

Velkommen til

Kryptering 101

Marts 2006

Henrik Lund Kramshøj
hlk@security6.net

<http://www.security6.net>



Støt OpenBSD - det hjælper også OpenSSH

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed eiusmod tempor incididunt et labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Et harum idem reuerentia et dignitate amorem laborum accusantium, rerum non recusantibus, quibusdam inventore et qui sint ut qui doctores. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed eiusmod tempor incididunt et labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Et harum idem reuerentia et dignitate amorem laborum accusantium, rerum non recusantibus, quibusdam inventore et qui sint ut qui doctores. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed eiusmod tempor incididunt et labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Et harum idem reuerentia et dignitate amorem laborum accusantium, rerum non recusantibus, quibusdam inventore et qui sint ut qui doctores.

- At introducere kryptering
- At forklare de sikkerhedsmæssige aspekter af aflytning
- Kendskab til eksempler på kendte krypteringsprogrammer
- Praktisk brug af programmer til hemmeligholdelse af data
- At inspirere jer til at bruge kryptering til blandt andet e-mail
- At udføre en keysigning - altså udveksle nøgler

Er kryptering interessant?

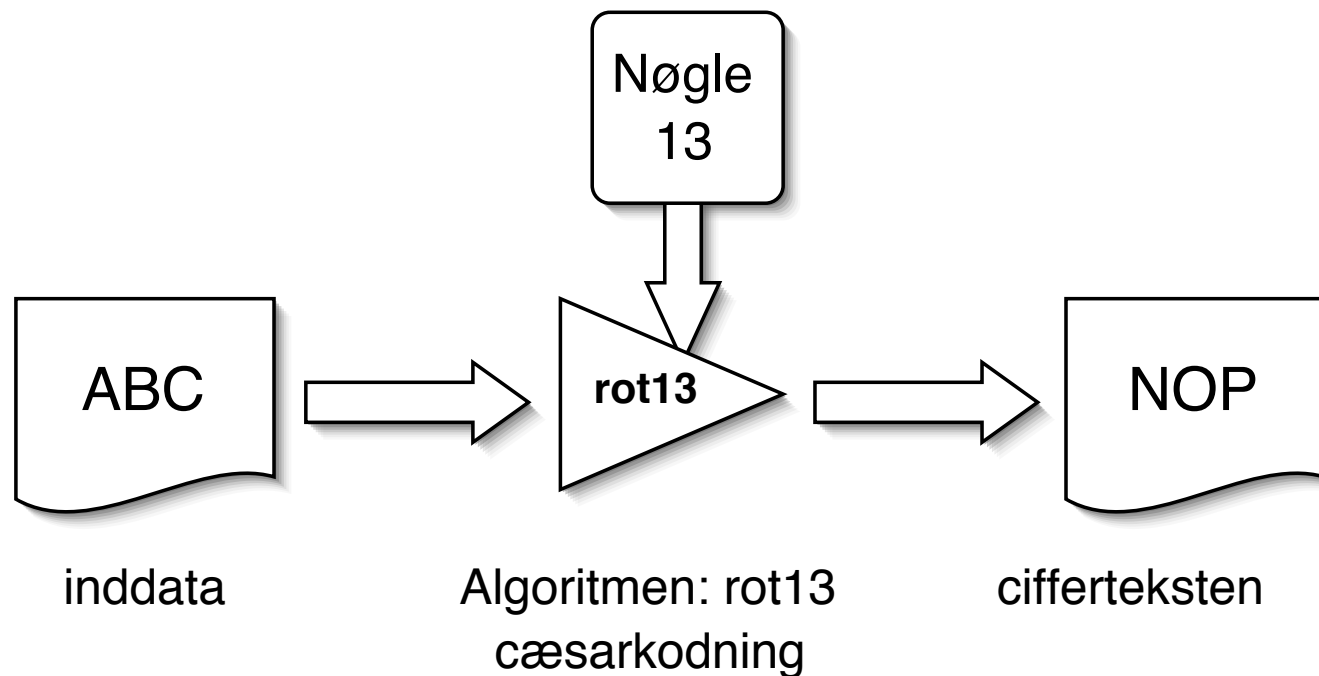
```
root@hlk: /home/hlk
[root@hlk hlk]# dsniff
dsniff: listening on fxp0
-----
05/20/03 08:53:38 tcp client.49154 -> server.110 (pop)
USER hlk
PASS secr3t!
-----
05/20/03 08:54:11 tcp client.49155 -> server.23 (telnet)
[poppe]
hlk
secr3t!
ls
exit
-----
05/20/03 08:55:33 tcp client.49156 -> server.23 (telnet)
[poppe]
an ja
an jnaan ja
an ja
```

- Sikkerhedsproblemer i netværk er mange
- Trådløst udstyr er blevet meget billigt! - endnu flere kan sniffe trafik!
- Man vil gerne udveksle hemmeligheder som password m.v. over e-mail
- Terrorpakken giver anledning til stor bekymring!

Der er nogle praktiske opgaver man kan udføre for at få erfaring:

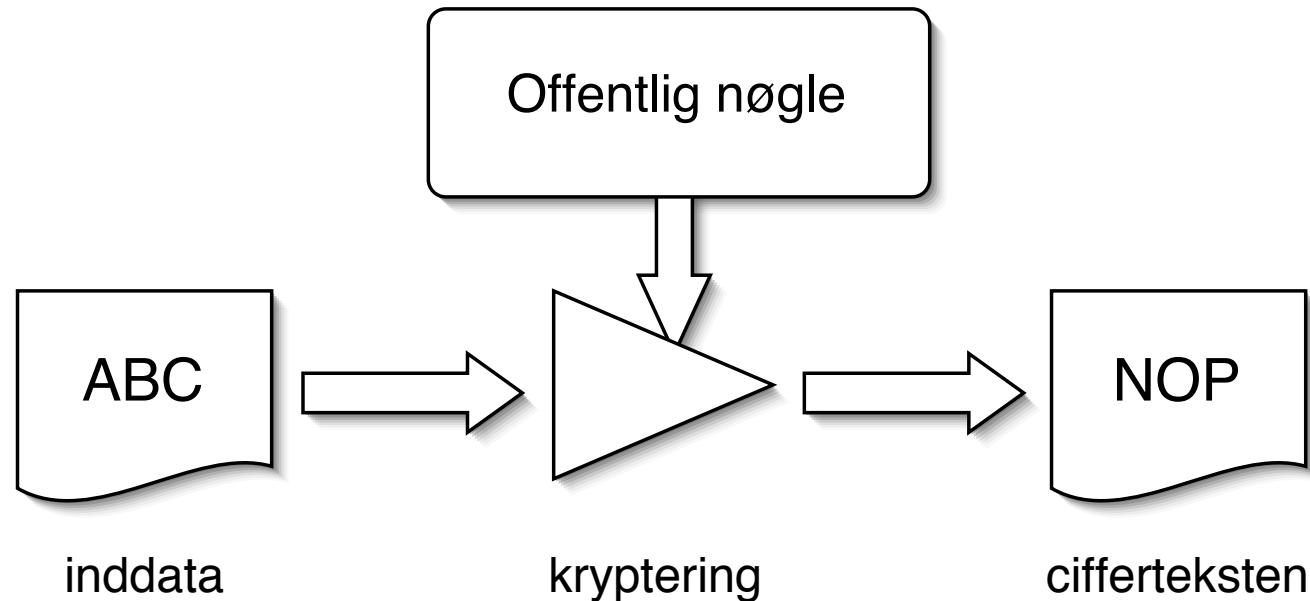
- installation af applikationer
- nøglegenerering
- signering af nøgler
- kryptering af filer
- kryptering af e-mail med GPG

- Introduktion - begreber og teknologierne
- PGP historik Phil Zimmermann
- Basale værktøjer PGP og GPG
- Harddisk kryptering
- Grafiske brugergrænseflader
- Keysigning - hvordan
- Keysigning - præsentation og identifikation



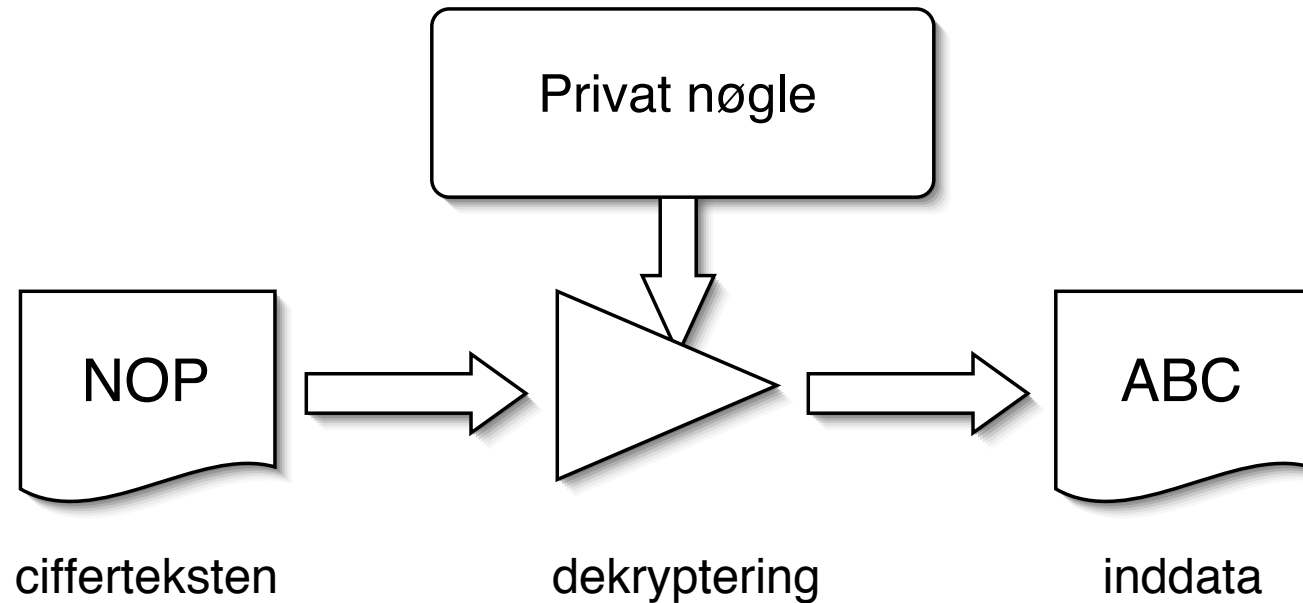
Kryptografi er læren om, hvordan man kan kryptere data

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



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



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

Algoritmerne er kendte

Nøglerne er hemmelige

Nøgler har en vis levetid - de skal skiftes ofte

Et succesfuldt angreb på en krypto-algoritme er enhver genvej som kræver mindre arbejde end en gennemgang af alle nøglerne

Nye algoritmer, programmer, protokoller m.v. skal gennemgås nøje!

Se evt. Snake Oil Warning Signs: Encryption Software to Avoid

<http://www.interhack.net/people/cmcurtin/snake-oil-faq.html>

AES

Advanced Encryption Standard

DES kryptering baseret på den IBM udviklede Lucifer algoritme har været benyttet gennem mange år.

Der er vedtaget en ny standard algoritme Advanced Encryption Standard (AES) som afløser Data Encryption Standard (DES)

Algoritmen hedder Rijndael og er udviklet af Joan Daemen og Vincent Rijmen.

Kilde: <http://csrc.nist.gov/encryption/aes/>
<http://www.esat.kuleuven.ac.be/~rijmen/rijndael/>

kryptering er den eneste måde at sikre:

fortrolighed

autenticitet / integritet

Kryptering af e-mail

- Pretty Good Privacy - Phil Zimmermann
- GNU Privacy Guard - Open Source implementation af OpenPGP
- OpenPGP = mail sikkerhed, OpenPGP RFC-2440, PGP/MIME RFC 3156)

Kryptering af sessioner SSL/TLS

- Secure Sockets Layer SSL / Transport Layer Services TLS
- krypterer data der sendes mellem webservere og klienter
- SSL kan bruges generelt til mange typer sessioner, eksempelvis POP3S, IMAPS, SSH m.fl.

Kryptering af netværkstrafik - Virtual Private Networks VPN

- IPsec IP Security Framework, se også L2TP
- PPTP Point to Point Tunneling Protocol
- OpenVPN m.fl.



FileVault

FileVault secures your home folder by encrypting its contents. It automatically encrypts and decrypts your files while you're using them.

WARNING: Your files will be encrypted using your login password. If you forget your login password and you don't know the master password, your data will be lost.

A master password is **set** for this computer.
This is a "safety net" password. It lets you unlock any FileVault account on this computer.

FileVault protection is **on** for this account.
Turning off FileVault may take a while.

[Change...](#)

[Turn Off FileVault...](#)

Kryptering findes i alle de gængse klient operativsystemer

- Microsoft Windows 2000 EFS Encrypting Filesystem - kryptering af filer
- Apple Mac OS X - krypterer nemt hjemmekataloget for en bruger med FileVault
- FreeBSD GEOM og GBDE - giver mulighed for at kryptere enheder generelt
- PGP disk - Pretty Good Privacy - laver en virtuel krypteret disk
- Nogle producenter har kodeord på disken - IBM harddisk BIOS kodeord

Hvad man vælger afhænger af operativsystemet og pengepungen

Tvind brugte Safeguard Easy fra det tyske firma Utimaco

Politiet *knækkede* harddiskene ved brug af kodeord som de enten gættede eller fik - ikke selve krypteringen

<http://www.utimaco.de>

En god algoritme i et godt produkt med en god nøgle kan ikke brydes

Demo af Safeguard PrivateDisk



- Fulgte med en IBM Thinkpad X31, men koster omkring Euro 49.00 (21. marts 2006)
- <http://www.utimaco.de>



- Pretty Good Privacy - PGP
- Oprindeligt udviklet af Phil Zimmermann
- nu kommercielt, men der findes altid en freeware version <http://www.pgp.com>
- Eksporteret fra USA på papir og scannet igen - det var lovligt
- I dag kan en masse information om PGP findes gennem: <http://www.pgpi.org>



Gnu Privacy Guard, forkortes GnuPG eller GPG

brug linket: <http://www.gnupg.org/>

Open Source med GPL licens.

Kan bruges på alle de gængse operativsystemer

```
$ gpg --version
```

```
gpg (GnuPG) 1.4.2
```

```
Copyright (C) 2005 Free Software Foundation, Inc.
```

```
This program comes with ABSOLUTELY NO WARRANTY.
```

```
This is free software, and you are welcome to redistribute it  
under certain conditions. See the file COPYING for details.
```

```
Home: ~/.gnupg
```

```
Supported algorithms:
```

```
Pubkey: RSA, RSA-E, RSA-S, ELG-E, DSA
```

```
Cipher: 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH
```

```
Hash: MD5, SHA1, RIPEMD160, SHA256, SHA384, SHA512
```

```
Compression: Uncompressed, ZIP, ZLIB, BZIP2
```

```
$
```

Ovenstående viser at GnuPG er installeret og hvilke algoritmer der understøttes

GPGME

GnuPG Made Easy (GPGME) is a library designed to make access to GnuPG easier for applications. It provides a High-Level Crypto API for encryption, decryption, signing, signature verification and key management. Currently it uses GnuPG as its backend but the API isn't restricted to this engine; in fact we have already developed a backend for CMS (S/MIME).

Because the direct use of GnuPG from an application can be a complicated programming task, it is suggested that all software should try to use GPGME instead. This way bug fixes or improvements can be done at a central place and every application benefits from this.

Especially authors of MUAs should consider to use GPGME. It is even planned to create a set of standard widgets for common key selection tasks.

See **download** section to download the latest tarball.

Et bibliotek der giver adgang til GPG fra applikationsprogrammer

Kilde: [http://www.gnupg.org/\(en\)/related_software/gpgme/index.html](http://www.gnupg.org/(en)/related_software/gpgme/index.html)

GUI FRONTENDS

GPA

Aims to be the standard GnuPG graphical frontend. **GPA** is hosted on this site.

GPGe

GPGe (GNU Privacy Guard Explorer Extension) is a shell extension that adds Windows explorer right-click menu support for GnuPG. It is a MS-Windows program to integrate GnuPG into the Desktop.

KGpg

Is a KDE frontend for GnuPG.

Seahorse

Is a GNOME frontend for GnuPG.

TkPGP

Is another graphical tool to control GnuPG.

WinPT

Is a MS-Windows program to integrate GnuPG into the Desktop.

XAP

Is the X application panel and filemanager.

Kilde: [http://www.gnupg.org/\(en\)/related_software/frontends.html](http://www.gnupg.org/(en)/related_software/frontends.html)

GnuPG - send en mail fra kommandolinien

```
#!/bin/sh
#
# encrypt a message and send to hlk and CEM

PROGRAM=`basename $0`

if [ $# -ne 1 ]; then
    echo " to encrypt a message I need a filename!"
    echo "Usage: $0 filename"
    echo "example $0 pentest-report"
    exit 0
fi

filename=$1
#hlk is D1EFBAA6
gpg -e -a -r D1EFBAA6 <$filename > $filename.pgp
$
```

.pgp filen kan nu vedhæftes en mail og sendes sikkert.

```
$ cd /userdata/download/src/postfix/  
$ ls -l *.sig  
-rw-r--r--  1 hlk  admin  152 13 Sep  2003 postfix-2.0.16.tar.gz.sig  
-rw-r--r--  1 hlk  admin  152  3 May 13:34 postfix-2.1.1.tar.gz.sig  
$ gpg --verify postfix-2.1.1.tar.gz.sig  
gpg: Signature made Mon May  3 19:34:08 2004 CEST using RSA key ID D5327CB9  
gpg: Good signature from "wietse venema <wietse@porcupine.org>"  
gpg:          aka "wietse venema <wietse@wzv.win.tue.nl>"  
$
```

Det er nødvendigt at verificere arkiver med kildekode!

Generering af key

```
$ gpg --gen-key
```

- Vælg "DSA and Elgamal"
- Vælg passende keysize - 4096 skader næppe
- Vælg passende udløbsdato - "no expire" vil virke for de fleste
- Brug din officielle mailadresse i forbindelse med dit navn, så Email klienter kan finde din key aytomatisk
- Brug en god passphrase.
En lang sætning som du kan huske, og som ikke kan gættes ud fra kendskab til dig.
- Når nøglen genereres, så hjælp med at generere "randomness" i systemet. Det får genereringen til at gå hurtigere, og det giver en bedre key.

samme spørgsmål i GUI programmerne

Generering af keys 2

Du har nu en GnuPG key klar til at blive signeret

Er du **sikker** på at du kan huske din passphrase?

Når nøglen er genereret bliver der vist et kort sammendrag af indholdet
Dette *fingerprint* kan også fås frem med:

```
$ gpg --fingerprint addr@domain.dk
pub      1024D/D1EFBAA6 2003-01-20
         Key fingerprint = 0FAE F19D DB46 DF2E D93D  9B05 21A6 469B D1EF BAA6
uid          Henrik Lund Kramshoej (work email) <hlk@security6.net>
uid          Henrik Lund Kramshoej (Kramse) <hlk@kramse.dk>
uid          [jpeg image of size 14412]
sub      2048g/6D08E6E6 2003-01-20
```

Vi sætter defaults der sikrer:

- Ingen brok over usikker brug af hukommelsen (at låse sider kræver root, dvs. SUID på UNIX)
- Valg af default keyserver
- Valg af default key (hvis du har flere)
- Valg af karaktersæt

```
$ tail ~/.gnupg/gpg.conf  
no-secmem-warning  
keyserver hkp://pgp.mit.edu/  
default-key D1EFBAA6  
charset ISO-8859-1
```

Det gør livet lidt lettere

For at andre kan signere din key skal de have en kopi af din publickey.

Dette kan enten gøres ved at du eksporterer den til en fil og sender filen via Email, diskette, scp, USBkey, etc.:

```
gpg -a --export addr@domain.dk
```

Eller det kan gøres ved at den uploades til keyserverne, hvorfra alle kan hente den:

```
gpg --send-keys 47A33XXX
```

Download af keys

Download kan enten foretages via en webside med søgemuligheder

<http://pgp.mit.edu/>

Herfra kan en publickey gemmes i en fil, og importeres med:

```
gpg --import FILE
```

Download kan også foretages direkte hvis keyid kendes:

```
gpg --recv-keys DC9C7XXX
```

Keys signeres med:

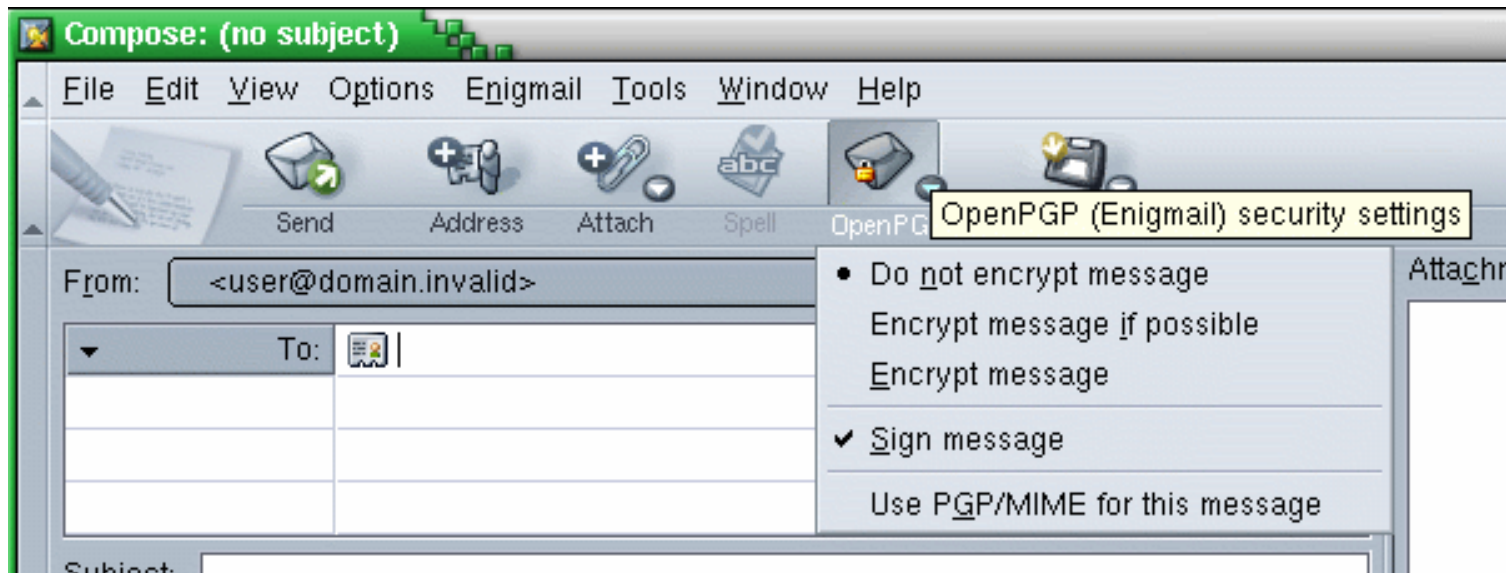
```
gpg --sign-key addr@domain.dk # Eller keyid
```

Husk at sikre at det nu også er den korrekte key i signerer

Kontroller med:

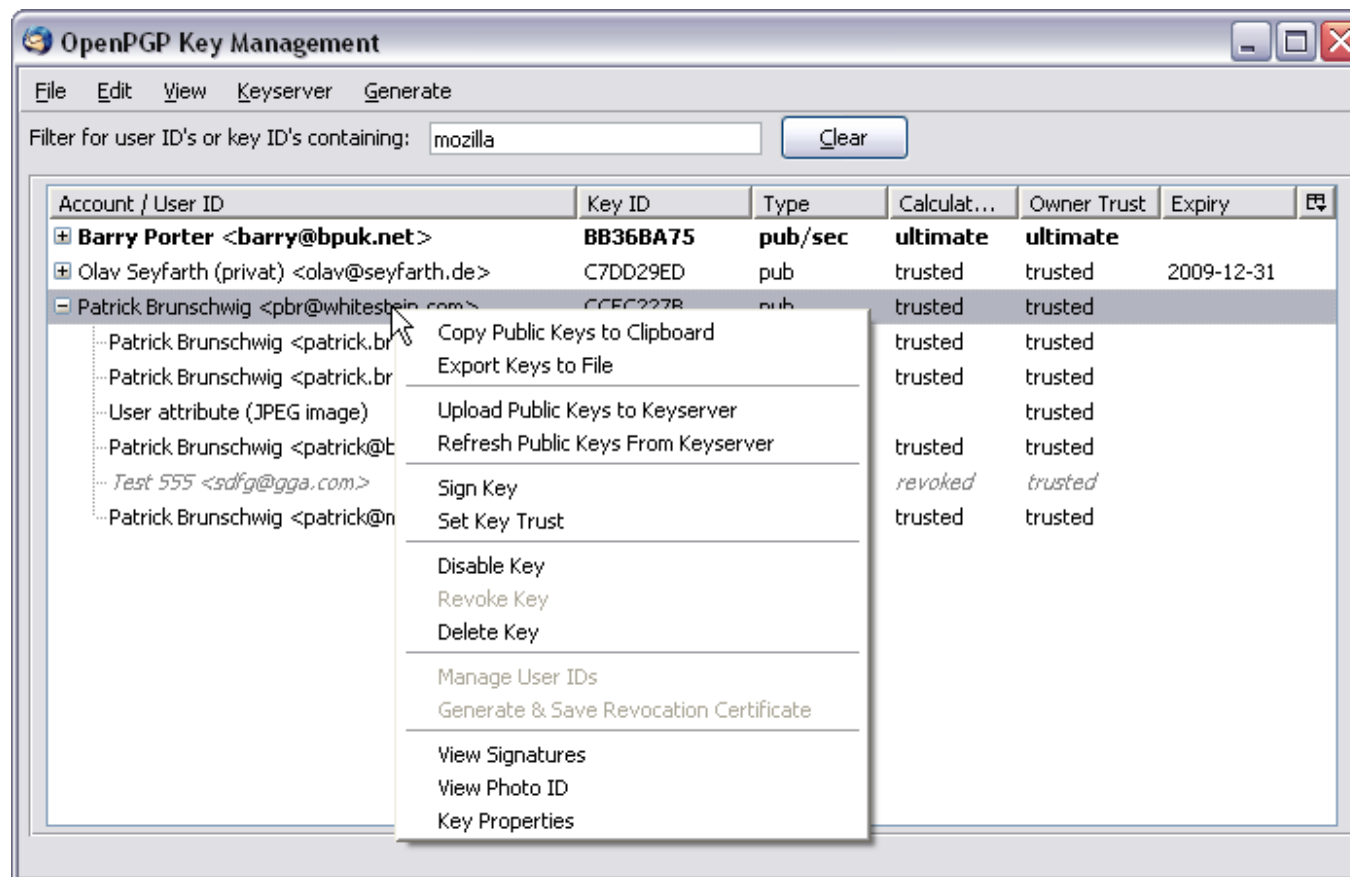
```
gpg --fingerprint addr@domain.dk
```

Enigmail - GPG plugin til Mail



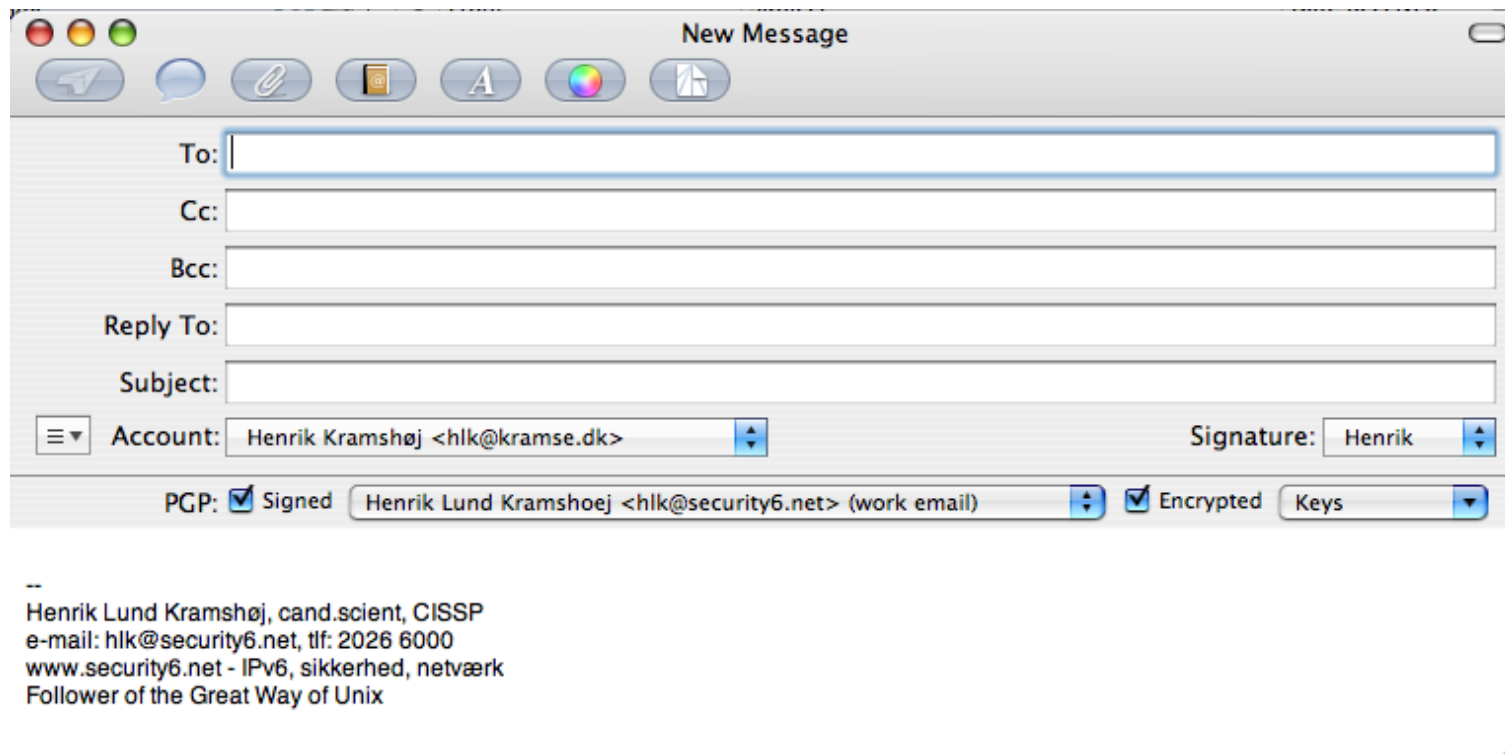
- Enigmail er en udvidelse til
- mailklienten i Mozilla/Netscape
- standalone mailklienten Thunderbird
- Billede fra <http://enigmail.mozdev.org>

Enigmail - OpenPGP Key Manager



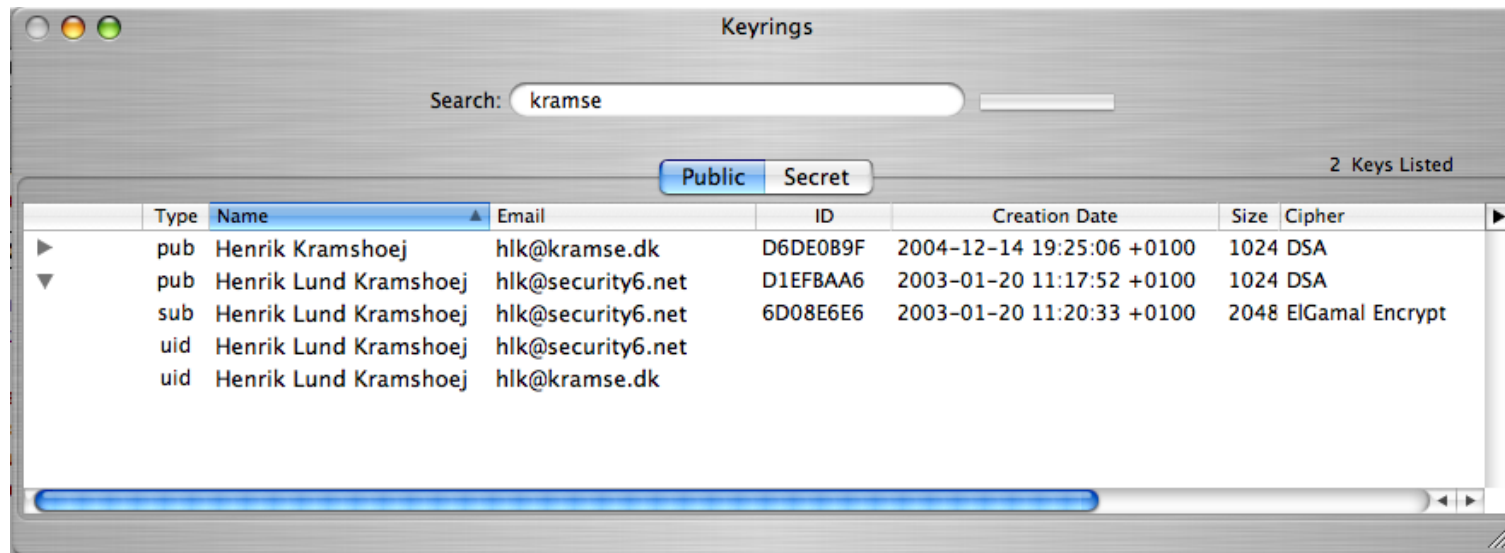
Key Manager funktionaliteten i Enigmail kan anbefales

GPGMail plugin til Mac OS X Mail.app



- Bruger GPG
- kilde: <http://www.sente.ch/software/GPGMail/English.lproj/GPGMail.html>

GPGKeys Key Manager for Mac OS X



- Bruger GPG
- Der er flere Mac GPG programmer tilgængeligt
- kilde: <http://macgpg.sourceforge.net>
- Der findes tilsvarende programmer til både KDE og GNOME

Computer Forensics involves the preservation, identification, extraction, documentation and interpretation of computer data.

Computer Forensics: Incident Response Essentials, Warren G. Kruse II og Jay G. Heiser, Addison-Wesley, 2002



Inspireret af TCT har Brian Carrier fra Atstake lavet flere værktøjer til forensics analyse

Det officielle hjem for TASK og autopsy er nu: www.sleuthkit.org

TASK kan betragtes som en erstatning for TCT the coroners toolkit lavet af Dan Farmer og Wietse Venema

Autopsy er en Forensic Browser - et interface til TASK

- Filsystemer skal være hurtige - skal ikke lave unødvendige operationer
- En harddisk er en fysisk disk med en arm der skal bevæges og et læse/skrivehoved som skal tændes og slukkes
- Hvis man kan undgå at skulle skrive over hele filen ved sletning er det hurtigere
- De fleste operativsystemer sletter derfor kun metadata og overskriver derfor ikke alle datablokke for filer
- Eksempel DOS FAT
Når man slettede en fil på MS-DOS fjernede man reelt kun det første bogstav i filnavnet undelete bestod i at skrive det første bogstav i filnavnet - og håbe på at alle datablokke der hørte til filen stadig var at finde på disken

Secure Deletion of Data from Magnetic and Solid-State Memory Peter Gutmann, 1996

Det er et klassisk paper om sletning af data som man bør læse

http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html

Der findes mange kommercielle værktøjer til sletning og en del Open Source - baseret på Guttman's dokument

Autoclave er efter min mening et af de bedste

<http://staff.washington.edu/jdlarios/autoclave/>

Sletning af diske kan foretages med eksempelvis autoclave

Den findes på følgende link:

<http://staff.washington.edu/jdlarios/autoclave/install.html>

Man kan nemt labe et CD image der kan skrives på en CD-R og bootes på nyere laptops - der sjældent har floppy drev

ad-hoc oprydning, formatering og sletning af filer giver ingen sikkerhed!

```
Darik's Boot and Nuke beta.2003052000
----- Options ----- Statistics
Entropy: Linux Kernel (urandom)      Runtime: 00:00:21
PRNG: Mersenne Twister (mt19937ar-cok) CPU Load: 96%
Method: DoD 5220-22.M                Throughput: 5973 KB/s
Verify: Last Pass                    Limiter: Disk I/O
Rounds: 1                             Errors: 0

(IDE 0,0,0,-) VMware Virtual IDE Hard Drive
[04.33%, round 1 of 1, pass 1 of 7] [writing] [5973 KB/s]
```

- Autoclave forfatteren henviser selv til DBAN
- følgende 4 punkter beskriver DBAN på hjemmesiden:
- Free.
- Fast. Rapid deployment in emergency situations.
- Easy. Start the computer with DBAN and press the ENTER key.
- Safe. Irrecoverable data destruction. Prevents most forensic data recovery techniques.
- <http://dban.sourceforge.net/>

Husk følgende:

Sikkerhed kommer fra langsigtede initiativer

Hvad er informationssikkerhed?

Data på elektronisk form

Data på fysisk form

Social engineering - *The Art of Deception: Controlling the Human Element of Security*
af Kevin D. Mitnick, William L. Simon, Steve Wozniak

Informationssikkerhed er en proces

Free software - free som i gratis software



AVG antivirus- www.grisoft.com

ZoneAlarm <http://www.zonelabs.com>

Utimaco SafeGuard PrivateCrypto <http://www.utimaco.com>

Spybot-Search and Destroy

<http://www.safer-networking.org>

Password Safe <http://passwordsafe.sourceforge.net>

Mozilla Firefox <http://www.mozilla.org>

PGP Freeware - begrænset version

<http://www.pgp.com/downloads/freeware/index.html>

Password Depot <http://www.password-depot.com/> - begrænset til 20 kodeord

Henrik Lund Kramshøj
hik@security6.net

<http://www.security6.net>

I er altid velkomne til at sende spørgsmål på e-mail

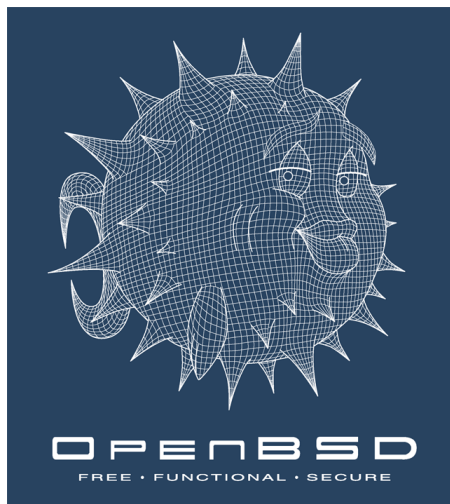
Oversigt over anbefalinger

Følg med! - læs websites, bøger, artikler, mailinglister, ...

Vurder altid sikkerhed - skal integreres i processer

Hændeshåndtering - du vil komme ud for sikkerhedshændelser

Lav en sikkerhedspolitik - herunder software og e-mail politik



Primære website: <http://www.openbsd.org>

Ved at støtte OpenBSD støtter du:

- OpenSSH - inkluderet i mere end 80-100 distributioner
- Udviklingen af OpenBSD PF - en super firewall, er med i FreeBSD, NetBSD
- Udvikling af stackprotection i Open Source operativsystemer
- OpenBGPD - en fri routing daemon, OpenNTPD - en fri NTP daemon, OpenCVS - en fri NTP daemon, CARP - redundancy must be free!

(ISC)^{2SM}

(CISSP)[®]

(SSCP)^{CM}

Approved marks of the International Information Systems Security Certification Consortium, Inc.

Primære website: <http://www.isc2.org>

Vigtigt link <http://www.cccure.org/>

Den kræver mindst 3 års erfaring indenfor et relevant fagområde

Multiple choice 6 timer 250 spørgsmål - kan tages i Danmark



Security Essentials - basal sikkerhed

Krav om en *Practical assignment* - mindst 8 sider, 15 sider i gennemsnit

multiple choice eksamen

Primære website: <http://www.giac.org>

Reading room: <http://www.sans.org/rr/>

Der findes en god oversigt i filen *GIAC Certification: Objectives and Curriculum*

http://www.giac.org/GIAC_Cert_Brief.pdf

Papers - der findes MANGE dokumenter på Internet


- CERT/CC <http://www.cert.org>
- AusCERT Computer Emergency Response Team for Australia
<http://www.auscert.org.au/>
- <http://www.securityfocus.com>
- CERIAS hotlist http://www.cerias.purdue.edu/tools_and_resources/hotlist/

Honeypots og sårbare systemer

- <http://www.project.honeynet.org> - diverse honeynet projekter information om pakker og IP netværk

Husk også at mange forlag tillader at man henter et kapitel som PDF!

- *Counter Hack: A Step-by-Step Guide to Computer Attacks and Effective Defenses*, Ed Skoudis, Prentice Hall PTR, 1st edition July 2001
- *CISSP All-in-One Exam Guide*, Shon Harris, McGraw-Hill Osborne Media, 2nd edition, June 17 2003
- *Practical UNIX and Internet Security*, Simson Garfinkel, Gene Spafford, Alan Schwartz, 3rd Edition, O'Reilly February 2003
- *Network Security Assessment: Know Your Network*, Chris McNab, O'Reilly March 2004
- *Secure Coding: Principles & Practices*, Mark G. Graff, Kenneth R. van Wyk, O'Reilly June 2003
- *Firewalls and Internet Security*, William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin, Addison-Wesley, 2nd edition, 2003
- *Building Firewalls with OpenBSD and PF*, Jacek Artymiak, 2nd edition 2003
- bøger om TCP/IP - Alle bøger af Richard W Steven kan anbefales!
- Reference books for the CISSP CBK domains - en liste der vedligeholdes af Rob Slade
<http://victoria.tc.ca/int-grps/books/techrev/mnbksccd.htm>

- nmap - <http://www.insecure.org> portscanner
- Nessus - <http://www.nessus.org> automatiseret testværktøj
- l0phtcrack - <http://www.atstake.com/research/lc/> - The Password Auditing and Recovery Application, kig også på Cain og Abel fra <http://oxid.it> hvis det skal være gratis
- Ethereal - <http://www.ethereal.com> avanceret netværkssniffer
- OpenBSD - <http://www.openbsd.org> operativsystem med fokus på sikkerhed
- <http://www.isecom.org/> - Open Source Security Testing Methodology Manual - gennemgang af elementer der bør indgå i en struktureret test
- Putty - <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html> terminal emulator med indbygget SSH
-  <http://www.remote-exploit.org/?page=auditor> - Auditor security collection - en boot CD med hackerværktøjer

Tænk som en hacker

Rekognoscering

- ping sweep
- portscan
- OS detection - TCP/IP eller banner grab
- Servicescan - rpcinfo, netbios, ...
- telnet/netcat interaktion med services

Udnyttelse/afprøvning: Nessus, whisker, exploit programs

Oprydning

- Lav en rapport
- Gennemgå rapporten, registrer ændringer
- Opdater programmer, konfigurationer, arkitektur, osv.

I skal jo også VISE andre at I gør noget ved sikkerheden.

Security6.net afholder følgende kurser med mig som underviser

- IPv6 workshop - 1 dag
Introduktion til Internetprotokollerne og forberedelse til implementering i egne netværk. Internetprotokollerne har eksisteret i omkring 20 år, og der er kommet en ny version kaldet version 6 af disse - IPv6.
- Wireless teknologier og sikkerhed workshop - 2 dage
En dag med fokus på netværksdesign og fornuftig implementation af trådløse netværk og integration med eksempelvis hjemmepc og virksomhedens netværk
- Hacker workshop 2 dage
Workshop med detaljeret gennemgang af hackermetoderne angreb over netværk, exploitprogrammer, portscanning, Nessus m.fl.
- Forensics workshop 2 dage
Med fokus på tilgængelige open source værktøjer gennemgås metoder og praksis af undersøgelse af diskimages og spor på computer systemer
- Moderne Firewalls og Internetsikkerhed 2 dage
Informere om trusler og aktivitet på Internet, samt give et bud på hvorledes en avanceret moderne firewall idag kunne konfigureres.

BSD-DK - dansk forening for BSD'erne,

<http://www.bsd-dk.dk>

SSLUG, Skåne Sjælland Linux User Group

<http://www.sslug.dk>

DKUUG, Dansk UNIX User Group

<http://www.dkuug.dk>

medlemskab giver god rabat på bøger gennem

<http://www.polyteknisk.dk>, typisk 15-20%



Et lille embedded system

- Soekris 4501-30 + case 1300,-
- Soekris 4801-50 + case 1750,-
- Strømforsyning 1.5A (lille) 130,-
- Strømforsyning 3A (stor) 170,-
- vpn1411 miniPCI 550,-
- 4801 Harddisk mount kit 2.5" 70,-
- Alle priser er cirkapriser og ekskl. moms. kontakt Catpipe for nøjagtige oplysninger!
<http://www.catpipe.net>
- Andre leverandører <http://www.kd85.com> og <http://www.cortexsystems.dk>

