Denne guide er oprindeligt udgivet på Eksperten.dk

COMPUTERWORLD

PGP og vigtigheden af at kryptere dine e-mails

Begynderguide til "Pretty Good Privacy" (PGP), skrevet på forståelig dansk. Når du sender e-mails, er de omtrent lige så hemmelige som postkort. Med PGP kan du kryptere dine e-mails eller bruge PGP som en slags digital signatur. Til Windows-brugere.

Skrevet den **05. Feb 2009** af **old-faithful** I kategorien **Sikkerhed / Kryptering** | ★★★☆☆

1. Hvad er PGP?
PGP eller "*Pretty Good Privacy*" er kort sagt et program som kan kryptere tekst og filer. PGP er særligt smart når du skal sende emails eller andre tekster, idet du kan:
1) Kryptere beskeden så kun modtageren kan læse den
2) Vedlægge en digital signatur, så modtageren for det første kan se at det der dig, der har sendt beskeden, og for det andet, at beskeden ikke er blevet ændret.
3) Kombinere punkt 2 - 3

2. Hvorfor kryptering?
Der er mange gode grunde til at kryptere dine mails. For det første er e-mails ikke spor private. Når du sender en e-mail bliver den nemlig normalt sendt ukrypteret. Undervejs når den at komme igennem flere servers, før den lander i modtagerens inbox. I princippet kan enhver der har adgang til disse servers læse dine breve, i nogle tilfælde op til flere år efter mailen er sendt.

Man plejer at sige, at en email er omtrent ligeså hemmelig som et postkort. Spørgsmålet er så, hvad du almindeligvis kunne finde på at skrive på et postkort. Dit CPR-nummer? Bankoplysninger? Slibrige kærestebreve? Oplysninger om din familie? Adgangskoder? Forretningshemmeligheder?

Nej vel? Derfor er kryptering en god løsning - ikke fordi der er stor sandsynlighed for at nogen læser din post, men fordi der kan være en stor risiko forbundet med særligt at sende personlige mails.

En anden fordel ved PGP er, at systemet kan fungere som en slags digital signatur. Dette betyder dels at ægtheden af tekstens indhold kan bekræftes, dels at afsenderen kan verficeres. Dette stiller dig også stærkere hvis du f.eks. vil indgå bindende aftaler via nettet, eller hvis det er vigtigt at en besked kan veriferes.

3. Men er det ikke besværligt at kryptere?
I starten kan PGP synes uoverskueligt, men systemet er egentlig meget enkelt. PGP installerer et lille ikon i din taskbar (nederst til højre på skærmen). For at kryptere en besked vælger man enten "*Current Window*" hvorved du kan kryptere/afkode det aktive vindue (det vindue der er åbent og markeret i hvilket som helst tekstprogram) eller du kan vælge "*Clipboard*", hvorved du kan kryptere/afkode beskeder som er kopieret til udklipsholderen/clipboard. For at kryptere eller afkode, skal du dog først have en såkaldt nøgle (mere om dette senere i artiklen).

PGP er baseret på asymmetrisk kryptering og digitale "nøgler", dvs. talkoder som bruges til hhv. at kryptere og afkode (sammenlign: lås og lås op). Der findes en offentlig nøgle (*public key*)og en privat nøgle. Den private har du kun selv. Den offentlige nøgle kan du derimod offentliggøre. Det er med andre

ord underordnet om andre kender til din offentlige nøgle.

Vil folk sende en krypteret besked til dig, bruger de blot PGP sammen med din offentlige nøgle. Det smarte ved PGP er så, at det kun er din *private* nøgle der kan dechifrere den krypterede besked. Du slipper med andre ord for at bekymre dig om at sende koder rundt til folk - de skal blot bruge den offentligt tilgængelige nøgle.

4. Hvilken udgave af PGP skal jeg bruge?
Der findes flere udgaver af PGP. Den oprindelige udgave blev udviklet af Phil Zimmerman i 1991. Siden da har koden været ejet af flere forskellige firmaer. Der findes derfor flere forskellige varianter af PGP. De tre mest populære er:

4.1. GnuPG
GnuPG er en gratis udgave af PGP. Den findes til flere styresystemer. Windows-udgaven er et "commandline" program, dvs. at du skal bruge programmet gennem DOS-vinduer. Der findes dog grafiske brugerflader (GUI'er) der gør at du kan bruge programmet som var det et almindeligt Windows-program.'
 Du kan download selve programmet her (kig under "Binaries"):
http://www.gnupg.org/(en)/download/index.html#auto-ref-1
 Derudover kan du downloade GUI'er, f.eks.: GPGShell
(http://home.datacomm.ch/winzozzz/gpgshell_en.html)

4.2. PGP 9
Den nyeste officielle udgave af PGP er udgave 9. Denne udgave understøtter - modsat flere tidligere udgaver - Windows XP. Grundfunktionerne i denne udgave er stadig gratis, mens andre funktioner kræver at man betaler for en licens.
 Den seneste officielle udgave kan hentes her: http://www.pgp.com/downloads/index.html

4.3. PGP v6.5.8 CKT (build 8) af Imad Faiad

PGP v6.5.8 CKT (Cyber Knights Templar) er baseret på version 6.5.8 men udviklet af en tredjepart, Imad Faiad. Personligt foretrækker jeg denne udgave af PGP. Den er som sagt baseret på en tidligere udgave af PGP (kildekoden til PGP var gjort offentlig). Fordelen ved at bruge denne udgave er, at den understøtter Windows XP mens flere af de funktioner som i senere udgaver kræver betaling, stadig forefindes i denne udgave af PGP. Og denne udgave er stadig helt gratis og uden irriterende registreringsskærme mv.

Du kan bl.a. finde denne udgave her (Build 8 - filen *pgp658ckt08s.zip* - er den mest populære):
 ftp://ftp.zedz.net/pub/crypto/pgp/pgp60/pgp658_ckt/
 http://www.ecn.org/crypto/soft/pgp.phtml
 Ellers prøv Google: http://www.google.com/search?hl=en&q=pgp658ckt08s.zip

Eftersom jeg personligt anser denne udgave for den bedste, vil den følgende gennemgang være baseret på denne udgave. Den nyeste udgave af PGP minder dog meget om denne udgave, så det burde ikke give anledning til problemer.

5. Hvordan kommer jeg i gang?
Start med at downloade den udgave af PGP som du ønsker at benytte (se afsnittet herover). Hvis filen er komprimeret (som zip-fil for eksempel), skal du bruge et program til at pakke dem ud. Du kan eksempelvis bruge WinZip elle IZArc.

Installér herefter programmet. Du skal normalt genstarte computeren efter PGP er blevet installeret. Når

computeren er blevet genstartet, vil du kunne se et lille ikon i din taskbar (nederst til højre). Ikonet ligner en hængelås - dette er PGP.

Klik på ikonet og vælg "PGPkeys" (det er her man holder styr på alle sine "nøgler"). Første gang du gør dette vil du blive anmodet om at oprette dit eget nøglesæt ("Key Generation Wizard"). Følg de trin som computeren fører dig igennem. Denne del af processen taler for sig selv - bare læs det der står på skærmen og følg rådene. Du kan, men behøver ikke, sende nøglen til en server. Den oprettede nøgle tilføjes til en "keyring" (et nøglebundt, dvs. en samling nøgler).

6. Hvad med al den snak om nøgler?
Som nævnt benytter PGP sig af digitale nøgler. Denne metafor er meget passende. Nøgler bruges normalt til at låse ting eller låse ting op. Tilsvarende bruges en digital nøgle til at kryptere og afkode beskeder.

PGP er baseret på et smart princip - "Public Key Encryption". Princippet virker på den måde, at hver bruger opretter et "nøglepar" ("key pair"). Dette nøglepar består af to nøgler - en offentlig nøgle ("public key") og en privat nøgle ("private key").

Den offentlige nøgle kan du frit - og uden fare - offentliggøre. Denne nøgle bruges til at kryptere beskeder, men da den ikke også kan bruges til at afkode beskeden, er der ingen risiko ved at andre folk kender den. Det er det smarte ved PGP - du behøver ikke at bruge tid og ressourcer på at sende koder så hemmeligt som muligt; du giver blot folk den offentlige nøgle.

Den private nøgle bruges derimod til at afkode beskeder, og denne nøgle SKAL holdes hemmelig.

Når du sender en krypteret besked bruger du således modtagerens offentlige nøgle. Når han sender en besked til dig, bruger han omvendt din offentlige nøgle.

De to nøgler fungerer altså kun hvis de bruges parvis - den ene til at låse, og den anden til at "åbne".

I PGP kan du holde styr på alle dine nøgler ved hjælp af et digitalt nøglebundt - en "key ring".

Huskeboks
Key pair:
  Public key ---------> Kryptérer
  Private key --------> Afkoder (og laver signaturer)

Key ring ----------> Et nøglebundt til alle dine nøgler

7. Kryptér, afkod og underskriv en besked

7.1. At kryptere beskeder
Som nævnt i afsnit 3 er det ganske let at kryptere en besked. Der er flere måder at gøre dette. Til at starte med kan du enten:
1) Have teksten liggende i et hvilket som helst tekstprogram (dvs. et aktivt vindue)
2) Have kopieret teksten til udklipsholderen/clipboard
3) Skrive teksten direkte i Outlook eller andre mailprogrammer (PGP installerer bl.a. en plug-in der giver dig en "PGP"menu direkte i Outlook når du skriver beskeder)

NB: Bruger du Microsoft Outlook (eller et andet mailprogram som er understøttet af PGP plug-ins) kan du enten bruge den flg. fremgangsmåde eller bruge den menu som PGP opretter inde i selve Outlook.

Herefter trykker du på det lille hængelås-ikon i nederste, højre hjørne af skærmen. Ligger teksten i udklipsholderen vælger du dernæst "Clipboard". Ligger teksten i et aktivt program (det program der ligger forrest og er i brug) vælger du derimod "Current Window".

Dine valgmuligheder er nu:
1) Encrypt & Sign -> Hvis beskeden både skal signeres og krypteres
2) Sign -> Hvis du kun vil underskrive beskeden (se afsnit 7.3 herunder)
3) Encrypt -> Hvis du kun vil kryptere beskeden

Vælg hvad du ønsker. Vælger du kun at signere, skal du kun skrive kodeordet til din egen nøgle. Vælger du kun at kryptere, skal du blot vælge hvem du vil sende til (hvilken offentlige nøgle du vil bruge). Vælger du både at signere og kryptere skal du naturligvis gøre begge dele.

Særlige indstillinger:

Secure Viewer -> Brug denne indstilling hvis beskeden på modtagerens computer skal beskyttes mod elektromagnetiske opfangningsudstyr.

Conventional Encryption -> Vælger du denne mulighed, vil der ikke blive brugt en "public key" men derimod et kodeord som du angiver.

Teksten bliver nu automatisk omformet ift. de valgte indstillinger. Du kan nu sende teksten, men du skal huske at sende det *hele*, inkl. den første og sidste linje. Et eksempel på en krypteret besked:

```
-----BEGIN PGP MESSAGE-----
Version: 6.5.8ckt http://www.ipgpp.com/

qANQR1DDDQQJAwJT6TBg4q7M+2DJlb+T5UH6WVidhfR2T4nBHhyNA/M7xiG/6L4G
FTAEOYYx+cu5MkLIFWaBWoACFyrJZb/V4EN6AWizQ555HFqd8hLVqMAu4sZkuPlQ
WgCt2Q2uCrQrXwG2i1P2kcPozbLnZVvlcj/IprO2orRbe/mw9RhnOsls4dcSrBqu
XJUk7letIsHau5TX9KKUzyQVQGE+RoFi2Uxy
=ZLWV
-----END PGP MESSAGE-----
```

7.2. At afkode beskeder
Afkodningen af beskeder foregår stort set på samme måde som krypteringen af beskeder. Her skal du blot vælge "Decrypt & Verify" i stedet.

7.3. At underskrive beskeder
Du kan bruge PGP til at lave en slags "digital signatur" eller underskrift. En sådan underskrift gør det muligt for folk at få bekræftet at beskeden rent faktisk stammer fra dig. Dette kan være praktisk f.eks. når man laver aftaler via e-mail. Den private nøgle bruges til at lave underskriften, og den verificeres af modtagerens offentlige nøgle.

For at signere e-mails skal du bruge "Sign" funktionen.

8. Hvad er en "public key server"

En "public key server" er blot en server (dvs. et sted på Internettet) hvor offentlige nøgler kan lægges. Så kan folk slå dem op, som var det en slags telefonbog.

9. Om at forstå nøglebundtet/nøgleoversigten

PGPkeys viser en oversigt over alle de nøgler du har - både andres og dine egne. Du får formentlig ikke brug for at vide så meget om denne oversigt, men herunder er nogle detaljer der kan hjælpe med at afmystificere.

IKONER i oversigten: (se generelt under "Description")
- Nøgle bagved angsigt -> Et nøglepar (privat og offentlig nøgle)
- Konvolut -> Navne tilknyttet nøglen
- Blyant -> Ikke-eksporterbar signatur (nøglen er underskrevet af én der ikke ønsker at videregive signaturen til eksempelvis servere)
- Blyant med pil -> Eksporterbar signatur (nøglen er underskrevet af én der ikke har noget imod at hans signatur bruges som ægthedsattest)
- Blyant med gråt ur -> En signatur som er udløbet (dvs. underskrevet men forældet)
- Sort blyant -> Meta-introducer, ikke-eksporterbar
- Sort blyant med pil -> Trusted Introducer, Eksporterbar

Menuen KEYS:
"Sign..." -> Bruges til at anerkende en nøgle som ægte. Dette sker automatisk når du opretter dine egne nøgler. Du kan anerkende andres nøgler ved at signere dem.
"Set as default key..." -> Gør det til standardnøglen
"Add"
- "Name" kan du tilføje et ekstra navn til samme nøglepar. Dvs. at du kan have flere aliasser under samme nøgle, hvilket er særligt smart hvis du f.eks. har flere adresser el.lign. Disse aliasser vises som konvolutikoner.
- "Photo" -> Tilføj et billede til nøglen
- "Revoker" -> Giver en anden nøgle mulighed for at tilbagekalde den valgte nøgle
- "Certificate" -> Tilføj et certifikat (kort sagt er et certifikat en tredjemands godkendelse af den angivne nøgle)
"Revoke..." -> Tilbagekald det valgte nøglesæt. Du vil ikke kunne bruge det mere og andre vil ikke kunne kryptere mere (med den offentlige nøgle)
"New key..." -> Her kan du lave et nyt sæt nøgler (f.eks. hvis du er kommet til at slette dit gamle, eller blot har brug for et nyt sæt)
"Share Split..." -> Du kan dele en nøgle op blandt flere nøglehavere, og dermed gøre brugen af nøglen betinget af at et vist antal af nøglehavere verificerer
"Import" -> Importér en (offentlig) nøgle
"Eksport" -> Eksportér en offentlig nøgle
"Properties" -> Ændr egenskaberne for den valgte nøgle, herunder tilføj/slet undernøgler ("subkeys")

Menuen SERVER:
"Server"-menuen er din indgang til public key servers (se herunder). Du kan søge efter andres nøgler, eller du kan lægge din egen offentlige nøgle ud.

Menuen GROUPS:
Du kan gruppere dine nøgler så de er lettere at holde styr på. Du kan have de samme nøgler i flere grupper. Du kan roligt slette en gruppe uden at det påvirke nøglerne i gruppen. Gruppen er med andre ord kun et organisatorisk redskab til at kategorisere (henvisninger) til nøgler.

10. Sådan sender du din "public key" til andre
For det første kan du lægge din offentlige nøgle på en såkaldt public key server - en slags online telefonbog. Se programmets hjælpfunktion ang. dette.

For det andet kan du højreklikke på den ønskede nøgle og vælge "Copy". Nøglen bliver da kopieret til udklipsholderen og du kan indsætte nøglen (som jo bare er en talkode) ved at bruge tekstprogrammets Indsæt/Paste funktion.

Du kan også trække og slippe nøglen til f.eks. skrivebordet, hvorved den offentlige nøgle oprettes som en fil. Denne fil kan du så lægge over på en diskette, USB-pen eller lignende, eller du kan hæfte den ved en e-mail. Alternativt kan du vælge nøglen og derefter "Export" (CTRL + E). Filen bliver gemt som en .asc fil.

11. PGP kan også kryptere filer
Du kan også bruge PGP til at kryptere filer på din computer. Brug funktionen PGPdisk til dette.

12. Sammenfatning
Lad dig ikke afskrække af denne artikels længde eller PGPs på nogle punkter indviklede brugerflade. Husk blot på flg. og så kommer forståelsen hurtigt:
1. Du skal oprette et sæt nøgler
2. Når du skal sende en krypteret besked til andre, skal du først have deres offentlige nøgler (public key)
3. Når andre skal sende en krypteret besked til dig, skal de først have din offentlige nøgle
4. Brug ikonet i taskbaren til at kryptere og afkode beskeder

Sværere er det sådan set ikke!

Appendiks 1 - Hvor sikker er PGP-kryptering?
PGP anvender noget nær den bedste kryptering der er tilgængelig.

PGPI.ORG skriver: "*Given all of today's computing power and available time even a billion computers doing a billion checks a second it is not possible to decipher the result of strong cryptography before the end of the universe.*"

Naturligvis kan man dog ikke forudsige evnerne af fremtidige computere, som PGPI også skriver: "*No one has proven that the strongest encryption obtainable today will hold up under tomorrow's computing power. However, the strong cryptography employed by PGP is the best available today. Vigilance and conservatism will protect you better, however, than claims of impenetrability.* "

Når det er sagt, må det tilføjes at ingen endnu har brudt PGPs kryptering, på trods af at kildekoden til kryptering er offentlig og mange eksperter har prøvet.

Således fremgår det af Andre Bacards FAQ: "*Almost daily, someone posts a notice such as 'PGP Broken by Omaha Teenager.' Take these claims with a grain of salt. The crypto world attracts its share of paranoids, provocateurs, and UFO aliens. To date, nobody has publicly demonstrated the skill to outsmart or outmuscle PGP.*"

Bruce Schneier har udtalt: "*Assuming you trust IDEA, PGP is the closest you're likely to get to military-grade encryption*"

Appendiks 2 - Teoretiske muligheder for sikkerhedsbrud
Naturligvis er PGP kun sikker fra beskeden er krypteret til den igen afkodes. Er der installeret overvågningsudstyr eller keyloggers hos afsenderen eller modtageren, kan det jo være lige meget hvor krypteret beskeden ellers er, hvis den opsnappes før den er blevet krypteret eller efter den er blevet afkodet.

Hvad angår keyloggers, er den bedste måde at sikre sig nok at sørge for altid at have et godt antivirusprogram installeret.

I samme dur er det vigtigt at man sørger for at få checket at ens PGP-installation(sfil) ikke er blevet ændret. Kort sagt, bør man checke sin installations checksum.

Man kunne også forestille sig det scenarie at det lykkes en mellemmand at opsnappe udvekslingen af public keys, og erstatte disse med sin egen public key. Dermed ville denne mellemmand kunne afkode beskeder, men ville kun kunne fortsætte med at gøre dette hvis han samtidig krypterede beskeden med den oprindelige (ægte) nøgle og sendte den videre - ellers ville parterne jo hurtigt opdage at noget var galt.

Selv om man frit kan offentliggøre public keys, er det ydermere mest sikkert at indhente sin public key direkte fra kilden/afsenderen. Dette skyldes, faren for at nogen kan have erstattet den oprindelige public key med deres egen. F.eks. kunne man forestille sig at en hacker erstatter en public key på en hjemmeside, med sin egen.

Læs mere om PGP-sikkerhed her:
- http://home.clara.net/heureka/sunrise/pgpsec.htm
- http://kb.iu.edu/data/adcb.html
- http://senderek.de/security/secret-key.protection.html

Anden litteratur:

Du kan med fordel kigge i PGPs medfølgende hjælp fil som går meget i dybden med de forskellige koncepter, samt hvordan man bruger PGP.

Nogle interessante artikler om PGP kan læses her:
- Om hvordan PGP virker: http://www.andrebacard.com/pgp.html
- Om hvordan PGP virker: http://www.pgpi.org/doc/pgpintro/#p9
- Wisegeek: "What is PGP?" (http://www.wisegeek.com/what-is-pgp.htm)
- Om at installere PGP: http://www.spywarewarrior.com/uiuc/ss/pgp8fw/pgp8fw.htm
- David Ross om PGP: http://www.rossde.com/PGP/index.html#links

Interessante links om PGP:
- http://pages.infinit.net/carbo1/pgp.html

Ændringslog:

14. oktober 2006:
- Rettede nogle stavefejl

13. oktober 2006:
- Tilføjet appendiks 1-2
- Andre småændringer

Kommentar af bondester d. 19. Oct 2006 | 1

Flot gennemarbejdet artikel, som virkelig kommer godt rundt om PGP.
Dog tvivler jeg lidt på påstanden om at mails krypteret med PGP ikke skulle kunne brydes uden nøglesættet. Hvis organisationer som NSA (med deres ECHELON netværk) vil have fat i oplysningerne, så er jeg ret sikker på de også får det. Dog uden at have beviser for min påstand ;-)

Keep up the good work...

Kommentar af mccookie d. 26. Oct 2006 | 2

super

Kommentar af r11jep d. 21. Nov 2006 | 3

Kommentar af fromsej d. 13. Oct 2006 | 4

Godt gennemarbejdet artikel.*S*

Kommentar af foxmulder58 d. 12. Oct 2006 | 5

Flot artikel med brugbart indhold.

Kommentar af miqe d. 12. Oct 2006 | 6

Udemærket artikkel.
Ét enkelt minus: Artiklen og specielt de praktiske eksempler henvender sig til Windowsbrugere, men dette er desværre ikke nævnt i teaseren.

Kommentar af psycosoft-funware d. 12. Oct 2006 | 7

utroligt godt skrevet for nybegyndere... godt arbejde! :)

/psycosoft-funware

Kommentar af nightsofdream d. 18. Oct 2006 | 8