nov. 2011

Hur hemlig är en hemlighet?

Viggo Wentzel

Om äkta och falskt och hemligheter. Kryptografi och kryptoanalys

Så länge vi har haft tal- och skriftspråk har det funnits ett behov av att hålla vissa uttalanden eller texter hemliga. Med tillkomsten av telekommunikation och internet har behovet av säkra förbindelser ökat och blivit mer komplicerat. Ett enkelt sätt är att gömma undan hemligheter, till exempel biskop Brasks klassiska lapp ” härtill är jag nödd och tvungen”. Men då existensen av ett hemligt dokument är känd finns alltid risken att det kan läsas av en obehörig. Kryptografi är en teknik där man med hjälp av ett regelverk och en nyckel gör texten oläslig. Endast den som har tillgång till regelverket och nyckeln kan återskapa texten till läslig form. Kryptering fanns redan på Caesars tid om än i elementär form.

Den här tekniken är tillämpbar även på öppna dokument då man vill vara säker på att dokumentet inte manipulerats på något sätt, till exempel resultatet av ett val. Identitetsverifiering är ett annat exempel i form av e-legitimation som vi använder när vi kommunicerar med banken eller skatteverket.

Det är givet att det ständigt pågår en kamp mellan krypteringsmetoder och de som försöker knäcka krypteringskoden. Det är heller inte ovanligt att säkerhetsorganisationer försöker begränsa tillåtna nyckellängder för att med sina kraftfulla datorer lättare kunna dekryptera dokument i övervakningssyfte. Att försöka dekryptera ett krypterat dokument utan att ha tillgång till nyckeln kallas för kryptoanalys.

Det finns två grundläggande metoder för kryptering:
antingen kastar man om tecknen i dokumentet enligt någon viss regel (transposition),
eller byter man ut tecknen i dokumentet mot andra symboler (substitution),
eller en kombination av bådadera.

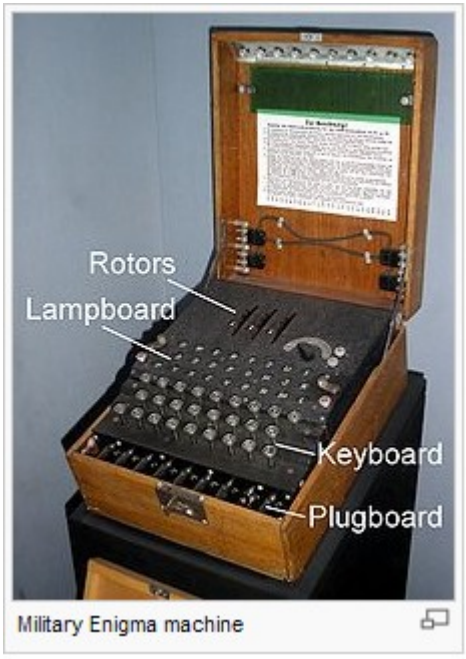
Exempel:Data Encryption Standard (DES) är en typ av symmetrisk kryptering som utnyttjar en kombination av substitution och transposition. DES arbetar på block av 64 bitar och har en nyckellängd av 56 bitar. Samma nyckel användes både vid kryptering och dekryptering, varför nyckeln måste överföras till mottagaren på ett säkert sätt. DES anses i dag som osäkert och har börjat ersättas med andra metoder.

Efter det att datorer blivit allmänt tillgängliga har andra metoder tillkommit som kräver mycket räknearbete.

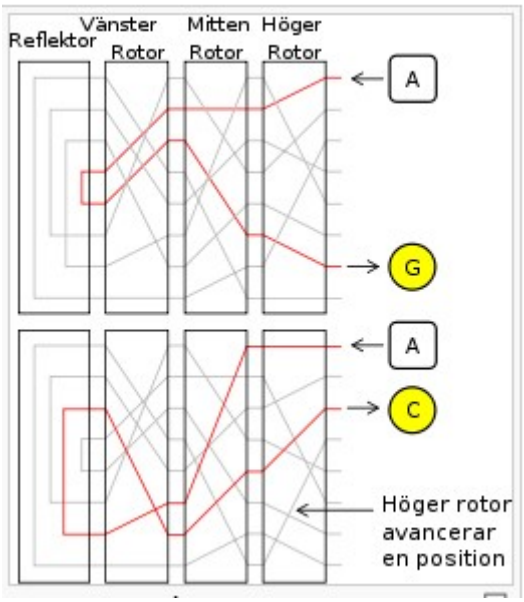
Kryptografi före datorn

Det går att kryptera ett dokument med enbart manuellt arbete men bara för enkel kryptering som är lätt att knäcka. För någorlunda säker kryptering är maskinella hjälpmedel en nödvändighet, och speciellt om kryptering och dekryptering skall utföras av okvalificerad personal och för ett stort

flöde av meddelanden. I slutet av första världskriget uppfann en tysk ingenjör en krypterings-maskin som fick namnet Enigma (namnet betyder gåta). Maskinen utvecklades i flera varianter och användes av många länder före och under andra världskriget. De versioner som utvecklades av den tyska krigsmakten var ytterst säkra. Att de allierade ändå lyckades knäcka de tyska koderna var delvis en följd av mänskliga misstag, erövrade kodböcker och liknande. Även om man lyckades komma över ett exemplar av Enigma var det hart när omöjligt att dekryptera ett meddelande om man inte kände till begynnelsevillkoren i maskinen.



Enigma



Rotornätverk

Enigma var en kombination av finmekanik och elektriska kretsar och följande är en förenklad beskrivning av maskinen: Enigma arbetade enligt substitutionsmetoden det vill säga en bokstav i klartextmeddelandet ersattes med en annan bokstav i det krypterade meddelandet enligt en viss regel Huvuddelarna bestod av ett tangentbord där det ursprungliga meddelandet skrevs in, en lamptablå där det krypterade meddelandet visades bokstav för bokstav samt tre eller fyra rotorhjul. Dessa hjul kunde vridas lika många steg som det finns bokstäver i alfabetet, och varje hjul var förbundet med det intilliggande hjulet genom ett nätverk av ledningar. Då en tangent trycktes ner slöts en strömkrets från tangenten genom rotorhjulen, därefter tillbaka genom rotorhjulen och slutligen till lamptablån. Om rotorhjulen stod stilla mellan successiva tangentinmatningar skulle det krypterade meddelandet följa en fast regel lika för alla bokstäver, och en sådan kryptering skulle vara lätt att knäcka. I stället flyttas ett eller flera rotorhjul ett steg mellan varje inmatning vilket ger en unik substitution för varje inmatad bokstav.

Enigma har den egenskapen att samma maskin kan användas även för dekryptering förutsatt att rotorhjulen har exakt samma begynnelseläge som vid krypteringen. Eftersom begynnelseläget av säkerhetsskäl måste vara unikt för varje nytt meddelande måste detta inledas med information om det använda begynnelseläget. Detta är en svag punkt i systemet.

Dramat på Atlanten.

Varje militär vet att en seger i strid är förgäves om inte försörjningen till den egna truppen fungerar. Varje stridande trupp har mycket stora behov av ersättningsmanskap, sjukvård, mat, bränsle och ammunition. Därför är det vitalt att försörjningslederna hålls öppna.

I början av andra världskriget då Tyskland behärskade större delen av Europa stod Storbritannien ensamt och var helt beroende av USA för sin försörjning, såväl civilt som militärt. En kraftmätning utspelades på Atlanten mellan de allierades konvojer och Tysklands ubåtsvapen. Bägge parter var hänvisade till radiotrafik för kommunikation och radiotrafik kan avlyssnas. Därför var det vitalt att alla meddelanden var krypterade. Samma situation upprepades några år senare då Tyskland anfallit Sovjetunionen men nu i nordatlanten och leden till Murmansk. Storbritanniens resurser för kryptoanalys var underutvecklade och det gällde i synnerhet Royal Navy. För att råda bot för detta organiserades en central grupp för alla tre vapenslagen som lokaliserades till ett engelskt herresäte vid namn Bletchley Park. Hur denna grupp så småningom lyckades knäcka den tyska Enigma koden är en av andra världskrigets mest dramatiska och spännande händelser och är numera väl dokumenterad. Men det gällde också att handskas med den nyvunna informationen med försiktighet. Motparten fick ju helst inte ana att man knäckt koden.

Efter kriget lär Churchill ha yttrat att kunskapen om den tyska krypteringen förkortade kriget med två år. Personligen har jag inte sett någon motsvarande redogörelse för den tyska kryptoanalysen men jag utgår ifrån att den var minst lika intensiv som de allierades.

I Bletchley Park samlades flera av Storbritanniens skickligaste matematiker däribland den unge Alan Turing. Gruppen fick en flygande start genom att några polska matematiker hade kommit ett bra stycke på väg att dekryptera Enigma-kodade meddelanden. Resultatet överlämnades till Storbritannien bara veckor före den tyska invasionen av Polen. I Bletchley Park gällde det att hitta matematiska metoder för dekryptering och här spelade Alan Turing en avgörande roll. Men det räckte inte med detta. För att ett meddelande skulle vara användbart måste dekrypteringen gå fort och man måste dessutom kunna hantera ett stort flöde av meddelanden. Maskinella hjälpmedel var alltså en nödvändighet, och för att få upp hastigheten måste dessa konstrueras med elektronik. Två konstruktioner såg dagens ljus, och de döptes till Bomb respektive Colossus. Den sistnämnda som framställdes i flera exemplar innehöll 1500 till 2500 elektronrör och var mig veterligen världens första storskaliga elektroniska räkneautomat.

Alan Turing hade redan före kriget dragit upp riktlinjerna till en generell programstyrd datamaskin men han fick aldrig se en sådan i verkligheten. Man skulle tro att Storbritannien skulle hysa stor tacksamhet till detta matematiska geni men så blev det inte. Alan Turing var homosexuell och detta var kriminellt vid denna tid. Han dömdes till fängelse men fick välja att i stället utsättas för hormonbehandling. Han stod inte ut med detta utan tog sitt eget liv.

Ett svenskt Bletchley Park

Den 9 april 1940 invaderade Tyskland Danmark och Norge. Det var en av militärhistoriens djärva ste och skickligaste operationer. Brittiskt underrättelseväsen togs totalt på sängen och inte heller svensk underrättelsetjänst visste något i förväg. Några dagar efteråt begärde Tyskland att få utnyttja den svenska västkustkabeln för sin trafik med hemlandet. Tyskarna använde teleprinter och naturligtvis begagnade svenskarna tillfället att avlyssna trafiken. Men redan under april månad installerade tyskarna en krypteringsapparat anpassad för teleprinter och som gick under namnet G-skrivaren. Det officiella namnet var T52 och den tillverkades av Siemens & Halske. Åtminstone de senare versionerna ansågs vara mer avancerade än Enigma. Naturligtvis skulle det vara av stort värde för den svenska regeringen och militären om man kunde följa trafiken på kabeln i klartext. Följaktligen organiserades en analysgrupp och den egentliga kryptoanalysen anförtroddes till Arne Beurling, professor i matematik vid Uppsala Universitet.

Analysgruppen hade inte tillgång till någon G-skrivare men arbetet underlättades av ett slarv från de tyska operatörernas sida: Man bytte inte alltid kryptonyckel mellan meddelandena. Till stor förvåning lyckades Beurling redan efter ett par veckors arbete knäcka den tyska koden men hur han bar sig åt tog han med sig i graven.

Nu följde en intensiv tid. För att hinna med den allt intensivare trafiken automatiserades delar av dekrypteringen med utrustning som Ericsson tillverkade. I början av 1944 hade 300 000 meddelanden dekrypterats. Så till exempel kände svenska regeringen i förväg till planerna på operation Barbarossa och via den svenske Moskvaambassadören informerades Stalin om dessa planer. Men Stalin valde att ignorera budskapet.

Datorns intåg, en revolution

Eftersom kryptoalgoritmer baseras på matematiska beräkningar innebar datorns introduktion på 1950-talet en fullkomlig revolution för kryptologin. I dag har kryptoteknik blivit en del av vardagen så fort vi skall kommunicera med banken via internet eller identifiera oss med e-legitimation.

Det skulle föra för långt att försöka redogöra för den mängd nya kryptotekniker som finns idag Men en förenklad beskrivning av RSA algoritmen kan vara intressant. RSA står för upphovsmännen

Rivest Shamir Adleman

RSA arbetar med två nycklar varav den ena är offentlig och den andra hemlig. Om ett meddelande krypteras med den offentliga nyckeln så kan endast den som innehar den hemliga nyckeln dekryptera meddelandet. Om å andra sidan jag vill styrka min identitet krypteras denna med den hemliga nyckeln varefter alla som har den offentliga nyckeln kan vara säkra på att jag är jag.

Man börjar med att välja ut två stora primtal, p och q, och definierar sedan tre tal n, e och d med relation till primtalen. n är i sin tur produkten av de två stora primtalen och säkerheten i kryptot är baserat på svårigheten att faktorisera n i de två primtalen. RSA använder exponentiella funktioner på så sätt att det krypterade meddelandet är lika med meddelandet upphöjt till e, räknat modulo n.

RSA

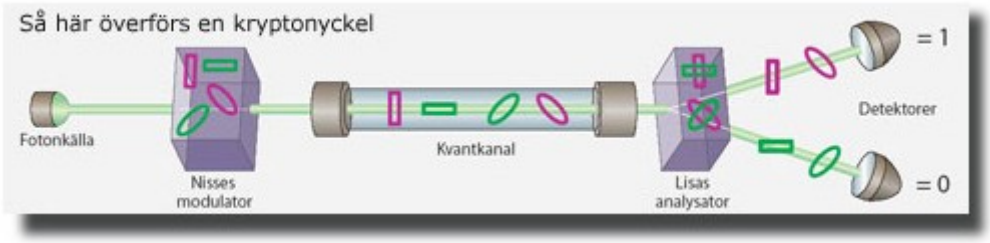
1. Två stora primtal, p och q
2. n=p * q
3. e relativt prim (p-1)(q-1)
4. ed kongruent 1 (modulo (p-1)(q-1))

E: meddelande i klartext
D: krypterat meddelande
Publik nyckel: e,n
Hemlig nyckel: d,n

$D=E^e$ modulo n
$E=D^d$ modulo n

Kvantkryptografi

Man skulle tycka att med dagens säkra kryptoalgoritmer i förening med kraftfulla datorer så finns det inget mer att uppfinna. Men så är inte människan beskaffad. För en tid sedan läste jag en liten notis i Corren om ett nytt laboratorium som invigts på universitetet och som var avsett för forskning och undervisning inom kvantkryptografi. Jag blev överraskad. Visserligen hade jag läst om användning av kvantfysikens lagar för kryptering men jag trodde att detta alltjämt tillhörde science fiction. Så efter fattig förmåga började jag att tränga in i ämnet. Det visade sig att kvant-fysik användes för att överföra hemliga nycklar mellan sändare och mottagare, en känslig procedur i alla kryptosystem.

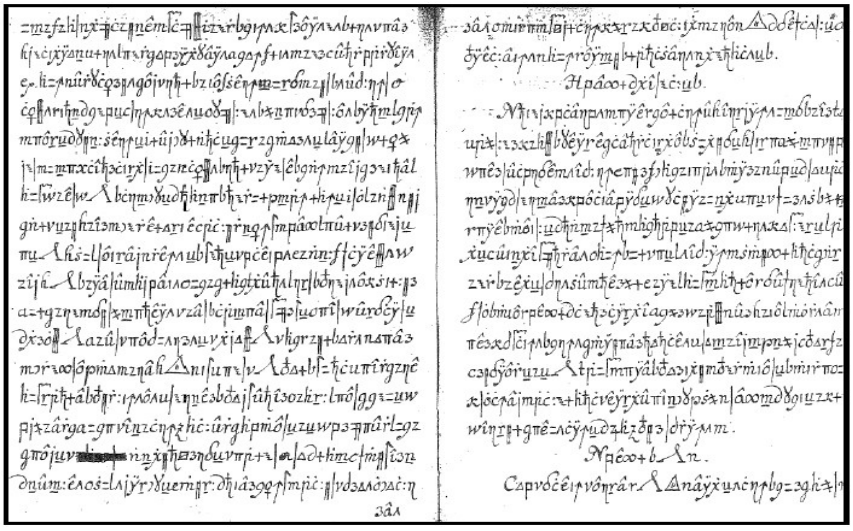


Fotonen är ljusets minsta beståndsdel, en partikel utan massa men med spinn i fyra olika riktningar samtidigt. En-lysdiod har förmågan att emittera en foton i taget vilket möjliggör att sända i väg ett kontrollerat flöde av fotoner i en optisk fiber. Om ett polarisationsfilter placeras efter sändaren ändras fotonens spinn till en enda riktning beroende på filtrets orientering. Om även mottagaren har ett filter passerar fotonen detta oförändrat om filtret har samma orientering som det i sändaren. I annat fall ändras spinnriktningen. Detta utnyttjas genom att låta fotonens spinnriktning representera binära ettor och nollor. Ett försök till avlyssning avslöjas obönhörligen genom att en elementarpartikel ändrar karaktär så fort den registreras.

Överföring av krypteringsnycklar har faktiskt genomförts med ovanstående metod i Schweiz 2007 i samband med en folkomröstning. Vi lär få se ännu mer spektakulära metoder i framtiden.

Hur hemlig är en hemlighet?

Ja vad skall man svara i en tid med Wikileaks och 100.000 hemliga lösenord som bjuds ut på nätet. Skall man peka på en generell trend är det att hemligheter tenderar att bli ganska kortvariga bland annat på grund av slarv, läckor och lösmynthet. Men det finns undantag. Ett spektakulärt sådant är Copiale-dokumentet som skrevs på sjuttonhundratalet och krypterades. Under flera hundra år har chiffret trotsat alla försök till kryptoanalys, ända tills nu. Men nyligen har en professor i Kalifornien tillsammans med två språkvetare i Uppsala lyckats knäcka koden med hjälp av moderna datorstödda analysmetoder. Det visade sig att dokumentet som är skrivet på tyska innehöll en beskrivning av de hemliga riterna i ett hemligt sällskap. Det är verkligen som gjort för att sätta fantasin i rörelse.



Två sidor ur Copiale-dokumentet

Så vad gör vi med våra hemligheter? För vi har alla ”lik i garderoben” och hade vi inte det så var vi inga människor utan änglar eller robotar. Mestadels är det ganska harmlösa saker men ibland gäller det liv eller död. Som i alla tider har vår överhet en strävan efter kontroll, att få så stor insyn som möjligt i undersåtarnas liv och leverne. I vår tid har ny teknik gett överheten nya verktyg i detta syfte och här gäller det för oss att sätta ner foten: hit men inte längre.

Rör inte våra hemligheter!

Referenser

1. *Cryptography and data security*, Dorothy Denning, ISBN 0-201-10150-5
2. *Alan Turing: The Enigma*, Andrew Hodges, ISBN 9780099116417
3. *Enigma machine*, http://en.wikipedia.org
4. *Så knäckte svenskarna Hitlers koder*, http://www.idg.se
5. *RSA*, http://sv.wikipedia.org
6. *RSA-kryptering i enkla steg*, http://www.oru.se
7. *Hemligare med atomer och fotoner*, http://foi.se
8. *How Quantum Cryptology works*, http://science.howstuffworks.com
9. *The Copiale Cipher*, Kevin Knight, Beáta Megyesi, Christiane Schaefer, http.www.isi.edu