Hvad er matematik? 3
ISBN 9788770668781

website: link fra kapitel 0 , afsnit 1. *Ballade om sikkerhed af Ole Grünbaum*

L&R Uddannelse
EGMONT

Ballade om sikkerhed af Ole Grünbaum

Onsdag 25. marts 1992 • **POLITIKEN**

Ballade om sikkerhed

USA's regering vil have lov til at udspionere computerbrugerne

Af Ole Grunbaum

SAN FRANCISCO (Politiken) — Det Lille californiske softwarefirma RSA har de senere år etableret sig som førende i computersikkerhed. Firmaets krypteringsmetoder er så gode, at alle computerbrugere verden over inden længe skulle kunne sikre deres elektroniske privatliv — og mere end det. RSA-teknikken blev oprindelig udviklet i 1977 på Bostons berømte universitet MIT (Massachusetts Institute of Technology), og i 1982 gik de tre professorer, der havde udviklet teknikken, på markedet med deres eget firma. Men selv om de fleste eksperter op gennem 80erne har været enige om, at RSA-teknikken er superb, er det gået så som så med udbredelsen.

Historien om RSA er på en måde et godt eksempel på, hvordan den amerikanske regering under den nationale sikkerheds banner ofte spænder ben for sin egen computerindustri. Selv regeringen og Pentagon har været blandt de tilfredse kunder hos RSA. Men NSA, National Security Agency, som er Washingtons elektroniske overvågningstjeneste, og som hævdes selv at bruge RSA-teknologien, spænder ben for dens udbredelse.

NSA

For tænk hvis al computer- og telefonkommunikation kunne kodes (og dekodes i den anden ende), så ingen i al hemmelighed kunne overvåge kommunikationen? Hvor ville NSA så være henne? I dag er man i stand til at lytte til al transatlantisk telefoni og meget mere end det. I morgen kunne denne verdens største spionvirksomhed (efter KGBs stormagtsdage er ovre) gå hen og blive en saga blot.

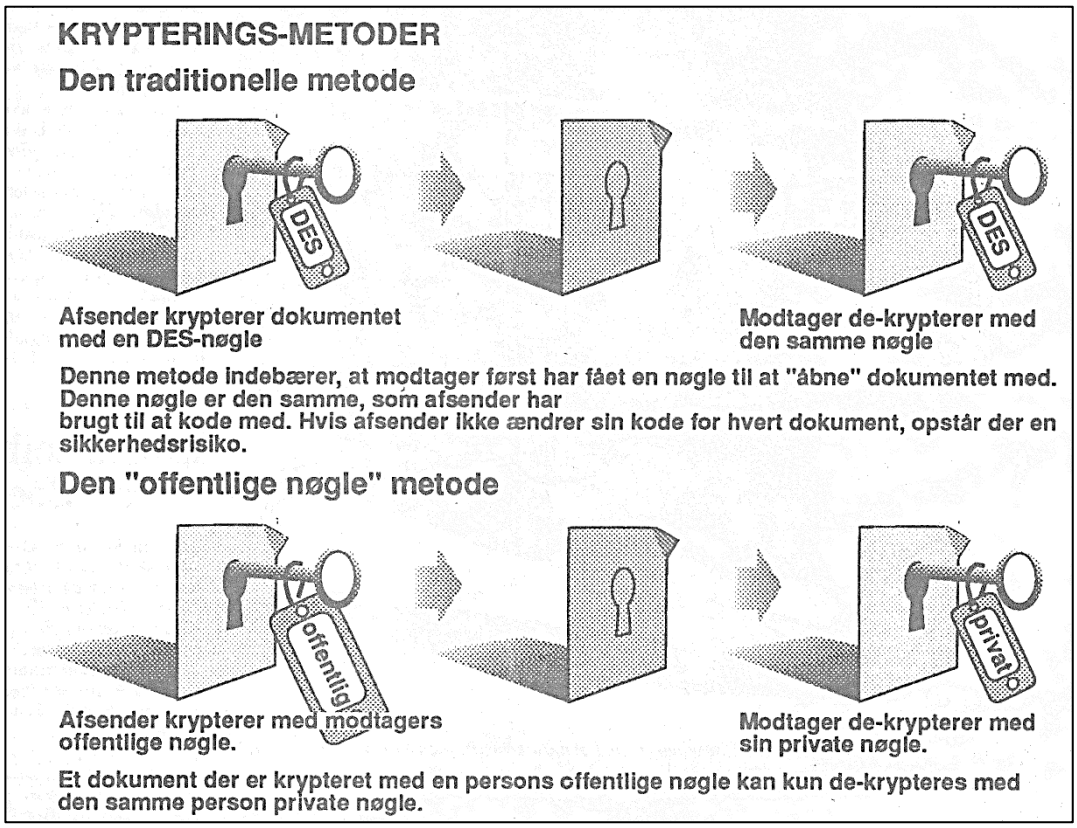
RSAs teknik forsyner en elektronisk kommunikation med en såkaldt 'digital underskrift', så modtageren kan være sikker på, at den elektroniske post virkelig kommer fra den person der står som afsender, og at der ikke er ændret i teksten. Endvidere kan både modtager og afsender være sikre på, at kun den tiltænkte modtager kan 'åbne' brevet.

Der findes traditionelle krypterings-teknikker, hvoraf DES-algoritmen er den mest kendte. Problemet ved disse teknikker er, at modtageren på forhånd skal være i besiddelse af en hemmelig elektronisk nøgle for at kunne åbne posten. Nøglen, som i praksis er en kode eller et lille program, kan altså ikke selv sendes elektronisk. Derfor egner disse teknikker sig kun til personer, som allerede kender hinanden godt og stoler på hinanden.

Med RSA-metoden kan man derimod sende krypteret til folk, man ikke før har været i kontakt med. Tanken er, at der udgives en slags telefonbog over alle modtager-koder. Disse er altså offentligt tilgængelige, og sikrer at posten kommer frem til den rette computer. Men modtageren har derudover sin helt egen hemmelige kode ved hjælp af hvilken han eller hun kan åbne posten. Kun den rette private kode kan åbne post, som er krypteret med personens offentlige kode.

Denne metode betyder, at man kan kode post til en person man aldrig har talt med før, idet personen åbner med sin egen hemmelige nøgle. Og ingen andre kan åbne. RSAs

metoder er langt mere omfattende end denne kryptering af teksten. De omfatter også sikring af, at modtageren virkelig er den, som vedkommende giver sig ud for at være samt at det modtagne dokument ikke er ændret undervejs.



Retsgyldig

Disse sikringer er altafgørende for at elektroniske dokumenter kan få virkelig retsgyldighed som underskrevne og stemplede papirer har det idag. Men de betyder samtidig, at heller ikke regeringsansatte spioner kan læse med i teksten eller lytte til digitale telefonsamtaler som bliver 'scramblet' med RSA-teknikken.

Det vil NSA og visse dele af den amerikanske regering selvfølgelig ikke have. Så hvad gør man? NSA har stor indflydelse på beslutninger om hvilke computerprodukter der må eksporteres frit. Så i første omgang har man nægtet RSA ret til frit at eksportere sine programmer, og amerikanske computere med indbygget RSA-teknologi må heller ikke eksporteres.

Denne eksportbegrænsning er nu delvis ophævet, men kun delvis. Forleden købte Apple RSA-teknologien til indbygning i Macintoshens fremtidige styresystem, så det bliver lidt af en prøve, når Apple om kort tid begynder at eksportere macintosher med RSA-kodning.

Den internationale computerverden er — både på regeringsside og inden for finanssektoren — ved at være godt træt af den amerikanske regerings evindelige forsøg på at stoppe udbredelsen af den mest avancerede sikkerheds-teknologi. Der skal af praktiske grunde snart foreligge en international standard for kryptering og dekryptering af computerkommunikation. Det er af yderste vigtighed, at den stigende trafik på computernetværkene bliver sikret mod overvågning, tyveri og forfalskning. Men på den anden side vil investeringerne i sikkerhed være så store, at mange venter til der foreligger en standard.

I USA er der som sagt gået politik i sagen. Alle indrømmer, at RSA har den bedste teknik. Men forsvarsministeriet ønsker ikke, at et enkelt firma skal have monopol på den krypteringsmetode som man vil bruge. Forsvarsministeriet så hellere, at RSA én gang for

alle solgte licensen, og metoderne blev offentlig ejendom. Men det kan RSA-folkene ikke se den helt store forretningsmæssige fidus i.

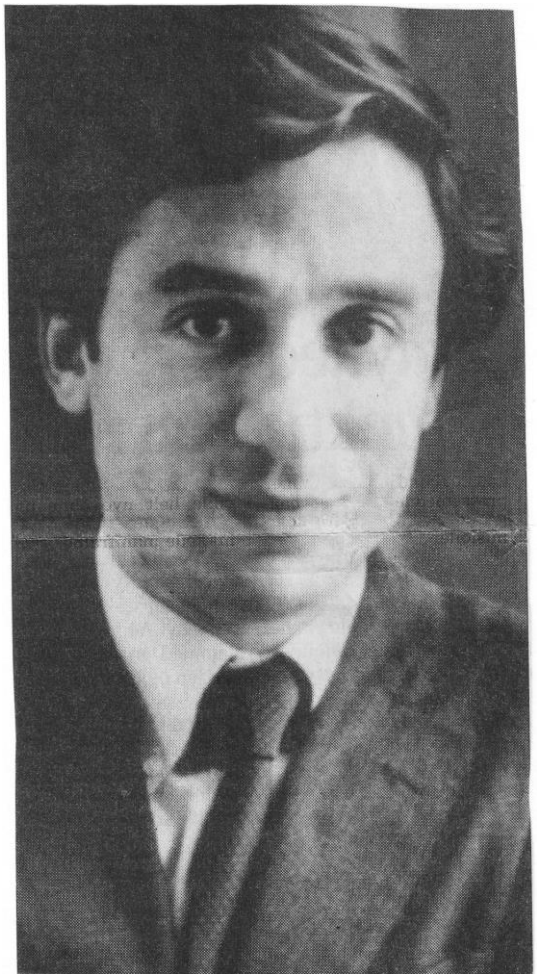
National Security Agency har som sagt helt andre motiver til at spænde ben for RSA, men resultatet er at det lille firma har nogle formidable modstandere — især bag kulisserne. Alligevel har RSA solgt sin teknik til firmaer som IBM, Digital, Lotus, Novell, Microsoft – og nu Apple.

Kampen har været årelang. I 1987 fik NSAs lobbyister Kongressen til at forlange, at der gennem National Institute of Standards and Technology (NIST), et departement under handelsministeriet, skulle fremsættes forslag til en standard. Denne blev langt om længe fremsat i efteråret 1991. Imidlertid blev det hurtigt efter fremkomsten afsløret, at metoden — bevidst eller ubevidst — lider af den mangel, at det meget vel kan lade sig *gøre* at lave 'bagdøre' til krypteringen — så en trænet computerprogrammør kunne[1]

Bagdøre

Nu krøb NIST til bekendelse og indrømmede, at man ikke selv havde fremstillet DSS-metoden, men kun lagt navn til. Metoden var fremstillet af... NSA! Det bliver nok aldrig hundrede procent opklaret, om NSA med vilje fremkom med en krypterings-metode, der indeholdt muligheder for bagdøre. Men det modsatte ville betyde, at NSA er inkompetent vedrørende kodning af elektroniske signaler, og det vil ingen vove at påstå.

Kredse omkring NSA og FBI fik sidste år en politiker til at fremsætte et lovforslag i Kongressen gående ud på, at det skulle være forbudt at sælge et sikkerhedsprogram, som ikke kunne brydes af de offentlige myndigheder. Der skulle ifølge lovforslaget bevidst laves bagdøre til krypteringen — så offentlige myndigheder via hemmelige dommerkendelser kunne få adgang til computerkommunikationen eller telefonsamtalerne.
RSA og en række borgerretsorganisationer sponsorerede en konference imod dette forslag i Washington.



Jim Bidzos fra RSA fik overbevist en amerikansk kongresmand om, at dennes lovforslag var en dårlig idé. Forslaget gik ud på, at alle sikkerhedsprogrammer skulle have indbygget en 'bagdør', som FBI og andre kunne bruge til at udspionere folk med. — Foto: Ole Griinbaum

RSAs direktør Jim Bidzos siger til Politiken, at han satte sig ned med den pågældende politiker og forklarede ham, at konsekvensen af lovforslaget ville blive, at USAs computerindustri simpelt hen ville blive koblet af udviklingen internationalt. Og det hele endte med, fortæller Bidzos, at politikeren lovede aldrig mere at fremsætte den slags forslag.
— Hvis vi ikke passer på, siger Jim Bidzos, — kan vi meget vel komme i en situation,

[1] Teksten er også mangelfuld i den originale avisartikel.

hvor regeringen kan læse alt og hvor borgerne intet kan få at vide om hvad regeringen gør bag de lukkede døre.