TEKNOLOGI-RÅDET

En dansk krypto-politik

Hvordan skal digitale informationer hemmeligholdes?

Projektledelse i Teknologirådets sekretariat:
Steffen Stripp (red.) og Lars Klüver

Teknologirådets rapporter 1995/5

ISBN: 87-890098-98-6
ISSN: 1395-7392

Indholdsfortegnelse

Forord

Denne rapport er resultatet af et projekt, gennemført i Teknologinævnet i perioden november 1994 til juli 1995, og udsendes af Teknologirådet, som fra 1. august 1995 har afløst Teknologinævnet.

Projektet er gennemført af konsulent Steffen Stripp. En række personer har skrevet bidrag som belyser baggrund og synsvinkler for en dansk politik for hvordan digitale informationer skal hemmeligholdes, og Teknologirådet vil gerne siger tak for denne indsats. Et rapport-udkast blev behandlet på et seminar den 29. maj med deltagelse af Joi Bay, Kriminalistisk Institut Københavns Universitet; Peter Blume, Retsvidenskabelig Institut B Københavns Universitet; Lisbeth Buhl, Telestyrelsen; Emil Bundesen, Forskningsministeriet; Lars Klüver, Teknologirådet; Peter Landrock, Cryptomatic; Søren Olesen, Institut for Datasikkerhed; Robert Hartmann Petersen, Registertilsynet; Birgitte Kofod Olesen, Det Danske Center for Menneskerettigheder. Teknologirådet vil også sige tak til deltagerne i seminaret for spændende og konstruktive bidrag.

Det skal understreges, at deltagerne i seminaret og bidragyderne ikke har noget ansvar i.f.t. dele af rapporten, som de ikke selv har skrevet.

Fastlæggelse af en dansk politik om kryptering er en vigtig brik i udformningen af info-samfundet. Det er Teknologirådets håb, at denne rapport vil igangsætte en debat herom og at den kan danne grundlag for udformning af en sådan politik.

Teknologirådet august 1995

Resume

Denne udredning fra Teknologirådet har som formål

* at skabe politisk og offentlig opmærksomhed om hvordan privatlivets fred skal sikres i datakommunikationen

* at give et alsidigt grundlag for debat om udformning af en dansk politik i forhold til EU-initiativer og evt. dansk lovgivning.

Problemstilling

Informationer digitaliseres i disse år og det forventes, at virksomheder og privatpersoner i fremtiden i vid udstrækning vil bruge computere til at behandle dokumenter og kommunikere med edb-systemer og andre mennesker. En forudsætning for denne udvikling er bla. at borgere og virksomheden kan sikres fortrolighed i kommunikation og dataopbevaring.

Det er teknisk muligt at forvanske de digitale data før transmissionen af e-posten eller telefonsamtalen så den ikke kan høres eller læses af andre end den modtager, som den er beregnet for. Tilsvarende kan data, der

opbevares i elektroniske postkasser eller i private datalagre, forvanskes og kun læses ejeren selv. Dermed kan man sikre fortrolighed i kommunikation og private papirer.

Hvis alle kan gøre de digitale data ulæselig har politi og efterretningstjenester mistet muligheden for at lytte og læse med og dermed mistet et middel i kriminalitets-efterforskningen. Det er det centrale problem - eller den gordiske knude - som en krypto-politik skal tage stilling til.

Der findes i dag ingen dansk krypto-politik for hvordan digitale information skal hemmeligholdes, men der er af såvel tekniske som politisk grunde behov for at formulere en politik for området.

I rapporten fokuseres kun på anvendelse af kryptering til at opnå fortrolighed, som er ét af flere sikkerhedsaspekter. I åbne systemer er anvendelse af kryptering en nødvendig del af en løsning på fortroligheden. Men selve krypteringen er kun en del af løsningen på hvordan den elektroniske kommunikation skal hemmeligholdes.

Et samlet krypto-system kan beskrives med tre elementer. For det første et **teknikelement**: krypterings-algoritmen og nøgle(er), kommunikations-protokoller og om det er en hardware eller softwareløsning. Dernæst et **systemelement**: er det en generel standardløsning eller individuelle løsninger, indbygges løsningen i det udstyr der sælges, hvordan opbevares og udveksles nøgler, indgår et nøglecenter (betroet trejdepart) og har nøglecenteret adgang til nøglen. Endelig findes et **retlig element**: Er anvendelse af kryptering reguleret i en lovgivning, findes der regler for nøglecenter, hvilke regler findes i retspleje- og straffelov.

Baggrund og synsvinkler

Problemstillingen belyses i en række bidrag.

Arne V. Gram og Ole Hasselgaard gennemgår reglerne i straffeloven, som beskytter privatlivets fred ved brev- og anden meddelelseshemmelighed. Dernæst behandles retsplejelovens regler for politiets mulighed for at bryde meddelelseshemmeligheden. Det konstateres, at der ikke i dansk ret er lovregler, som forbyder borgerne at anvende kryptering, og dermed kan en hver form for kryptering frit anvendes. Endelig behandles bevisspørgsmål. Det vil af tekniske årsager ikke vil være muligt for anklagemyndigheden at anvende krypterede informationer som brugbart bevis.

Peter Landrock giver en introduktion til kryptografi. Han gennemgår konventionelle (symmetriske) systemer, Public key (asymmetriske) systemer og envejsfunktioner, og endelig beskrives anvendelse af escrow-værdier. Kryptologi er det sidste tiår blevet et vigtigt fag ved de højere læreanstalter. Det er et område med det ene ben i matematikken og det andet i datalogien. Denne anvendte videnskab bygger på talteori og kompleksitetsteori, som århundreders forskning har vist er svære. Man kan således sige at hele det matematiske samfund garanterer for, at de kryptografiske systemer er bygget så sikre som muligt.

Leif Nielsen beskriver sikkerheden i telenettet. For aflytning gælder generelt, at jo tættere dette sker på afsender eller modtager, jo større er risikoen for uautoriseret aflytning. Accesnettet (dvs. nettet ud til den enkelte kunde) anses for vanskeligt at beskytte 100% mod fysiske indbrud, mens aflytning af det overordnede telenet vurderes at være yderst vanskeligt.

Steffen Stripp referer i et bidrag om faglige standarder en række kritikpunkter mod det krypto-system, som

Clinton-administrationen har foreslået. Han understreger det almindeligt accepterede faglige krav, at krypto-systemer bygger på teknikker som er offentlige og frit kan analyses af eksperter og videnskabelige miljøer.

Birgitte Kofod Olsen beskriver omfanget af den beskyttelse, som er fastlagt i den Europæiske Menneskerettighedskonvention. Det antages, at et generelt forbud mod alle eller bestemte krypterings-teknikker vil være i strid med konventionens artikel 8 og 10. Videre vurderes en ordning, hvorefter krypterings-systemernes underliggende algoritme kontrolleres af staten, som problematisk fra en menneskeretlig synsvinkel.

Henning Thiesen konstaterer, at det ud fra en politimæssig vurdering må anses for absolut påkrævet, at politiet fortsat kan aflytte telekommunikationen. Aflytning af telekommunikation er et meget betydningsfuldt - og ofte et helt afgørende - redskab ved efterforskning af alvorlig kriminalitet, herunder bla. narkotikakriminalitet. Det fremhæves, at der ikke er tale om at tillægge politiet mulighed for at gennemføre nye former for strafprocessuelle tvangsindgreb, men alene om at bevare eksisterende muligheder.

Steffen Stripp belyser erhvervsinteresser, idet han konstaterer, at dansk industri tilsyneladende ikke har klargjort sine positioner. I bidraget refereres en udtalelse fra tre internationale industriorganisationer til G-7 landenes møde om informationssamfundet i februar 1995, som anbefaler at man enes om offentlige kryptografiske teknikker, som bygger på internationale standarder.

En dansk krypto-politik

I et afsluttende bidrag sammenfatter *Steffen Stripp* det grundlag for en dansk krypto-politik, som er fremlagt i de foregående afsnit, i en række valgmuligheder. Selv om en krypto-politik handler om en informations- og kommunikationsteknologi er udgangspunktet ikke forskellige tekniske løsninger, men de krav der kan stilles til den tekniske løsning. Der fremlægges følgende valg:

Er der overhovedet et problem?

1 Intet behov for kryptering

Den simple løsning

2 Forbud mod kryptering med mindre der er givet tilladelse

3 Intet behov for myndighedsinitiativ

Infrastruktur

4 Statslig initiativ til et tilbud om fortrolighed ved kryptering

Kontrol med kommunikationen

5 Kontrol med anvendt krypto-system

Hvem skal have nøglen?

6 Private nøgle udelukkende hos ejeren

7 Nøglen opbevares hos nøglecenter med myndighedsadgang

8 Nøglen opbevares hos nøglecenter, men kun ejeren har adgang

Retlige elementer

9 Ændring af retsplejen

10 Offentlig eller privat nøglecenter

Teknisk element

11 Kendt og analyseret teknisk løsning

Dansk - Europæisk - International løsning

12 Krypto-systemet skal være europæisk og helst internationalt

13 Etablering af dansk krypto-system.

I en opsamling på disse valgmuligheder konstateres, at det ikke er muligt at indføre et forbud mod kryptering. Det vil være hensigtsmæssigt at skelne mellem telefoni og datakommunikation og datalagring.

For *telefonien* vil et krypto-system, hvor myndighederne har adgang til nøglen efter en retskendelse kunne accepteres.

For *datakommunikation og -lagre* bør der ikke etableres et krypto-system, som har indbygget myndighedsadgang til nøglerne og dermed mulighed for aflytning. Tværtimod bør et krypto-system opbygges så det giver maksimal troværdighed, og det vil sige med fuld kontrol over fortroligheden for den enkelte.

Summary

The objectives of this report from the Danish Board of Technology are:-

* to stimulate political and public awareness as to how privacy in the communication of electronic data can be ensured

* to present a comprehensive basis for the debate on drafting Danish policy in relation to EU initiatives and possible Danish legislation

The problematic

In these years, data is being digitalized and it is expected that companies and individuals will in the future, to a large extent, use computers to handle documents and to communicate with electronically processed data systems and with other people. A precondition for this is, inter alia, that citizens and companies can be ensured confidentiality in the communication and storage of data.

It is technically possible to encypt digital data prior to transmission by e-mail or the telephone so that it cannot be heard or read by anyone other than the recipient for whom it is intended. Similarly, data stored in electronic post boxes or in private data bases can be disguised so that they can only be read by the owner. In this way, the confidentiality of communication and private papers can be ensured. Were everyone to make digital data undreadable, then the police and the criminal investigation authorities have lost the chance to eavesdrop and hence have lost a means of criminal investigation. This is the crucial problem, the Gordic knot, that an encryption policy must address.

There is, currently, no Danish encryption policy but, for both tehnical and political reasons, there is a clear need to formulate a policy in this field.

The report focusses only on the use of encrypting to achieve confidentiality; just one of several security aspects. In open systems, the use of encrypting is a necessary part of the solution to the problem of confidentiality. But even encrypting is only part of the solution to the problem of how electronic communication is to be kept secret.

A complete encryption system consists of three elements. First, a **technical element**: the encrypting algorithm and key(s), communication protocols and whether it is a hardware or software solution. Secondly, a **system element**: is this a general standard solution or an individual solution? Is the solution part of the equipment that is sold? How are the keys to be stored and exchanged? Is there a key centre? (a thrusted third party) and does the key centre have access to the key? Thirdly there is a **legal element**: Is the use of the encryption controlled by legislation ? Are there rules governing the key centre? What rules are found in civil and criminal law?

Background and viewpoints

A number of contributions examine the problematic.

Arne V. Gram and Ole Hasselgaard discuss the regulations in criminal law which protect the privacy of correspondence and other confidential communication. Thereafter the law governing the right of the police to violate communication confidentiality. They show that, under Danish law, there are no regulations prohibiting citizens from using encryption and hence any kind of encrypting can be freely used. Finally, the question of evidence is discussed. For technical reasons, it is not possible for the prosecution to use encrypted information as legal evidence.

Peter Landrock gives an introduction to cryptography. He examines conventional (symmetrical) systems, Public Key (assymetrical) systems and one-way functions and, finally, he describes the use of escrow values. During the last decade, cryptography has become an important subject in universities: a field with one foot in mathematics and the other in computer science. The applied science uses number theory and complexity theory which a century of research has proven to be a difficult field. One can say that the whole mathematics community is a guarantor that cryptographical systems are as safe as possible.

Leif Nielsen describes security in the telephone net. For eavesdropping it is generally the case that the closer this occurs to the sender or receiver the greater the risk of unauthorized eavesdropping. It is considered difficult to protect the access net (ie. the net to each individual customer) against physical break-in but eavesdropping the overall telephone system is considered extremely difficult.

Steffen Stripp examines professional standards and a number of critiques of the encryption system which the Clinton administration has proposed. His contribution emphasizes the generally accepted professional norm that encryption be based on techniques that are publically available and can be freely analyzed by experts and scientific communities.

Birgitte Kofod Olsen describes the degree of protection as laid down in the European Human Rights Convention. It is assumed that a general prohibition against all or certain types of encrypting techniques will be in conflict with articles 8 and 10 of the convention. Furthermore, from a human rights perspective, a procedure whereby the underlying algorithmic systems are controlled by the state is problematic.

Henning Thiesen demonstrates that from the point of view of the police it is considered mandatory that the

police can continue to eavesdrop telecommunications. Eavesdropping telecommunications is an extremely important - and frequently quite decisive - tool in the investigation of serious crime, including drug-related crime. It is stressed that it is not the intention to increase police coercive powers but merely to retain existing powers.

Steffen Stripp examines the interests of the private sector. Apparently, Danish industry has not clarified it's position on the issue. The paper describes statements by three international industrial associations to the meeting of the G-7 countries in February, 1995 recommending that agreement is reached on publically available cryptographical techniques based on international standards.

A Danish crypto-policy

A final contribution by *Steffen Stripp* summarizes the basis for a Danish encryption policy -as presented in in the previous sections - into a number of options. Even though a crypo-policy involves information and communication technology, the starting point for such a policy is not different technical solutions but the demands to be put to the technical solutions. The following options are proposed:-

Is there a problem at all?

1. There is no need for encrypting

The simple solution

2. Prohibition of encrypting without special permission

3. No need for an initiative from the authorities

Infrastructure

4. An initiative by government in the form of a proposal governing the confidentiality of encryption.

Control of communication

5. Control of the encryption system in use

Who shall have the key?

6. Private keys to be exclusively the property of the owner

7. Keys to be kept at a key centre to which authorities have access

8. Keys to be kept at a key centre but only the owner has access

Legal Aspects

9. Changes in legislation

10. Public or private key centres

Technical aspects

11. Known and analysed technical solutions

Danish - European - International solutions

12. Crypto-systems must be European-wide and, preferably, international

13. The establishment of Danish encryption systems

It is noted in a final recommendation, that it is not possible to introduce a prohibition against encryption. It will be useful to distinguish between telefoni and data communication and storage.

> As to *telefoni*, a crypto-system in which authorities have access to the key on a legal warrant could be accepted.
>
> As to *data communication and files*, a crypto-system in which the authorities have access to the keys and hence the chance of tappping should not be established. To the contrary, a crypto- system should be established so that it gives maximal credibility and this means full control over confidentiality for the individual.

Indledning

Af Steffen Stripp

Informationer digitaliseres i disse år og det forventes at virksomheder og privatpersoner i fremtiden i vid udstrækning vil bruge computere til at behandle dokumenter og kommunikere med edb-systemer og andre mennesker.

Breve vil blive sendt som elektronisk post over telefonlinjer og datalinjer. Den enkelte vil ordne indkøb, bankforretninger osv. via telefon og pc'er. Meddelelser, aftaler og andre dokumenter vil blive sendt elektronisk. Helbredsoplysninger vil blive sendt fra lægen til apotek, speciallæger og sygehuse; og patienten vil få adgang til sin elektroniske patientjournal. Den offentlige sektor vil udbyde selvbetjening, hvor man kan give besked til offentlige myndigheder om private forhold og få overført attester, skatteoplysninger osv. Den elektroniske post vil blive opbevaret elektronisk dels i elektroniske postkasser hos teleoperatøren indtil modtageren har tid til at kigge på den; dels i modtagerens eget edb-system på harddisken eller på disketter til man får brug for oplysningerne igen.

Med udbredelse af pc'er i arbejdslivet og i hjemmene vil stadig flere oplysninger, private breve og dokumenter findes i elektronisk form. Den enkelte vil i stedet for brevordnere på hylderne have disketter med sine private "papirer".

På sigt vil også telefonsamtaler ske over digitalnet. Det er muligt at få en ISDN forbindelse, hvor telefonsamtalen vil være digitaliseret fra apparat til apparat. Da teleselskabet skal lægge en ny forbindelse ud til abonnenten og denne skal have ny telefonapparat er der vanskeligt at forudse hvor hurtigt denne ændring vil slå bredere igennem.

Det er teknisk muligt at forvanske de digitale data før transmissionen af e-posten eller telefonsamtalen så de ikke kan høres eller læses af andre end den modtager, som den er beregnet for. Tilsvarende kan data der opbevares i elektroniske postkasser eller i private datalagre forvanskes og kun læses af ejeren selv. Dermed kan man sikre fortrolighed i kommunikation og private papirer, som er rettigheder, der hører til privatlivets fred og bla. kendes som brevhemmelighed.

Hvis alle kan gøre de digitale data ulæselig har politi og efterretningstjenester mistet muligheden for at lytte og læse med og dermed mistet et middel i kriminalitets-efterforskningen. Det er det centrale problem som en krypto-politik skal tage stilling til. På den anden side vil skiftet til elektronisk kommunikation forrykke mulighederne for at foretage indgreb i meddelelseshemmeligheden. Det er langt lettere og mindre mandsskabskrævende at aflytte en digitaliseret kommunikation. Elektronisk post vil ofte findes i postkasser man kan skaffe sig adgang til uden ejerens viden. Man kan sige at privatlivets fred og brevhemmeligheden

bliver svækket med udbredelse af den elektroniske kommunikation, men den kan styrkes, endda bedre end i dag, med anvendelse af et generelt system til hemmeligholdelse af kommunikationen. Samtidig betyder udbredelse af elektronisk kommunikation uden samfundsmæssige tiltag til hemmeligholdelse, at samfundet som helhed bliver mere sårbart og kriminelles muligheder overfor borgere og virksomheder kan blive meget alvorlig

Den teknik der anvendes er kryptering, som forvansker dataene på en kontrolleret måde, så den med kendskab til en nøgle kan genskabes i den oprindelige læselige udgave. Umiddelbart handler krypto-politikken om hvilken krypterings-teknik, der skal vælges. Men spørgsmålet er bredere og handler om hvem der skal have adgang til nøglen, der kan gøre den ulæselige tekst læselig igen, hvem skal have kontrol over systemet, hvordan skal den retlige regulering være.

Spørgsmålet har været livligt debatteret i USA siden 1993, hvor Clinton administrationen, som led i National Information Infrastructure (NII) programmet, forslog en ny udviklet løsning. [1] Den har forskellige navne: Clipper, Capstone og senest Escrowed Key Encryption. USA's vicepresident Al Gore forklarer forslaget med disse ord: "Our policy is designed to provide better encryption to individuals and businesses while ensuring that the needs of law enforcement and national security are met." [2]

I EuropaKommissionens "Green Paper" om informations-systemers sikkerhed behandles emnet "To reconcile the human right to privacy and the obligations of law enforcement to protect public order" uden man fremkommer med konkrete løsningsforslag [3]. I et forslag fra EU-Kommissionen om etablering af "Europe-wide Thrust Services for public information services (ETS)" [4], foreslås bla.

"to provide for the establishment og Europe-wide confidentiality services for non-classified information. These could indlude the following categories:

- *minimum IS assurance* to be maintained by all service providers (level of present mail and telephony under national privacy legislation)

- *enhanced IS assurance* for private and professional use (level of registered mail or courier delivery as needed for normal business transactions such as ordering and billing)

- *professional IS assurance* as needed for recognised categories of commercially (or otherwise) sensitive information".

Der er i dag ikke nogen enighed mellem landene i EU om en fælles krypto-politik. I Frankrig findes der et forbud mod at anvende kryptering. I Tyskland skal politiet kunne lytte med på kommunikation i offentlige netværk. I Holland har man behandlet et forslag om forbud mod kryptering, men det faldt væk. I Belgien overvejes et forslag om forbud. Den svenske holdning er, at der ikke kan være tale om et forbud. Fra engelsk side vil man ikke hindre kryptering, men ønsker at undgå eksport af krypterings-teknologi[5].

I Rusland har præsident Boris Jeltsin udstedt et dekret, som forbyder udvikling, import, salg og brug af krypterings-teknikker med mindre der er indhentet licens fra et regeringsbureau.[6]

Der findes i dag ingen dansk krypto-politik, men der er af såvel tekniske som politisk grunde behov for at formulere en politik for området. Tidligere Justitsminister Erling Olsen [7] udtalte, som kommentar til Tele Danmarks opfindelse af en RSA-chip (se afsnit 8), at han ikke ønsker "..at lovgive på området. Han mener ikke, at masseproduktion af RSA-chippen er noget problem: "Vi bør have som princip, at aflytning kun finder sted i sjældne tilfælde", siger han. Ifølge justitsministeren er det de internationale forbrydersyndikater, der er problemet, fordi de er allerede i stand til at kryptere deres informationer: "Derfor er man i det

internationale politisamarbejde ved at bryde hjernerne for at finde ud af, hvordan man kan udvikle et antivåben, der kan bryde krypteringskoderne", siger Erling Olsen". I justitsministeriet har man nedsat en arbejdsgruppe, som ser på dette krypterings-problem.

Fortrolighed - et sikkerhedsaspekt

Edb-sikkerhed etablerer generelt sikkerhedsforanstaltninger, som skal sikre:

Integritet	At edb-systemet fungerer uden fejl og at data er korrekte.
Tilgængelighed	At edb-systemet til stadighed kan anvendes og der er adgang til data.
Fortrolighed	At adgang til edb-systemer og data kan beskyttes så uvedkommende ikke kan benytte systemet eller få adgang til dataene.

I forbindelse med udveksling af data kan integritet og fortrolighed opdeles i fire aspekter:

Autenticitet:	Sikkerhed for, hvem der har afsendt og modtaget dataene.
Integritet:	Sikkerhed for, at data ikke er ændret eller tabt under datatransmissionen.
Uafviselighed:	Sikkerhed for at hverken afsender eller modtager kan afvise at have sendt henholdsvis modtaget dataene (dokumentet/brevet).
Fortrolighed:	Sikkerhed for at uvedkommende ikke kan få adgang til at læse dataene under transmissionen.

I denne rapport fokuseres alene på fortrolighed i relation til data. I mange tilfælde vil en sikkerhedsforanstaltning i praksis rette sig mod flere af disse sikkerhedsaspekter, men det vil vi ikke tage op i denne rapport.

Behovet for fortrolighed er en følge af en række trusler, der kan betyde brud på fortroligheden, dvs. at data læses af uvedkommende. Blandt disse trusler kan nævnes

- Aflytning. Datatransmissionen kan aflyttes f.eks. ved at koble sig på telefonlinjen eller lokalnettet. Det kan faktisk gøres med simpelt udstyr og uden større vanskeligheder. Med mere avanceret udstyr kan man også aflytte kommunikation mellem edb-systemets forskellige komponenter.

- Uautoriseret adgang. Systemfolk hos netoperatør eller i et lokalnet kan få adgang til den elektroniske postkasse og læse breve og andre dokumenter. Hackere kan skaffe sig adgang til postkasser. Personer kan skaffe sig adgang til pc'ens datalager og læse dokumenterne. Er pc'en koblet til et lokalnet er der yderligere risici for uautoriseret adgang.

- Fejl. Ved teknisk fejl kan data sendes til en forkert adresse eller på anden måde gøres tilgængelig for uvedkommende.

Sikkerhedsforanstaltninger som generelt skal sikre fortrolighed er f.eks. fysisk sikring i form af adgangskontrol og opbevaring af data i aflåste skabe, adgangskontrol til edb-systemet med password og

kryptering af data. Sikkerhedsforanstaltninger ved datatransmission kan omfatte tavshedspligtregler for medarbejdere hos netoperatører og kryptering.

I dag sker den meste kommunikation uden sikkerhedsforanstalninger, som sikrer fortroligheden. Dog er der i systemer, som behandler betalingstransaktioner, f.eks. i Dankortsystemet mellem terminaler og PBS og i bankernes internationale system S.W.I.F.T., indbygget en hemmeligholdelse af datatransmissionens indhold.

Situationen i dag kan sammenlignes med at alle dokumenter blev sendt på postkort. Selvom det måske ikke bliver læst af uvedkommende i postvæsnet eller når det er afleveret, så er der næppe nogen som vil sende vigtige aftaler eller meget personlige forhold på et postkort.

Uanset risikoens størrelse er det rimelig at anlægge en "forsikrings-betragtning" som betyder, at man tager visse tiltag for at være på den sikre side. Man låser døren til sit hus selv om risikoen for at tyve opdager at døren er ulåst og går ind er ringe, men det bidrager til, at ens generelle oplevelse af tryghed er større. Tilsvarende kan man se kryptering af ens digitale informationer som en tryghed mod at uvedkommende læser den - bare tanken om risikoen er ubehagelig.

Hvis man ønsker at hemmeligholde sin elektroniske kommunikation og datalagre er det muligt. Der findes produkter på markedet, som kan kryptere indholdet så det ikke kan læses af andre end den som har nøglen. Man kan også hente et edb-program på "Internet". Dette program, "Pretty Good Privacy", anvendes af privatpersoner, men også af menneskerettighedsgrupper i f.eks. El Salvador og andre lande, hvor statsmagten forfølger sådanne grupper.

Krypto-system

Anvendelse af kryptering er en nødvendig del af en løsning på fortroligheden i kommunikation i åbne systemer. Men selve krypteringen er kun en del af løsningen på hvordan den elektroniske kommunikation skal hemmeligholdes.

Et samlet krypto-system kan beskrives med tre elementer. For det første et **teknikelement**: krypterings algoritmen og nøgle(er), kommunikations protokoller og om det er en hardware eller softwareløsning. Dernæst et **systemelement**: er det en generel standard løsning eller individuelle løsninger, indbygges løsningen i det udstyr der sælges, hvordan opbevares og udveksles nøgler, indgår et nøglecenter (betroet trejdepart) og har det adgang til nøglen. Endelig findes et **retlig element**: Er anvendelse af kryptering reguleret i en lovgivning, findes der regler for nøglecenter, hvilke regler findes i retspleje- og straffelov.

Svar på spørgsmålet, hvordan skal elektronisk kommunikation - og bredere elektronisk lagrede informationer - hemmeligholdes handler om det samlede krypto-system. Der er en tendens til at diskussionen koncentreres om valg af algoritme, men det må anses for en meget uheldig indsnævring af diskussionen. I stedet må den bredes ud og handle om hvilke krav samfundet vil stille til et sådant system. Teknisk kan der laves løsninger, som opfylder de krav som stilles. Når vi ved hvordan forskellige hensyn skal afbalanceres kan der opbygges et system og vælges krypteringsalgoritme som opfylder disse krav.

Escrowed Encryption Standard (EES)

EES kan ses som eksempel på en krypto-politik med dens løsning på en række krav, som den amerikanske regering har stillet.

En udbredt anvendelse af kryptering skal ske på en måde så hensyn til national sikkerhed og politiets efterforskning ikke forringes. Muligheder for en effektiv kommunikationsefterretningsvirksomhed skal

sikres med den øgede elektroniske kommunikation.

Regeringens skal så vidt muligt have kontrol med udbredelsen af krypteringsteknikker. Man har ikke har villet gentage "fejlen" med DES, som blev offentliggjort og dermed spredte ikke bare den konkrete teknik, men også viden og udvikling af krypterings-teknikker. Det er centralt for efterretningsvirksomheden, at udviklingen sker så at sige i små skridt så man hele tiden kan følge med og tage sine forholdsregler. Et særligt problem er at bevare evnen til at spore den relevante kommunikation og kunne tappe den. Derfor er løsningen en hemmelig algoritme, som implementeres i en hardware løsning. På den måde hindres offentlige studier og efterligninger. Samtidig giver denne løsning suppleret med eksport-kontrol lovgivning en høj grad af kontrol med udbredelsen, herunder klar viden om hvor den bliver anvendt. Og sikkerhed for, når krypteringen anvendes andre steder, har efterretningstjeneste mulighed for at gennemføre sin efterretningsvirksomhed.

Endelig opfylder løsningen et krav om at tilbyde privatpersoner og erhvervsliv en stærk kryptering som kan sikre privatlivets fred og fortrolighed i kommunikationen.

Clinton-administrationen har understreget, at man ikke vil forbyde andre krypteringteknikker.

En dansk krypto-politik

Man kan vælge at sige, at problemet løser sig selv. Den nuværende lovgivning indeholder ingen regler om kryptering, og giver dermed den enkelte ret til at kryptere. Indenfor den eksisterende lovgivning er der således også mulighed for at opbygge generelle løsninger, hvor det er et integreret element i f.eks. pc'ens udstyr og programmer at data kan hemmeligholdes med kryptering. I den udstrækning folk faktisk oplever problemet - eller bliver bekendt med det ved omtale af brud på fortroligheden - vil de efterspørge produkter, der kan give fortrolighed og der vil op stå et marked for sådanne produkter.

Der kan umiddelbart peges på to problemer i denne synsvinkel. Da hemmeligholdes af kommunikationen vil blive anvendt af kriminelle, specielt den organiserede kriminalitet som f.eks. mafia- og narkotikaorganisationer, og dermed vanskeliggøre politiets arbejde med efterforskning kan samfundet ikke blot se til at hemmeligholdelse udbredes, men er nød til at overveje reguleringsmuligheder.

Dernæst er elektronisk kommunikation ved at blive en vigtig del af samfundets infrastruktur. Etablering af sikkerhedsforanstaltninger så denne infrastruktur kan fungere må siges at være en del af dens opbygning. Men en ren markedsstyret udvikling vil betyde ukoordinerede løsninger, der ikke vil sikre det åbne system som er en generel målsætning for "informations motorvejen". Samtidig må det antages, at denne udvikling generelt vil være langt dyrere for samfundet, da omkostningerne ved at indbygge sikkerhed i informations- og kommunikationssystemer efterhånden er langt større end omkostningerne, hvis de er en del af systemets grundlæggende opbygning. Derfor må der overvejes en generel samfundsmæssig løsning på hvordan elektronisk kommunikation skal hemmeligholdes.

Hvis man ønsker at påvirke anvendelsen af kryptering og evt. tage statslige initiativer [8] vil man være nød til at tage stilling til en række spørgsmål og valgmuligheder.

De følgende kapitler 2 - 8 fremlægger bidrag og synsvinkler, som grundlag for udformning af en dansk krypto-politik. I det afsluttende kapitel 9 fremlægges en liste af valgmuligheder, som der kan tages stilling til med en krypto-politik.

Baggrund og synsvinkler

Hvad siger loven?

Af Arne V. Gram og Ole Hasselgaard [9]

Det strafferetlige værn

For at beskytte hensynet til hemmeligholdelse af kommunikationen mellem borgerne indeholder straffeloven blandt andet regler om straf for uberettiget åbning af andres breve samt uberettiget aflytning og optagelse af telefonsamtaler, som vedkommende ikke selv deltager i. Tilsvarende straffes den, som uberettiget skaffer sig adgang til andres oplysninger eller programmer, der er bestemt til brug i et edb-anlæg. Strafferammen er bøde, hæfte eller fængsel indtil 6 måneder, dog således at straffen under skærpende omstændigheder kan stige til fængsel i indtil 4 år.

Politiets indgreb i meddelelseshemmeligheden

Det er således i almindelighed strafbart at skaffe sig adgang til den private kommunikation mellem andre personer. Dette udgangspunkt er dog fraveget i retsplejeloven, der giver politiet visse beføjelser til at gribe ind i meddelelseshemmeligheden til brug for efterforskningen af straffesager. Den nærmere afgrænsning af politiets beføjelser er foretaget af lovgivningsmagten ud fra en afvejning af på den ene side hensynet til borgernes frihedsrettigheder, herunder retten til meddelelseshemmelighed, og på den anden side hensynet til statsmagtens ønske om at opklare og straffe forbrydelser, herunder at politiet kan benytte sig af efterforskningsmidler, der er egnede til at opklare en forbrydelse. Denne afvejning af to modstående hensyn har ført til, at en række betingelser skal være opfyldt, for at politiet kan foretage brud på meddelelseshemmeligheden og f.eks. aflytte en telefonsamtale.

For det første skal der foreligge bestemte grunde til at antage, at der gennem den pågældende kommunikation gives meddelelser til eller fra en mistænkt. Dernæst skal indgrebet i meddelelseshemmeligheden være af afgørende betydning for efterforskningen. D.v.s., at der ikke er mulighed for anvendelse af andre egnede efterforskningsskridt i den pågældende sag, eller at andre efterforskningsskridt ville være uforholdsmæssigt resourcekrævende (f.eks. skygning af et større antal personer) eller ødelæggende for den videre efterforskning. For det tredje er det i almindelighed en betingelse for politiets indgreb i meddelelseshemmeligheden, at efterforskningen vedrører en forbrydelse, som kan straffes med fængsel i 6 år eller derover. Desuden kan indgreb i meddelelseshemmeligheden foretages, hvis efterforskningen angår forbrydelser mod staten, de øverste statsmyndigheder m.v. Der skal med andre ord være tale om en mistanke, der retter sig mod grov kriminalitet.

Efter grundlovens §72 kan indgreb i blandt andet post- og telefonhemmeligheden kun ske efter retskendelse, medmindre den enkelte lov indeholder en særlig undtagelse. Som følge heraf er det i retsplejeloven fastsat, at brud på meddelelseshemmeligheden kun kan ske efter rettens afgørelse herom, medmindre formålet med indgrebet ville gå tabt, hvis man skulle afvente en retskendelse.

Den mistænkte bliver i de konkrete tilfælde - naturligvis - ikke underrettet om politiets indgreb i meddelelseshemmeligheden, så længe det varer. Derimod skal der under rettens behandling af, om politiet kan få tilladelse til at gennemføre indgrebet, beskikkes en advokat til varetagelse af den mistænktes interesser. Når indgrebet senere er afsluttet, skal den mistænkte som hovedregel have underretning om det foretagne indgreb.

De nævnte regler om indgreb i meddelelseshemmeligheden omfatter alene meddelelser, der er undervejs i en kommunikation. Indgreb, der gennemføres inden kommunikationens påbegyndelse eller efter dens afslutning, er ikke omfattet af disse regler, men derimod af retsplejelovens regler om ransagning og beslaglæggelse. Sidstnævnte regler finder bla. anvendelse, såfremt politiet ønsker at sætte sig i besiddelse af en båndoptagelse af en allerede ført telefonsamtale. Virkningen af, at et indgreb bedømmes efter reglerne om ransagning og beslaglæggelse - og ikke reglerne om indgreb i meddelelseshemmeligheden - er dels, at der generelt er lempeligere betingelser for indgrebets foretagelse, dels at indgrebet ikke kan foretages hemmeligt.

Det skal bemærkes, at retsplejelovens regler om indgreb i meddelelseshemmeligheden samt om ransagning og beslaglæggelse naturligvis gælder for alle dele af politiet, herunder også Politiets Efterretningstjeneste.

Regler om kryptering

Der findes i dansk ret ikke regler, der forbyder anvendelse af kryptering eller besiddelse, køb og salg af teknisk materiale til brug for kryptering. Dette område er således i det hele ulovreguleret.

Bevisspørgsmål

Det er anklagemyndigheden, der under en straffesag skal føre bevis for den tiltaltes skyld. Kravet er, at beviset skal have en sådan styrke, at der ikke er rimelig tvivl om tiltaltes skyld.

Til brug for bevisførelse kan anklagemyndigheden blandt andet fremlægge oplysninger, der måtte være fremkommet ved politiets (lovlige) indgreb i meddelelseshemmeligheden. Det kan f.eks. ske ved fremlæggelse af en aflyttet telefonsamtale.

Såfremt der har været tale om krypteret kommunikation, er det imidlertid af tekniske årsager ikke muligt for anklagemyndigheden at anvende kommunikationen som et brugbart bevis, medmindre man måtte have kendskab til den "nøgle", der kan dechifrere kommunikationen. Kryptering af kommunikation kan derfor efter omstændighederne gøre det umuligt for anklagemyndigheden at føre det fornødne bevis i en staffesag. Da det som nævnt er anklagemyndigheden, der har bevisbyrden, vil en sådan bevismangel føre til, at den tiltalte bliver frifundet, medmindre retten efter en bedømmelse af sagens øvrige beviser finder, at der ikke er rimelig tvivl om tiltaltes skyld.

Kryptering og nøgler

Af Peter Landrock [10]

Kryptografiske systemer

Indtil slutningen af 1970'erne kendte man kun én type af såkaldte kryptografiske systemer, nemlig det konventionelle eller symmetriske system, også kaldet 1nøgle system, hvor dekrypteringsalgoritmen umiddelbart lader sig beskrive ved hjælp af enkrypteringsalgoritmen og omvendt. Men i 1976 foreslog to forskere ved Stanford University, W. Diffie og M. Hellman, en ny type af systemer, såkaldte public key eller asymmetriske systemer, også kaldet 2nøgle systemer, hvor den ene nøgle kan offentliggøres, samtidig med at den anden kan hemmeligholdes. Diffie og Hellman beskrev selv et system i artiklen, som kunne bruges til hemmeligholdelse, men ikke til digitale signaturer. Snart efter Diffie-Hellmans artikel begyndte forskere rundt omkring at foreslå sådanne, hvoraf det mest udbredte i øjeblikket er RSAsystemet, som blev konstrueret på M.I.T. i 1978 af R.L. Rivest, A. Shamir og L. Adleman.

> **Grundlæggende terminologi:**
> Forvandlingen fra såkaldt *klartekst* (på engelsk plaintext), altså teksten før brug af kryptering til såkaldt *kryptotekst* eller *chiffertekst* (på engelsk ciphertext), kaldes *enkryptering*. Forvandlingen tilbage til klartekst kaldes *dekryptering*. Disse processer er som regel styret af *nøgler*, hvoraf hele sikkerheden ofte afhænger.

De kryptografiske systemer kan klassificeres i to grupper: Enkrypterings- eller kryptosystemer, og envejsfunktioner. Og kryptosystemerne findes i to hovedudgaver: Konventionelle og public key systemer.

Konventionelle (symmetriske) kryptosystemer

Fra en klartekst "m", genereres en tilhørende kryptotekst ved hjælp af en enkrypterings-transformation E, karakteriseret ved en parameter, en såkaldt nøgle, "k". Hvis enkrypteringen er styret af nøglen k, skriver vi E_k. Vi har altså

$c = E_k(m)$

Tilsvarende har vi en dekrypteringstransformation D, styret af samme nøgle, således at

$D_k(c) = m$

Det afgørende ved et konventionelt system er altså netop, at algoritmerne D_k og E_k er styret af den samme nøgle. Med andre ord: Det kan ikke lade sig gøre at offentliggøre den ene algoritme og samtidig hemmeligholde den anden. Vi bemærker altså, at enhver, der kan dekryptere, også kan enkryptere. Det har bla. den konsekvens, at et konventionelt system ikke kan bruges direkte til identifikation. Hvis to brugere A og B kommunikerer v.h.a. et konventionelt system, kan en dommer ikke bagefter afgøre, om en kryptotekst er produceret af A eller B. Hvis identifikation ønskes, er det nødvendigt at indføre en betroet tredje part, der spiller rollen af notarius publicus.

DES Algoritmen, hvis betegnelse står for Data Encryption Standard, er et konventionelt kryptosystem, som blev udviklet af IBM i samarbejde med National Bureau of Standards (NBS) i USA, og offentliggjort i

1977. DES anvendes kun til civil kryptering, og er langt det mest udbredte system. Specielt er DES meget brugt i bankverdenen, også i DANKORTsystemet.

DES er en såkaldt blokkode, hvor klarteksten deles op i blokke på 64 bits og nøglen er 56 bits lang. Nøglerummets størrelse er altså 2^{56}, som i dag er under grænsen af, hvad de aller kraftigste computere i verden kan klare på rimelig tid ved udtømmende søgning. Dette klares imidlertid ved at bruge en nøgle af dobbelt længde, og så erstatte hver DESkryptering af tre DESkrypteringer. Det vil føre for vidt her at beskrive algoritmen i detaljer. Det skal blot anføres, at vi nu er på vej mod en situation, hvor en nøglelængde på 56 bits er for lille. Derfor har man lavet en variant af DES, som kaldes triple-DES, med dobbelt nøgle, hvor man først enkrypterer med den første nøgle, derefter med den anden nøgle, hvorefter man dekrypterer med den første nøgle (altså tre DES-krypteringer)

Public key (asymmetriske) systemer

Forskellen på et konventionelt system og et public key system er kort og godt, at det ikke er beregningsmæssigt muligt at finde dekrypteringsnøglen, selvom enkrypteringsnøglen er kendt, og omvendt. Derfor taler man ikke om enkryptering og dekryptering (med mindre systemet kun bruges til konfidentialitet), men om en hemmelig transformationsnøgle S (S for "secret") og en offentlig transformationsnøgle P (P for "public"). Specielt må vi nu for alle bitstrenge (og det har ikke længere mening at skelne mellem klartekst og kryptotekst) X kræve

$P(S(X)) = X, S(P(X)) = X$

Til sammenligning, som illustrativ forklaring af forskellen på konventionelle systemer og public key systemer, kan tænkes på et sæt ordbøger, f.eks. kinesiskdansk (S) og danskkinesisk (P). Selv om man har en danskkinesisk ordbog, vil det være en praktisk meget krævende opgave derudfra selv at udarbejde en kinesiskdansk ordbog.

Et public key system kan både bruges til konfidentialitet og autenticitet, ja endog til at producere digitale underskrifter. Det skal dog pointeres, at for hver enkelt bruger A, der vælger sig en nøgle, eller rettere et par, (P_A), kan A bruge S_A til modtagelse af hemmelige meddelelser samt til *egen* digital underskrift og *andres* offentlige nøgler til at sende hemmeligholdte meddelelser. Omvendt kan andre bruge A's offentlige nøgle til at sende hemmeligholdte meddelelser til A:

1. Konfidentialitet.

Hvis B ønsker at sende en klartekst M til A, således at den hemmeligholdes undervejs, bruger B A's offentlige nøgle , som A har offentliggjort til alle og sender

$P_A(M) = C$

Kun A kan dekryptere, da kun A kender den tilhørende hemmelige nøgle S_A og $S_A(C) = M$. (Et praktisk spørgsmål, som naturligvis kan løses, er, hvorledes B kan have vished for, at det nu også er A's offentlige nøgle).

2. Autenticitet (digital signatur).

Hvis A ønsker at sende en klartekst X til B, enkrypteret således at B kan checke, at meddelelsen kommer fra A, sender hun

$S_A(X) = Y$

B prøver da med A's offentlige nøgle og finder at (Y) = X. Hvis X er meningsfuld, må S_A have været anvendt, da kun A kan enkryptere, således at B kan dekryptere til noget meningsfyldt. Læg dog mærke til, at *autenticitet kun sikres første gang, meddelelsen X underskrives*. Derfor må en sådan meddelelse i praksis have karakter af en engangsmeddelelse, f.eks. v.h.a. et tidsstempel.

3. Konfidentialitet og autenticitet på én gang

Uden at gå i detaljer skal blot nævnes, at begge egenskaber opnås på én gang ved først at lade A bruge sin hemmelige nøgle til autenticitet og derefter B's offentlige nøgle til konfidentialitet.

Envejsfunktioner

I USA er man meget langt fremme med opbygning af systemer, der yder konfidentialitet med mulighed for aflytning mod dommerkendelse. I USA har public key systemet RSA længe været en torn i øjet på NSA (National Security Agency). Dels kan RSA bruges både til digitale signaturer og enkryptering som beskrevet ovenfor, dels er algoritmen patenteret og ejet af "Public Key Partners" (PKP), der blandt andet har Stanford University og MIT som aktionærer, udover RSA Inc.

Man besluttede sig derfor til i NSA at udvikle "sin egen" algoritme, DSA (Digital Signature Algorithm), som skulle have den egenskab, at den ikke kunne bruges til enkryptering, altså hemmeligholdelse. Resultatet var ikke overraskende. Det blev en variant af El Gamal algoritmen, en algoritme fra 1982 baseret på diskrete logaritmer. Det pudsige er, at denne algoritme, som er designet til ikke at kunne hemmeligholde, er en matematisk variant af den oprindelige Diffie-Hellman algoritme, som kun kunne bruges til hemmeligholdelse.

Princippet i Diffie-Hellman algoritmen er følgende:

Man konstruerer en funktion f, der som input har to værdier: En offentlig værdi, g, som alle kender, og en individuel værdi, x, som den enkelte bruger vælger. Herved fremkommer et output, f(g,x). Funktionen siges at være envejs, hvis, givet f(g,x) og g, det er praktisk umuligt at finde x. Hvis samtidig denne funktion har yderligere en grundlæggende egenskab, nemlig at

$f(f(g,x), y) = f(f(g,y),x)$,

(f.eks. eksponentiering: $f(g,x) = g^x$ for to tal g og x),

har vi Diffie-Hellman systemets banebrydende egenskab:

Personen X vælger en hemmelig værdi x, og sender værdien f(g,x) til Y. Personen Y vælger en hemmelig værdi y og sender værdien f(g,y) til X. Da X kender x og f(g,y) kan X beregne f(f(g,y),x), mens Y kan beregne f(f(g,x),y). Da disse to værdier er ens, kan denne værdi bruges som en fælles nøgle til enkryptering med et konventionelt kryptosystem, såsom DES.

Krav til kryptosystemer

De fundamentale krav til et godt krypteringssystem eller envejssystem er:

1. Nøglerummet skal være så stort, at det ikke ved udtømmende søgning er muligt at checke alle nøgler.

2. Det må ikke være muligt at lave et angreb baseret på statistisk analyse af chifferteksten, ej heller selvom den er på binær form f.eks v.h.a. ASCIIkoder.

3. Selv et kendtklartekst angreb af en betragtelig længde må ikke resultere i, at hele nøglen kan bestemmes.

Forskning

RSApublic key systemet er baseret på en række erfaringer, matematikere over flere tusinde år har gjort sig om primtal, dvs tal, som kun kan deles med sig selv og 1: Det er relativt nemt at afgøre, om et fast valgt tal n er et primtal eller ej, men, hvis det viser sig, at det ikke er et primtal, så vokser besværligheden med at finde ud af, hvilke primtalsdivisorer, det så har, exponentielt med størrelsen af tallet, selv under anvendelsen af alle de trick og kunstgreb, matematikere i tidens løb har forsøgt at udvikle, og naturligvis derfor også, selvom man tager selv de kraftigste computere i brug. Der findes således oceaner af tal på omkring 160 cifre (512 bits) , som er praktisk umulige at opløse i primfaktorer. (Grænsen går idag omkring 105110 cifre, ved anvendelse af et stort antal computere i parallelle sessioner).

Diffie-Hellman, El Gamal og DSA bygger alle på et andet svært matematisk problem, det såkaldte diskrete logaritme problem: Givet et stort primtal p og et vilkårligt (naturligt) tal g mindre end p, kan vi beregne g^x mod p: Find først tallet g^x, divider derefter med p og find heltalsresten, som betegnes g^x mod p. Problemet er så, derfra at finde x.

Kryptologi er det sidste tiår blevet et meget vigtigt fag ved højere læreanstalter. Kryptologi er dels læren om kryptografi, dels kryptanalyse, dvs udvikling af metoder til at evaluere styrken af kryptografiske systemer. I Danmark dyrkes denne nye forskningsgren kun på Aarhus Universitet. Det er et område med det ene ben i matematikken og det andet i datalogien. Et af de mest fascinerende aspekter ved denne anvendte videnskab er, at den bygger på områder, som indtil for 15 år siden var anset for rene grundforskningsområder, som lå så langt fra anvendelser som overhovedet muligt, nemlig talteori og kompleksitetsteori. Som nævnt tidligere bygger vi systemerne omkring problemer, som århundredes forskning har vist er svære. Man kan således sige, at hele det matematiske samfund garanterer for, at systemerne er bygget så sikre som muligt. De en konstant under bombardement af det svære skyts, nemlig verdens førende talteoretikere.

Det store praktiske problem: Nøgleadministration

Det lød så let, at vi alle kan verificere A's signatur v.h.a. hendes offentlige nøgle, og at alle kan sende hemmeligheder til A enkrypteret under A's offentlige nøgle. Spørgsmålet er blot, hvorledes vi får kendskab til den? Det er naturligvis ikke nok, at A blot sender den sammen med f.eks. den digitale signatur, vi skal verificere. Enhver person X kunne jo påstå at være A og sende en offentlig nøgle, hvortil X kendte den tilsvarende hemmelige nøgle. Det vil heller ikke være praktisk muligt, for at forebygge dette, at A først overbringer os nøglen ved selv at rejse rundt som kurér.

Måden, hvorpå problemet løses, et v.h.a. det, vi kalder certifikater. I et åbent system, hvor enhver principielt kan melde sig som bruger, er vi nødt til at have en myndighed (på engelsk, certification authority, CA), som registrerer brugere og deres offentlige nøgler, efter først at have checket deres identitet efter afstukne sikkerhedsprocedurer. Denne myndighed er selv udstyret med et public key par, (P,S). Når A så er registreret med sin offentlige nøgle , udstedes certifikatet som CA's digitale signatur v.h.a. S på en meddelelse, som blandt andet består af information, som identificerer brugeren A og . Samtidig får A ved

registreringen udleveret CA's offentlige nøgle P.

Når A så sidenhen skal kommunikere med B, sender hun først sit certifikat til B. B checker v.h.a. P, at certifikatet er CA's digitale signatur på en meddelelse som fortæller, at en vis bruger A af CA er registreret med den offentlige nøgle . Dette fortæller *ikke* B, at A er i den anden ende. Det sikrer udelukkende, at B kan stole på, at en bruger kendt under navnet A er registreret med den offentlige nøgle . B er herefter i stand til at verificere A's eventuelle efterfølgende underskrift på en eller anden meddelelse, eller sende en hemmelighed enkrypteret under A's offentlige nøgle. Vi har hermed løst problemet med at kommunikere de forskellige brugeres offentlige nøgler. Til dette forudsættes kun kendskab til én eneste nøgle, nemlig den certificerende myndigheds offentlige nøgle. Tilbage er blot at tilføje, at den offentlige nøgle i praksis bruges til udveksling af såkaldte sessionsnøgler, f.eks. DES-nøgler, hvorefter en meddelelse så enkrypteres under denne sessionsnøgle. Modtageren dekrypterer først til sessionsnøglen, hvorefter chifferteksten dekrypteres med denne nøgle. Ved næste session fremsendes så en ny sessionsnøgle.

Clipperchippen, Skipjack og Escrowværdier.

Clintonadministrationen annoncerede 16. april sidste år udviklingen af den hemmelige "skipjack"algoritme til enkryptering. Algoritmen er lagt ind på en speciel chip, "Clipper-chippen" og er udviklet til hemmeligholdelse ved kommerciel og civil kommunikation.

Der er bare den ekstra finesse, at Clipperchippen indeholder en fast masterkey. Ved kommunikation sender chippen først det såkaldte "law enforcement access field" (LEAF) som indeholder oplysninger om sessionsnøglen, der bliver anvendt til den efterfølgende enkrypterede information. Samtidig vil der ved to uafhængige TTP'er ligge nogle såkaldte "escrowværdier", som afhænger af masternøglen på en sådan måde, at man ved hjælp af disse, og indholdet af LEAF kan bestemme sessionsnøglen, men ikke selve "escrow"-værdierne. Politiet og andre offentlige myndigheder i USA har således gennem en dommerkendelse mulighed for at få lov til at gå ind at læse den enkrypterede information. Dette princip er beskrevet i den såkaldte escrow-standard:. Det der kan undre, er, at selve nøgleudvekslingen mellem de kommunikerende partnere ikke er beskrevet. Dette må bygges ovenpå.

De systemer der overvejes i Europa, forbinder escrow-princippet med nøgleudvekslingen.Der er ingen tvivl om, at det kan lade sig gøre at bygge sikre systemer, hvor nøgleudvekslingen er en del af systemet, og hvor samtidig myndighederne med en dommerkendelse kan få adgang til den sessionsnøgle der benyttes under sessionen. Det kan dog være et praktisk problem, at begge parters system bidrager til den fælles sessionsnøgle.

Sikkerhed i telenettet

Af Leif Nielsen [11]

Sikkerhed i telenettet dækker mange aspekter. Nedenfor beskrives alene den del, der vedrører sikkerhed for fortrolig overførsel af data i Tele Danmarks net og altså ikke f.eks. fysisk sikring af komponenter i nettet eller forhold vedrørende almindelig telefoni.

Såvel teknologi som måden at opbygge nettet på har ændret sig over tid. I konsekvens heraf har også måden at udveksle data på ændret sig.

- Det fysiske medium var tidligere almindelig kabel. Dette er i dag erstattet af skærmede kabler, lysledere og radioforbindelser.

- Transmissionsmåden er ændret fra at være analog til at være digital.

- Transmission af en "samtale" pr. kabel er ændret, så samme kabel eller radioforbindelse i dag overfører 10.000 "samtaler". Dette sker i kraft af multiplex-teknik, der omsætter informationer fra et antal individuelle kanaler på en bærer/forbindelse, så mange informationer sendes "samtidigt".

Den grundlæggende transmissionsform i det overordnede telenet er den samme uanset tjeneste: Telefoni, Datel, Datapak, Datapost, ISDN, NMT eller GSM.

I det overordnede telenet er der tale om en kraftig multiplexering af "samtaler" på samme forbindelse, og det fysiske transmissionsmedium er meget svært tilgængeligt (typisk nedgravet). Ligeledes overføres information om afsender og modtager for en given "samtale" typisk via andre forbindelser end selve "samtalen"/datatransmissionen. Aflytning af det overordnede telenet vurderes derfor at være yderst vanskeligt. Etableres aflytning alligevel, vurderes det ligeledes at være yderst vanskeligt at identificere afsender og/eller modtager for en given transmission.

For aflytning gælder generelt, at jo tættere dette sker på afsender eller modtager, jo større er risikoen og/eller muligheden for aflytning af en given "samtale".

Selv om accesnettet (dvs. nettet ud til den enkelte kunde) anses for vanskeligt at beskytte 100% mod fysiske indbrud, skal man ikke langt fra modtagers eller afsenders bygning/terminal, før det bliver vanskeligt at identificere en given "samtale"/transmission.

I denne sammenhæng skelnes ikke mellem de forskellige tjenester. Vanskelighederne ved at etablere aflytning er dog mere eller mindre komplekse, afhængig af den enkelte tjeneste. GSM afviger således væsentligt i kompleksitet fra øvrige tjenester og vurderes som relativ vanskelig at aflytte.

Telenettet er karakteriseret ved, at overførsel af information sker umiddelbart i forbindelse med afsenderen. Der oplagres altså ikke information.

Kun ved to tjenester lagres information til senere afsendelse. Det drejer sig om tjenesterne Datapost og Superfax.

Datapost er et offentligt MHS-system (Message Handling System), der gør det muligt for brugere at distribuere data til en eller flere brugere samtidig. De lagrede data slettes straks ved afsendelse til modtageren.

Superfax er en applikation til den almindelig fax-tjeneste, de gør forsendelse af samme information til mange modtagere muligt. Som et supplement giver tjenesten afsenderen mulighed for at lade fax-meddelelser forblive i en postkasse i Superfax. Først efter fornøden identifikation kan modtageren få tilsendt sine telefax.

Hverken ved Datapost eller Superfax lagres informationerne krypteret, men kun meget få personer i Tele Danmark har adgang til at læse de lagrede informationer. Dette kan i øvrigt kun ske efter nødvendig identifikation overfor systemerne.

Kun få medarbejdere i Tele Danmark har generelt adgang til diverse systemkomponenter og transmissionsveje.

I forbindelse med drift af nettet og vedligeholdelsesarbejde foretages yderst sjældent indlytning på en forbindelse. Det sker i så fald kun kortvarigt og yderst sjældent med instrumenter til detektering af datatransmission.

Alle medarbejdere i Tele Danmark underskriver ved deres ansættelse en tavshedserklæring, der skal sikre, at ingen informationer vedr. ovenstående forhold videregives til 3. mand.

Faglige standarder

Af Steffen Stripp

I udformning af et krypto-system indgår en række spørgsmål, hvor bidrag fra en edb-faglig sikkerhedsvinkel er væsentlige. Det er ikke en professionel opgave at opstille mål og krav til et sådant system. På den anden side er der forskellige spørgsmål, som bør belyses fra en faglig side, som led i fastlæggelse af disse mål og krav.

Det er vigtigt at understrege, at der findes en risiko for at datakommunikation aflyttes og at e-post læses af uvedkommende. En række mere eller mindre alvorlige tilfælde er blevet offentlig rapporteret.[12]

Der er givet behov for at sikre fortroligheden i kommunikationen. F.eks. kræver registerlovgivningen, at den registeransvarlige sikrer, at data fra et edb-register, der kommunikeres elektronisk ved e-post, fax eller lignende, ikke kommer til uvedkommendes kendskab. Elektronisk udveksling af oplysninger i breve, dokumenter vil i de kommende år vokse mellem myndigheder, f.eks. i social- og sundhedssektoren, i virksomhedernes interne kommunikation og mellem virksomheder, herunder udveksling af handelsdata som EDI, i finansielle transaktioner, der allerede er beskyttet af kryptering og endelig vil privatpersoner i stigende grad kommunikere elektronisk såvel indbyrdes som til virksomheder og myndigheder.

Det er ikke muligt at indføre sikkerhed i kommunikation i åbne net uden at inddrage kryptering. De fire aspekter for sikkerhed ved datakommunikation (autenticitet, integritet, uafviselighed og fortrolighed) understøttes alle med løsninger, hvor kryptering indgår. I flere situationer vil en løsning understøtte flere aspekter på en gang.

Offentlig krypto-system

Da man i USA overvejer at udbrede kryptering baseret på algoritmer, som ikke er offentlig kendte, er der behov for at understrege det er et alment accepteret fagligt standpunkt, at styrken ved en kryptering ikke ligger i en hemmeligholdelse af algoritmen, men i selve algoritmen. Dette synspunkt formuleres således i en udbredt lærebog: "Now a new class of algoritms is proposed. These algortihms would be distributed as sealed encryptions devices, so that neither the algoritm nor its implementation or analysis would be made public. In doing this, the NSA hopes to make it harder for someone to discover a flaw in an algoritm: First you have to infer the algoritm you can begin to analyze it. Although this does provide an extra measure of security, it limits the ability of the research community to inspire confidence in the devices because there can be no rigorous analysis of the algoritm. The important issue of thrust in scientific invention is supported by public analysis and criticism. Public scruntiny and security are by their very nature conflicting goals."[13]

Svagheder ved Skipjack

I forlængelse heraf kan der knyttes nogle yderligere kommentarer til Escrow Key Encryption (EES). Det er en ret ny krypteringsfremgangsmåde og det må vurderes, at der er behov for en vis tid, hvor den åbent analysere og vurderes i det internationale sikkerheds- og videnskabelige miljø.

Der er særlige problemer knyttet til Skipjack algoritmen, som anvendes i det amerikanske initiativ. Algoritmen, er som sagt, ikke offentlig. For at imødekomme kritikken heraf indbød man et panel af sikkerheds- og kryptografieksperter til at vurdere algoritmen. Dette studie refereres således i ACM's rapport [14]: "A panel of cryptography and security experts (including two members of this panel) invited by NIST to study the quality of the SKIPJACK algorithm concluded that SKIPJACK appeared to be both strong and resistant to attack. The effort was limited in scope. Working within a tight time frame, they could not attempt a complete investigation of the algorithm's security. However, they examined the structure of the algorithm, and the procedures followed by NSA in developing and evaluating the algorithm, and they were satisfied. Nonetheless, public skepticism of classified design has been fueled by the recent discovery that under certain circumstances the function of the LEAF [15] can be subverted."

Der har været fremlagt forskellige tekniske kritikpunkter af Skipjack. Det er blevet påvist, at man med forskellige teknikker kan gennemføre krypteret kommunikation mellem to EES enheder uden at transmittere LEAF-feltet [16]. Hvis denne mulighed udnyttes forsvinder så at sige hele pointen med Key Escrow krypto-systemet.

Andre har rejst muligheden for producere falske meddelelser på grundlag af LEAF-feltet. [17]

Tilgængelige oplysninger om SKIPJACK siger at den er opbygget "DES lignende" og at nøglen er på 2x40 bit. Det er kendt at enkelt DES nøgle på 56 bit idag ikke kan regnes for sikker. Må man derfor ikke konstatere, at en nøgle på 80 bit er for kort til at sikkerheden ikke kan brydes af organisationer med tilstrækkelig avancerede computere?

Kontrol

Det overvejes ved indførelse af bestemte krypto-systemer samtidig at indføre en kontrol af om krypteret digital kommunikation faktisk er krypteret med dette system. Denne tanke kan diskuteres fra flere vinkler. Her er spørgsmålet: er det overhovedet muligt. Det er min vurdering, at i åbne net med betydelig datatransmission af alle mulige typer af data vil det næppe være muligt at gennemføre en sådan kontrol. Hvis der findes visse kendetegn, som kontrollen kunne tage udgangspunkt, vil det være muligt sikre at en datatransmission "ligner" denne.

Privatlivets fred

Af Birgitte Kofod Olsen [18]

Privatlivets fred er beskyttet ved den Europæiske Menneskeretskonventions (EMRK) art. 8. Denne bestemmelse fastslår, at en enhver person, der opholder sig indenfor dansk jurisdiktionskompetance har ret til respekt for sit privatliv og familieliv samt for sit hjem og sin korrespondance. I relation til hemmeligholdelse af datakommunikation er beskyttelsen af privatlivet som helhed relevant, foruden den specifikke beskyttelse af korrespondance. Derudover påkalder art. 10 om ytringsfrihed sig interesse i nærværende sammenhæng.

I det følgende vil omfanget af den beskyttelse, som er fastlagt i EMRK blive beskrevet og det vil blive vurderet, om den menneskeretlige privatlivsbeskyttelse fordrer adgang til en særlig krypteringsteknik, herunder om der på baggrund af de menneskeretlige regler kan stilles krav om adgang til krypteringsteknikker, der ikke defineres eller kontrolleres af offentlige myndigheder.

Den menneskeretlige beskyttelse af korrespondance

EMRK art. 8 har følgende ordlyd:

> Stk. 1. Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin **korrespondance.**
>
> Stk. 2. Ingen offentlig myndighed må gøre indgreb i udøvelsen af denne ret, medmindre det sker i **overensstemmelse med loven** og er **nødvendigt i et demokratisk samfund** af hensyn til den nationale sikkerhed, den offentlige tryghed eller landets økonomiske velfærd, for at **forebygge uro eller forbrydelse**, for at beskytte sundheden eller sædeligheden eller for at beskytte andres rettigheder og friheder. (min udhævning)

Alle former for kommunikation må antages at være omfattet af beskyttelsen i EMRK art. 8, stk. 1 af privates korrespondance, herunder såvel mundtlig som skriftlig kommunikation samt kommunikation ved hjælp af elektroniske medier. Korrespondance af privat karakter ligger indenfor beskyttelsens kerneområde. Derudover kan korrespondance af forretningsmæssig karakter efter omstændighederne også anses som omfattet af beskyttelsen.

Det betyder, at det enkelte individ skal kunne kommunikere frit og uden statens indgreb i form af brevåbning, aflytning, registrering og lignende. I relation til elektronisk kommunikation betyder dette antageligt, at kommunikation i åbne net som udgangspunkt skal kunne gennemføres uden risiko for tapning, netovervågning, registrering eller lignende fra statens side. Konventionsorganerne i Strasbourg, d.v.s. den Europæiske Menneskeretskommission og den Europæiske Menneskeretsdomstol, har imidlertid ikke i konkrete tilfælde taget stilling til den elektroniske kommunikationsform i relation til art. 8.

Meddelelseshemmeligheden efter stk. 1 er ikke absolut. Forebyggelse af uro og forbrydelse er således et blandt flere hensyn, som kan påberåbes af staten i forbindelse med indgreb i privates korrespondance. Retspraksis fra den Europæiske Menneskeretskommission og den Europæiske Menneskeretsdomstol viser da også, at netop dette hensyn er påberåbt i sager, hvor straffeprocesuelle indgreb i meddelelseshemmeligheden har været anset for nødvendige som led i efterforskningsarbejde.

Udover hensynet til forebyggelse af uro og forbrydelse (eller et af de andre opregnede hensyn) skal yderligere to kriterier være opfyldt, førend staten kan foretage indgreb i den private korrespondance. For det

første skal indgrebet være i overensstemmelse med en national lovbestemmelse, og dernæst skal indgrebet være nødvendigt i et demokratisk samfund. **Legalitetskravet** indebærer, at indgrebet skal have et grundlag i national ret, der er tilgængeligt for borgerne og hvis indhold er rimeligt klart og præcist, således at borgerne med en vis sikkerhed kan forudse retsgrundlagets konsekvenser. **Nødvendighedskravet** betyder, at staten skal påvise, at indgrebet efter statens skøn er begrundet i et påtrængende samfundsmæssigt behov. Som modvægt til statens skønsmargin stilles der i medfør af konventionen krav om **proportionalitet**, hvilket bla. betyder, at indgrebets intensitet skal stå i rimeligt forhold til det angivne mål samt at staten altid skal vælge en mindre indgribende foranstaltning fremfor en mere indgribende.

Den konventionsfæstede adgang for staten til under visse omstændigheder at foretage indgreb i en beskyttet rettighed er udtryk for accept og anerkendelse af den holdning, som genfindes i diskussionen om brugen af selvvalgte krypteringsteknikker, nemlig at der i en vis udstrækning er behov for, at staten kan bryde ind i den private sfære, som korrespondance - herunder elektronisk kommunikation - er en del af.

Beskyttelse af krypteret kommunikation

Elektronisk kommunikation er som nævnt omfattet af beskyttelsesområdet for art. 8, stk. 1, men kan dog under særlige omstændigheder gøres til genstand for statens indgreb i medfør af art. 8, stk. 2.

I relation til hemmeligholdelse af elektronisk kommunikation, er spørgsmålet herefter, om staten har adgang til sikre sine indgrebsmuligheder i privat korrespondance ved at forbyde private at gøre brug af kryptering eller ved at kræve obligatorisk anvendelse af statsligt kontrollerede algoritmer til brug ved udvikling af krypteringssystemer og i tilknytning hertil registrering af såkaldte "escrow-værdier".

Et forbud mod kryptering må anses som et indgreb i retten til respekt for korrespondance, idet et sådant forbud vil hindre individet i at opnå en ønsket hemmeligholdelse af materiale, der kommunikeres elektronisk. Staten vil dog i medfør af art. 8, stk. 2 have mulighed for i konkrete tilfælde at iværksætte et forbud mod brug af kryptografi, såfremt de involverede personers kommunikation giver anledning til mistanke om aktiviteter, der truer fx. den nationale sikkerhed eller den offentlige ro og orden.

For så vidt angår offentligt kontrollerede algoritmer, herunder registrering af escrow-værdier, er det ikke ganske klart om sådanne ordninger kan betragtes som værende i overensstemmelse med art. 8. Det kan således hævdes, at den konventionsbeskyttede fri kommunikation har som afledet effekt, at staten ikke kan pålægge den enkelte borger at gøre brug af en særlig krypteringschip, der sætter statslige myndigheder i stand til generelt og på permanent basis at få adgang til krypteret kommunikation. Muligheden for borgerne til at fastholde korrespondancens private karakter synes svækket ved en sådan ordning. Undtagelsesestemmelsen i art. 8, stk. 2 åbner dog mulighed for, at indgreb i meddelelseshemmligheden kan iværksættes, såfremt dette kan anses for strengt nødvendigt af hensyn til de demokratiske institutioner i samfundet, fx. politiets efterforskningsarbejde [19] . Bestemmelsen i stk. 2 må dog også i denne sammenhæng forstås således, at den ikke giver staten adgang til at iværksætte systemer, der kan anvendes til generelt at føre kontrol med borgernes kommunikation, men alene under helt særlige omstændigheder åbner mulighed for, at staten kan foretage konkret begrundede indgreb i enkeltpersoners korrespondance. Hverken den Europæiske Menneskeretskommission eller den Europæiske Menneskeretsdomstol har dog haft lejlighed til konkret at vurdere konventionsmæssigheden af offentligt kontrollerede algoritmer med tilknyttet registrering af escrow-værdier.

I relation til såvel forbud mod kryptering samt offentligt kontrollerede algoritmer er det væsentligt at nævne EMRK art. 10, som beskytter ytringsfriheden, herunder retten til at meddele og modtage ytringer. Begrebet ytring er i art. 10-sammenhæng meget bredt og dækker såvel verbale som non-verbale ytringer.

Meddelelser, der er forvansket ved hjælp af kryptografi, må derfor antages at ligge indenfor bestemmelsens beskyttelsesområde.

Ytringsfriheden kan dog ligesom retten til respekt for korrespondance begrænses i en vis udstrækning, herunder hvis det må anses for påkrævet af hensyn til fx. forebyggelse af uorden og forbrydelse (art. 10, stk. 2). Et indgreb i ytringsfriheden stiller ligeledes krav om lovhjemmel og nødvendighed i et demokratisk samfund. Vurderingen af, om et indgreb er legitimeret ved art. 10, stk. 2 er konkret, d.v.s. at det i det enkelte tilfælde må vurderes, om legalitets- og nødvendighedskravet er opfyldt, og om der er proportionalitet mellem indgrebet og formålet med indgrebet.

Set i det lys forekommer en generel begrænsning af muligheden for den enkelte til selv at vælge metode, udformning og sprog i forbindelse med elektronisk kommunikation uproportional i forhold til den kriminalitetsbekæmpelse, som er opstillet som mål. Et forbud mod at kommunikere i kryptotekst i konkrete tilfælde forekommer også at være ganske vidtgående, idet de implicerede personer herved forhindres i at kommunikere og dermed udtrykke sig på en måde, som de selv ønsker.

Derimod vil en pligt i konkrete tilfælde til brug af en krypteringsteknik med en for brugeren ukendt underliggende algoritme og automatisk registrering af escrowværdier antageligt kunne pålægges af staten i overensstemmelse med art. 10, stk. 2.

Omvendt bevisbyrde og obligatorisk lagring

De alternativer, der i debatten [20] er nævnt til offentligt kontrollerede algoritmer og forbud mod kryptografi er omvendt bevisbyrde, obligatorisk lagring af al elektronisk kommunikation samt lagring af hashværdier hos en uvildig tredjepart.

En regel om **omvendt bevisbyrde**, hvorefter en sigtelse vil kunne fastholdes mod en tiltalt, såfremt denne ikke frigiver sin private krypteringsnøgle, kan muligvis gennemføres uden tilsidesættelse af retten til en retfærdig rettergang efter EMRK, art. 6. Art. 6, stk. 2 fastslår princippet om, at enhver skal anses for uskyldig indtil andet er bevist. Denne bestemmelse indebærer, at bevisbyrden for tiltaltes skyld påhviler anklagemyndigheden. I praksis har den Europæiske Menneskeretsdomstol dog ikke fundet, at en bevisbyrde, der tillægges tiltalte, er i modstrid med art. 6, stk. 2, hvis den holdes inden for rimelige grænser. Der ses ikke at være fastlagt nøjere kriterier for, hvornår dette rimelighedskrav er opfyldt. Dette udgangspunkt må dog suppleres med det af domstolen på baggrund af art. 6, stk. 1 knæsatte princip om, at en person ikke kan tvinges til at udlevere oplysninger, der vil være til skade for personen selv i en straffessag, såkaldt "selvinkriminering". Som følge af dette princip vil anklagemyndigheden være afskåret fra at pålægge en tiltalt at fremlægge materiale, som den har fået kendskab til via beslaglagt materiale, men som ikke er omfattet af beslaglæggelseskendelsen. Såfremt der på baggrund af en retskendelse sker beslaglæggelse af krypteret materiale, synes det således ikke uden videre at forårsage en konventionskrænkelse, hvis dette materiale kræves fremlagt i klartekst. Der vil i dette tilfælde ikke være tale om supplerende og uddybende dokumenter, men alene om en forklaring af det beslaglagte materiale, der vil være en forudsætning for, at dette materiale kan anvendes meningsfuldt.

Et forpligtelse til **obligatorisk lagring** af elektronisk korrespondance vil være nyttig i forbindelse med efterforskningsarbejde, idet kommunikation mellem bestemte parter eller i afgrænsede perioder lettere vil kunne identificeres og dermed gøres til genstand for beslaglæggelse. Det forekommer dog at kunne udgøre et indgreb i den enkelte borgers privatliv, såfremt al privat korrespondance kræves logget. Derimod synes det i menneskeretlig henseende at være mindre kritisabelt, at der opstilles et krav om logning af virksomheders korrespondance. Sådan korrespondance er da også på flere områder genstand for regulering

med et samfundsmæssigt formål, fx. området for told og skat. Et krav om obligatorisk lagring kunne for virksomhedernes vedkommende nok knyttes sammen med en obligatorisk, periodevis indberetning af hashværdier af lagret krypteret kommunikeret materiale uden menneskeretlige konsekvenser. Opgaven med at opbevare hashværdier kunne med fordel knyttes til en **uvildig tredjepart**, fx. et centralt nøglecenter (Certificating Authority), der som hovedopgave vil kunne have registrering og certificering af brugere samt evt. opbevaring af krypteringsnøgler. Beslaglæggelse efter retskendelse bør med en realisering af en sådan ordning kunne foretages hos CA'en, der følgelig vil være forpligtet til at udlevere bestemt materiale samt krypteringsnøgler.

Sammenfatning

Sammenfattende kan det konstateres, at det ud fra en menneskeretlig synsvinkel er problematisk at indføre et forbud mod kryptering. En ordning, hvorefter krypteringssystemernes underliggende algoritme kontrolleres af staten og der stilles krav om lagring af escrow-værdier er derimod mindre tvivlsom i menneskeretlig henseende. Det samme gælder indførelse af en regel om omvendt bevisbyrde i tilfælde, hvor en tiltalt ikke vil medvirke til dekryptering af beslaglagt krypteret materiale. Derimod synes der ikke at være menneskeretlige problemer forbundet med en ordning om obligatorisk lagring, herunder hos en uvildig tredjepart, for så vidt angår forretningsmæssig korrespondance. Tilsvarende vil indgreb i privat korrespondance i efterforskningsøjemed i form af beslaglæggelse af materiale samt krav om dekryptering antageligt ligge indenfor statens adgang til i konkrete tilfælde at tilsidesætte den konventionsbeskyttede ret til meddelelseshemmelighed.

Efterforskning af kriminalitet

Af Henning Thiesen [21]

Den legale situation

Indledningsvis skal det bemærkes, at der i Danmark ikke sondres mellem indgreb i meddelelseshemmeligheden foretaget af politiet og efterretningstjenesten, idet Politiets Efterretningstjeneste er en del af politiet og underlagt det samme regelsæt som det øvrige politi (retsplejelovens kapitel 71).

Rigspolitiet har i øvrigt bemærket, at et særligt afsnit (kapitel 2: Hvad siger loven?), hvor Rigspolitiet forudsætter, at regelsættet for (legale) indgreb i meddelelseshemmeligheden beskrives.

Rigspolitiet finder dog anledning til at anføre følgende:

Det nærmere indhold af retsplejelovens kapitel 71 skal ikke beskrives i dette notat, men det skal fremhæves, at aflytning alene kan foretages (legalt) af politiet som led i efterforskning af visse særlige alvorlige kriminalitetstyper, ligesom aflytning alene kan ske (legalt) i henhold til retskendelse. Hertil kommer, at de institutioner og selskaber (både offentlige og private), der beskæftiger sig med kommunikation, har pligt til at bistå politiet med udførelse af indgreb, jf. retsplejelovens §786, stk. 1, der har følgende ordlyd:

"Det påhviler post- og telegrafvæsnet, telefonselskaberne og andre tilsvarende offentlige og private virksomheder at bistå politiet ved gennemførelsen af indgreb i meddelelseshemmeligheden, herunder ved at etablere aflytning af telefonsamtaler m.v. ved at give de i §780, stk. 1 nr. 3, nævnte oplysninger

(teleoplysning) samt ved at tilbageholde og udlevere forsendelser m.v.".

Bestemmelsen i retsplejelovens §786, stk. 1 og øvrige bestemmelser i kapitel 71 regulerer ikke udtrykkeligt omkostningsspørgsmålet ved aflytninger. I praksis er omkostningsspørgsmålet ved traditionelle telefonaflytninger blevet løst således, at politiet har betalt de konkrete udgifter ved aflytningen, d.v.s. *dels* et fast beløb for etableringen - dækkende telefonmontørløn m.v. - samt *dels* de løbende udgifter forbundet ved at få telefontrafikken fra den aflyttede telefon bragt til politiets bygninger. Det er således uafklaret, om telefonselskaberne m.v. kan pålægges at afholde udgifter til indrettelse af deres telekommunikationssystemer, således at politiet kan foretage aflytning.

Det skal endvidere bemærkes, at Rigspolitiet er opmærksomme på, at et særligt udvalg [22] tidligere har overvejet, hvorvidt der var behov for at foretage lovmæssig regulering af kryptologi, f.eks. således, at der indføres offentlige "nøglecentre", hvorved offentlige myndigheder altid vil kunne få en "nøgle" til at dechifrere kryptograferede signaler. Dette udvalg nåede til den konklusion, at der ikke var behov for lovregulering af området. Det skal dog fremhæves, at politiet ikke var repræsenteret i dette udvalg, der muligvis ikke har været fuldt bekendt med der retshåndhævelsessynspunkter, der taler for tiltag, som kan bevare muligheden for reelt af foretage aflytning.

De praktiske problemer

Aflytning af det traditionelle (ledningsførte) telefonnet har i årtier været gennemført uden væsentlige praktiske problemer, idet der teknisk er tale om et forholdsvist simpelt indgreb, der rutinemæssigt foretages af telefonselskaberne, således, at disse sørger for, at politiet parallelt med vedkommende telefonabonnement får adgang til telefontrafikken.

Rigspolitiet har fra slutningen af 1980'erne været opmærksomme på, at nye former for telekommunikation systemmæssigt er konstrueret således, at aflytning teknisk er vanskeligt, ligesom kryptograferingsudstyr af høj kvalitet inden for de seneste år er blevet meget billigt og let tilgængeligt, hvorved politiet nok kan aflytte det transmitterede (kryptograferede) signal, men ikke dechifrere dette.

Disse problemstillinger har konkretiseret sig i relation til GSM-mobiltelefonnettet, idet politiet rent praktisk ikke for tiden kan aflytte dette mobiltelefonnet, da de tekniske specifikationer for GSM netop er udviklet bla. med det formål at undgå (uautoriseret) aflytning.

Politiet har inden for de seneste år i forbindelse med efterforskning konstateret, at mistænkte - som befolkningen i almindelighed - i stærkt stigende omfang benytter mobiltelefoner, herunder GSM-telefoner. Dette forhold udgør dagligt en væsentlig hindring i efterforskningsarbejdet, hvilket skal ses i sammenhæng med, at kriminelle kredse er fuldt bevidste om det forhold, at politiet ikke - eller kun meget vanskeligt - kan aflytte mobiltelefonsamtaler.

Rigspolitiet er af den opfattelse, at kriminelle kredse også vil anvende andre former for aflytningssikrede kommunikationssystemer, når disse er tilgængelige. I begrænset omfang har politiet allerede konstateret kryptograferet datatransmission mellem mistænkte.

Politimæssige overvejelser

Ud fra en politimæssig vurdering må det anses for absolut påkrævet, at politiet fortsat kan aflytte telekommunikation.

Rigspolitiet er bekendt med, at modstående interesser - specielt kommercielle inden for telekommunikationsbranchen - taler for ikke at indbygge aflytningsfaciliteter i de nye telekommunikationsnet og regulere anvendelsen af kryptologi. Rigspolitiet finder imidlertid, at det ud fra en samfundsmæssig helhedsbetragtning må anses for nødvendigt, at politiet bevarer muligheden for at foretage aflytning m.v. i relation til telekommunikation.

Rigspolitiet er af den bestemte opfattelse, at aflytning af telekommunikation er et meget betydningsfuldt - og ofte et helt afgørende - redskab ved efterforskning af alvorlig kriminalitet, herunder særligt narkotikakriminalitet og de forbrydelser, der er nævnt i straffelovens kapitel 12 og 13 (bla. spionage og terrorisme), samt andre former for organiseret kriminalitet.

Organiseret kriminalitet er bla. karakteriseret ved, at den kriminelle adfærd er grundigt planlagt og forudsætter medvirken af flere gerningsmænd, som særligt i planlægningsfasen har et stort kommunikationsbehov. Aflytning af telekommunikation er derfor et velegnet efterforskningsskridt i sager angående organiseret kriminalitet.

Hertil kommer, at båndoptagelser af samtaler og teleoplysninger, jf. retsplejelovens §280, stk. 1 nr. 3, samt andre resultater af indgreb i meddelelseshemmeligheden, kan tjene som bevis midler af objektiv karakter, hvilket - også henset til, at det i sådanne sagstyper, hvor frygt for repressalier er udbredt, ofte er vanskeligt at fremskaffe vidner - må anses for uhyre vigtigt.

Politiet foretager i dag relativt hyppigt aflytning, som led i efterforskningen af bla. narkotikakriminalitet. Det er den generelle opfattelse, at aflytning er et meget værdifuldt efterforskningsmiddel, idet blot det forhold at konstatere kontakt mellem to mistænkte personer kan være af afgørende betydning.

Af de ovennævnte grunde tillægger Rigspolitiet det derfor stor betydning, at politiet fortsat får mulighed for i praksis at foretage aflytning af telekommunikation. Det må herved fremhæves, at der ikke er tale om at tillægge politiet mulighed for at gennemføre nye former for strafprocessuelle tvangsindgreb, men alene spørgsmål om gennemførelse af foranstaltninger til at bevare eksisterende muligheder.

Alternativet til (passivt) at opgive aflytning, som et efterforskningsredskab, er ikke at undlade at efterforske de alvorlige former for kriminalitet, som i henhold til retsplejelovens kapitel 71 kan danne basis for aflytning. Dette ville efter Rigspolitiets opfattelse være samfundsmæssigt uacceptabelt. Derimod må politiet i givet fald foretage andre - typisk mindre effektive - for efterforskning, der *enten* vil være mere ressourcekrævende, f.eks. observationer ("skygninger") *eller* være mere indgribende i forhold til den individuelle retssikkerhed, f.eks. rumaflytninger og anvendelse af agenter.

Produkter og eksport

Af Steffen Stripp

Det har været ganske markant at industrien i USA har mødt den amerikanske regerings Clipper-udspil med betydelig skeptisk. En af bekymringerne har været, at sammenhængen mellem en regeringskontrolleret kryptering og de amerikanske eksportkontrol love vil forringe amerikansk computer-industris konkurrence muligheder.

Op til G-7 landenes møde om informationssamfundet den 25. og 26. februar 1995 formulerede tre

internationale industriorganisationer deres synspunkter [23]. The European Association of Manufactures og Business Machines and Information Technology Industry (EUROBIT), the Information Technology Industry Council (ITI), og the Japan Electronic Industry Development Association (JEIDA) udtalte:

- We want governments to recognize that their explicit support for the Global Information Infrastructure necessarily entails implicit support for the general use of cryptographic technology. Without pervasive cryptographic technology there can be no basis for privacy or trust, and main benefits of the new industrial revolution cannot be realized. If the Information Society is to develop, public policy must reflect the fact that this technology will be used everywhere. Cryptografphy is essential both to the confidentiality of information and to information integrity, including proof of correctness and electronic signatures...

- We do of course recognize the legitimate needs of national authorities to enforce the rule of law, and to maintain national security, but individuals and businesses have needs too - the need for privacy, and the need to operate on a basis of trust - and unless those needs are met the Information Society may not happen.

The organizations made the following recommendations:

* That goverments, industry and users must agree on the cryptographic techniques to be used in the Global Information Infrastructure and on the procedure for verifying that products conform to the techniques so agreed;

* That the agreed techniques and the agreed verification procedures must be made public;

* That the agreed techniques must be based on private sector led, voluntary consensus international standards;

* That products implementing the agreed techniques should not be subject to import controls, restrictions on use within the law, or restrictive licensing;

* That products implementing the agreed techniques should be exportable to all countries, except those which are subject og UN embargo; and

* That users and suppliers of products implementing the agreed techniques should be free to make technical and economic choices about modes of implementation and operation, including a choice between implementation in hardware or software where relevant.

Den særlige Information Technology Steering Committee (ITSTC), som er fælles for alle tre europæiske standardiserings organisationer, CEN, CENELEC og ETSI, har set på hvilke sikkerhedskrav, der findes indenfor de "10 applikationer, der skal bane vejen for informationssamfundet" Bangemann rapporten[24] pegede på. I et notat [25] fra en række workshops om hver applikation hedder det bla. "CONFIDENTIALITY was found essential for many areas, e.g. Electronic Tendering, Teleworking, Healthcare (as a consequence techniques for legal interception have to be aggreed upon)", men man peger på "Issues that cannot be resolved by the standardisation bodies themselves include" bl.a. "a European approach to the issue of encipherment and legal interception".

Dansk industri har tilsyneladende endnu ikke klargjort sine positioner. Men det er værd at fremhæve at JTAS og Datalogisk Afdeling ved Aarhus Universitet har gjort en "forrygende flot opfindelse, som kan komme til at sætte sit præg på vores datasikkerhed - ikke blot i Danmark, men over hele verden"[26]. Der er tale om en chip, som kan kryptere med anvendelse af RSA-algoritmen. Det banebrydende består i, at man normalt går ud fra at RSA-kryptering er for langsom til at kryptere datastrømme og at denne kryptering derfor må ske med andre algoritmer. Tele Danmark redegør nedenfor nærmere for denne

RSA-krypteringskreds. Sikkerhedsbladet afslutter sin omtale med at håbe, at det bliver "en kommerciel succes, og ikke blot en skuffe-opfindelse. Der er behov for den alle vegne i vores informationssamfund".

Tele Danmarks RSA-krypteringskreds

Generel beskrivelse

Udviklingsafdelingen ved Tele Danmark/Jydsk Telefon har i samarbejde med Datalogisk Afdeling på Aarhus Universitet som de første i verden udviklet en enkelt kreds, der kan kryptere efter RSA algoritmen med en 561 bits krypteringsnøgle ved en transmissionshastighed på 64kbits/s.

RSA-kredsen har en størrelse, der gør det muligt at bygge den ind i enhver form for kommunikationsudstyr. Den foreligger i dag som prototype og er afprøvet med tilfredsstillende resultat. Den kan anvendes, som den foreligger. Det er dog sandsynligt, at den skal forsynes med et af køberen specificeret interface.

Tele Danmark har besluttet ikke at gå ind som producent i terminalmarkedet, hvor RSA kryptering anvendes. Den udviklede kreds passer således ikke ind i Tele Danmarks udbud af tjenester. Tele Danmark vil derfor sælge rettighederne til RSA kredsen til en interesseret producent af kommunikationsudstyr eller en producent af integrerede kredse i silicium.

Tele Danmark vil være i stand til at redesigne kredsen med anvendelse af en videreudviklet realiseringsmetode og en mindre procesteknologi, så kredsen bliver 5 gange hurtigere og halvt så stor.

Anvendelsesmuligheder

RSA-kredsen kan anvendes i civile- og militære kommunikationsudstyr, hvor man ønsker at forhindre, at data i form af tale, tekst, billeder eller økonomiske oplysninger kan aflyttes eller modificeres af uvedkommende under den elektroniske overførsel fra sted til sted.

Anvendelsesområder:

* Krypteringssystemer med offentlig nøgle

* Sikring af bank-, forretnings- og kurtagetransaktioner

* Sikring af transmission i både pakke- og kredsløbskoblede net

* Sikring af tale- og datatransmission på ISDN i reel tid

* Digital underskrift

Sikkerhed

Ved elektronisk overførsel af penge, fortrolige tegninger, fortrolige data, eller fortrolige samtaler anvendes kryptering, og man er selvsagt interesseret i en så høj grad af sikkerhed som overhovedet muligt.

RSA-kredsen krypterer med nøgler på 561 bit, og det er nøglens længde, der bestemmer, hvor lang tid det vil tage for f.eks. en hacker at bryde koden. Hvis man forsøger, vil dermed verdens hurtigste datamater tage flere millioner år.

En RSA kreds kan benyttes til kryptering af data, hvor afsenderen skal kunne identificeres med samme retsgyldige sikkerhed som ved en traditionel underskrift.

Kredsen kan således anvendes til hemmeligholdelse og integritet af data samt til digital underskrift.

Tele Danmark

En dansk krypto-politik

Spørgsmål og valgmuligheder

Af Steffen Stripp

I dette afsluttende bidrag sammenfattes det grundlag for en dansk krypto-politik, som er fremlagt i de foregående afsnit, i en række valgmuligheder. Det er ganske klart, at der ikke er et enkelt svar på hvordan fortroligheden skal sikres. Derfor opstilles en række valgmuligheder, som kan indgå i svaret. Spørgsmål og svar i dette kapitel er ikke et "beslutningstræ" med en logisk og ordnet rækkefølge, hvor man kan tage stilling undervejs og ende med en konklusion. Faktisk kan valgene ses i forskellige sammenhænge. Med opdelingen i en række afsnit er det alligevel forsøgt at give en vis struktur for diskussionen og i et afsluttende afsnit samles valgmulighederne i et oplæg til en dansk krypto-politik.

Selv om vi diskuterer en informations- og kommunikationsteknologi løsning er udgangspunktet ikke forskellige tekniske løsninger, men de krav der kan stilles til den tekniske løsning. Der er derfor heller ikke et valg mellem forskellige krypterings-algoritmer.

En krypto-politik drejer sig om hvordan digitale informationer skal hemmeligholdes. Der kan være tale om en telefonsamtale over ISDN-nettet, eller om forskellige former for elektronisk post (datakommunikation) hvor fortroligheden skal sikres under transmissionen, eller om lagrede digitale data i f.eks. e-postkasser og på disketter hjemme eller i virksomheden. Det er i alle tilfælde det samme problem og den samme teknik der kan anvendes. Men det er ikke givet at det er samme krypto-system, som skal udvikles for de tre anvendelser. Denne opdeling vil kun indgå i mindre omfang i de følgende afsnit, men vil blive taget op i kapitlets afsluttende afsnit.

Er der overhovedet et problem?

Det første spørgsmål man må stille er vel om der overhovedet er et problem som kræver en løsning.

Valg 1: Intet behov for kryptering

Det er en almindelig forventning at elektronisk kommunikation til forskellige anvendelser vil være stigende i de kommende år. Men som Leif Nielsen, Tele Danmark redegør for i kapitel 4 er transmission i nettet ikke uden sikkerhed, idet selve transmissionssystemet giver en betydelig sikkerhed mod uautoriseret aflytning og medarbejdere, som har adgang til de steder på nettet, hvor aflytning kan foretages har tavshedspligt. Man kan vælge at betragte denne sikkerhed som en tilstrækkelig basissikkerhed for almindelig kommunikation.

Dette synspunkt rejser dog en række problemer. For det første anvendes kryptering til hemmeligholdelse af kommunikation som involverer penge, f.eks. er datatransmissioner når Dankortet anvendes krypteret. Når sådanne transaktioner bliver almindelig i åbne net vil der så ikke være samme behov? Med udbredelse af elektronisk kommunikation vil stadig flere og herunder også borgerne kommunikere private og følsomme

oplysninger, vil transmissions-systemets sikkerhed være tilstrækkelig?. Endelig er der mere principielle synspunkter om at vi bla. af hensyn til privat livets fred ikke skal kommunikere på "åbne postkort", men bør have en højere grad af sikkerhed for at kommunikationen er privat. Det kan ses som en uundgåelig følge af info-samfundet, at der skabes krypto-systemer, som sikrer fortroligheden i den elektroniske kommunikation.

Den simple løsning

Der er i spørgsmålet om fortrolighed to modstående hensyn. På den ene side borgernes krav om privatlivets fred og fortrolighed i kommunikationen og på den anden myndighedernes ønske om i visse situationer at kunne bryde meddelelseshemmeligheden. Med udgangspunkt i sådanne modstående hensyn er det en nærliggende mulighed at vælge en simpel løsning: ensidigt at tilgodese det ene eller det andet hensyn.

Valg 2: Forbud mod kryptering med mindre der er givet tilladelse

En i og for sig enkel løsning. Kryptering af kommunikation spredes ikke ud i samfundet og myndighedernes behov for i efterforskning m.v. at kunne lytte med er fuldt tilgodeset. Der kan gives tilladelse til kryptering i situationer, hvor der er behov og hvor krypteringsanvendelsen kan kontrolleres. Set i forlængelse af valg 1 ovenfor kan almindelige behov for fortrolighed anses for tilgodeset i transmissions-nettets opbygning. Et sådant forbud findes i Frankrig og er overvejet i andre europæiske lande.

Valget er forbundet med forskellige problemer. Et forbud må anses for at være i strid med den Europæiske Menneskerettighedskonvention og vil derfor næppe kunne opretholdes.

Med et forbud må man forvente, at der vil blive givet tilladelse til anvendelse af kryptering i en række erhvervsmæssige sammenhænge og til kommunikation mellem myndigheder. En udvikling, hvor krypto-systemer efterhånden bliver en anvendt teknologi, men ikke må benyttes af befolkningen, forekommer i strid med demokratiske traditioner. Videre vil der opstå det praktiske problem, at forbudet ikke kan kontrolleres og håndhæves. Det er ikke muligt generelt i transmissionsnettet, at kontrollere om datastrømmen er krypteret eller i klartekst. Konsekvensen kan derfor blive at almindelige borgere ikke selv sikrer fortroligheden, med risiko for af deres kommunikation afsløres af kriminelle, mens kriminelle krypterer deres kommunikation. Det kan man så selvfølgelig straffe dem for, men straffen for at bryde krypteringsforbudet, må antages at være mildere og kun ramme de umiddelbart implicerede og derfor være klart attraktivt for den organiserede kriminalitet.

Valg 3: Intet behov for myndighedsinitiativ

Den nuværende retstilling, som den er beskrevet i kapitel 2, bevares. Borgere, virksomheder og andre kan iværksætte de krypto-systemer de finder nødvendige for at hemmeligholde deres digitale informationer. I den udstrækning det giver problemer for f.eks. politiet er det opgaven her at finde midler som kan sikre, at

den nødvendige efterforskning kan finde sted ved at bryder krypteringen eller (mere sandsynligt) at anvende andre efterforskningsmetoder. Dette synspunkt kan suppleres med den vurdering, at aflytning samlet set kun spiller en lille rolle i efterforskningsarbejdet.

Uden myndighedsinitiativ vil kryptering blive spredt af markedskræfterne. Krypto-systemer vil blive taget i anvendelse af borgerne efterhånden som de føler et behov og i takt med at der udbydes produkter. Set fra interessen i at bevare muligheden for at bryde meddelelseshemmeligheden kan en sådan udvikling ses som positiv, da en langsom spredning vil give politimyndighederne de bedste muligheder for at udvikle passende modtræk. Samtidig kan en markedsudvikling betyde, at det til stadighed vil være relativ kompliceret at sikre fortroligheden specielt som følge af de organisatoriske problemer med nøgleudveksling. Udbredelsen kan dog få et meget hurtigere forløb, hvis centrale softwareudbydere og/eller informations-serviceudbydere enes om et krypto-system (en defacto standard) i deres produkter.

Infrastruktur

Det kan anses for en samfundsopgave at sikre en generel løsning for tilvejebringelse af fortrolighed i den elektroniske kommunikation. Et generelt tilgængeligt krypto-system kan anses for en infrastruktur på "informations vejene".

Valg 4: Statslig initiativ til et tilbud om fortrolighed med kryptering

Tilvejebringelse af sikkerhed omkring informations- og kommunikationsteknologien kan anses for en samfundsopgave på linje med behandling af trafiksikkerhed på almindelige veje. For en åben kommunikation er det helt afgørende med tekniske standarder for krypto-systemet, som fastlægger valg af krypterings-teknik (algoritme), nøgleudveksling, protokoller osv. Dette synspunkt fremføres netop i den udtalelse, som blev citeret i kapitel 8, fra en række internationale industriorganisationer.

En fornøden edb-sikkerhed er en forudsætning for at opnå et robust samfund i forhold til de sårbarheder, der kommer sammen med forandringen af samfundet i retning af et info-samfund. Behovet for en infrastruktur kan også ses som en konsekvens af, at fortroligheden er en grundlæggende rettighed, som staten er forpligtiget til at sikre. Det kan videre vurderes, at en infrastruktur løsning samfundsøkonomisk vil være attraktiv, da man kan opnå besparelser ved at koncentrere udvikling og drift. Videre vil en infrastruktur være med til at udbrede anvendelse af elektronisk kommunikation, da det vil være vanskeligt for den enkelte serviceudbyder eller organisation at tilvejebringe dette sikkerhedselement uden etablerede standarder.

Et sådant statsligt initiativ må omhandle såvel telefonsamtaler, elektronisk post og opbevarede digitale informationer. Men det er ikke givet at der er bør blive tale om et og samme krypto-system.

Etablering af en infrastruktur kan imidlertid ses som en ganske anden sag end accept af, at der på markedsvilkår udvikler sig forskellige løsninger for fortrolighed. Man kan sige at myndighederne kan acceptere, at kryptering anvendes, men det kan ikke være statens opgave at udstyre alle - inkl. den organiserede kriminalitet - med denne mulighed.

Kontrol med kommunikationen

En udløber af problemerne med at sikre såvel fortrolig kommunikation og muligheder for at bryde meddelelseshemmeligheden er overvejelser om at opnå en vis kontrol med kommunikationen. Det er ikke tanken, at man skal styre hvem der kommunikerer sammen eller at al kommunikation skal aflyttes.

Den kontrol man kan overveje handler om at kunne sikre at et givent - typisk et af myndighederne fastlagt - krypto-system anvendes.

Valg 5: Kontrol med anvendt krypto-system

Hvis man har et udbredt krypto-system, som man har besluttet afbalancerer borgernes krav på fortrolighed og myndighedernes behov for at bryde fortroligheden i efterforskning, kunne det være en oplagt konsekvens, at man vil kontrollere at dette system anvendes.

Problemerne her befinder sig på to planer. For det første om det er acceptabelt at etablere generelle overvågningssystemer. Selvom det ikke etableres for at gennemføre en generel overvågning vil det indebære en risiko for misbrug, som det meget nøje må overvejes om man vil skabe.

For det andet må man konstatere, at det næppe vil være muligt, at opbygge et overvågningssystem, som vil være i stand til automatisk og tidstro, at afsløre kommunikation, som er krypteret med en ikke tilladt kryptering.

Hvem skal have nøglen?

Centralt i diskussionen om hvordan en løsning for fortrolighed skal udformes er, hvem skal have kontrol med og adgang til de "nøgler", som kan dekryptere den digitale information. Vi skal her fremlægge tre valgmuligheder: udelukkende ejeren, nøglecenter med myndighedsadgang og nøglecenter med indehaver adgang. Et nøglecenter er en Trusted Third Party (TTP), en betroet trejdepart som indgår i løsningen som systemansvarlig, medvirker til udveksling af nøgler, udsteder certifikat for "nøglers" indehaver og evt. opbevarer af private nøgler.

Valg 6: Private nøgle udelukkende hos 'ejeren

Nøglen som kan dekryptere informationen findes udelukkende hos ejeren, som f.eks. kan opbevare den på computerens harddisk, på et ic-kort eller på en smart-diskette.

Denne løsning imødekommer borgernes krav om kontrol med fortroligheden, men udelukker at myndighederne kan læse kommunikationen uden personens viden. Myndighederne vil kunne lagre informationerne, men kan ikke sikres adgang til senere dekryptering, hvis borgeren nægter at udlevere

nøglen eller har mistet denne.

Valg 7: Nøglen opbevares hos nøglecenter med myndigheds adgang

Krypto-systemet opbygges så nøglen opbevares hos et nøglecenter. Myndigheden har mulighed for efter en retskendelse at få denne udleveret til at bryde meddelelseshemmeligheden. Et sådan krypto-system kan tilbyde borgerne en lettilgængelig sikring af fortrolighed med digitale informationer, samtidig med at politiets muligheder for efterforskning bevares.

Svagheder i denne løsning er, at det er muligt at kryptere med en anden kryptering enten selvstændigt eller før kryptering med denne løsning. Derfor vil også en kontrol af om krypteringen er anvendt kunne omgås. Som diskussionen allerede har vist er det muligt, at løsningen ikke vil kunne få almindelig accept, og derfor vil der så alligevel kunne komme en systematisk udbredelse af alternative krypto-systemer.

Valg 8: Nøgle opbevares hos nøglecenter, men kun ejeren har adgang

En tredje mulighed er, at nøglecenteret har en backup som kun ejeren kan give adgang til. En sådan løsning kunne f.eks. etableres ved at nøglecenteret udleverer nøglen på et ic-kort og samtidig danner et backup kort som TTP opbevarer. Begge kort, men i denne sammenhæng specielt backup-kortet, kunne beskyttes med en biokode som kortindehaver identifikation. Dermed sikres at nøglen findes, og at det f.eks. er muligt at anvende den til dekryptering af en kommunikation politiet har lagret, men kun med ejerens accept.

Problemet med denne opbevaring af nøglen er om den i tilstrækkelig grad tilgodeser interessen i at kunne bryde meddelelseshemmeligheden.

Det må endvidere belyses om borgerne reelt er sikret mod misbrug. Vil det være muligt for myndighederne at omgå systemet ved at indlæse værdier for biokoden (f.eks. fingeraftryk) eller møde op med kopi heraf? Hvis det er muligt vil det så være tilstrækkeligt med et udtrykkelig forbud mod at nøglecenteret - som jo er betroet - medvirker hertil?

Retlige elementer

Et krypto-system indeholder en række retlige elementer. Her fremlægges først nogle overvejelser ændringer af retsplejen og dernæst peges på spørgsmålet om organiseringen af nøglecentre.

Da kryptering er tilladt og kan give vanskeligheder i politiets efterforskning kan det overvejes om der bør gennemføres ændringer af retsplejelovgivningen.

Valg 9: Ændring af retsplejen

Det er foreslået [27], at man overvejer, at se på muligheder for at håndtere den krypterede information fra politi og domstole i stedet for at fokusere på muligheden for altid at kunne dekryptere informationen.

En mulighed er at omlægge bevisbyrden, hvis der foreligger en bestyrket mistanke, som kan blive be- eller afkræfter af en krypteret information. Hvis den sigtede nægter at udlevere en nøgle han er i besiddelse kunne domstolene få mulighed for at flytte bevisbyrden over på den sigtede med den konsekvens at, at det nu er op til sigtede at modbevise, at de krypterede informationer ikke belaster ham. Problemet med forslaget er, at det bryder med de grundlæggende principper i retsplejen, at en sigtet ikke skal tilvejebringe materiale mod sig selv, og at man er uskyldig indtil det modsatte er bevist. En mindre radikal mulighed er at udnytte domstolenes mulighed for at vurdere den samlede bevisførelse. Domstolene kan lade det belaste en sigtet, hvis han afviser at medvirke til en dekryptering, som han faktisk har mulighed for. Det er op til dommerne at vurdere om han faktisk har denne mulighed, lige som de må vurdere andre udsagn fra en sigtet. En sådan bevisførelse kan ske uden lovændringer, eftersom dansk bevisret bygger på fleksible og generelle regler. Det kan således siges, at retspraksis må udvikle sig i takt med krypterede informationer begynder at dukke op i retssager. Der er i denne udvikling en risiko for at der vil ske en glidende udvikling så der reelt bliver tale om omvendt bevisbyrde for at hindre at kriminelle dækker sig ind under mængder af krypterede informationer.

I forlængelse af dette forslag kan der indføres en ret for politiet til at lagre krypterede informationer på tidspunkter, hvor der i dag er adgang til at bryde meddelelseshemmeligheden. Et problem med dette forslag er, at man hos netoperatører og andre nødvendigvis må opbygge et system til tapning af kommunikation og data, der indebærer en risiko for misbrug til udbredt overvågning.

Da netop strafferetspleje er helt afgørende for retssikkerheden i et demokratisk samfund bør det overvejes at gennemføre et udvalgsarbejde forud for evt. lovændring.

Valg 10: Offentlig eller privat nøglecenter

Såfremt krypto-systemet indebærer et nøglecenter (Trusted Third Party) bliver det nødvendig at tage stilling til om det skal være offentlig eller privat. Der må videre tages stilling om der skal kunne være både et offentlig og flere private nøglecentre. Det må antages at et offentlig nøglecenter er reguleret ved lovgivning, men det er nødvendigt at tage stilling til om private nøglecentre skal reguleres ved lovgivning, certifisering eller slet ikke.

Nøglecentre vil spille en helt afgørende rolle i et krypto-system og tilliden til systemet vil være helt afhængig af at det er en betroet trejdepart. Det vil derfor være naturligt, at nøglecentre er reguleret ved lovgivning og underkastet et uafhængigt tilsyn. Såfremt der findes en række private nøglecentre, som

brugere kan vælge imellem, kan troværdigheds problemet siges at blive løst af markedsmekanismen.

Teknisk element

Den tekniske udformning af et krypto-system må naturligvis følge af de krav til og betingelser for systemet, som opstilles i krypto-politikken.

Valg 11: Kendt og analyseret teknisk løsning

På grund af det afsæt debatten har fået i den amerikanske krypto-politik med en løsning, som bygger på en algoritme (Skipjack), der ikke er offentliggjort, og som kun leveres i en chip, kan det være rimeligt på et tidligt tidspunkt at tage stilling til dette spørgsmål om i den tekniske løsning.

Et krav baseret på almindelig faglige standarder vil være, at den tekniske løsning er offentlig kendt og bygger på internationale standarder. Løsningen skal kunne vurderes frit af eksperter med alle synspunkter.

Escrow løsningen er en ny teknisk løsning i krypto-systemer og der bør derfor gennemføres analyserer heraf *før* den evt. tages i anvendelse.

Dansk - Europæisk - International løsning

En af informations- og kommunikationsteknologiens muligheder omtales som en global kortslutning, der åbner for en kommunikation uafhængig af tid og sted. Visionen for fremtidens kommunikation er global.

Valg 12: Krypto-systemet skal være europæisk og helst internationalt

Det vil derfor være naturligt at søge internationale løsninger. Men realiteterne er, at en international løsning sandsynligvis ikke er mulig inden for en nærmere fremtid. Der er ikke meget som tyder på at EU-landene kan finde en fælles holdning og i det internationale standardiserings-arbejde er det reelt ikke muligt overhovedet at behandle kryptering med henblik på hemmeligholdelse.

Det behøver ikke betyde at kommunikation internationalt ikke kan beskyttes med kryptering. Programmet "Pretty Good Privacy" er et eksempel på en de facto standard som udbredes via Internettet, og som må forventes at få stigende betydning med mindre det hindres ved forbud og eksporthindringer.

Valg 13: Etablering af et dansk krypto-system

Fremfor at afvente en EU/international udvikling kan man der søges etableret en dansk løsning. Et dansk krypto-system kunne bygge på den tradition for samlede løsninger som kendes fra finansverdenen med Dankort og Telesec. Et led i krypto-systemet kunne være et ic-kort med de nødvendige krypterings-nøgler udstedt af det offentlige eller af private nøglecentre.

Et dansk krypto-system kunne blive en udvikling af danske produkter, såvel hardware som software. I Danmark har pengeinstitutterne udviklet Telesec til digital underskrift og Tele Danmark har udviklet specifikationer for en RSA-chip, der kan indgå i en løsning. En sådan udvikling vil kunne give eksportmuligheder og arbejdspladser.

Dernæst bør det overvejes om sikring af fortrolighed ikke er et så væsentlig element i udviklingen af et dansk info-samfund i fortroppen, at det simpelthen er et led en strategi herfor at der dannes en dansk krypto-løsning.

Etablering af en dansk løsning kan ses som udnyttelse af disse muligheder fremfor at afvente evt. beslutninger i EU og internationalt.

Vanskeligheden med en dansk løsning er umiddelbart, hvordan den skal udformes, hvem skal træffe beslutninger herom og hvem skal udføre den i praksis.

Et næste problem er om løsningen vil kunne fungere i EU/internationalt. Det er næppe muligt at give en forudsigelse heraf. Ved at træffe systemvalg, der i så høj grad som muligt bygger på internationale standarder kombineret med en aktiv dansk deltagelse i standardiseringsarbejdet, kan man fremme at det danske krypto-system bliver en del af et internationalt system.

Opsamling

Der er en generel enighed om, at der er behov for krypto-systemer, som kan sikre fortrolighed for digitale data i kommunikation og datalagre. De teknologier som skal anvendes findes og derfor skulle det i og for sig blot dreje sig om at komme i gang. Men på grund af frygten for, at politi og efterretningstjenester vil miste vigtige muligheder i deres virksomhed er vi endt med noget der har karakter af en gordisk knude. Der findes ganske enkelt ikke én enkel løsning, som uden at skabe ny problemer, kan hugge knuden over og tilfredsstille de forskellige hensyn. Hvis man ikke vil overlade den nærmere udformning af krypto-systemet enten til markedskræfterne eller til beslutninger i internationale fora uden klare danske holdninger vil det være nødvendigt med en snarlig fastlæggelse af en dansk krypto-politik.

Det er næppe muligt at indføre et forbud mod kryptering. For det første vil det være i strid med principper i de grundlæggende rettigheder om privatlivets fred, brevhemmelighed o.l., og derfor antagelig også i strid med den Europæiske Menneskerettighedskonvention. For det andet er det ikke praktisk muligt at hindre, at krypterings-programmer er tilgængelige og anvendes, og kontrollere om kryptering benyttes - i hvert fald ikke uden end en meget omfattende kontrol og overvågningsindsats, der ikke kan anses for acceptabel i et demokratisk land.

Hvis man politisk vil lægge rammerne for et dansk krypto-system, bla. fordi der er behov for en

sikkerheds-infrastruktur på "informationshoved- og bivejene" er det nødvendigt, at tage politisk stilling til de valg, som er fremlagt i de foregående afsnit.

Det vil her være hensigtsmæssigt at skelne mellem telefonsamtaler og elektronisk post og datalagre. Telefonen er en velkendt teknologi, hvor spillereglerne er indarbejdet og som fungere selvstændigt. Om denne skelnen vil være lige så klar i fremtiden er ikke sikkert, hvis telefonen så at sige "smelter sammen med" computeren. Sker dette må det forventes at det bliver computerens muligheder og regler, der overtager pladsen også for telefonen.

Da et krypto-system vedrører et centralt og følsomt emne for den enkelte og samfundet som helhed, nemlig privatlivets fred må det være et centralt mål, at der findes en udbredt konsensus i befolkningen om et sådant system. Der er da heller ikke nogen gevinst ved at søge at indføre sikkerhedsforanstaltninger, som ikke har bred opbakning, da de i den situation ikke vil kunne fungere. Endvidere vil et krypto-system, som ikke har opbakning, blive erstattet af alternative krypto-systemer til skade bla. for ønsket om en generel infrastruktur.

På grundlag af John Rawls teori om retfærdighed kan der opstilles tre principper for edb-systemer [28]:

- *De svageste.* Forøg ikke ulemper eller skadevirkning for de svage grupper som systemet vedrører.

- *Skaderisiko.* Risiker ikke at forøge ulemper og skadevirkning i allerede risikofyldte miljøer.

- *Offentlighedstest.* Anvend en offentlighedstest, dvs. kan beslutningen forsvares for en informeret offentlighed, i vanskelige eller umulige cost-benefit opgørelser.

Det er min opfattelse, at for telefonsamtaler vil et krypto-system, hvor myndighederne har adgang til nøglen efter en retskendelse, kunne accepteres. Dette system kan indføres efterhånden som den enkelte telefonabonnent vælger at gøre det ved at anskaffe det fornødne udstyr. I forhold til de tre principper øges ulemper og skadevirkninger ikke og der er ikke tale om at svage gruppers situation forringes. Endelig indebærer dette system ingen ændring i forhold til situationen i dag, hvor telefonsamtaler enkelt kan aflyttes. Det må antages at være almindelig kendt og den enkelte indretter sig på situationen i dagligdagen. Offentlighedstesten forudsiger dermed, at der kan skabes konsensus om et sådant system.

Anvendelse af elektronisk post i bred forstand og en mere udbredt opbevaring af information elektronisk er en nyere udvikling, som i disse år skal finde sin form. Spørgsmålet om fortrolighed opstår netop som en følge af denne udvikling, og ses en forudsætning for at mulighederne kan udnyttes. Der er således tale om en væsentlig forskellig problemstilling i forhold til telefonsystemets udvikling.

Der kan på grundlag af de nævnte Rawl-baserede principper peges på en række alvorlige kritikpunkter af et krypto-system med aflytning.

Princippet om de svageste bliver brudt, fordi stærke grupper (organisationer, virksomheder, enkeltpersoner) med resurcer og viden kan vælge at anvende alternative krypteringer og dermed undgå aflytningen, hvis de opfatter den mulighed som en trussel.

Princippet om skaderisiko bliver brudt, fordi der indbygges en risiko i det der netop er en sikkerhedsforanstaltning. En sådan konstruktion er principielt kritisabel. Hvis der dernæst gennemføres forskellige kontroller med om krypto-systemet benyttes indføres yderligere risici, som alene er en følge af krypto-systemet.

Om princippet om offentlighedstest kan opfyldes er tvivlsomt. Vil tanken om at indrette samfundets teknologier, så der er indbygget muligheder for kontrol med borgerne kunne opnå bred konsensus? Vil et sådan krypto-system kunne skabe den troværdighed som er nødvendig for at elektronisk kommunikation kan

udbredes til f.eks. varekøb og betalinger, udveksling af følsomme personoplysninger og handelsaftaler?

Det er min opfattelse, at for disse digitale informationer bør der ikke etableres et krypto-system, som har indbygget myndighedsadgang til nøglerne og dermed mulighed for aflytning. Tværtimod bør et krypto-system opbygges så det giver maksimal troværdighed, og det vil sige med fuld kontrol over fortroligheden for den enkelte.

Ordliste

Baud

En måleenhed for datatransmissionshastigheder, der udtrykker det maksimale antal signaler pr. sekund på linjen. Baud kan være identisk med bit/s, men vil oftest være forskellig, da der overføres flere bit med hver signal. Baud udtales "bo".

Bit

Forkortelse for binary digit. Anvendes nu som selvstændigt ord for de binære cifre nul og en.

Bit/s

Bit pr. sekund. Forkortes BPS. En måleenhed for datatransmissionshastighed. Et modem på en pc kan f.eks. overføre data med hastigheder fra 300 bit/s til

19.900 bit/s. ISDN-nettet har en hastighed på 64kbit/s og højhastighedsnet 2Mbit/s. Hvor kbit står for kilobit, dvs. 1000 bit og M står får megabit, dvs. en million bit.

Byte

Det antal bit, som netop indeholder et tegn, f.eks. et bogstav. Består i ASCII tegnsættet af 8 bit.

Capstone

Navn på en chip, som kan udføre kryptering efter Escrow Encryption Standard til anvendelse ved datatransmission mellem computere.

Chiffertekst

Betegnelse der anvendes i forbindelse med kryptering for teksten (data, dokument osv.) efter krypteringen og dermed ulæselig.

Clipper

Navn på en chip, som kan udføre kryptering efter Escrow Encryption Standard til indbygning i digitale telefoner.

Datapost400

Navnet på en Tele Danmarks tjeneste til bla. elektronisk post. Datapost400 er baseret på den internationale kommunikationsstandard X.400

Datatransmission

Den fysiske transport af data mellem sender og modtager. Synonymt anvendes ofte datakommunikation. Kommunikation anvendes også om både den fysiske transport af data og de processer, som etableres for at udnytte denne transport.

Datel

Navnet på Tele Danmarks tjeneste for datatransmission over telefonnettet

Datex

Navnet på Tele Danmarks kredsløbskoblede net til datatransmission. Kredsløbskoblede net er en teknik, hvor der etableres en permanent forbindelse mens datatransmissionen foregår.

Datapak

Navnet på Tele Danmarks pakkekoblede net til datatransmission. Pakkekoblede net er en teknik, hvor data overføres i pakker med dataene og adresse på modtageren så pakkerne kan sendes ad forskellige veje i nettet.

Dekryptering

Betegnelse for den proces ved kryptering, som omformer en chiffertekst (en krypteret tekst) tilbage til klarteksten (den oprindelige tekst).

DES

Forkortelse for Data Encryption Standard. DES er en konventionel (enkeltnøgle) kryptering. Oprindelig udviklet af IBM og blev amerikansk standard i 1987, men senere tilbagekaldt. Anvendes f.eks. i Dankort-systemet.

Digital underskrift

En værdi dannet ved public key kryptering, der er knyttet til et elektronisk dokument, og uafviseligt dokumenterer hvem der er afsender - har underskrevet dokumentet.

Enkryptering

Betegnelse for den proces som ved enkryptering gør en tekst ulæselig. Synonymt anvendes ofte blot kryptering.

Escrow Encryption Standard

Forkortes EES. Standard for en kryptering udviklet af en gren af det amerikanske militær, NSA. Når denne kryptering anvendes transmitteres oplysninger om den anvendte sessionsnøgle i et særligt Law Enforcement

Access Field (LEAF).

GSM

Forkortelse for Global System for Mobil Communication. Trådløst mobilt telefonnet.

Hashfunktion

En hashfunktion er en matematisk beregning på en bitstreng, som entydigt giver en tilfældig værdi, typisk på 64 eller 128 bit. Anvendes bla. til digital underskrift, således at kun dokumentets hashværdi underskrives for at spare tid og plads.

Ic-kort

Et plastkort i samme format som de kendte betalingskort med en indbygget computer (en integreret kreds -engelsk: integrated circuit).

ISDN

Forkortelse for Integrated Service Data Network. Digitalt datatransmissionsnet som sender digitale data fra sender til modtager. ISDN kombinerer flere teletjenester: tale, tekst, data, billeder, video mv.

Klartekst

Betegnelse, der anvendes i forbindelse med kryptering for teksten (data, dokument osv.) i sin oprindelige læselige form.

Kryptering

Betegnelse for et system som kan forvanske en tekst på en kontrolleret måde så den er ulæselig uden kendskab til en nøgle. Anvendes også synonymt med enkryptering.

Modem

Forkortelse for moduler og demodulerer. Modem, er et apparat, som anvendes ved datatransmission over det almindelige telefonnet. Modemet omformer (modulerer) bit (digitale signaler) til toner (analoge signaler), som kan transmitteres. Ved modtagelsen omformes (demoduleres) det analoge signal til en bitstreng (en række af bit).

OSI

Forkortelse for Open System Interconnection. OSI eller OSI-modellen er en række stander vedtaget af ISO (International Organization for Standardization) som fastlægger protokoller mv. for udveksling data.

Multipleksering

En teknik som samler en række transmissionslinjer med lavere hastighed til en linje med højere hastighed.

Sessionsnøgle

En nøgle til kryptering som kun anvendes til en session. Med en session menes tidsrummet for en åben forbindelse mellem to enheder som gennemfører en datatransmission.

Skipjack

Algoritme for krypteringen anvendt i Escrow Encryption Standard. Algoritmen er ikke offentlig tilgængelig.

SmartDisk

En "diskette" som er en lille computer, der kan anbringes i diskette drevet.

Tjeneste

Betegnelse for de forskellige former for datatransmission (teletjenester) der udbydes.

Åbne Systemer

Fælles betegnelse for edb-systemer, hvor imellem data og programmer frit kan flyttes.

Litteratur

Stewart A. Baker:
Why Clipper is Good for You. Wired, june 1994.

John Perry Barlow:
A Plain Text on Crypto Policy. Communication of the ACM November 1993/vol. 36 No. 11 s. 21-26.

Dansk Standard/inf 43:
Krytografi & Datasikkerhed. (1988)

Dorothy E. Denning:
Encryption and Law Enforcement. (February 21, 1994)

Poul Frahn:
Answers to FREQUENTLY ASKED QUESTIONS About todays Cryptography. (September 20, 1993)

Stephen Kent:
Internet Privacy Enhanced Mail. Communication of the ACM August 1993/vol. 36 No. 8 s. 48-60.

Susan Landau et. al.:
Codes, Keys and Conflicts. Issues in U.S. Crypto Policy. Report of a Special Panel of the ACM U.S. Public Policy Committee (USACM) june 1994.

Geoff Marshall (ed):
Secrets of the Crypt. Secure Computing january 1995 s. 12-21.

OTA:
Information Security and Privacy in Network Environments. US Office of Technology Assessment. OTA-TCT-606. (1994)

Charles P. Pfleeger:
Security in Computing. (1989)

William Stallings:
Protect Your Privacy. A Guide for PGP Users. (1995)

Preben Wilhjelm:
Tvangsindgreb. (1988)

Noter

1. For en generel introduktion kan henvises til rapporterne fra OTA og ACM (Landau et.al.).

2. Presseudtalelse 4. february 1994.

3. EU Commission: Green Paper on the Security of Information Systems.

4. European Commission: Proposal for a Council Decision Adopting a multi-annual action concerning the establishment of Europe-wide Thrust Services for public information services (ETS). Draft revision 14.02.95.

5. Oversigten bygger på udsagn fra forskellige personer, som deltager i forskellige EU sammenhænge.

6. EPIC-Alert vol 2.06 af 28. april 1995

7. Det Fri Aktuelt

8. Et sådan initiativ kunne f.eks. ske i forbindelse med udstedelse af et borgerkort, som indeholder anvendelsen kryptering. Se herom rapporterne:

-Indenrigsministeriet: Rapport vedrørende FORPROJEKT OM ELEKTRONISK BORGERKORT, december 1994

-Steffen Stripp: Plastkort som borgerkort. TeknologiNævnets rapporter 1994/2.

9. Forfatterne er begge fuldmægtige i Justitsministeriet.

10. Bidraget er skrevet af Dr. Peter Landrock, Aarhus Universitet og Cryptomathic.

11. Leif Nielsen er sikkerhedschef i Tele Danmark.

12. Se f.eks. Peter G. Neumann: Computer Related Risks (1995)

13. Charles P. Pfleeger: Security in Computing (1989) s. 123.

14. Landau et. al.: Codes Keys and Conflicts

15. LEAF er en forkortelse for law enforcement access field, der indeholder informationer om den krypteringsnøgle der anvendes i den følgende kommunikation.

16. Matt Blaze: Protocol Failure in the Escrowed Encryption Standard. **Preliminary Draft.** 1994

17. Mark Lomas and Michael Roe: Forging a Clipper Message. Communication of the ACM nr. 12 1994 s. 12.

18. Dette oplæg: Hemmeligholdelse af elektronisk kommunikation - en menneskeretlig synsvinkel, er skrevet af cand.jur. Birgitte Kofod Olsen, Det Danske Center for Menneskerettigheder.

19. Se herved den Europæiske Menneskeretsdomstols afgørelse i Klass m.fl. mod BRD (6/9 1978), Publications of the European Court of Human Rights, Series A, No. 28.

20. Se herved fx. Mads Bryde Andersen, Kryptering og efterforskning, DataSikkerhedsBladet Nr. 14, marts 1994.

21. Dette notat vedrørende hemmeligholdelse af datakommunikation i relation til indgreb i meddelelseshemmeligheden som led i efterforskning af kriminalitet er skrevet af Henning Thiesen, politimester hos Rigspolitichefen.

22. Der henvises til en arbejdsgruppe under Telestyrelsen, der afleverede sin "Hovedrapport: Vedrørende et eventuelt myndighedsinitiativ på krypteringsområdet" juni 1993. (Red).

23. Udtalelsen hentet fra EPIC Alert 2.04 fra 11. Marts 1995. Et elektronisk nyhedsbrev fra Electronic Privacy Information Center (EPIC).

24. Bangemann rapporten: Europa og det globale informationssamfund. Anbefalinger til de Europæiske Råd. Maj 1994.

25. ITSTC: Security Requirements for "EUROPE AND THE GLOBAL INFORMATION SOCIETY" Executive Summary. 24.5-94

26. DatasikkerhedsBladet Nr. 14. Marts 1994 s. 12

27. Mads Bryde Andersen og Peter Landrock fremlagde forslaget på konferencen Sikkerhed '95 den 24. og 25. januar 1995. Det vil indgå i en artikel i tidsskriftet Juristen i efteråret 1995.

28. W. Robert Collins, Keith W. Miller, Bethany J. Spielman and Phillip Wherry: HOW GOOD IS GOOD ENOUGH? An Ethical Analysis of Software Construction and use. I Communication of The ACM January 1994/vol. 37, No. 1 s. 81-91.

22.12.97 Teknologirådet tekno@tekno.dk