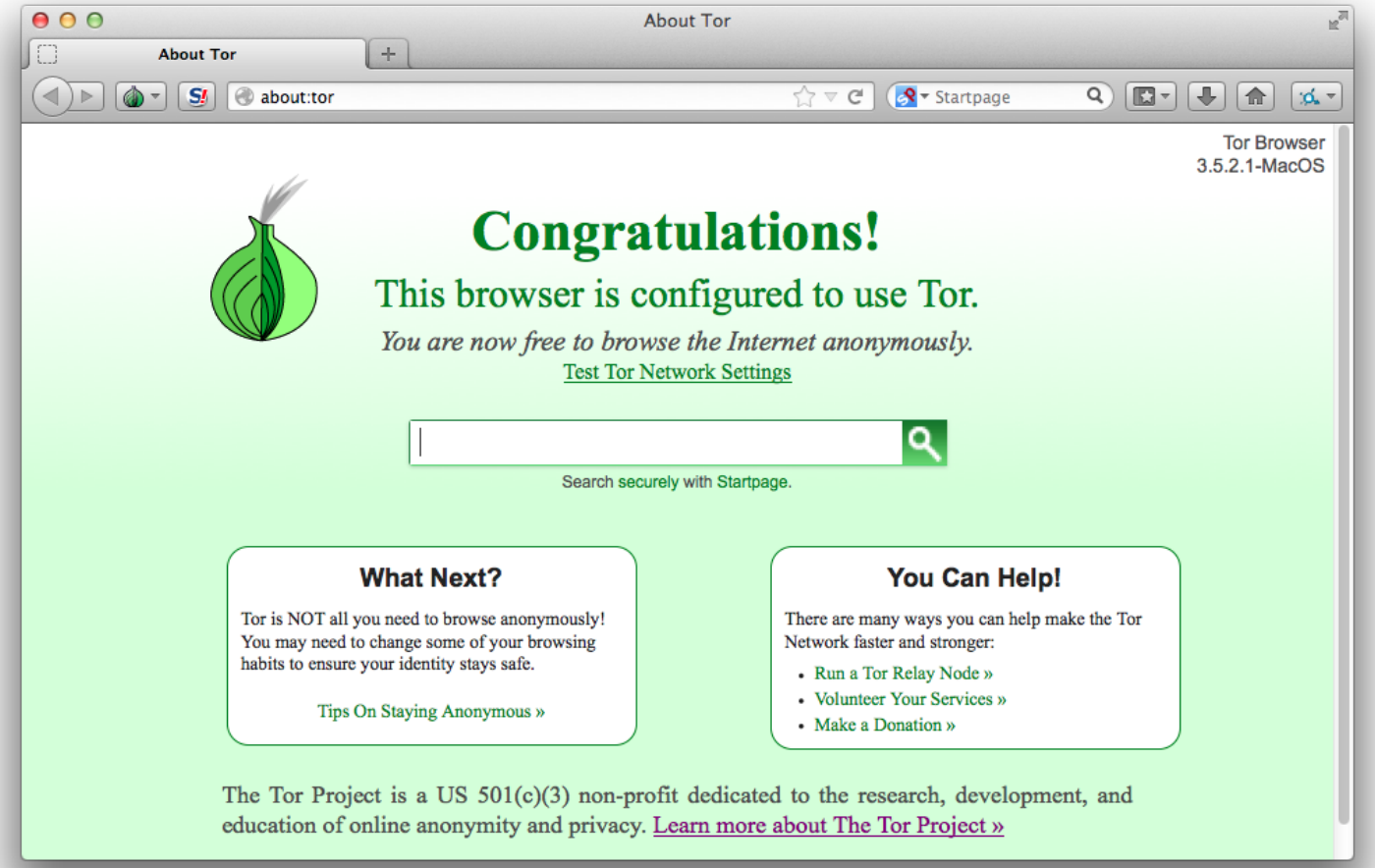




pictures from https://www.torproject.org/about/overview.html.en

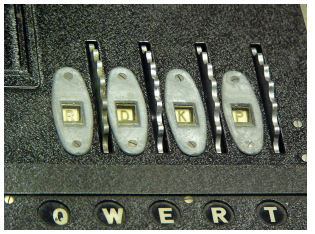
Torbrowser - anonym browser

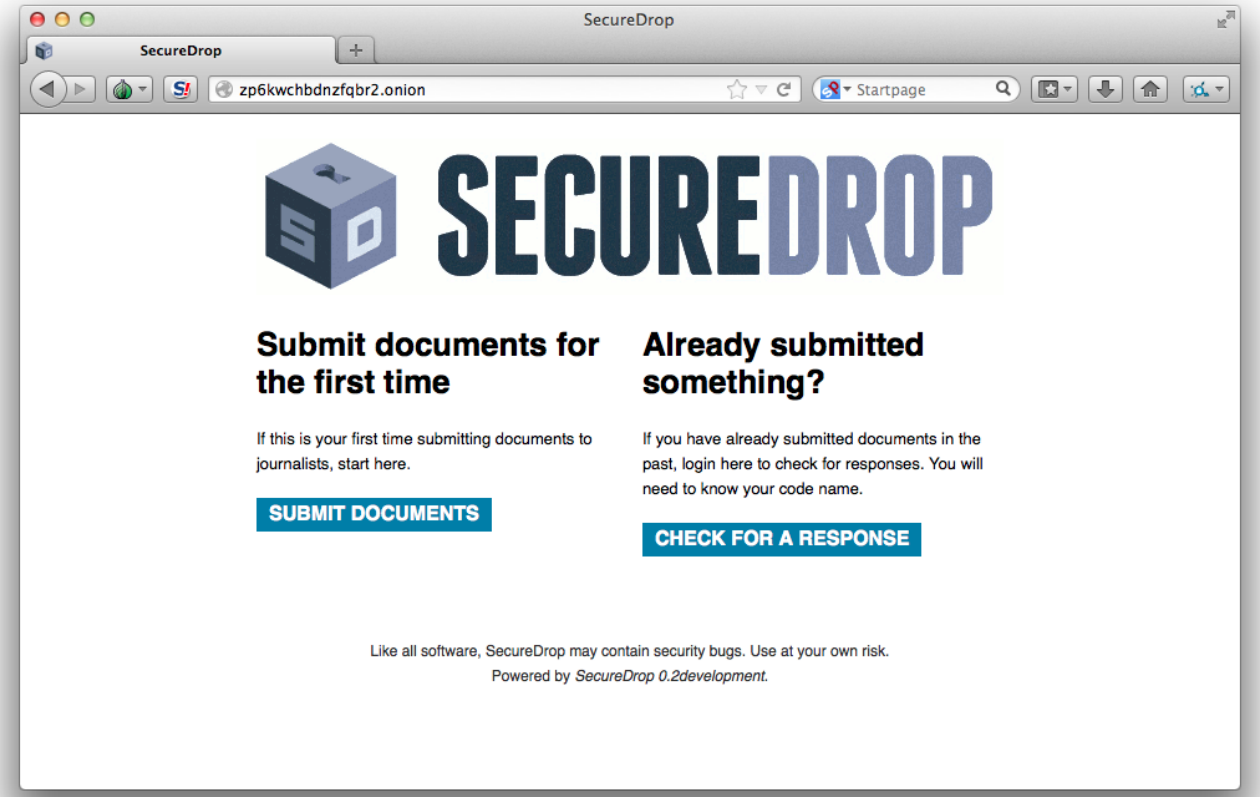




Mere anonym browser - Firefox i forklædning

Torbrowser - hidden service web site





.onion er Tor adresser - hidden sites

`http://www.radio24syv.dk/dig-og-radio24syv/securedrop/`