Hvad er KRYPTERING ?

Kryptering er en matematisk teknik. Hvis et dokument er blevet krypteret, vil dokumentet fremstå som en uforståelig blanding af bogstaver og tegn – og uvedkommende kan således ikke læses indholdet.

Kryptering kendes helt tilbage fra oldtiden, hvor kodningen blot kunne bestå i at forskyde alle tegn i en besked et bestemt antal bogstaver i alfabetet. For eksempel kunne ABC erstattes med BCD - hvor der er flyttet en plads i alfabetet. Dette kaldes i øvrigt for Cæsar-kode, da man mener, metoden har været brugt i det gamle Rom.

Hvorfor bruge kryptering ?

Kryptering bruges til at sikre, at fortrolige dokumenter og informationer som for eksempel kodeord og kontonumre ikke kan løses eller misbruges af andre. Du kan bruge kryptering til at beskytte et bestemt dokument - eller måske hele din harddisk - mod at blive læst, i tilfælde af, at andre får adgang til din computer. Kryptering kan også bruges, når du vil være sikker på, at et fortroligt brev eller en privat mail kun kan læses af den tilsigtede modtager.

Kryptering anvendes i netbanker og e-butikker for at beskytte kontonumre, kreditkortoplysninger og andre fortrolige oplysninger. Desuden bruges kryptering på mange websites, hvor du skal bruge kodeord.

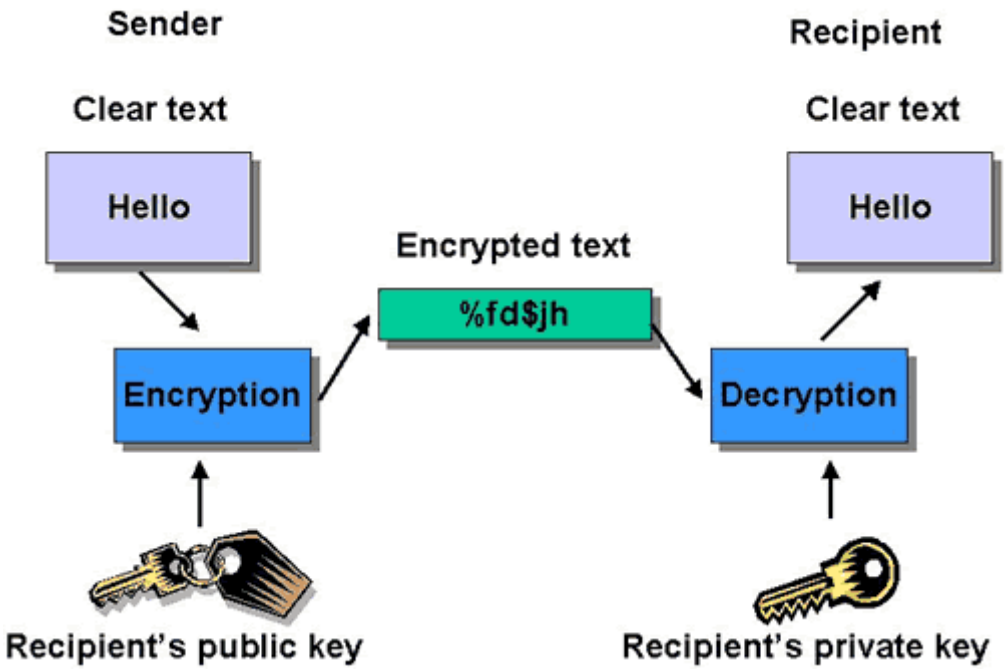
Metoder

Der findes to forskellige krypteringsmetoder: Symmetrisk og asymmetrisk (offentlig-nøgle) kryptering.

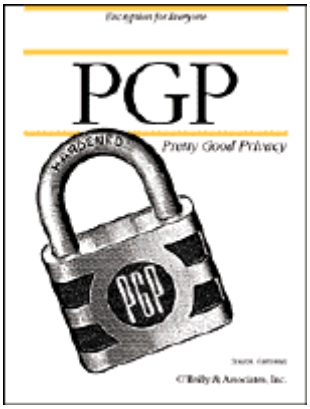
En **symmetrisk** krypteringsmetode bruger kun en enkelt nøgle, som både bruges til at kryptere og dekryptere information. Denne metode kan med fordel bruges, når du skal kryptere information, som kun du selv må kunne løse. For eksempel når en hel harddisk skal krypteres.

Asymmestrisk kryptering = ”offentlig-nøgle kryptering” (engelsk: **Public Key**) benytter to forskellige nøgler: En privat nøgle og en offentlig nøgle, der matematisk set hører sammen. Den ene nøgle bruges til kryptering og den anden nøgle til dekryptering. Denne metode bruges som regel, når to parter skal udveksle fortrolige dokumenter. Hver part har sin egen, private nøgle, og begge parter har hinandens offentlige nøgler.

Når du skal sende et fortroligt dokument til en anden person, skal du kryptere dokumentet med den anden persons offentlige nøgle. Han kan så dekryptere og åbne dokumentet ved a bruge sin egen private nøgle. Det lyder indviklet, men i praksis er det heldigvis nemmere, når du bruger et krypteringsværktøj. Du skal nemlig kun fortælle, om du vil kryptere eller dekryptere et dokument – så klarer programmet resten.



Sammenbindingen af en persons identitet og offentlige nøgle kan ske ved brug af et digitalt **certifikat**. Certifikater beskrives i et senere afsnit.



Kryptering af mail

Hvis du skal kryptere en mail, kan du for eksempel bruge mail-programmerne Outlook eller Notes, som begge kan integreres med krypteringsværktøjer. Hvis du ikke har et mail-program med indbygget mulighed for kryptering, kan du for eksempel bruge krypteringsværktøjet **Pretty Good Privacy** (PGP). Du skal dog være opmærksom på, at modtageren af dine krypterede mails skal bruge det samme krypteringsværktøj.

Hvad er digital signatur ?

En digital signatur er, ligesom en underskrift på fysiske breve, en mulighed for at **verificere**, hvem der er ophavsmand til brevet. Forskellen mellem den fysiske underskrift og den digitale signatur er, at man i stedet for underskriften på et fysisk dokument bruger kryptografiske metoder, der indeholder matematik.

Den digitale signatur er ekstra information, som er dannet ud fra selve dokumentet, der skal underskrives. Denne ekstra kode bliver vedhæftet dokumentet inden det sendes. Den digitale signatur dannes ved hjælp af kryptering og en privat nøgle. Kun den, som har den private nøgle, kan sende beskeder med den rigtige signatur.

Modtageren af dokumentet bruger afsenderens offentlige nøgle til at verificere, at det er den korrekte afsender. Sammenbindingen af afsenders identitet og offentlige nøgle kan ske ved brug af et digitalt certifikat.

Hvis du benytter en digital signatur, kan du samtidig kontrollere, om det underskrevne dokument er blevet ændret, efter det blev underskrevet. Det svarer til, at man i gamle dage påførte en konvolut et laksegl, så det kunne ses, om konvolutten var blevet åbnet.

Du skal dog være opmærksom på et vigtigt forhold: Bare fordi en digital signatur giver sikkerhed for, at indholdet kommer fra den rigtige afsender og ikke er ændret, er der ingen garanti for, at indholdet er korrekt og absolut uskadeligt.

Hvorfor bruge digital signatur ?

Brugen af mail og andre former for udveksling af data via internettet er kraftigt voksende. Derfor er det i mange situationer rart at være sikker på, at den person, du kommunikerer med digitalt, også er den han/hun udgiver sig for at være. Det vil også være rart at kunne se, om der er ændret i teksten undervejs.

Det er lettere at forfalske afsender og indhold i en mail end det er at forfalske et almindeligt brev eller underskrift. Derfor kan du bruge en krypteringsmetode til at sikre, at mailen kommer fra den afsender, som er angivet. Samtidig kan du sikre dig, at indholdet af dokumentet ikke er ændret. Når kryptering bruges på denne måde, kaldes det generelt for en digital signatur.

En digital signatur kan altså bruges til at bekræfte identiteten på afsender af en mail, og til at vise om indholdet af et dokument er blevet ændret, efter det blev sendt til dig.

Alle danskerne over 15 år kan gratis bestille en digital signatur hos TDC, som er den officielle udsteder af den danske digitale signatur. Læs nærmere på:

http://privat.tdc.dk/digital

Efter et par dage modtager man en hemmelig pinkode via posten (lige som til ens Dankort blot med flere tal i).

Visse banker har dog oprettet deres egen digitale signatur f.eks. til brug i deres egen netbank.

Hvad er certifikater ?

Et certifikat er et elektronisk dokument, som sammenbinder oplysninger om en persons eller et firmas identitet og samme persons eller firmas offentlige nøgle.

Indholdet i et certifikat skal entydigt identificere ejeren af certifikatet, og derfor indeholder et certifikat mange oplysninger. Et certifikat indeholder blandt andet navn og den offentlige nøgle, der gør, at du som bruger kan verificere den digitale signatur.

Nogle af oplysningerne kan virke meget indviklede, men der er nogle ret simple ting, som du bør kontrollere for at sikre, at certifikatet er gyldigt.

Du bør for eksempel kontrollere, om certifikatet er udstedt af en anerkendt organisation, som du har tillid til, og om certifikatet blev brugt, mens det var gyldigt. Desuden bør du verificere udstederens digitale signatur, så du er sikker på, at certifikatet ikke er forfalsket.

Et certifikat udstedes af en troværdig instans, som i Danmark kaldes for et nøglecenter (engelsk: certificate authority). KMD og TDC er eksempler på danske nøglecentre, mens VeriSign er et amerikansk nøglecenter.

Certifikater og digitale signaturer bruges også i forbindelse med software. For eksempel kan et firma underskrive en softwareopdatering med firmaets private nøgle. Når du så vil downloade en opdatering til det pågældende program, kan du kontrollere, om opdateringen virkelig stammer fra firmaet. Samtidig kan du kontrollere, at opdateringen ikke er ændret af andre, efter at det pågældende firma har udgivet softwareopdateringen.

Hvorfor bruge certifikater ?

Når du modtager et dokument, som er underskrevet digitalt, skal du have en metode til at kunne verificere, at afsenderen er den, han/hun udgiver sig for at være. Det vil sige, at du skal kunne verificere, at signaturen er ægte. For at kunne bekræfte, at en signatur er ægte, skal du bruge underskriverens offentlige nøgle. Underskriveren har jo brugt sin private nøgle til at danne den digitale signatur med.

Underskriverens offentlige nøgle kan du typisk verificere ved hjælp af et certifikat, der giver sikkerhed for at afsenderen er den, som vedkommende giver sig ud for at være. Når du verificerer en nøgle ved hjælp af et certifikat, stoler du på, at certifikat-udstederen har verificeret identiteten af afsenderen på det tidspunkt, hvor certifikatet er udstedt.

Betaling og netbanker

Når du betaler for varer i e-butikker eller regninger i din netbank, foregår det via en sikker forbindelse. Det betyder, at forbindelsen mellem din computer og butikken eller netbanken er krypteret. Krypteringen sikrer, at uvedkommende ikke kan løse dit kontonummer, kodeord og andre fortrolige oplysninger.

Når forbindelsen er krypteret, vil du nogle gange få en meddelelse (i et pop-up vindue) om, at forbindelsen er sikker. Men du kan også selv kontrollere, om den er krypteret ved at kigge på adressefeltet i din browser. Normalt starter en adresse med "http", men hvis forbindelsen er sikker, vil der stå "https" i stedet for. ("S" står for secure).

De fleste browsere bruger også et lille billede af en hængelås til at vise, om din forbindelse er krypteret. Hvis du for eksempel bruger Netscape, er der et lille billede af en lukket hængelås nederst i browser-vinduet. Hvis din forbindelse ikke er krypteret, er der et billede af en åben hængelås.

Bruger du Internet Explorer, er der et billede af en lukket hængelås nederst til højre i browser- vinduet, hvis forbindelsen er krypteret. Hvis forbindelsen ikke er krypteret, er der ikke noget billede i Internet Explorer.

De fleste websites bruger SSL (Secure Socket Layer), der er den mest benyttede sikkerhedsstandard i forbindelse med e-handel. SSL er indbygget i de fleste moderne browsere, og der kræves ikke installation af ekstra software for at benytte SSL. Metoden bruges som regel til at kryptere alle informationer mellem kunde, forretning og pengeinstitut.

Læs mere om kryptering og digital signatur på:

http://privat.tdc.dk/digital/