KUNGLIGA TEKNISKA HÖGSKOLAN
Kommunikation i ingenjörsvetenskap
Handledare: Per-Anders Forstorp

HT 2004

Kryptodilemmat

Andreas Boström

ABSTRACT

The dilemma of cryptography. A study about the consequenses of having public access to strong and free encryption.

Author: Andreas Boström
Subject: Communication in Engineering Science

It has always been important to keep secrets secret, but to until thirty-forty years ago the secrets of governments and armed forces were the only ones prioritied. This changed with the appearance of personal computers. Nowadays, thanks to the Internet, even common people can use encryption to protect their own secrets. In fact, we are forced to protect our private information if we want to communicate or carry trough transactions over the Internet. Lots of honest people use strong encryption to guard against intrusion in their private lifes, but the problem is that not all people have honest intensions. Many use encryption to protect criminal activity instead. It is painfully obvious that computer crimes increase rapidly, and authorities around the world want of course to change the numbers about. The aim of this study is to describe and analyze the possible solutions to this problem. The authorities feel that only those with good intensions should be allowed to use encryption, while criminals should be banned from all usage; but civil rights organisations feel strongly that it is a civic right for each and everyone to have access to encryption. My conclusion is that encryption should be kept free, and that no restrictions should be imposed. However, I feel that computer crime and computer intrusion are getting to be serious problems, and that it is imperative to make digital communication even more safe than it is today. The final conclusion is that digital verification and certification are the best options there are.

Keywords: cryptography, encryption, RSA, PGP, public-key, computer crimes, key escrow, digital communication, civil rights, verification, certification.

INNEHÅLLSFÖRTECKNING

FÖRORD

Med kryptering är sanning och skönhet samma sak. Man vet att man har kommit närmare sanningen när riktiga ord och meningar börjar växa fram ur rappakaljan. Kryptering är något som de flesta av oss använder varje dag, de som använder Internet gör det hela tiden. Ändå är det många som inte känner till, eller snarare tänker på, hur viktig kryptering är nuförtiden. Vi är tvingade att använda kryptering när vi genomför banktransaktioner eller handlar på Internet. Att inte göra det är som att aldrig låsa ytterdörren. När som helst kan vad som helst hända.

KÄLLKRITIK

De flesta av mina källor har ett par år nacken, huvuddelen har faktiskt till och med publicerats så länge sedan som förra årtusendet. Det betyder däremot inte att de är inaktuella, för det är de inte. Det kanske är svårt att tro sex-sju år gamla källor om avancerad datakommunikation fortfarande kan hålla sig färska, men det har de gjort eftersom inga avgörande genombrott inom kryptologin egentligen har uppnåtts och inte heller lagarna ändrats så nämnvärt att en omfattande revidering blivit nödvändig. De flesta källorna är hämtade från Internet, men måste anses tillförlitliga då huvuddelen kommer från olika myndigheter. Många finns också i tryckt form, men har samtidigt lagts upp på Internet för att göra dem mer tillgängliga.

SYFTE

Att utreda huruvida det är en medborgerlig rättighet att använda fri kryptering (utan begränsningar) eller om det är ett privilegium som kräver motprestationer av var och en? Är det möjligt att ordna det så att bara de som använder kryptering i ett gott syfte får fortsätta använda den, medan kriminella nekas? Kan en sådan lösning uppnås utan att inskränka de medborgerliga rättigheterna?

BAKGRUND

När man talar om krypterad kommunikation mellan två parter är det inofficiell standard att kalla sändaren och mottagaren för Alice och Bob, och en möjlig tjuvlyssnare för Eve (*the Eavesdropper).* Ända sedan *kryptologin* uppfanns för ett par tusen år sedan har det varit ett ofrånkomligt faktum att om två människor vill skicka krypterade meddelanden till varandra måste de båda känna till *nyckeln* så att de kan *dekryptera*. Om Alice vill skicka ett meddelande till Bob måste de på något sätt komma överens om en nyckel, och detta faktum motsäger själva krypteringens egentliga syfte.

Detta nyckeldistributionsproblem löstes för första gången på 1970-talet av ett amerikanskt forskarlag bestående av Whitfield Diffie, Martin Hellman och Ralph Merkle. Diffie-Hellman-Merkles metod för nyckelutbyte bygger på enkelriktade matematiska funktioner. Metoden, som inte är alldeles för simpel, går ut på att Alice och Bob först kommer överens om två värden, som bestämmer funktionens utseende, via telefonlinjen om de så önskar. Sedan väljer de båda var sitt tal som de håller hemligt och stoppar i det i funktionen. Därefter skickar de svaret de erhållit till varandra, detta stoppas in i varandras funktioner och

båda kommer då att få samma svar. Detta blir nyckeln. Metoden var ett stort genombrott men den var inte fullkomlig. Största problemet var bristen på smidighet eftersom Alice och Bob måste båda vara med om att skapa nyckeln. Vad som behövdes härnäst var en mer effektiv metod. Denna tänktes faktiskt ut av Whitfield Diffie också, men han kunde inte formulera sin teori så att den kunde användas praktiskt också. Diffie hade uppfunnit ett nytt sorts chiffer, med en *asymmetrisk* nyckel, baserad på *kryptering med öppen nyckel* (*public-key kryptering*). I ett asymmetriskt krypto är krypteringsnyckeln och dekrypteringsnyckeln inte identiska, vilket de är i de alla andra chiffren, de *symmetriska*. Tanken var att Alice och Bob skulle skapa var sitt nyckelpar, en publik nyckel och en privat nyckel. Den publika nyckeln är offentlig så att vem som helst kan få tillgång till den. Om då Bob vill skicka ett meddelande till Alice letar han upp hennes publika nyckel och krypterar meddelandet med den. Alice kan sedan dekryptera det med hjälp av sin egen hemliga, privata nyckel. Detta låter ju jättefint, men det är inte lätt att hitta en funktion som kan få en sådan sak att fungera.

1977 lyckades ett forskarlag bestående av Ronald Rivest, Adi Shamir och Leonard Adleman formulera en praktisk lösning. Deras krypto kallas för RSA och är ett av de viktigaste av alla krypton. Kärnan i RSA är utgörs av variabeln N, som är en del av envägsfunktionen. När Alice ska bestämma sitt eget värde på N är tanken att hon väljer ut två stora primtal, p och q, som sedan multipliceras med varandra och ger N. N, den publika nyckeln, är lätt att skapa men mycket svår att dela upp i *primtalsfaktorer*. Att spjälka upp N, att faktorisera, är väldigt svårt, ja nästan omöjligt om man använder primtal i storleksordningen 10^{308}. RSA, systemet som bygger på public-key-kryptering är helt säkert om tillräckligt stora primtal används, och så länge ingen hittar en genväg till faktoriseringen.[1]

Det enda som därefter återstod var att göra RSA tillgängligt för allmänheten, men detta visade sig vara lättare sagt än gjort. Problemet var att företaget RSA Data Security Inc., som startades för att marknadsföra kryptot och som hade patentet, bara inriktade sig på storföretag, försvaret och regeringen eftersom dessa var de enda som hade tillräckligt kraftfulla datorer. Datalogen Phil Zimmermann ansåg att envar hade rätt till en sådan ostörd kommunikation som RSA kunde erbjuda och därför skapade han ett dataprogram i vilket han bakade in RSA, men gjorde programmet så effektivt att kapaciteten för en vanlig PC inte överskreds. Programmet fick namnen PGP (*Pretty Good Privacy)*, och släpptes fritt på Internet i juni 1991.[2] Äntligen kunde vem som helst kommunicera med varandra utan att behöva oroa sig för att bli avlyssnade. Allt kommer dock med ett pris, och det är jag ska diskutera i resten av rapporten. Vem som helst är just vem som helst, inklusive mördare, hackare, pedofiler och terrorister.

ANALYS AV ETT BROTT

Det är mycket gott man kan använda kryptering till. Skicka brev till farmor, handla på Internet och betala räkningar on-line. Tyvärr, som med allting annat, är det inte bara snälla och ärliga människor som använder sig av kryptering. Världen är full med människor som visserligen försöker skydda sina privatliv men gör det för att slippa åtal. Databrott och dataintrång har ökat för varje år, speciellt de senaste tio åren då antalet människor som fått tillgång till både dator och Internet ökat dramatiskt. Endast i Sverige ökade antalet anmälda dataintrångsbrott i hela riket från 9 st (1999) till 407 (2001) och till 731 (2003).[3] Mörkertalet är säkert större än vad man kan tro, eftersom en hel del intrång inte ens upptäckts. Då kan man även fråga sig

[1] Singh, Simon, 2002. *Kodboken*. Sid. 281-309.
[2] Ibid. Sid. 323-332.
[3] http://statistik.bra.se/solwebb/action/anmalda/urval/urval?menyid=43 (Brottskod 0415).

hur många av dessa brottslingar som använder kryptering. Det är omöjligt att veta, men myndigheterna är säkra på, och det är jag också, att de blir fler och fler för varje år som går. Jag tror inte jag överdriver om jag säger att mörkertalet här är i jämförelse med stor säkerhet ännu större. Många brottslingar, även svenska, använder sig av kryptering. En del kanske planerar brott och skyddar kommunikationen med medbrottslingar (exempelvis terrorister eller lönnmördare), andra skyddar istället de bevis som finns mot dem själv (exempelvis barnpornografer). Av alla dessa är det bara ett fåtal som grips och åtalas, för mot resten har polisen inga bevis. Det är så enkelt att använda bra och stark kryptering att även tioåringar kan göra det, så då borde väl fullvuxna kriminella också kunna göra det. Det låter säkert överdrivet, men det är det inte. Det är verklighet. Rättsskipande myndigheter (även svenska) fruktar att situationen förr eller senare kommer att bli ohållbar.

I många år har en debatt rasat över hela världen om det är rätt eller fel att tillåta vem som helst att få använda kryptering. Debatten har sitt epicentrum i USA, och allt som händer där påverkar i sin tur resten av världen. Det är i USA RSA och PGP har utvecklats, och därför är det kanske inte så konstigt att det är där det mesta händer. Europa i allmänhet och Sverige i synnerhet är på detta område mycket mer liberala, men påverkas så klart av de beslut som fattas och de lagar som stadsfästs i Nordamerika. USA, den moderna kryptologins födelseplats, har på grund av sin yta och folkmängd mycket svårare att få ett grepp om situationen. USA:s betydelse i detta sammanhang är så stort att lejonparten av analysen i detta och nästkommande kapitel kommer att utgå från den amerikanska kryptodebatten, även om jag också har för avsikt att utreda Sveriges ståndpunkt i frågan.

Kryptodebatten är i USA mycket hätsk, och den visar ”inga tecken till avmattning”[4] enligt Simon Singh som skrivit den underbara och djupt rekommenderade *Kodboken*. Debattens grundfråga handlar om staten bör lagstifta mot kryptering eller inte. De rättsvårdande och rättsskipande myndigheterna i USA har länge tyckt att lagstiftning är nödvändig. Myndigheter som står längst fram i ledet är speciellt FBI och NSA[5]. Deras ståndpunkt är att kriminellas användning av kryptering har blivit ett så stort problem att något måste göras. Jag håller med dem. Något måste göras, för problemet är verkligt.

Med största sannolikhet så är det så att kryptering används i kriminella sammanhang först och främst av den organiserade brottsligheten. Dorothy Denning och William Baugh skrev 1997 en rapport om organiserad brottslighet och kryptering. De anser att ”… the total number of criminal cases involving encryption world-wide is at least 500, with an annual growth rate of 50-100%”. Denning och Baugh ger dessutom många exempel på kända brottslingar och terrorister som bevisligen använt sig av kryptering. Bland exemplen återfinns sekten *Aum Shrinri Kyo* (som spred ut sarin i Tokyos tunnelbana 1995), bolivianska terrorister som mördade fyra amerikanska marinsoldater, Ramsey Yousef (som var det mest kända namnet bakom bombdåden mot World Trade Center 1993 och flygbolaget Manila Air 1995) och Mr. Leary som 1995 dömdes till 94 år i fängelse för sitt brandbombsattentat i New Yorks tunnelbana. När det gäller organiserad brottslighet nämner Denning och Baugh den nederländska organiserade brottsligheten (prostitution och knark), den amerikanska ”national drug ring”, *Cali*-kartellen i Colombia och den italienska maffian. Dessutom har kryptering använts av landsförrädare, såsom Aldrich Ames, en före detta CIA-agent; och inom industrispionaget. Myndigheterna har också råkat på krypterade e-mail och filer i utredningar angående pedofili och barnporr. Ofta var det PGP som hade används för krypteringen. Mark Pollitt, programansvarig för CART (*The FBI’s Computer Analysis Response Team*), uppskattade enligt rapporten (1997) att det över hela världen fanns mellan 500 och 1,000 fall med kryptering inblandat; medan Eric Thompson, styrelseordförande för *AccessData Corporation*, var ännu värre och placerade siffran mellan 1,000 och 5,000 fall. 5,000 fall

[4] Singh, 2002. Sid. 333-334.
[5] *National Security Agency*, USA:s motsvarighet till FRA (*Försvarets Radioanstalt*).

motsvarade i sin tur mellan en fjärdedel och hälften av alla internationella databrott (!).[6] Med största sannolikhet använde sig *al-Qaida* av kryptering under planeringen och utförandet av *elfte september-attentaten* 2001, men det är en egen inofficiell teori. Allt detta är mycket skrämmande läsning, och jag anser att det är väldigt viktigt att hitta en lösning innan det hela spårar ur totalt. Rapporten är redan sju år gammal, och siffrorna har knappast sjunkit.

De amerikanska myndigheternas så kallade lösning har antagligen förvärrat problemet, för den lösningen är inte bara naiv utan också fullkomligt oacceptabel. Det är viktigt att veta att trots allt så har inget har bestämts än och ingen lag som godkänt myndigheternas ståndpunkt har än så länge stiftats. Ändå så är det svindlande läsning att gå igenom listan över alla lagförslag och motioner till kongressen och senaten. När man läser den så är det inte lätt att veta exakt hur situationen är nu.[7] Ett av dessa lagförslag, *The Secure Public Networks Act* från 1997, innehöll precis det som myndigheterna önskade. Om den hade antagits så hade envar blivit tvingade att lagra sina privata nycklar på ett ”säkert” ställe, nämligen hos en *nyckeldepositionsmyndighet (key escrow agent)*. Bara de som godkänts och lämnat en kopia på nyckeln där skulle få fortsätta använda kryptering. Haken var bara att myndigheterna skulle ha fått kontrollen över alla nycklarna, vilket det i för sig krävdes domstolsbeslut för.[8] Föga förvånande gav lagförslaget upphov till ett ramaskri från motståndarna och det hela rann ut i sanden. Det mest berömda försöket att införa nyckeldeposition är *American Escrowed Encryption Standard*, som lanserades 1994. Den innefattade två system – *clipper* för telefon och *capstone* för data. Clipper är den mest kända och omdebatterade av dem två, och innebar helt enkelt att vanliga telefoner skulle ha ett clipperchip förinstallerat, som i sin tur skulle innehålla användarens privata nyckel. Vid köpet av telefonen skulle en kopia av nyckeln skickas till två federala myndigheter. Utanför regeringskretsarna var inte det många som stödde idén. Motståndarna gjorde en jämförelse med att ge staten kopian på allas husnycklar.[9]

Fiaskot med nyckeldepositionen beror till stor del på att myndigheterna agerade oförsonligt, enväldigt och fullständigt tank- och taktlöst. De trodde att allmänheten skulle finna sig i besluten utan vidare, men det gjorde den inte. Inte alls.

ANALYS AV EN RÄTTIGHET

Som tur är, är det inte bara pest och kolera med detta kryptodilemma. Som jag redan har nämnt finns det många goda saker kryptering kan användas till, och majoriteten av användarna har goda avsikter. Att brottslingar brukar kryptering är ett problem, vilket jag visat i det föregående avsnittet; men de är än så länge i minoritet. Även om man jämför med andra brott som begås är inte kryptering i kriminella sammanhang så vanligt, snarare tvärtom. Det finns alltid två sidor av samma mynt, och även fast det finns så många oärliga saker man kan göra med kryptering tycker jag att man måste se till båda sidorna. Allmänhetens tillgång till fri kryptering är enligt mig själv och många andra en grundläggande rättighet i dagens samhälle. Den får absolut inte inskränkas.

Motståndarna till obligatorisk nyckeldeposition utgörs föga förvånande av de flesta medborgarrättsorganisationer, men även av de stora företagen. Att företagen står på den fria krypteringens sida är ett stort avbräck för myndigheterna, som inte insåg från början att företagen hade stora pengar att hämta i Internethandeln. Företagen insåg tidigt att ett förbud

[6] Denning, Dorothy E. – Baugh, William E., Jr., 1997. *Encryption and evolving technologies as tools of organized crime and terrorism.*
[7] http://rechten.uvt.nl/koops/cryptolaw/cls2.htm
[8] Lewis, Ted, 1997. *We Don't Need No Regulation (Cyber View).* Sid. 27.
[9] Singh, 2002. Sid. 341.

mot fri kryptering skulle slå hårt mot deras intäkter, och det är inte bra *business*. De stora namnen inom kryptologin som Whitfield Diffie, Ronald Rivest och Phil Zimmermann står också på medborgarrättskämparnas sida. Detta bevisade de 1994 när de tillsammans med annat känt folk (däribland Ingemar Ingermansson från Linköpings Universitet) från medborgarrättsorganisationer, kryptologi och säkerhet samt industrin och fackvärlden, skickade ett brev till president Clinton vilket de avslutade med ”… we respectfully ask the White House to withdraw the Clipper proposal”.[10]

Motståndarna stöder sig på först och främst den amerikanska författningen, speciellt det fjärde tillägget till konstitutionen. Det tillägget säger att “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause […] “.[11] Även den svenska lagen har motsvarigheter. 6 § i regeringsformen deklarerar nämligen att ”Varje medborgare är gentemot det allmänna skyddad mot påtvingat kroppsligt ingrepp även i annat fall än som avses i 4 och 5 §§ [dödstraff resp. kroppsstraff – min kommentar]. Han är därjämte skyddad mot kroppsvisitation, husrannsakan och liknande intrång samt mot undersökning av brev eller annan förtrolig försändelse [min understrykning] och mot hemlig avlyssning eller upptagning av telefonsamtal eller annat förtroligt meddelande. *Lag (1976:871)*”.[12] Som svensk kan man vidare hänvisa till brottsbalkens 4 Kap ”Om brott mot frihet och frid vars 8 och 9 §§ är de mest relevanta. 8 § säger att den som stjäl annans post döms för brytande av post- eller telehemlighet till högst två år i fängelse, och 9 § meddelar att den som bryter brev eller telegram döms för intrång i förvar i också två år.[13] Hårda bud, alltså. Varför begränsa sig till endast svenska eller amerikanska lagar? Många organisationer för fri kryptering verkar med FN:s deklaration om de mänskliga rättigheterna i tankarna, vars 12:e artikel deklarerar att ”Ingen må utsättas för godtycklig ingripanden i fråga om privatliv, familj, hem eller korrespondens, ej heller angrepp på heder och anseende. Envar har rätt till lagens skydd mot sådana ingripanden eller angrepp”.[14] Dessa lagar väger förstås tungt, men olika tolkningar finns förstås. Trots allt så är inte den amerikanska författningen väldigt tydlig (delvis för att den skrevs för 250 år sedan), och man kan fråga sig om den verkligen kan förhindra obligatorisk nyckeldeposition. Dr. Jaap-Koops, som jag kommer att återkomma till, tycker inte det. Enligt hans åsikt är det inte en konstitutionell rättighet att få använda kryptering. Därför kan man enligt honom inte stödja sig på endast tilläggen, även om de är viktiga.[15] Författningen och den svenska regeringsformen är dock fortfarande lagar, och för att införa obligatorisk nyckeldeposition i USA krävs omfattande federal lagstiftning.

Situationen i USA är dock fortfarande mycket känslig, speciellt efter 11/9 2001. Landet löper stor risk att komma tillbaka till *McCarthy*-eran främst tack vare antiterroristlagen *Patriot Act*, som ironiskt nog inte bara riktar sig mot terrorister utan egentligen mot det amerikanska folket som helhet. Lagen ger de amerikanska myndigheterna rätt till sådan övervakning som de svenska myndigheterna aldrig skulle få tillåtelse att utöva, men att dekryptera privatpersoners brev är fortfarande inte tillåtet. Detta kan i värsta fall komma att ändras i framtiden, och i så fall blir det ett kraftigt slag i magen på medborgarrättsrörelsen, som redan nu har mycket att stå i.

Den svenska regeringens och de svenska myndigheternas hållningar står i bjärt kontrast till de amerikanska. Sverige är faktiskt när det gäller kryptodebatten nästan självuppoffrande liberalt. IT-kommissionen, som avslutade sin verksamhet 2003, har adresserat frågan i två

[10] http://www.eff.org/Privacy/Key_escrow/Clipper/experts_v_clipper.letter
[11] http://www.house.gov/Constitution/Amend.html
[12] http://62.95.69.3/sfsdoc/03/030593.pdf
[13] http://www.notisum.se/rnp/SLS/LAG/19620700.HTM
[14] http://www.unhchr.ch/udhr/lang/swd.htm
[15] Jaap-Koops, Bert, 1999. *The crypto controversy. A key conflict in the information society*. Sid. 129.

skrivelser. I den första från 1997 är det enligt kommissionen helt nödvändigt att det finns en ”tillgång till och möjlighet för alla att använda en säker metod för kryptering / - - - / Kraven på användning av krypto skall samtidigt balanseras mot kraven på effektiv brottsbekämpning och nationell säkerhet”. Kommissionen fortsätter med att säga att ”En begränsning i enskildas möjlighet att använda kryptering får negativa följder för enskildas förtroende till vad som är säkert i informationssamhället / - - - / IT-kommissionen menar att ett depositionssystem innebär alltför stora risker i sig för att kunna genomföras på ett säkert sätt”. Kommissionens förslag till uppdragsgivaren Kommunikationsdepartementet är följande: ”IT-kommissionen föreslår att det inte införs några begränsningar i enskildas, organisationers, företags och myndigheters möjligheter att använda krypteringsteknik […] Kommissionen avfärdar således olika former av nyckelhanteringssystem för privata nycklar såsom deponering och återskapande”.[16] 1999 slog IT-kommissionen till igen, i en skrivelse till Näringsdepartementet. Enligt kommissionen torde ett allmänt bruk av kryptering i själv verket motverka brottslighet, och att ett förbud skulle begränsa förutsättningarna för en positiv utveckling av användningen av IT. ”Kommissionen avfärdar varje form av obligatoriskt system för deponeringen av nycklar. / - - - / Regeringen bör klart ge uttryck för att det är fritt i Sverige att använda stark kryptering och att de så kommer att förbli.”[17] Tydligen så lyssnade regeringen för bara två månader efter IT-kommissionens andra rapport gav Utrikesdepartementet ut skrivelse 1998/99:116 som tillkännagav att ”För närvarande föreligger det inte skäl att begränsa användningen av kryptoteknik i Sverige. Alla ska ha rätt att själv välja sådan teknik”. Regeringen menar också att ”Skulle utvecklingen motivera skärpta regler kommer regeringen att överväga lämpliga åtgärder…”, men inga förändringar har till dags dato skett.[18]

Personligen tycker jag att det är dumt att begränsa och förbjuda något som så många har så stor användning för. Ronald Rivest, RSA:s skapare, skrev i en artikel från 1998 i *Scientific American* att ”The government’s concern is that the ’bad guys’ will benefit from the new cryptographic technology. This is certainly possible – the sun shines on the evil as well as the good. But it is poor policy to clamp down indiscriminately on a technology merely because some criminals might be able to use it to their advantage”. Rivest gör därefter en rolig analogi med ett par handskar, en liknande analogi finns i Singhs *Kodboken* (antagligen ett citat från Rivest). Analogin går ut på att jämförelsen mellan kryptering, som skyddar data; och handskar som skyddar händer. Kryptologi skyddar data från hackare, spioner och bedragare; medan handskar skyddar händerna från skärsår och kyla. Det ena hindrar FBI från att läsa dina meddelanden, det andra hindrar FBI från att analysera dina fingeravtryck. Dessutom kan man ladda hem exempelvis PGP billigare än vad ett par handskar kostar. Rivest sammanfattar analogin med ”… we should also consider cryptography’s benefit to society as a whole. Most people use cryptography to prevent crime rather than to hide it, just as most people wear gloves to protect their hands rather than to hide their fingerprints”. “On balance, the advantages of more widespread use of cryptography outweigh the disadvantages. / - - - / For the U.S. to restrict the right to use cryptography would be a setback for democracy – and a victory for Big Brother.”[19] Här håller jag med Rivest fullständigt. Även fast kryptering används i olaga syften finns det ingen egentlig anledning att begränsa andras möjligheter till en säker kommunikation. Allmänheten måste väga tyngre än brottslingarna, oavsett hur många de än har dödat eller bestulit.

Innan jag avslutar detta kapitel med att diskutera varför nyckeldeposition inte kommer att fungera ska jag uppehålla mig ett litet tag hos doktor Bert Jaap-Koops som 1999 skrev en

---

[16] IT-kommissionen, 1997-05-26. *Avseende användning av kryptering (Dnr IT96/103)*. Sid. 3-6.
[17] IT-kommissionen, 1999-04-15. *Vikten av användning av kryptering*. Sid. 1-2.
[18] Utrikesdepartementet, 1999-05-06. *Om kryptografi (SKR 1998/99:116)*. Sid. 1.
[19] Rivest, Roland L., 1998. *The Case against Regulating Encryption Technology*. Sid. 88-89.

mycket omfattande doktorsavhandling i ämnet. Hans åsikt är att ”A crypto ban is not enforceable” eftersom ”A crypto ban will simply not be able to deny easy access to strong, non-LEAK crypto[20]. A second argument […] is that it is hard to monitor. Obviously, the police cannot check all computers and diskettes for the presence of banned cryptography”. Hur skulle ett förbud påverka allmänheten då? Jaap-Koops menar att ”A crypto ban does hamper good guys”. Möjligheten till ett privatliv skulle försvåras, balansen mellan allmänheten och myndigheterna skulle svikta till myndigheternas favör, och dessutom skulle ett ekonomiskt bakslag inträffa eftersom den internationella handeln skulle få lida hårt. ”Banning cryptography or mandating LEAKing crypto systems is simply not an option.” Jaap-Koops citerar även Phil Zimmermanns profetiska ord: ”If cryptography is outlawed, only outlaws will have cryptography.”[21]

Nyckeldeposition är ett konstigt försök att kontrollera sådant som inte går att kontrolleras. Det finns som Jaap-Koops sade ingen möjlighet att polisen skulle kunna kontrollera alla. Att lämna in kopior på sina privata nycklar till myndigheterna är ett förslag som är i bästa fall skrattretande. Det är min åsikt i alla fall. Att det bara skulle vara frivilligt är illa nog, att göra det obligatoriskt skulle motsvara scenariot från *1984*. Det Storebrorssamhälle Rivest nämnde skulle i så fall bli total verklighet. Ändå så låter det så oskyldigt. Lämna en kopia bara, som bara ska hållas i förvar. Vad för garantier får man att staten inte kommer utnyttja folkets välvilja och läsa deras personliga korrespondens? Inga. Även om staten inte gör det som en enhet så kan det mycket väl finnas skurkaktiga tjänstemän som inte drar sig för något. Sedan måste ju kopiorna lagras någonstans. I ett register skyddat av stark kryptering möjligtvis. Tänk om någon lyckas hacka sig in i det registret för att sedan tillverka egna kopior? Då skulle var och ens privatliv vara till salu för högstbjudande på eBay.

Som jag diskuterade tidigare är det tyvärr så att man måste välja mellan det mindre onda av två onda ting. Allt är inte frid och fröjd, men som tur vad inte pest och kolera heller. Det kanske finns en lösning, genom vilken säkerheten kan förhöjas utan förbud och begränsningar till höger och vänster.

ANALYS AV EN KOMPROMISS

Det är i alla fall för mig klart att det inte går att välja rakt av mellan fri eller begränsad kryptering. Jag anser fri kryptering vara en rättighet som var och en har, brottslingar också. Det går inte att begränsa möjligheterna till fri kryptering utan att samtidigt begränsa de medborgerliga rättigheterna. Ändå så är det mycket viktigt att på något annat sätt ta tag i de problem som ändå finns. Det går inte att bestämma vem som får och inte får använda fri kryptering, det är en praktisk omöjlighet. Enda sättet som återstår är att internationellt arbeta för att säkerheten på speciellt Internet stärks avsevärt. Det är redan nu, och det har det varit i flera år, plågsamt klart att Internet lider av många säkerhetshål, som utnyttjas av illasinnade människor. Dessa bör täppas till, och en hel del kan åstadkommas med hjälp av just kryptering. Som många experter har sagt så förhindras brott med hjälp av kryptering.

Ett stort problem med öppen-nyckel-kryptering är att mottagaren inte kan vara helt säker på att avsändaren verkligen är just den han eller hon utger sig för att vara. Detta problem gäller förstås även för både e-post och vanliga brev. Om Bob får ett krypterat brev från Alice kanske han ändå inte är helt säker på att det är Alice som har skickat det även om det är undertecknat med ”Alice”. Avsändaren skulle kunna vara Eve, som försöker bedra Bob.

---

[20] *Law-Enforcement Access to Keys* – Jaap-Koops egen benämning på nyckeldeposition.
[21] Jaap-Koops, Bert, 1999. Sid. 125-132.

Lyckligtvis kan man med just öppen-nyckel-kryptering lösa detta verifikationsproblem, nämligen så här: Alice krypterar brevet som vanligt med sin privata nyckel, men därefter krypterar hon den igen med Bobs publika nyckel. Bob dekrypterar sedan först med sin egen privata, därefter med Alices publika. Om meddelandet verkar begripligt kan Bob vara säker på att det verkligen är Alice som har skickat det.[22] Med hjälp av sådan avsändarverifikation (*message authentication*), även kallad *digitala signaturer*, kan säkerheten skärpas i och med att det blir mycket svårare att genomföra bedrägerier och annat falskspel.

Det räcker dock inte bara med avsändarverifikation, för det finns ett problem till som måste lösas. Alice måste också vara helt säker på att det är Bobs äkta publika nyckel hon har tillgång till, för Eve skulle återigen kunna vara inblandad. Självklart finns det ett behov av en så kallad *certifieringsmyndighet*. En sådan myndighet lagrar inte allas privata nycklar som en nyckeldeponeringsmyndighet gör, utan godkänner helt enkelt bara var och ens privata nycklar. Bob kan därför gå till en sådan myndighet, få sin nyckel certifierad, och när Alice vill skicka Bob ett meddelande kan hon enkelt få reda på om Bobs nyckel är godkänd eller inte. I USA finns det sedan förslagen om nyckeldeponering förstås viss skepsis mot att statliga myndigheter skulle ha med sådant att göra. Därför sköter enskilda företag certifieringen, de mest kända är VeriSign och GTE CyberTrust. Warwick Ford på VeriSign kallar certifikatet för ”the cyberspace equivalent of a driver’s license”.[23] Om man av någon anledning besöker områden på Internet som bara är tillgängliga med lösenord, kan det komma upp meddelanderutor angående kryptering och certifiering. Man kan med hjälp av webbläsaren godkänna exempelvis företag och banker, varpå certifikat skapas och lagras i programmet.

I Sverige ligger certifieringsproblemet istället på myndighetsnivå. I kanske den mest färska svenska skrivelsen på området analyserade Statskontoret i en promemoria från november 2003 implementeringen av certifikat och signaturer i de nordiska länderna. Statskontoret hade nämligen den 4 februari 2003 fått av Nordiska ministerrådet uppdraget att vara ”värdinstitution för ett personnätverk om digitala signaturer”. Nätverket kallas *NorDigSign* (*Nordiskt nätverk för digitala strukturer*), och har i uppgift att finna en lösning för ”ömsesidig acceptans av elektroniska signaturer, vid elektronisk kommunikation mellan myndigheterna i de nordiska länderna” samt att föreslå en lämplig elektronisk tjänst som även kräver en säkerhetslösning. Statskontoret kom fram till i promemorian att samtliga nordiska länder har som första steg infört EG-direktivet (1999/93/EG) om ett ramverk för signaturer i de nationella lagarna, och som andra steg börjat anpassa övrig lagstiftning för att underlätta elektronisk kommunikation. Länderna har däremot valt olika ”organisatoriska, tekniska och ekonomiska lösningar”, och har kommit olika långt med spridningen av certifikat till privatpersoner, företag och myndigheter. Norge och Island ligger sämst till, ingen av dem hade 2003 någon infrastruktur för digitala signaturer. Finland var samtidigt det enda land som kunde erbjuda sina medborgare ett certifikat som motsvarade EG-direktivets samtliga krav. Danmark och Sverige ligger trots allt inte långt efter.

I Sverige hade ingen leverantör (2003) anmält till Post- och Telestyrelsen (PTS), som blev tillsynsmyndighet, att man utfärdar certfikat för ”kvalificerade digitala signaturer”. Vem som helst har rätt att utfärda så kallade e-certifikat. Leverantörer som samma år hade ett avtal med Statskontoret var Föreningssparbanken och Handelsbanken (BankID), Nordea bank, Posten samt Telia. Man har tillsammans valt en sådan teknik att alla kan kommunicera med alla, och allt bygger på e-legitimationen som standardiserats och upphandlats. Var och en kan enkelt få en egen e-legitimation. När det gäller bankerna kan kunden få en redan vid anslutningen till Internetbanken. I fallet med Posten och Telia måste kunden dock först besöka Svensk Kassaservice för att där få en säkerhetskod, med vilken han eller hon kan erhålla legitimationen via Internet. Distributionen via bankerna startade under våren 2003, och

[22] Zimmermann, Philip R., 1998. *Cryptography for the Internet*. Sid. 84.
[23] Ford, Warwick, 1998. *How Computer Security Works: (2) Digital Certificates*. Sid. 80.

det uppskattas att det kommer att finnas över en miljon e-legitimationer 2005. Bankernas egen användning spelar stor roll, och det är möjligt att siffran istället kommer att ligga på 3 miljoner.

Redan nu finns det ett antal tjänster på myndighetsnivå som erbjuds allmänheten. Från 2003 är det möjligt att deklarera via Internet; men även Försäkringskassan, Arbetsmarknadsstyrelsen, Finansinspektionen, RSV, PRV och CSN erbjuder omfattande e-tjänster. E-tjänster planeras även inom den privata sektorn, där Svensk Adressändring var först ut. Framtiden får utvisa när det blir möjligt att rösta via Internet.

Statskontoret anser att ”de viktigaste hindren för att öka användningen av offentliga e-tjänster […] är tillgång till applikationer och myndigheternas bristande kompetens inom området”.[24] Jag anser att ett annat hinder är gemene mans bristande intresse och kunskaper inom området. Jag känner själv flera som aldrig i livet skulle våga lämna ut kontokortsnummer via Internet eller än mindre betala räkningar on-line. Dessutom så har inte spridningen av datorer och Internet nått hela befolkningen. Vissa geografiska områden är särskilt utsatta, men även speciella befolkningsgrupper där användningen är låg i jämförelse. Den främsta av dessa grupper är de äldre, men även människor i medelåldern som inte växt upp med datorer och aldrig behövt eller velat lära sig använda dem. Jag tycker att det är viktigt att sprida kunskaperna över hela landet och att arbeta för att tekniken blir så säker att man ärligt kan säga att det inte finns några risker. Som det är nu är det många som är skeptiskt inställda och litar inte på tekniken som finns. De är rädda för att råka ut för bedrägerier och stölder, och det med viss fog. Man kan inte därför bara släppa e-legitimationen lös och vänta på att alla börjar använda den, inte heller kan man bara behålla tjänster som kräver just en sådan. Detta skulle inte fungera och man skulle få samma problem som med nedsläckningen av det analoga tv-nätet. Många företag som lågprisflygbolagen Ryanair och WizzAir godkänner endast biljettbokning via Internet för det är en av faktorerna som håller priset nere. Det är därför mycket tråkigt att somliga tvingas till att välja dyrare och mer traditionella alternativ för att de inte vågar lämna ut privata uppgifter via Internet. Myndigheterna måste på något sätt stävja denna rädsla och övertyga allmänheten om att det är där framtiden ligger. Samtidigt måste man komma ihåg att det är viktigt att endast låta tekniken arbeta för oss, och inte så att det går så långt att vi blir slavar under tekniken.

[24] Statskontoret, 2003-11-24. *Digitala signaturer i Norden – Elektronisk identifiering och elektroniska signaturer i de nordiska länderna*. Sid. 7-8, 27-31.

SLUTSATSER

Jag tillhör dem som tycker att fri kryptering ska få förbli helt fri. Det finns nackdelar med allting, men man kan inte kollektivt bestraffa alla människor bara för att vissa enstaka envisas med att utnyttja sina medmänniskor. Nyckeldeposition är inte ett godtagbart alternativ eftersom de medborgerliga rättigheterna hamnar i farozonen. Att inte göra någonting kan i för sig vara en lösning, men att inte göra något kan i vissa fall också vara ett brott. Det är synnerligen klart att det är mycket viktigt att göra det digitala samhället mycket säkrare. Jag anser att när det gäller kryptering är verifiering och certifiering den rätta vägen att gå. Hederliga människor förlorar absolut ingenting, samtidigt som kriminella visserligen inte blir utan ”jobb” men ändå får det svårare att genomföra brott.

Jag avslutar härmed denna rapport med att gå igenom de problem som jag tidigare har formulerat:

1) Jag anser det vara en medborgerlig rättighet att använda fri kryptering. Det är samtidigt ett privilegium, men inga motprestationer kan krävas utan att begränsningar införs. Kryptering bör förbli vara fri tycker jag, och den åsikten grundar sig visserligen delvis på mina egna etiska värderingar, men främst på de åsikter som svenska myndigheter, kryptoexperter, medborgarrättsorganisationer och lagstiftningen har uttryckt. Det är inte praktiskt möjligt att förhindra kriminella från att använda kryptering. Det går inte att göra en skillnad mellan godkända och icke-godkända användare utan att införa övervakning, vilket skulle krocka med de medborgerliga rättigheterna.

2) Om man inte vill inskränka de medborgerliga rättigheterna finns det ändå en väg att gå. En lösning, eller snarare kompromiss, kan uppnås genom verifiering och certifiering. Jag tycker att det är en bra kompromiss. Hellre det än övervakning, hellre det än anarki. Situationen i världen kan givetvis förändras, och då måste man kanske se problemet i ett annat ljus, men som det är nu finns det inga egentliga skäl att byta riktning. Nyckeldeposition är inte ett bra alternativ, certifiering är ett mycket bra alternativ. Myndigheterna bör fortsätta utveckla de elektroniska tjänster och legitimationer som existerar och samtidigt försöka öka kunskaperna och förståelsen om dessa hos allmänheten. Det faller på deras ansvar att göra tekniken så säker och så användbar att de flesta vill använda den. Inte för att de inte har några andra alternativ, utan för att de själva insett hur enkelt, hur tids- och kostnadsbesparande, och hur säkert det i själva verket är.

KÄLLFÖRTECKNING

Brottsförebyggande rådet (BRÅ), 2003. *Anmälda brott (Riket) – Dataintrång (brottskod 0415)*.
2004-10-18.
http://statistik.bra.se/solwebb/action/anmalda/urval/urval?menyid=43

Denning, Dorothy E. – Baugh, William E., Jr., 1997. *Encryption and evolving technologies as tools of organized crime and terrorism*.
Rapporten publicerades juli 1997 av *the National Strategy Information Center's US Working Group on Organized Crime (WGOC)* och hittades som textfil 2004-10-18 på:
http://www.cosc.georgetown.edu/~denning/crypto/oc-rpt.txt

Ford, Warwick, 1998. *How Computer Security Works: (2) Digital Certificates* i *Scientific American*, oktober 1998.

IT-kommissionen, 1997-05-26. *Avseende användning av kryptering (Dnr IT96/103)*.
Skrivelsen hittad som pdf-fil 2004-09-16 på:
http://www.itkommissionen.se/doc/244.html

IT-kommissionen, 1999-04-15. *Vikten av användning av kryptering*.
Skrivelsen hittad som pdf-fil 2004-09-16 på:
http://www.itkommissionen.se/doc/233.html

Jaap-Koops, Bert, 1999. *The crypto controversy. A key conflict in the information society*.
Haag: Kluwer Law International.
Denna doktorsavhandling publicerades på Internet 1998-12-18.
http://rechten.uvt.nl/koops/THESIS/thesis.htm

Jaap-Koops, Bert, 2004. *Overview per country. Version 22.2*.
2004-10-18.
http://rechten.uvt.nl/koops/cryptolaw/cls2.htm

Lewis, Ted, 1997. *We Don't Need No Regulation (Cyber View)* i *Scientific American*, november 1997.

OHCHR, 1998-07-20. *Universal Declaration of Human Rights (Swedish version)*.
2004-10-11.
http://www.unhchr.ch/udhr/lang/swd.htm

Rivest, Roland L., 1998. *The Case against Regulating Encryption Technology* i *Scientific American*, oktober 1998.

Singh, Simon, 2002. *Kodboken*. Stockholm: Norstedts förlag.

Statskontoret, 2003-11-24. *Digitala signaturer i Norden – Elektronisk identifiering och elektroniska signaturer i de nordiska länderna*.
Promemorian hittad som pdf-fil 2004-10-23 på:
http://www.statskontoret.se/upload/Publikationer/2003/2003124.pdf

Svensk författningssamling, 1962. *Brottsbalken*.
2004-10-16.
http://www.notisum.se/rnp/SLS/LAG/19620700.HTM

Svensk författningssamling, 2003. *Regeringsformen (SFS 2003:593 Omtryck)*.
Grundlagen hittad som pdf-fil 2004-09-19 på:
http://62.95.69.3/sfsdoc/03/030593.pdf

The United States of America. (Publiceringsdatum och år okänt – originalet ratificerat 1791-12-15). *Amendments to the Constitution*.
2004-09-19.
http://www.house.gov/Constitution/Amend.html

Utrikesdepartementet, 1999-05-06. *Om kryptografi (SKR 1998/99:116)*.
Skrivelsen hittad som pdf-fil 2004-09-16 på:
http://www.regeringen.se/content/1/c4/13/82/021db96c.pdf

Whaley, Al (Red.), 1994-01-24. *Crypto Experts Oppose Clipper: Letter to the President of the United States*.
2004-09-19.
http://www.eff.org/Privacy/Key_escrow/Clipper/experts_v_clipper.letter

Zimmermann, Philip R., 1998. *Cryptography for the Internet* i *Scientific American*, oktober 1998.