PGP håller posten hemlig

Även den som har rent mjöl i påsen kan vilja dölja innehållet i sin e-post. Ett sätt är att kryptera den med PGP, Pretty Good Privacy, som har blivit en succé efter den inledande striden mellan upphovsmannen och de amerikanska myndigheterna.

Att krypterad e-post ännu inte har slagit igenom på bred front är en gåta. Det är väldigt enkelt att använda krypterad e-post. När systemet för krypteringen är på plats krävs inte mycket arbete för att kryptera utgående meddelanden.

Kanske får den nästan mytiska auran kring kryptering många att tro att det är svårt. Vi ska sticka hål på den myten och visa att det är enkelt att med PGP, Pretty Good Privacy, göra det omöjligt för obehöriga att läsa din e-post.

PGP är omfångsrikt och det finns ofta flera sätt att göra samma sak på. Om du vill veta mer finns det utmärkt dokumentation på www.pgpi.org och i de handböcker du kan välja att ta med i installationen.

Vad är PGP?

Amerikanen Phil R Zimmermann utvecklade PGP 1991 som svar på ett lagförslag i USA. Förslaget gick ut på att all amerikansk krypteringsteknik skulle innehålla så kallade bakdörrar så att amerikanska myndigheter och institutioner skulle kunna öppna krypterad kommunikation.

Förslaget blev aldrig lag, men upprörde Zimmermann så till den milda grad att han var beredd att sitta i fängelse för sin önskan att förse världen med ett helt säkert krypteringssystem.

Det faktum att Zimmermann publicerade sitt alster med öppen källkod gjorde att vem som helst kunde försäkra sig om att hans system inte innehöll bakdörrar.

Det var (och är) en stor fördel jämfört med slutna och kommersiella system. Zimmermann koncentrerade sig i sitt program på att göra kommunikation via e-post säker.

Zimmermann blir folkhjälte

Nu inträdde PGP i den fas som gav systemet dess enorma berömmelse. Det gjorde Zimmermann till hjälte och i det närmaste en internets Che Guevara.

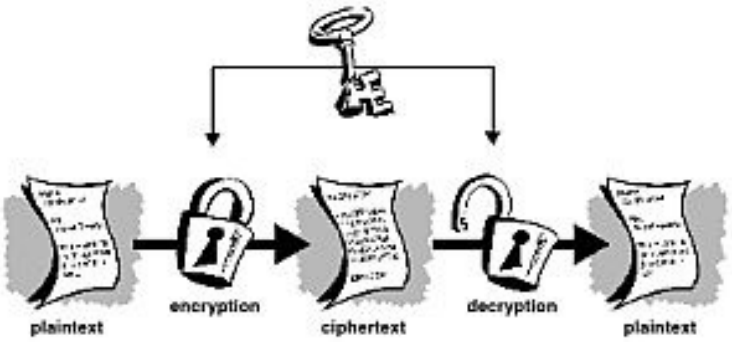
Företaget RSA ägde det asymmetriska kryptosystem som Zimmermann använde och tyckte att Zimmermann brutit mot deras licensregler. Amerikanska myndigheter ansåg också att Zimmermann genom att läcka ut PGP på internet brutit mot förbudet att exportera stark kryptering.

Tusentals användare i hela världen hade kopierat PGP och Zimmermann låg risigt till. Han stod dock på sig och kom till slut undan helskinnad. Mer om det här finns att läsa på PGP:s webbplats.

Asymmetrisk kryptering är kärnan

PGP bygger huvudsakligen på asymmetrisk kryptering, som först presenterades av Whitfield Diffie och Martin Hellman, forskare vid MIT-universitetet i Boston.

Det är ett kryptosystem som inte bygger på att sändare och mottagare har samma nyckel. Forskarna kom på ett matematiskt system där två olika, men likvärdiga, nycklar kunde kryptera respektive dekryptera samma text.



Det är en missuppfattning att asymmetrisk kryptering är bättre än symmetrisk och att den senare har blivit förlegad på grund av den nyare tekniken. Symmetrisk kryptering används som aldrig förr. Asymmetrisk kryptering används mest för att distribuera symmetriska nycklar samt för signering och autentisering.

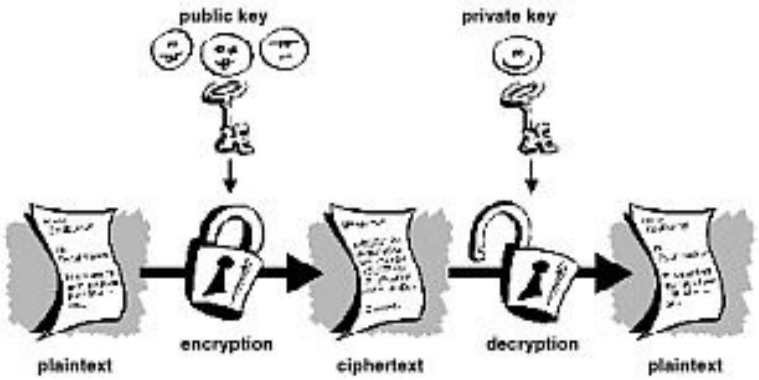
Problemet med symmetriska nycklar har alltid varit att hitta en säker metod för att distribuera de hemliga nycklarna. Med asymmetrisk kryptering var det här problemet löst i en handvändning.

Diffie-Hellman-algoritmen (D-H) tillämpades och vidareutvecklades till RSA-systemet, som har dominerat sedan dess. RSA fick sitt namn efter grundarna Rivest, Shamir och Adleman, även de vid MIT.

NSA (National Security Agency) var starkt emot RSA-systemet, men Shamir var israel och kunde publicera innovationen utanför USA. NSA gormade, men fick ge sig för den i forskarvärlden mycket starka driften att publicera sina rön.

Privat och publik nyckel

Både D-H och RSA bygger på ett matematiskt, komplicerat system där en av nycklarna i ett nyckelpar kan användas för att kryptera ett meddelande och den andra kan användas för att dekryptera samma meddelande. Nycklarna kallas privat respektive publik och används som namnen antyder.



PGP använder asymmetrisk kryptering för att distribuera symmetriska nycklar, som står för krypteringen av e-breven. Den symmetriska nyckeln, eller sessionsnyckeln, skickas tillsammans med brevet och fungerar som en engångsnyckel.

Om vi vill skicka ett brev skapar PGP en sessionsnyckel, krypterar med den och inkluderar den i brevet. PGP krypterar sessionsnyckeln med mottagarens publika, asymmetriska nyckel. Mottagaren använder sin privata nyckel för att ta fram sessionsnyckeln och kan därefter dekryptera brevet.

A och B kan kommunicera säkert genom att A använder B:s publika nyckel för att kryptera sitt meddelande. B använder sin privata nyckel (som bara B har) för att dekryptera meddelandet.

Även om alla andra också har B:s publika nyckel (den är ju publik) kan bara den privata användas för dekryptering av text som krypterats med den publika nyckeln.

A kan också signera sina meddelanden med sin privata nyckel. B kan bekräfta att meddelandet kommer från A, eftersom det endast kan dekrypteras med A:s publika nyckel.

Asymmetrisk kryptering tar tid

Nackdelen med asymmetrisk kryptering är att algoritmen är så komplicerad att det tar tid att utföra kryptering och dekryptering. Därför används asymmetrisk kryptering framför allt för att kryptera symmetriska nycklar inför distributionen av dem.

Den asymmetriska krypteringen av symmetriska nycklar behöver utföras endast vid enstaka tillfällen. De asymmetriskt krypterade symmetriska nycklarna kan sedan distribueras säkert och användas till kryptering av meddelanden.

Symmetrisk kryptering är så enkel att utföra att den kan byggas in i hårdvara, vilket medför att den är perfekt för krypteringsoperationer som behöver utföras i en strid ström.

Symmetrisk kryptering lever kvar i all önskvärd välmåga, i motsats till vad många kanske tror. Asymmetrisk kryptering är inte bättre eller starkare ur ett säkerhetsperspektiv, vilket är en vanlig missuppfattning. Det är genom att kombinera asymmetrisk kryptering med symmetrisk kryptering som vi får en stor fördel.

Installation

Vi börjar med att hämta den senaste versionen av PGP för Windows från www.pgpi.org. I skrivande stund är 6.0.2i den senaste internationella versionen, men kontrollera vad som gäller för dig.

PGP finns även som tilläggsprogram till e-postprogram som Outlook och Eudora. Vi valde versionen för Outlook eftersom den kan det mesta, medan versionen för Outlook Express kan lite mindre. Allt det här finns väl dokumenterat på PGP:s webbplats.

Installationen av PGP ska inte vålla några problem. Det finns dock ett par små saker att tänka på.

Kontrollera vilket eller vilka tilläggsprogram som gäller för dig. Bocka för att de ska installeras.

Installationsguiden är mycket enkel och smidig. Välj rätt tilläggsprogram och svara nej när guiden frågar dig om du vill använda en befintlig nyckelring (såvida du inte har en från en tidigare installation).

Om du vill testa funktioner för filkryptering med mera ska du bocka för de andra komponenter som ska ingå i installationen.
I slutet av installationen frågar programmet om du vill använda en befintlig nyckelring (nycklar du samlat på dig tidigare). Svara nej om det här är din första installation av PGP.

När installationen är klar behöver vi skapa ett nyckelpar: en hemlig, privat nyckel och en publik, allmänt tillgänglig nyckel. Det är viktigt att dessa hålls isär på rätt sätt, men det sköter PGP automatiskt åt dig.

Skapa ditt första nyckelpar

Om installationsguiden inte frågar dig om du vill skapa nycklar kan du starta guiden genom att klicka på det grå hänglåset i aktivitetsfältet och välja Launch Pgpkeys. När programmet har startat klickar du på nyckeln längst till vänster. Pgpkeys kan även startas från startmenyn.

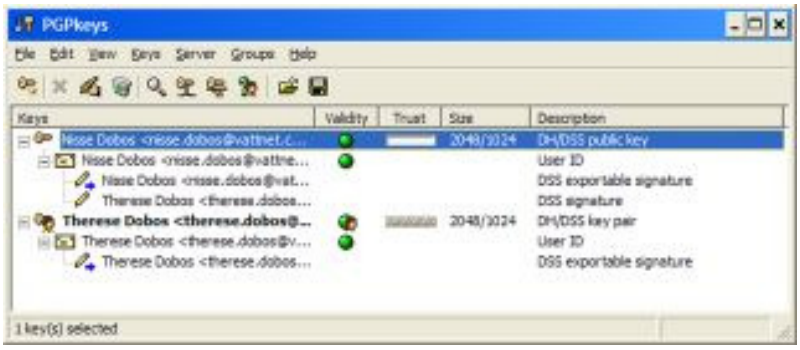
De förvalda alternativen duger gott och det finns ingen anledning att välja andra alternativ om du inte är överdrivet noga med säkerheten.

I guiden för att skapa ett nyckelpar kan du till exempel ange nyckellängden. Det förvalda alternativet tar sisådär tio miljoner år att knäcka med en Pentium 4-dator.

Några roliga detaljer i guiden är mätningen av hur säkert ditt lösenord är och genereringen av slumptalsfrön utifrån dina rörelser med musen.

PGP:s guide för att skapa nyckelpar har några roliga och nyttiga detaljer. Här ser vi en mätare som visar hur bra lösenord vi valt till nyckelparet. Ju mer indikatorn fyller upp åt höger desto bättre lösenord.

När guiden är klar kommer du tillbaka till programmet Pgpkeys. I huvudfältet ser du ditt nya nyckelpar tillsammans med andra (publika) nycklar från medarbetare på PGP. Även grundaren Phil R Zimmermanns nyckel finns där. Nycklarna som finns med från början kan du ta bort om du tycker att de är i vägen, såvida du inte absolut vill kommunicera säkert med en eller flera personer i listan.



Pgpkeys hanterar dina och andras nycklar. När vi har skapat vårt nyckelpar visas det i listan tillsammans med nycklar från medarbetare på PGP. Här har vi även installerat en publik nyckel från Nisse, som vi därefter kan skicka krypterad e-post till.

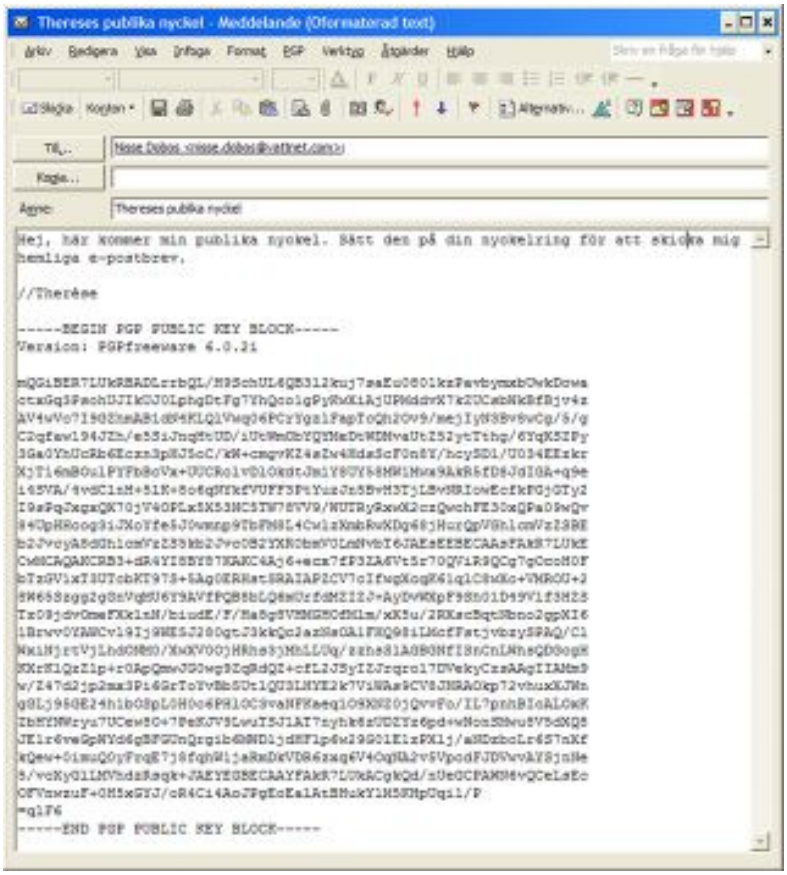
Distribuera nycklar

Asymmetrisk kryptering går ut på att du distribuerar din publika nyckel till de personer du vill kommunicera säkert med. Du behöver ha dina kommunikationspartners publika nycklar i din nyckelring.

Det är smidigt att publicera publika nycklar via PGP:s servrar, men vi ska göra det via e-post för att göra det lite mer pedagogiskt. Det går att distribuera en nyckel manuellt på två sätt: exportera till en fil eller kopiera och klistra in i ett e-brev. Båda sätten är lika bra, men vi väljer det sistnämnda.

För att kopiera och klistra in din nya publika nyckel i ett e-brev markerar du nyckeln (nyckelparet i huvudfältet i Pgpkeys), högerklickar och väljer att kopiera (copy). Öppna sedan ett nytt e-brev i ditt e-postprogram (vi använder Outlook här), högerklicka i e-brevets textfält och välj Klistra in (paste).

Nu har e-brevet fyllts med text som ser ut som rappakalja. Skriv din vanliga text, mottagare och rubrik och skicka brevet.



Du kan distribuera din publika nyckel på flera sätt. Vi väljer ett som alltid fungerar: Att klistra in den i ett e-brev. Högerklicka på nyckeln, kopiera och klistra in i e-brevets textfält. När mottagaren får ditt e-brev med nyckeln markerar hon nyckeldelen av texten i textfältet, kopierar och klistrar in i huvudfältet i Pgpkeys samt anger lösenord för nyckeln.

Om dina vänner använder PGP kan de skicka sina publika nycklar till dig på samma sätt. När du får ett e-brev med en publik nyckel markerar du hela nyckeldelen i textfältet (men inte e-brevets övriga text), högerklickar och kopierar. Högerklicka på någon tom del av huvudfältet i Pgpkeys. Välj att klistra in (paste). Programmet visar en dialogruta där du ska välja att importera nyckeln.

Är det verkligen Pelles nyckel?

Nyckeln är nu importerad och om den kommer från Pelle är det hans nyckel du ska använda för att skicka e-post till honom. Han ska göra på samma sätt med din nyckel.

Läsare med huvudet på skaft tänker: Hur vet jag att Pelles nyckel verkligen kommer från Pelle? Det vet du inte. Du kan i alla fall inte vara helt säker på att så är fallet.

Någon kan skapa en nyckel i Pelles namn, med Pelles e-postadress och skicka den till dig. Prova själv i Pgpkeys. Det finns lösningar på det här problemet, men det kräver lite mer pyssel och de ingår inte i PGP-paketet.

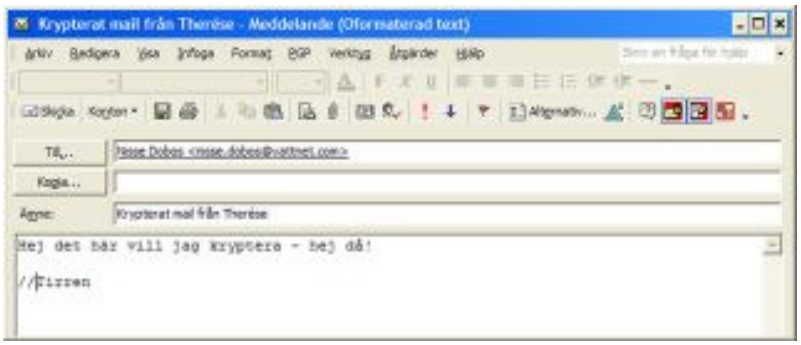
En lösning är att skriva en viss text i e-brevet och ringa personen i fråga för att få texten bekräftad. En annan lösning är att skapa en digital signatur med till exempel sha-1 och kontrollera den över telefon. Om du har ett bankcertifikat kan du importera det i e-

postprogrammet och signera e-brevet med din publika nyckel med din e-legitimation.

Skicka krypterad post

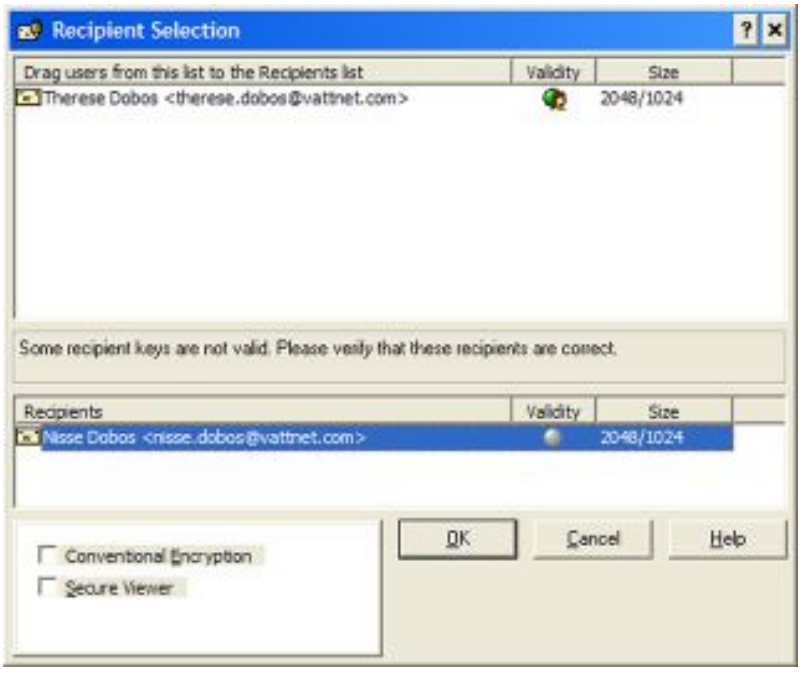
Nu är PGP installerat och klart att använda för att skicka e-brev till de personer du har utväxlat nycklar med. Om du tittar i raden av ikoner i Outlook ser du några nya. De används för att antingen kryptera eller signera meddelanden eller för att både kryptera och signera dem.

Det hela är synnerligen enkelt. Skriv ditt meddelande som vanligt med mottagare, rubrik och text. Klicka på ikonen för kryptering (den högra), ikonen för signering (den i mitten) eller båda.



Dags att skicka ett krypterat e-brev till Nisse. Skriv brevet med mottagare, rubrik och text och använd de nya, röda ikonerna längst till höger i ikonraden. När den vänstra ikonen (med brev och hänglås) har en blå ram kommer brevet att krypteras. När ikonen i mitten har en blå ram kommer det att signeras. Om båda har blå ram sker både och.

Klicka på skicka. Nu kommer PGP att fråga vilken nyckel som meddelandet ska krypteras med. Välj den som du har fått av personen som e-brevet ska skickas till. Ange lösenordet och klicka på OK. Meddelandet skickas iväg.



När vi klickat på skicka i e-postprogrammet visas det här fönstret. Innan brevet krypteras och skickas iväg ska vi välja publik nyckel för krypteringen. Vi väljer den nyckel som vi fått från mottagaren. Om brevet ska till fler personer läggs även de till i listan. Dra och släpp mottagare till Recipients och klicka på OK så går brevet iväg.

Dekryptera e-brev via urklipp

När du får ett meddelande från någon som har din publika nyckel använder du din privata nyckel för att dekryptera det.

Du behöver inte hålla reda på nycklarnas typ, det sköter PGP åt dig. Öppna meddelandet och markera hela den krypterade texten, som ser ut som rappakalja. Klicka på ikonen för dekryptering och ange lösenordet. Sedan ser det ut som om det inte händer ett dugg.

PGP kan inte skriva in texten i ett statiskt e-brev. Den dekrypterade texten finns i stället i dina urklipp och du kan klistra in den på lämpligt ställe.

Om ikonen inte fungerar, vilket hände oss ett flertal gånger, kan du göra på ett annat sätt. Markera den krypterade texten, högerklicka och välj att kopiera. Klicka på PGP-ikonen i aktivitetsfältet och välj Decrypt & Verify Clipboard.

Ange lösenord i rutan som visas. Nu öppnas ett fönster där du kan se meddelandets dekrypterade text. Klicka på Copy to Clipboard. Välj Redigera och Redigera meddelande i Outlook. Högerklicka i texten och välj att klistra in. Nu kan du spara meddelandet med den dekrypterade texten.

Svårare än så här är det faktiskt inte. Vi kan varmt rekommendera dig att studera innehållet på PGPs webbplats för mer information.