

hvis du vil noget med it

COMPUTERWORLD

Publiceret
22. januar 2014 kl. 16:01
på cw.dk/art/229651
Printet 29. januar 2014

IDG

Guide: Så nemt kommer du i gang med e-mail-kryptering

Undgå at andre kan snage i dine e-mails og bliv klogere på kryptering. Her kan du læse, hvordan du får opsat din e-mail-klient til at understøtte en af de mest anerkendte krypteringsstandarder.

Jens Holm

Er du nervøs for, at uvedkommende læser med, når du sender mails? Og er det overhovedet sikkert at sende en god gammeldags e-mail?

Det spørger mange sig selv efter afsløringerne af, hvordan den amerikanske efterretningstjeneste, NSA, høster gigantiske mængder data over hele verden.

En af metoderne til at undgå e-mail-snageri er at benytte sig af kryptering, som (formentlig) kan gøre dine beskeder ulæselige for uvedkommende.

På de følgende sider kan du læse og se, hvordan du kan sikre din kommunikation ved at sende krypterede mails med de fire populære mail-klienter [Microsoft Outlook 2013](#), [Mozilla Thunderbird](#), [Apple Mail](#) og [Gmail](#).

Derfor er krypteringen vigtig

Vi har allieret os med sikkerhedseksperter Henrik Kramshøj, som til daglig benytter sig af krypterede mails, så ofte han kan slippe af sted med det.

"Jeg finder det lige så vigtigt som at få breve med mit cpr-nummer sendt i lukkede konvolutter, og lige så vigtigt som det er at låse min bil eller cykel, når jeg går fra den," mener Henrik Kramshøj.

En af metoderne til e-mail-kryptering hedder PGP (Pretty Good Privacy), der i dag er en af de mest populære og anerkendte krypteringsmetoder til e-mail.

Undgå at alle kan læse med

Når du benytter den konventionelle ukrypterede e-mail-standard, betyder det i praksis, at alle personer, der har adgang til netværket eller mail-serverne, som din e-mail passerer på sin vej, kan kigge ned i din e-mail og læse alle informationer.

"Hvis ikke de netværk, vi bruger til internet-kommunikation, er opsat rigtigt, ja så kan alle i princippet lytte med og se, hvad du skriver i din e-mail," siger han.

Hvor meget bruger du selv PGP i din e-mail-kommunikation?

"Jeg prøver at bruge det, hver gang jeg skal sende noget, som jeg betragter som hemmeligt. Det vil sige adgangskoder, brugernavne eller andre forretningshemmeligheder," fortæller Henrik Kramshøj.

Hvis du vil vide mere om kryptering og de tekniske aspekter af PGP, kan du læse videre på [side 2](#) af denne artikel.

Guiderne til de fire e-mail-klienter finder du her:

[Side 3: Microsoft Outlook 2013](#)

[Side 4: Mozilla Thunderbird](#)

[Side 5: Apple Mail](#)

[Side 6: Gmail](#)

Sådan fungerer PGP

Krypteringsstandarden PGP blev oprindeligt udformet af krypto-pioneren Phil Zimmermann i 1991, og den er i sin tekniske struktur udarbejdet sådan, at du som slutbruger selv er i fuldstændig kontrol over din egen sikkerhed.

I al sin enkelhed benyttes PGP til at kryptere din rene tekst til (for os mennesker)

uforståeligt og sikkert indhold.

"Din krypterede PGP e-mail indeholder matematik, som PGP-programmerne kan bruge til at verificere, at mailen er blevet sendt fra den rigtige person. Det er det helt overordnede formål med krypteringen," fortæller Henrik Kramhøj.

PGP kræver ekstra programmer

Det kræver dog lidt teknisk snilde og arbejde fra forbrugerens side at få de krypterede e-mails til at fungere.

"Man skal have et mail-program, der forstår PGP, og det forstår de fleste programmer i dag ikke fra fabrikken af, men her findes der en masse nemme og enkle plugins til de mest gængse e-mail-programmer, som kan aktivere PGP," siger han.

På de følgende sider kan du læse, hvilke PGP-programmer du kan bruge til PGP-opsætning med Microsoft Outlook 2013, Mozilla Thunderbird, Apple Mail og Gmail.

Hjørnestenen i PGP-kryptering: Krypteringsnøglerne

For at forstå funktionaliteten bag PGP-krypteringen er det vigtigt at bide mærke i to særlige krypteringsnøgler, som både bruges til at kryptere selve indholdet af din e-mail, men også til at verificere, at dine mail-kontakter også er, hvem de udgiver sig for at være.

Begge nøgler genereres af slutbrugeren, når PGP opsættes til e-mail-klienten. Den ene af de nøgler er en offentlig nøgle, public key, som skal bruges af din kontaktpersoner, når rette vedkommende skal lave en krypteret e-mail til dig.

"Den offentlige nøgle kan man vidt og bredt udbrede, og alle, der har din offentlige nøgle, kan sende krypterede e-mails til dig," fortæller Henrik Kramshøj.

Den anden nøgle er straks mere hemmelig. Her er der tale om den såkaldte private nøgle, private key, som du bruger til at afkode den krypterede e-mail, så den bliver læselig for almindelige mennesker.

Modsat den offentlige nøgle er den private nøgle hemmelig og skal ikke falde i hænderne på andre.

Alle, der kender din private nøgle, kan nemlig afkode krypterede e-mails, som er blevet afsendt til dig.

"På den måde kan man skabe fortrolighed og kommunikere sikkert til rette vedkommende person," siger Henrik Kramshøj.

Sådan sender du en krypteret e-mail

For at sende krypterede e-mails frem og tilbage mellem afsender og modtager, kræver det, at begge parter kender hinandens offentlige nøgler.

Udveksling af de offentlige nøgler kan foregå manuelt ved at sende dem til hinanden, men udvekslingen kan i dag også foregå helt automatisk gennem PGP-programmerne, der installeres sammen med din e-mail-klient.

"Visse PGP-klienter har gjort det hele lidt nemmere ved at lave nogle netværk af nøgle-servere, hvor du kan uploade din offentlige nøgle, så PGP-programmerne automatisk kan hente nøglen ned, når du vil kommunikere krypteret med en ny person," fortæller Henrik Kramshøj og fortsætter:

"Lægger du din nøgle op der og knytter nøglen til din e-mail-adresse, kan andre nemt finde din nøgle uden at surfe rundt på nettet efter den eller få den udleveret af dig manuelt."

Her skal du være opmærksom

Selv om automatiseringen og synkroniseringen af offentlige nøgler gør udvekslingen nemmere, er der én enkelt faldgrube, du skal være opmærksom på.

"Når du downloader en tilfældig offentlig nøgle, som er tilknyttet en person, du vil sende en krypteret e-mail til, fra nøgleserveren, kan det i princippet være en helt anden person, som har lagt nøglen op på serveren. Derfor bør man altid verificere, at den nøgle, man downloader, virkelig tilhører den person, man vil kommunikere med," mener Henrik Kramshøj.

For at verificere nøglen har du flere forskellige muligheder.

"Du kan verificere nøglen med det fingeraftryk den har, fingerprint, som du kan få fra personen, der har nøglen, eller ved at se på den signatur, nøglen er afsendt med. Der kan være andre, som du allerede kender, der har skrevet under på, at nøglen rent faktisk tilhører den person, du ønsker at kommunikere med. Dette kaldes Web of trust," siger Henrik Kramshøj.

Ingen kan garantere 100 procent sikkerhed

PGP-krypteringen gør det naturligvis svært for udefrakommende at aflure dine beskeder, men sommerens efterretningsafsløringer viser samtidig, at der ikke findes garantier for, at selv dine krypterede e-mails ikke kan aflures.

I efteråret blev det afdækket af flere medier, at den amerikanske efterretningstjeneste, NSA, har allieret sig med kommercielle krypterings-tjenester, som giver NSA mulighed for at dekryptere beskeder gennem bagdøre. Det kan du læse mere om [her](#).

Guiderne i denne artikel er baseret på det frie og uafhængige OpenPGP, der er udgivet som open source, som NSA, så vidt vides, endnu ikke kan dekryptere.

Opsætning: Microsoft Outlook 2003

Denne guide tager udgangspunkt i, at du allerede har opsat din e-mail-adresse i

Microsoft Outlook 2013.

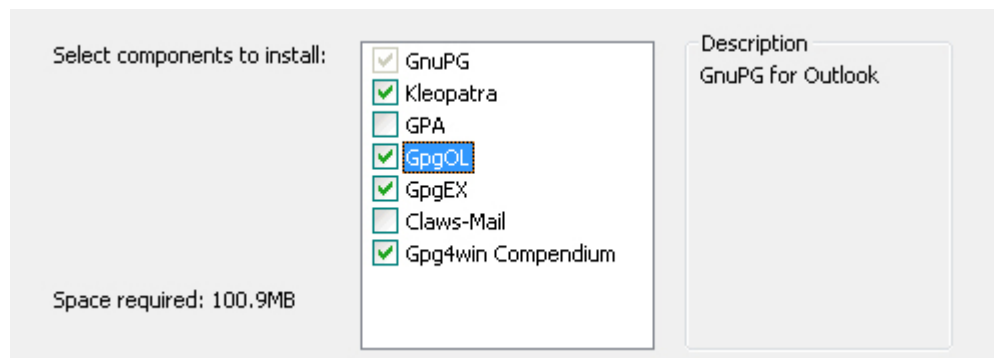
For at bruge PGP med Outlook 2013 er det nødvendigt at gøre brug af et stykke open source-software, fordi e-mail-klienten ganske enkelt ikke kan forstå PGP som standard.

Følg guiden nedenfor for at opsætte Outlook 2013 til krypteret e-mail.

Guiden følges på eget ansvar.

1) Installer Gpg4win

Luk Outlook 2013, hent [Gpg4win](#) og installer Gpg4win i Windows. Her er det vigtigt, at du installerer Gpg4win med GPGOL, se billedet nedenfor.



Genstart Windows.

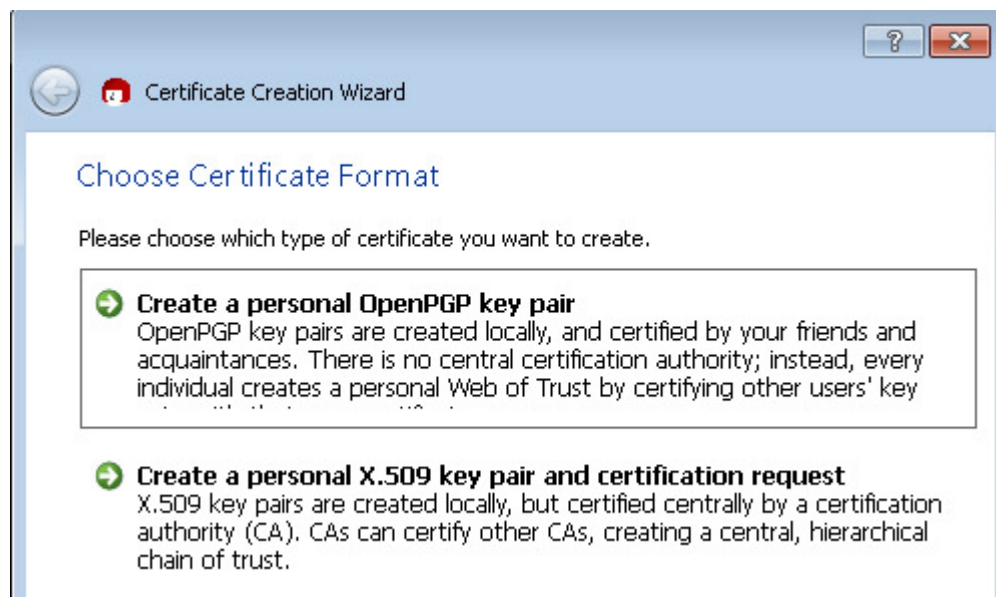
2) Generer dine PGP-nøgler

Gå til din Gpg4win i startmenuen og åbn programmet Kleopatra, som er Gpg4win's program til at generere og håndtere private og public keys.

Er du i tvivl om, hvad PGP-nøgler er, så start med at læse side [to](#) af denne guide.

Gå til 'file' og tryk på 'New Certificate' for at generere dine to PGP-nøgler.

Klik derefter på 'Create a personal OpenPGP key pair'.



Indtast dit navn og e-mail adresse i de næste felter og tryk 'Next'.

Vælg en adgangskode til dine nøgler. Her er det meget vigtigt, at du husker denne kode, fordi du kommer til at bruge den igen, hver gang du skal afsende en krypteret e-mail, eller hvis du ønsker at bruge dine nøgler på andre systemer.

Lad Kleopatra-programmet generere din nøgle, sæt kryds i fluebenet 'ASCII armor' og gem derefter nøglen på din computer ved at trykke på 'Make a Backup Of Your Key Pair'.

3) Klar til afsendelse

Outlook 2013 er nu opsat med PGP, og du kan nu teste afsendelse af krypto-e-mail.

Som standard sender Outlook 2013 e-mails med HTML-koder, som kan bruges til at opsætte e-mailen grafisk, men hvis du vil afsende krypterede e-mail, er det en god idé at skifte denne indstilling til klar-tekst.

Hvis ikke ændringen til klar-tekst sker, vil modtageren af din krypterede e-mail godt nok få din besked, men vedkommende vil samtidig få en masse HTML-kode med, som ikke vil blive aflæst rigtigt, når e-mailen er blevet dekrypteret hos modtageren.

Indstillingen til at ændre e-mail indhold fra HTML til klar-tekst finder du ved at gå til 'Indstillinger for Outlook', derefter 'Mail'. Her kan du skifte indstillingen 'Opret meddelelser i dette format' fra HTML til klar-tekst.



For at sende krypteret e-mail kræves det, at du kender modtagerens public key. Du kan tilføje dine kontaktpersoners nøgler i Kleopatra programmet. Enten ved manuelt at importere nøglerne fra en tekstfil, ellers kan du slå din modtagers nøgle op på en nøgle-server, hvis vedkommende har uploadet sin nøgle.

Opsætning: Mozilla Thunderbird

Denne guide tager udgangspunkt i, at du bruger Windows som styresystem, og at du allerede har opsat din e-mail-adresse i Mozillas Thunderbird e-mail-klient.

For at bruge PGP med Thunderbird er det nødvendigt at gøre brug af et stykke open source-software og et tredjeparts-plugin, fordi e-mail-klienten ganske enkelt ikke kan forstå PGP som standard.

Følg guiden nedenfor for at opsætte Thunderbird til PGP.

Guiden følges på eget ansvar.

1) Installer Gpg4win

Luk Thunderbird, hent [Gpg4win](#) og installer Gpg4win i Windows.

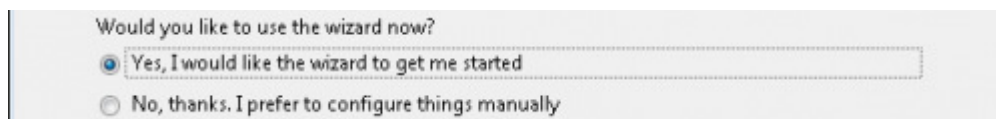
2) Installer Enigmail-plugin til Thunderbird

Start din Thunderbird-klient og find Enigmail i Thunderbirds plugin-database.

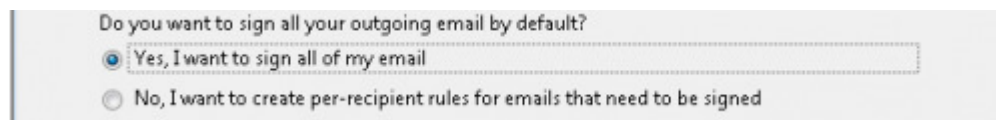
Enigmail kan findes ved at gå til Thunderbirds menupunkt 'Tilføjelser', her skal du derefter søge efter det omtalte plugin Enigmail, installer plug-in og genstart derefter Thunderbird.

3) Følg Enigmails PGP-opsætningsguide

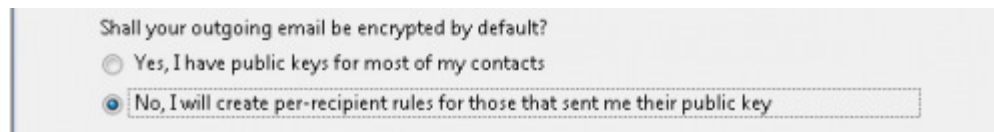
Vælg den øverste option om at følge guiden 'OpenPGP Setup Wizard', som popper op automatisk, når Thunderbird åbner igen.



Vælg den øverste option og vælg at signere alle dine krypterede e-mails som standard.



Her kan du vælge, om alle dine udgående e-mails skal krypteres. Som standard er denne option sat til, at du selv vælger, om og hvornår du vil kryptere din udgående mail.

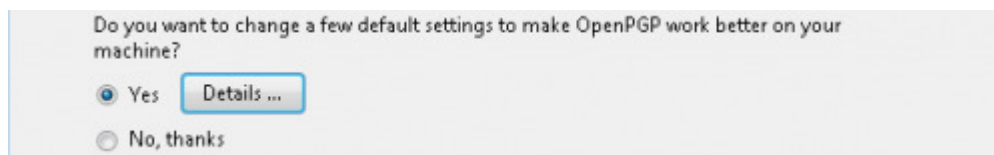


Shall your outgoing email be encrypted by default?

Yes, I have public keys for most of my contacts

No, I will create per-recipient rules for those that sent me their public key

Vælg den første option 'Yes' for at lade Enigmail optimere Thunderbird til PGP og tryk på næste.



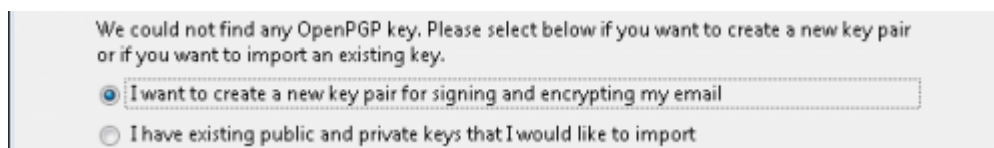
Do you want to change a few default settings to make OpenPGP work better on your machine?

Yes

No, thanks

Vælg den første option for at generere din private og public key.

Hvis du er i tvivl om, hvad en key er, så kan du læse side [to](#) af denne guide.

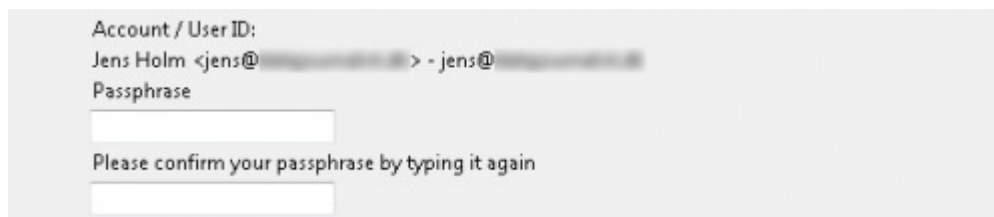


We could not find any OpenPGP key. Please select below if you want to create a new key pair or if you want to import an existing key.

I want to create a new key pair for signing and encrypting my email

I have existing public and private keys that I would like to import

Vælg en adgangskode, der bruges til at benytte din private key, som ingen andre end dig selv må få fingrene i.



Account / User ID:
Jens Holm <jens@... > - jens@...

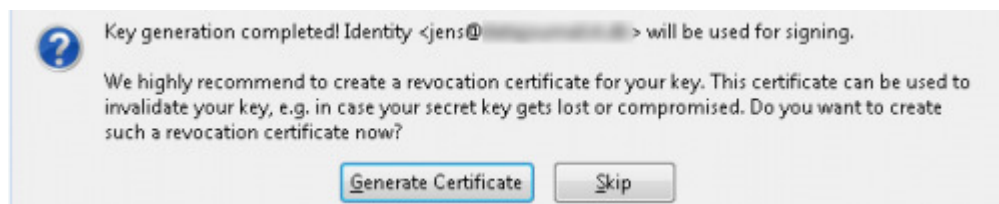
Passphrase

Please confirm your passphrase by typing it again

Tryk derefter næste på status side, hvorefter programmet går i gang med at generere din public og private key.

Derefter bliver du bedt om at generere et certifikat til PGP, der viser dine modtagere, at du virkelig er den, som du udgiver dig for at være.

Her skal du trykke på 'Generate Certificate' og gem derefter din fil et sikkert sted på din computer. Da filen indeholder både din private og public key, er det vigtigt, at du gemmer den et sikkert sted, hvor ingen andre end dig har adgang til den. Gem eventuelt filen, så du kan importere nøglerne på en anden computer i fremtiden.

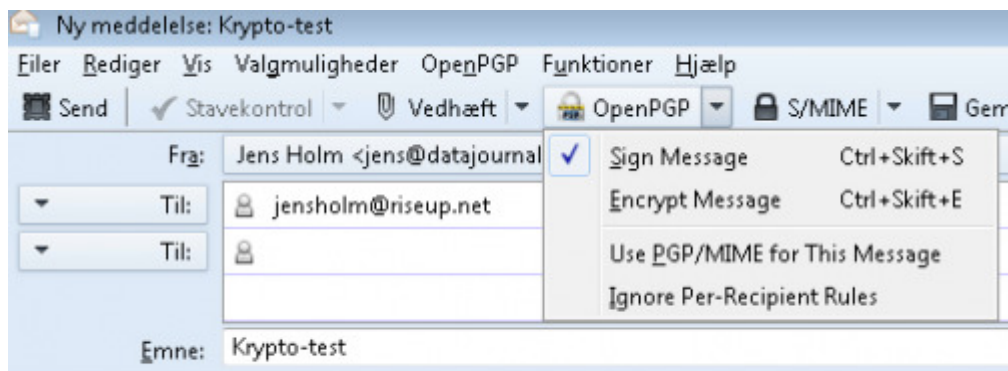


Indsæt din adgangskode, som du oprettede tidligere i guiden, i dialogboksen.

4) Klar til afsendelse

Thunderbird er nu opsat med PGP, og du kan nu teste afsendelse af krypto-e-mail.

Opret en ny e-mail i Thunderbird og klik på ikonet 'OpenPGP' øverst i menubjælken. Her kan du blandt andet se, om din PGG-signatur er på plads.



Dette er en krypteret besked

For at kryptere selve e-mail teksten skal du blot trykke på Encrypt.

Når du derefter sender beskeden, kontrollerer Thunderbird, om du har tilføjet modtagerens public key i din database.

Hvis ikke Thunderbird kender modtagerens offentlige PGP-nøgle, vil du blive mødt med et skærmbillede, hvor du får mulighed for at tilføje den.

Opsætning: Apple Mail

Denne guide tager udgangspunkt i, at du bruger Apple OSX som styresystem, og at du allerede har opsat din e-mail-adresse i Apples e-mail-klient Mail.

For at bruge PGP med Mail er det nødvendigt at gøre brug af et stykke open source-software, fordi e-mail-klienten ganske enkelt ikke kan forstå PGP som standard.

Følg guiden nedenfor for at opsætte Mail til PGP.

Guiden følges på eget ansvar.

1) Installer GPGMail

Luk Mail, hent programmet GPGMail og installer GPGMail i OSX.

2) Generer PGP-opsætningsguide

Start applikationen GPG Keychain Access, der gennem GPGMail er blevet installeret på din Mac.

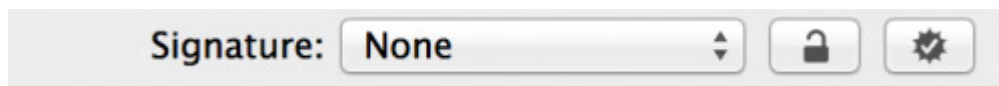
Tryk på 'New' øverst til venstre og generer nu dine to PGP-nøgler, public og private key. Er du i tvivl om, hvad PGP-nøglerne bruges til, kan du læse mere om nøglerne på [side to](#) i denne artikel.

Din nøgler er nu genereret og er klar til brug. Det er en god idé at eksportere dine

nøgler, så du kan bruge dem igen på en anden maskine i fremtiden.

3) Klar til krypto-afsendelse

Start mail og opret ny e-mail. Før at kryptere din kommunikation og sende e-mails med PGP skal du trykke på hængelåsen yderst til højre.



Opsætning: Gmail

Hvis du bruger Gmail eller Google Apps med dit eget domæne, og hvis du samtidig benytter dig af Google Chrome-browseren, kan du bruge PGP med Googles e-mail-service.

Men for at bruge PGP med Gmail og Google Chrome er det nødvendigt at installere et tredjeparts-plugin, så Google Chrome i det hele taget kan forstå PGP-standarden.

Følg guiden nedenfor for at opsætte Google Chrome med Gmail til PGP.

Guiden følges på eget ansvar.

1) Installer Mailvelope-plugin

Start din Chrome Browser, og installer Mailvelope, der kan findes [her](#).



2) Indstil Mailvelope

Før du kan afsende krypterede e-mails, skal du have genereret de vigtige PGP-nøgler. Hvis du er i tvivl om, hvad PGP-nøgler er, kan du læse side [to](#) af denne artikel.

For at generere din private og public key skal du trykke på Mailvelope ikonet i

Google Chrome og derefter trykke på 'Options'.

Vælg derefter 'Generate Key' i menuen til venstre.

Indtast dit navn, e-mail-adresse og en adgangskode. Her er det særligt vigtigt, at du enten kan huske din adgangskode, eller gemmer adgangskoden til fremtidig brug. Adgangskoden skal bruges igen, hvis du skifter e-mail klient eller har brug for dine PGP-nøgler et helt andet sted.

Nu genererer Chrome din public og private key. Når den er færdig, kan du se dine nye nøgler ved at gå til 'Display Keys' i menuen til venstre.

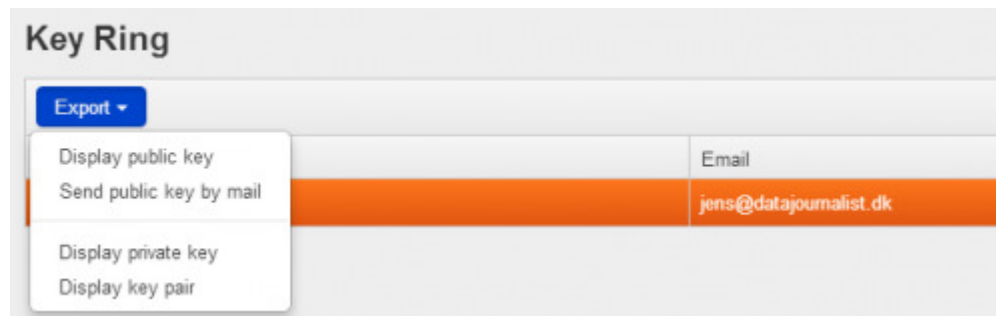


3) Eksporter din nøgle til fremtid brug

Tryk på dit navn i menuen for at vælge dine nye nøgler. Feltet bliver nu orange, og Chrome er klar til at eksportere dine nøgler.

Tryk nu på den blå Export-knap over dit navn og vælg at få vist din public og private key. Kopier teksten fra dem ind i et dokument, som du gemmer et sikkert sted.

Det er yderst vigtigt, at det kun er dig selv, der har adgang til din private key. Alle med denne nøgle kan dekryptere de PGP-mails, som du modtager i fremtiden.



4) Importer nøgler

Når du skal sende en krypteret e-mail til din modtager, skal du kende vedkommendes public key.

Når du har fået udleveret denne nøgle, kan den importeres ved at gå til menu-punktet 'Import Key' til venstre.

5) Klar til afsendelse

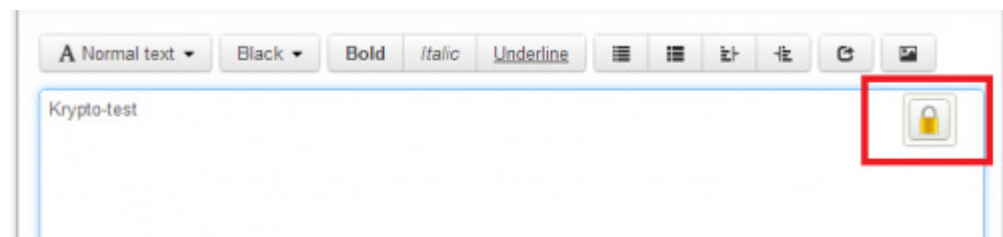
Efter importeringen af modtageren nøgle er du nu klar til at afsende en krypteret e-mail med PGP.

Det kan du gøre ved at oprette en ny e-mail i Gmail og indtaste de nødvendige oplysninger om modtager-adresse, emne og e-mailens indholds-tekst.

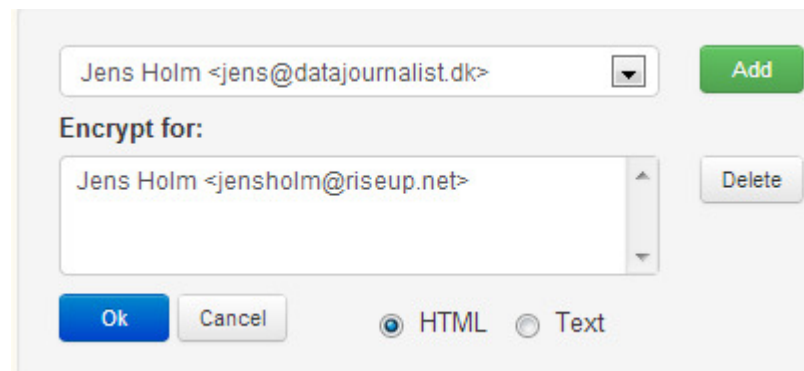
Tryk derefter på Mailvelope knappen, der er placeret inden i vinduet for den nye e-mail.



Nu popper der et nyt vindue op i Chrome, hvor du igen skal trykke på en Mailvelope knap.



Vælg nu modtageradressen og tryk på 'Add'. Derefter 'Ok'.



Tryk derefter 'Transfer'. Nu er e-mailens indhold krypteret til din modtager og er klar til at blive sendt af sted.