Nämnarens kryptoskola

3. Kryptots historia

I denna del av Kryptoskolan tar vi en titt på kryptots historia. Här finns några glimtar som kan vara intressanta för en större krets. De flesta uppgifterna i denna del kommer från tre böcker som är särskilt läsvärda om man är intresserad av kryptering. Dessa är Kahn: The Codebreakers [1], Bengt Beckman: Svenska kryptobedrifter [2] samt Simon Singh: Kodboken [3]. Innehållet i dessa böcker beskrivs närmare i slutet av denna del, där man även finner en ordlista.

De andra delarna finner du på ncm.gu.se/arkivN. Kryptoskolan är ett material som är skyddat av upphovsrättslagen. Studiematerialet får dock fritt kopieras för användning i undervisning eller för enskilt arbete och rekommenderas från årskurs 4 till gymnasiet.

Användning av hemlig skrift är mycket gammal. Konsten att kryptera var känd i det gamla Egypten och i Babylonien. Men låt oss börja i romarriket för cirka 2000 år sedan. Det är belagt att man då använde det krypto som nu går under benämningen Caesar-krypto.

Införandet av Caesar-krypto anses vara en stor förbättring av möjligheterna att sända hemliga meddelanden jämfört med den metod som användes i följande anekdot: Om man ville skicka ett meddelande från Rom till någon av provinserna utan att några fientligt sinnade personer kunde ta reda på innehållet rakade man av håret på en slav, ristade in texten i huvudsvålen och lät sedan håret växa ut. Slaven skickades iväg till den behörige mottagaren som rakade av slavens hår och som sedan kunde läsa meddelandet. Detta sätt att dölja ett meddelande är inte kryptering utan ett exempel på *steganografi*, dold skrift. Sanningshalten hos denna berättelse kan betvivlas.

Krypteringsprocessen för Caesar-krypto går till så här: Texten i ett meddelande skall ersättas, bokstav för bokstav, genom att man som kryptobokstav tar den som ligger ett visst antal steg längre fram i alfabetet, säg tills vidare tre. Om den första klartextbokstaven är *H* blir den första kryptobokstaven *K*.

Det tal som styr krypteringen behöver inte vara just tre, som romarna nöjde sig med, utan vilket annat heltal som helst mellan 1 och 28; vi kallar det i det följande för *kryptonyckeln* och betecknar den N, $1 \leqslant N \leqslant 28$ för det svenska alfabetet. Den som bestämmer kryptonyckeln får överlämna den till den andra personen på ett säkert sätt t ex vid ett sammanträffande. Med en matematisk formel kan man beskriva krypteringsförfarandet så här

$$C = K + N \pmod{29}, \qquad (1)$$

där (mod 29) här betyder att vi subtraherar 29 om summan blir större eller lika med 29.

Rökstenen

Foto: Bengt A Lundberg

Vid Rök kyrka i Östergötland står en märklig runsten, ristad på 800-talet. Denhar världens längsta runinskrift, över 800 runtecken. Huvudsakligen används runor ur alfabetet med sexton bokstäver, men det finns också tecken från den äldre runraden om tjugofyra bokstäver. Dessutom finns lönnrunor, dvs kryptotext som erhållits med tre eller fyra olika krypteringsmetoder.

Mest iögonfallande av lönnrunorna är runkorsen. Här har runristaren tänkt sig att runalfabetet är indelat i tre segment. Lönnrunan anger segment och ordningsnumret för tecknet i segmentet.

Med ett annat sätt att bilda lönnrunor används på rökstenen metoden att från en ”klartextruna” flytta sig ett steg fram i runalfabetet. Dit man då kommer blir motsvarande lönnruna. Men detta är ju Caesarkrypto med kryptonyckeln N = 1! Har runristaren på något sätt fått kännedom om detta krypto eller har han listat ut det själv? I vilket fall som helst måste det anses vara en stor bravad.

Bilden och uppgifterna om Rökstenen har jag hämtat ur en uppsats i Forskning och Framsteg nr 5, 1998, [5] där det också finns beskrivet både äldre och nyare tolkningar av runskriften, när den väl är dekrypterad, transkriberad och översatt till modern svenska. Se även [6].

Enkel substitution

Det stod snart klart att ett meddelande krypterat med Caesars metod är mycket lätt att forcera. Man behöver bara pröva igenom de 28 olika nyckelmöjligheterna och se efter vilken av de 28 olika ”klartexterna” som blir meningsfull. Ett något mer svårforcerat krypto får man om man ersätter kryptoalfabetet med en omordning, *permutation*, av bokstäverna i alfabetet, t ex så här:

Kryptonyckel $\mathcal{N}$:

Klartext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	å	ä	ö
Krypto	Q	G	M	C	Z	P	T	H	R	U	L	A	V	Y	Ö	D	Ä	Å	I	B	X	N	S	F	O	K	W	E	J

$\mathcal{N}$ är här inte ett heltal utan substitutionen/funktionen som definieras av tabellen. När man krypterar letar man upp klartextbokstaven i den övre raden. Motsvarande kryptobokstav står i den undre raden, under klartextbokstaven. Sålunda blir klartextbokstaven *g* kryptobokstaven *T*. Krypteringsformeln blir

$$C = \mathcal{N}(K) \qquad (2)$$

Här är ett påbörjat exempel med nyckeln ovan:

Klartext	t	j	u	v	e	n	s	t	a	l	b	å	t	e	n
Kryptotext	B	U	X	N											

Vigenères krypto

Så småningom blev man uppmärksam på att även en enkel substitution är lätt att forcera om meddelandets längd inte är väldigt kort. Forceringen bygger på att olika bokstäver uppträder olika ofta (med olika frekvens) i vanlig text. Om bokstaven *a* förekommer i svensk text i tolv fall på hundra, gäller att motsvarande kryptobokstav, Q med nyckeln beskriven ovan, förekommer med samma frekvens i en kryptotext. Läs gärna mer om detta i *Kodboken* av Simon Singh [3].

En förbättring av Caesarkryptot brukar tillskrivas den franske diplomaten Blaise de Vigenère, född 1523, och kallas därför *Vigenèrekrypto*. Detta är enkelt att beskriva om vi går ut från krypteringsformeln (1) ovan. Med Vigenèrekrypto använder man olika tal N för varje bokstav som skall krypteras:

$$C_j = K_j + N_j \pmod{29} \qquad (3)$$

där C_j och K_j är siffermotsvarigheterna till klartextbokstav respektive kryptobokstav nr. j i respektive text. N_j är det tal som skall kryptera klartextbokstav nr j.

För att följden med talen N_j inte skall bli för svår att hantera, är den periodisk för Vigenèrekryptot. Dessutom kan de ha uttalbara motsvarigheter i alfabetet. Om nyckelordet är *BEDA* blir de första N-talen 1, 4, 3, 0, 1, 4, 3, 0, 1, 4, ... Låt oss kryptera vår favoritmening med denna nyckel.

Klartext	t	j	u	v	e	n	s	t	a	l	b	å	t	e	n
Klartext m. tal	19	9	20	21	4	13	18	19	0	11					
Addera nyckel	1	4	3	0	1	4	3	0	1	4					
Kryptotext m. tal	20	11	3	21	5	17	21	19	1	15					
Kryptotext	U	N	X	V	F	R	V	T	B	P					

Ett krypto som arbetar enligt formeln (3) kallas i denna uppsats linjärt. En annan typ av krypto får vi om vi i stället går ut ifrån formeln (2) för enkel substitution och använder olika substitutionsalfabeten $\mathcal{N}_j$ för bokstäverna som skall krypteras. Här blir det än mer nödvändigt att begränsa antalet olika $\mathcal{N}_j$ och sedan upprepa deras användning. Formeln blir

$$C_j = \mathcal{N}_j(K_j) \qquad (4)$$

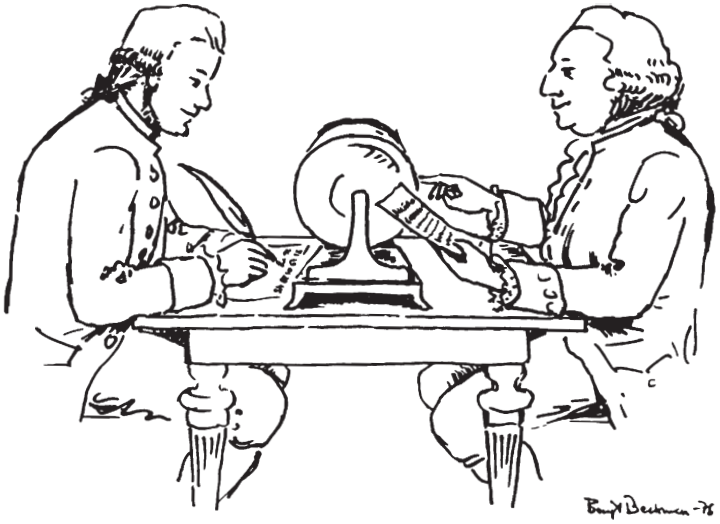
Ett sådant krypto kallas ibland *oordnad Vigenère* men här kallar vi det *olinjärt*.

Allteftersom forceringstekniken utvecklades blev det nödvändigt att göra kryptonycklarna mer omfattande, dvs öka perioden för N(j) respektive $\mathcal{N}$(j). Nycklarna blev svårare att hantera och krypterings- och dekrypteringsarbetet blev mer tidsödande. Antalet fel i arbetet ökade. Så småningom byggde man mekaniska apparater som utförde arbetet, sedan elektrifierades de. När elektroniken kom blev krypteringsapparaterna elektroniska och så småningom lät man datorer utföra krypteringen. Dock, under lång tid arbetade krypteringsapparater alltid (eller åtminstone nästan alltid) enligt en av de två principerna (3) eller (4).

Världens första krypteringsapparat

På 1400-talet uppfanns den s kchifferskivan, en mycket enkel mekanisering av Caesarnyckeln. Men om man inte räknar med den, så var världens första mer avancerade krypteringsapparat svensk. Den presenterades år 1786 i ett brev till Gustaf III. Uppfinnaren, tillika brevskrivaren, hette Fredrik Gripenstierna (1728-1804). Hans morfar är mera känd, Christofer Polhem.

De viktigaste delarna i Gripenstiernas krypteringsapparat är ett antal hjul, vartdera försett med alfabetet i ordning. På ena sidan av det bord där apparaten står, sitter den behörige ämbetsmannen och ställer in en klartextrad med en bokstav för varje hjul. På den andra sidan sitter den obehörige sekreteraren och skriver av motsvarande kryptotext; varje kryptotecken är ett tal mellan 0 och 99. Dessa tal står i oordning på baksidan av hjulen. Kryptot är alltså olinjärt. Teckningen, liksom uppgifterna i detta avsnitt, kommer från ”Svenska kryptobedrifter” av Bengt Beckman, [2] där det finns en utförlig beskrivning av Gripenstiernas krypteringsapparat och hur man skulle kunna tänka sig att fullständigt rekonstruera kryptot utgående från en kryptotext och *pålägg*, dvs från ett stycke av den motsvarande klartexten.



Första världskriget

När första världskriget bröt ut var man ganska väl förberedd när det gäller krypton – trodde man. Man använde handkrypton och krypteringsapparater samt även koder. En kod för kryptobehov består av förutom enskilda tecken vanligen förekommande ord och fraser samt deras krypterade motsvarigheter. En kod blev ofta en ganska stor bok. En fördel var att meddelandena blev kortare i krypterat skick. Nackdelen var att det blev oerhört viktigt att hålla koden hemlig. När den avslöjats, genom forcering eller stöld, gällde det att distribuera en ny till alla dem som man ville kommunicera med.

Men även på forceringssidan hade man gjort förberedelser. Särskilt i Frankrike hade man efter det förödmjukande Fransk-tyska kriget 1870-1871 byggt upp resurser för signalspaning och forcering av kryptomeddelanden. Även i andra länder fanns både kryptometoder och forceringsorgan. Marconis uppfinning av radion gav möjligheter för de krigförande men också tillfällen för den avlyssnande fienden. Behovet av krypto hade ökat.

Men de som konstruerat krypton hade långt ifrån alltid förutsett de geniala forcörernas möjligheter att knäcka deras krypton. På alla håll fick man fram värdefulla underrättelser genom forcering och dessa var långt ifrån oväsentliga för krigets förlopp. Störst betydelse hade nog forceringen av det s k Zimmermanntelegrammet. Detta var ett kodmeddelande från den tyske utrikesministern Arthur Zimmermann till Mexikos president där man dels aviserade det obegränsade ubåtskriget dels uppmanade Mexiko att anfalla USA, eventuellt med stöd av Japan. Telegrammet avlyssnades, forcerades i Storbritannien och delgavs USA. Där bidrog dessa underrättelser starkt till att man bröt sin neutralitet och inträdde i kriget.

Betydande delar av forceringsverksamhet i olika länder under andra världskriget dokumenterades 1931 av den svenske kryptologen Yves Gyldén: Chifferbyråernas insatser i världskriget till lands [7].

Mellankrigstiden

Erfarenheterna från världskriget togs till vara och man utnyttjade tekniken, särskilt möjligheten att använda elektromekaniska apparater. Det fanns ett särskilt behov av att åstadkomma långa följder av slumptal eller åtminstone följder av tal som liknande slumptal så mycket som möjligt. Redan på 1800-talet hade Vigenèrekryptot med kort nyckel visats vara osäkert. Men om man med teknikens hjälp kunde alstra långa följder av nyckeltal?

Ett sätt att åstadkomma långa slumpliknande tal eller matematiska transformationer var att använda flera lika stora hjul, vartdera med en indelning i delar, t ex 26 som antalet bokstäver i det internationella alfabetet. Hjulen monteras på en axel och fås att rotera efter varje krypteringssteg som ett räkneverk. Hjulet längs till höger flyttas ett steg för varje krypteringssteg, nästa hjul flyttas ett steg när det första gått ett varv osv. Om vi exempelvis använder fem hjul dröjer det 26^5 eller nästan 12 000 000 steg innan man kommer tillbaka till ursprungsläget. Det verkar vara betryggande mycket större än ett ganska stort skriftligt meddelande. Om man kan utnyttja hjulens möjligheter borde man kunna åstadkomma en stark kryptering, åtminstone vad gäller periodens längd.

I Tyskland konstruerades Enigma-kryptot efter denna princip. Vart och ett av hjulen, som kunde vara tre eller flera till antalet, hade två uppsättningar om 26 kontakter och mellan dessa 26 elektriska kopplingar som överförde en signal från en bokstav till en annan. Kryptot blev olinjärt.

Japanerna konstruerade ett krypto som i USA kallades Purple. Principen för Enigma var känd i Japan och man kan anta att kryptot var av liknande typ.

Ett annat sätt att med hjälp av hjul åstadkomma långa slumpliknande serier av tal är att använda hjul med olika långa indelningar som parvis inte skall ha några gemensamma faktorer och sedan låta alla hjulen flytta sig ett steg efter varje krypteringssteg. Hjullängderna 26, 25, 23, 21, 19 och 17 ger exempelvis totala perioden $26 \times 25 \times 23 \times 21 \times 19 \times 17$ eller drygt 100 000 000 steg, också det mycket större än ett långt meddelande.

I Tyskland tog man också fram andra typer av krypton. Ett kallades Geheimschreiber. Med fjärrskrift kunde man med långa avstånd elektriskt koppla ihop två elektromekaniska terminaler med tangentbord och utskriftsanordning. Man skrev sin text på den ena terminalen och med försumbar fördröjning skrevs texten ut på den apparat som man var uppkopplad med (den tidens

chat). Varje bokstav och typografiskt tecken kodades med en fembitskod. Men eftersom den överförda texten var lätt att avlyssna, gällde det att kryptera den, om ledningen var tillgänglig för obehöriga (läs annan stat). Geheimschreiber var därför försedd med ett inbyggt krypto, som var olinjärt och där periodlängden säkerställdes med hjul av olika längd.

I Sverige ledde den uppfinningsrike ingenjören Boris Hagelin konstruktionen av en familj av mekaniska krypteringsapparater. Franska staten beställde 5 000 st. men de kom inte till leverans. Kriget kom emellan. Hagelin lyckades dock mitt i brinnande krig ta sig till USA med en nermonterad apparat i bagaget. Amerikanerna blev intresserade och 140 000 exemplar tillverkades enligt konstruktörens anvisningar. Efter kriget startade Hagelin en firma i Schweiz, ett företag som fortsatte att utveckla och tillverka olika typer krypteringsapparater som såldes och säljs i ett stort antal länder. Hagelins krypteringsapparater arbetade med olika långa hjul och var väsentligen linjära.

Ett tredje sätt att åstadkomma långa sekvenser är att helt enkelt låta en god slumpmekanism lotta fram så många tal som motsvarar totallängden av alla meddelanden som man kan tänkas vilja sända till en viss mottagare och distribuera denna nyckelmängd i förväg med kurir till sändare och mottagare. Sedan gäller det också att aldrig använda ett tecken i nyckeln mer än en gång. Rätt hanterat är ett sådant engångskrypto oforcerbart. Varför slog dessa krypton aldrig igenom på bred front? Det visade sig att svårigheterna med att alstra nycklarna och distribuera dem till användarna i praktiken oftast var oöverstigliga. Det gällde att skicka mycket nyckelmassa på ett säkert sätt till varje par av enheter som behövde kommunicera med varandra. Användningen fick därför begränsas till ett fåtal användare som hade mycket hemliga meddelanden att utväxla. Även vid andra världskrigets början var man alltså väl försedd med för den tiden moderna krypteringsapparater. Men även på forceringssidan hade man tagit tillvara erfarenheterna från första världskriget.

Andra världskriget

Om man var väl förberedd kvalitativt när det gäller hantering och forcering av krypton, så var det betydligt sämre när det gäller kvantiteten. Vid och strax efter krigsutbrottet rekryterades många personer, män och kvinnor, till denna tjänst. I Sverige tog man kontakt med duktiga korsordslösare och publicerade också enkla kryptouppgifter. De som skickade in rätt lösning blev en god rekryteringsgrund. Forceringsorganisationerna lyckades väldigt väl i det underrättelsekrig som fördes med krypto, signalspaning och forcering – *kriget i etern* brukar det kallas. Här beskrivs tre av de mest omtalade fallen.

Enigmakryptot forcerades som resultat av ett lagarbete. Fransmännen hade fått tillgång en detaljerad beskrivning av en av de varianter som användes av tyskarna. Underlaget lämnades vidare till polackerna som gjorde stora framsteg när det gällde forceringen. Strax innan Polen anfölls av tyskarna flydde några polska forcörer till Storbritannien med tillräckligt underlag för att man där kunde fortsätta arbetet med att avslöja mycket av tyskarnas hemliga radiotrafik. Både i Storbritannien och i Frankrike hade man trott att Enigma var oforcerbar och man blev mycket förvånad när man fick höra om polackernas framgångar. Men hela tiden förbättrade tyskarna Enigma och nya modeller kom ut som med tiden blev allt svårare att forcera. Till sin tjänst tog britterna forceringsapparater som blev föregångare till dagens datorer. Av flera anledningar är det synd att

knappast någon dokumentation av dessa ”predatorer” finns kvar. Allt förstördes efter krigets slut. Det skulle dröja ända till 1970-talet innan det blev allmänt känt att engelsmännen lyckats knäcka ett av Tysklands viktigaste krypton.

I USA hade man lyckats knäcka Purple. Den prestationen utfördes av en grupp matematiker där William F. Friedman var den ledande. Friedman hade redan under första världskriget börjat arbeta med kryptologi och under mellankrigstiden fortsatte han att utveckla konsten och organisationen. Trots forceringsframgångarna kunde man inte få underrättelser som varnade för japanernas anfall av Pearl Harbor. Detta är en fråga som har analyserats i detalj flera gånger. Man kan nog sammanfatta resultaten som så att det helt enkelt inte fanns några meddelanden, forcerade eller i klartext, som tillräckligt tydligt angav anfallsplanerna. Det har inte kommit fram något stöd för antagandet att USA lät bli att varna flottbasen för att få anledning att inträda i kriget.

I Sverige var det till att börja med främst Yves Gyldén som stod bakom framgångarna. Den forcörsgrupp han ledde lyckades väl med att forcera olika länders koder. Men en annan forcör, som också till att börja med sysslade med att knäcka koder, blev det stora namnet inom svensk kryptologi, matematikern Arne Beurling. År 1940 skedde något mycket väsentligt för svensk underrättelsetjänst. För sin krypterade fjärrskrifttrafik med Geheimschreiber (på svenska G-skrivaren) behövde ockupationsstyrkan i Norge en teleledning till Berlin. Den gick över Sverige och tappades på alla meddelanden. Dessutom avlyssnades linjen mellan Berlin och tyska beskickningen i Stockholm. Det var en mycket stor bedrift av Beurling, när han utan förkunskap om G-skrivarens funktion, lyckades rekonstruera den och forcera en dags snappade meddelanden. Under flera år blev de forcerade G-skrivartelegrammen en mycket god underrättelsekälla. Bland annat kunde man få reda på att tyskarna inte skulle invadera Sverige, vilket innebar att vi inte behövde genomföra någon allmän mobilisering. Det sparade mycket pengar åt Sverige.

Fanns det då inga krypton som motstod forceringsförsöken? Jo, då. Som berättats ovan införde tyskarna under kriget alltmer sofistikerade Enigmamodeller. Alla kunde inte forceras. På samma sätt var det med G-skrivaren. Under krigets sista skeden kunde inte de nya modellerna forceras med någon större framgång.

Tre namn att minnas

I Storbritannien var logikern Alan M. Turing en av de tongivande vid forceringen av Enigma. Före kriget hade han varit en av pionjärerna för automatteorin. Han ställde sig frågan: ”Kan en automat, i en viss klass av generella teoretiska maskiner, (läs dator,) göra 'allting'?” Hans svar blev: Ingen automat kan göra allting, till exempel generellt avgöra om ett program till sist stannar eller inte. Efter kriget arbetade Turing med att utveckla det som vi i dag kallar dator. I SIGMA, band VI, sid 2203 - 2227 finns en lättläst uppsats av Alan Turing: ”Kan en maskin tänka?” [11]

Matematikern Claude E. Shannon arbetade under andra världskriget vid Bell Telephone Laboratories med två ämnen som visade sig vara beroende av varandra, nämligen informationsteori och kryptologi. Resultatet av denna forskning publicerades i två artiklar 1948 och 1949. ”A Mathematical Theory of Communication” [13] kom först. Där beskrev han hur mycket extra data, redundans, som måste läggas till för att ett meddelande skulle kunna avkodas efter att ha överförts på en brusig kanal. Det är ingen större överdrift att säga att Shannon

med denna uppsats blivit informationsteorins fader. Ett år senare kom ”Communication Theory of Secrecy Systems” [14]. Här kunde han matematiskt visa hur stor nyckel (hur mycket nyckelinformation) som krävs för att teoretiskt dölja en viss mängd klartext. Shannon gav en teoretisk förklaring till varför det är lätt att forcera enkel substitution och Vigenèrekryptot, varför man inte får använda en engångsnyckel två eller flera gånger samt att varje krypto med begränsad nyckel är teoretiskt forcerbart. Det sista påståendet innebär att det bara finns en kryptonyckel hörande till en kryptotext som inte är alltför kort. Så om man kan provdekryptera med alla tänkbara nycklar hittar man den enda och rätta klartexten bland alla provresultaten. En matematisk teori som visar när ett krypto är forcerbart med i praktiken tillgängliga resurser saknar dock fortfarande sin lösning.

Även Shannon har skrivit en populärvetenskaplig uppsats i SIGMA, band VI: ”En schackspelande maskin.” [12]

Det sista namnet jag vill framhålla i detta avsnitt är Arne Beurling. Som ovan beskrivits gjorde Beurling Sverige stora tjänster under andra världskriget bland annat genom att forcera tyskarnas G-skrivare. Han var en oerhört produktiv forskare inom matematisk analys. En av hans elever, Yngve Domar, som senare blev professor i matematik vid Uppsala universitet, tvekar inte att beteckna Beurling som ett geni (se [2]). Ett verkligt mattesnille, alltså. (Och tänk nuförtiden behöver man inte kunna så mycket mer än multiplikationstabellen för att kallas ”mattesnille” på en svensk skolgård!)

Mig veterligt har Beurling inte lämnat efter sig något populärvetenskapligt verk, men vill man veta mer om hans särpräglade personlighet, rekommenderas Bengt Beckmans bok [2]. Där finns också en detaljerad beskrivning av Beurlings metod för att forcera G-skrivaren.

DES - en standard för kryptering

År 1972 utlyste två amerikanska standardiseringsorgan en tävling om en krypteringsalgoritm, avsedd att användas för att skydda data som lagrades på en dator eller kommunicerades mellan två terminaler. IBM vann tävlingen och 1976 antogs algoritmen som USA-standard. Detaljerna hade publicerats något år tidigare tillsammans med en försäkran från IBM att garantera alla användare en avgiftsfri användarlicens. Det senare blev en av orsakerna till den stora framgång som algoritmen fick för IT-säkerheten under många år. Namnet blev Data Encryption Standard, DES.

DES innebar ett nytänkande på åtminstone tre sätt. För det första publicerades kryptoalgoritmen in i minsta detalj. Visserligen fanns det många godkända kryptopatent tidigare, men man hade åtminstone försökt dölja den exakta utformningen så gott det gick.

För det andra introducerades med DES ett blockkrypto. Algoritmen krypterar inte en bit, ett tecken eller en byte i taget utan ett block om 64 bitar. Härigenom kan man lätt tillverka speciell hårdvara som krypterar mycket snabbt. Men konstruktionen medger även att simuleringar i en standarddator kan göras ganska snabba.

För det tredje blev det startskottet till en enormt stor användning av krypto utanför den klassiska användarsfären, försvar och utrikesförvaltning. En bra redogörelse för DES finns i [4], ”Applied Cryptography” av Bruce Schneier.

Publicerade kryptonycklar - går det för sig?

Nyckelhantering – att tillverka, distribuera, hålla reda på, förvara, hantera och till sist förstöra kryptonycklar när de inte behövs längre har alltid varit ett stort problem. En anledning är förstås att kryptonycklar är hemliga. Obehöriga, varav främmande länders underrättelseorganisationer torde vara de mest resursstarka, är givetvis mycket intresserade av att få reda på vilka nycklar som använts för att kryptera meddelanden av värde för deras uppdragsgivare.

År 1976 lade två amerikanska matematiker fram ett helt nytt koncept för kryptering. Whitfield Diffie och Martin Hellman, presenterade vid ett symposium om informationsteori i Ronneby ”öppen nyckel-kryptering”. Hösten samma år kom deras resultat ut i tryck, ”New Directions in Cryptography” [15]. Grundidén innebär att man använder nycklar, som är uppdelade i två delar, en öppen, publicerbar nyckel används för kryptering och en hemlig för dekryptering.

Den som räknar med att få ett hemligt meddelande alstrar en dekrypteringsnyckel och håller den hemlig hos sig samt en tillhörande öppen krypteringsnyckel och publicerar denna i en allmänt tillgänglig katalog. Avsändaren krypterar meddelandet med den publika (öppna) nyckeln och skickar det till mottagaren, som tar fram sin privata (hemliga) nyckeldel och dekrypterar meddelandet.

Helt har man dock inte löst problemet med nyckeldistribution på detta sätt. Den som skall sända ett hemligt meddelande måste försäkra sig om att den öppna nyckel som han hämtar i den publicerade katalogen, verkligen tillhör den avsedde mottagaren så att han inte skickar hemligheter till någon annan. Sekretessproblemet har ersatts av ett autenticitetsproblem.

Tre amerikaner, de två datalogerna Ron Rivest och Adi Shamir samt matematikern Leonard Adleman, har uppfunnit det mest använda sättet för öppen nyckel-kryptering. Tillsammans konstruerade de det så kallade RSA-systemet efter initialerna i deras efternamn. Metoden bygger på att det i praktiken är svårt att uppdela stora tal i primfaktorer, om talet inte innehåller några små faktorer. Nämnaren nr 4, 2001, sid. 47 - 51 [8] innehåller en lättläst och enkel beskrivning av RSA-systemet.

Kvantfysiken i kryptologins tjänst

Två drömmar har alltid hägrat för kryptologerna, nämligen att uppfinna det oforcerbara kryptot och att forcera ett krypto som av många förklarats som praktiskt oforcerbart. Den första av dessa drömmar är som vi sett tidigare i denna uppsats förverkligad i och med engångskryptot, men vi önskar ett krypto som inte har engångskryptots ohanterliga nyckelhantering. På senare tid har man med utnyttjande av kvantfysikens förklaringar till vissa märkliga beteenden hos fotoner och elementarpartiklar kommit en bit på vägen mot dessa drömmars mål. Möjligheterna kallas kvantkryptering och kvantforcering. Båda finns beskrivna på ett så lättillgängligt sätt som förefaller vara möjligt i Kodboken [3]

Kvantkryptering

Ett kvantkrypto använder fotoner som är polariserade i olika riktningar på ett slumpartat sätt. Avsändaren av ett meddelande alstrar slumpmässigt polariserade fotoner och skickar dem till mottagaren som i sin tur använder slumpmässigt orienterade filter för att med viss sannolikhet ta reda på vad avsändaren sänt. Efter ett antal utbyten av fotonsekvenser och ”vanliga” data har avsändare och mottagare hos sig en identisk följd av bitar som kan användas för fortsatt kryptering och ingen avlyssnare på linjen kan ha fått del av dessa. Det är nämligen så att det inte går att avlyssna fotonsekvensen utan att förstöra den och det kan de behöriga användarna avgöra. Det finns också möjligheter att utväxla fotonsekvenser trots en avlyssnare och använda resultatet som ovan. Än så länge är kvantkryptoutvecklingen i sitt inledningsskede.

Man måste också övertyga sig om att de behöriga parterna verkligen kommunicerar med varandra och inte med någon obehörig. Vi har ett autenticeringsproblem att lösa dessutom.

Kvantforcering

Ett krypto som inte är ett (oforcerbart) engångskrypto kan enligt Shannon alltid forceras i teorin genom att man prövar att dekryptera en kryptotext med alla tänkbara nycklar och säger bingo! när ”klartexten” blir begriplig. För ett starkt krypto är detta antal är mycket stort. Låt oss anta i ett tänkt exempel att detta är 2^{100}, vi talar då om en 100 bitars nyckel. För en vanlig dator, som skall genomföra detta med en nyckel i taget, blir tidsåtgången orimligt stor. Men för en kvantdator kan det komma att bli möjligt.

En vanlig dator arbetar med bits, elektroniska vippor som kan inta värdet noll eller ett. En kvantdator använder i stället qubits (quantum bits) som samtidigt intar värdena noll och ett. Den utnyttjar elementarpartiklar som först givits ett visst värde för sitt spin, säg att de spinner medsols. Om man sedan skickar en svag energiimpuls till dem kan de komma i ett läge där det inte går att avgöra om de spinner med- eller motsols så länge vi inte försöker avläsa deras spinvärde. De spinner åt båda hållen samtidigt. Enligt kvantdatoridén kan man sedan ”räkna” (i vårt fall provdekryptera) med dessa qubits och skulle i princip kunna få alla möjliga ”klartexter” samtidigt!
I vårt fall med 100 bitars nyckel skulle ett register med 100 qubits räcka som utgångsvärde för de 2^{100} möjliga nycklarna.

Ännu finns endast mycket rudimentära tekniska realiseringar av kvantdatorer. Men om de blir verkliga och användbara i tillräckligt komplicerade fall, blir inga nuvarande krypton säkra - inte ens i praktiken.

Fyra böcker

År 1967 utkom en bok om kryptots historia från en tid långt före vår tideräkningsbörjan fram till våra dagar. Det är en riktig tegelsten. Själv har jag en förkortad version om 476 sidor. Författare och titel: David Kahn: The Codebreakers [1]. Tyngdpunkten ligger på tiden för de båda världskrigen och perioden däremellan. Upplägget är mer historiskt än matematiskt.

Den svenska kryptohistorien beskrivs på ett medryckande sätt i Bengt Beckman: Svenska kryptobedrifter [2]. Den innehåller bland annat en beskrivning av Gripenstiernas krypteringsapparat från 1700-talet (se ovan), Boris Hagelins mest kända krypteringsapparat samt en beskrivning av den svenska radiospaningen och forceringsverksamheten under första världskriget och mellankrigstiden. Men tyngdpunkten ligger på Arne Beurlings bravad att knäcka G-skrivaren och dess betydelse för svenskt försvar under andra världskriget. Både apparatens funktion och forceringsmetoden beskrivs detaljerat. Boken avslutas med en ordlista som förklarar de termer som vanligen används i Sverige inom kryptoområdet.

En detaljerad beskrivning av Enigma-kryptot och hur det forcerades före och under andra världskriget finns i Simon Singh: Kodboken [3]. Men boken innehåller också mycket annat av intresse, t.ex. ett kryptos betydelse för Maria Stuarts dödsdom och avrättning, Vigenères metod samt krypton hos Conan Doyle och Edgar Allan Poe. Singh beskriver också hur man löste gåtorna med hieroglyferna och Linear B. Amerikanerna använde under andra världskriget navajoindianer som på sitt stamspråk överförde radiomeddelanden mellan stridande enheter i Stilla-havsområdet. I boken beskrivs hur dessa indianer valdes ut och användes. Singh behandlar också modern kryptologi, bland annat DES, RSA och andra nutida kryptometoder, även kvantkryptering och kvantforcering.

En fjärde, mycket innehållsrik bok är Bruce Schneier: Applied Cryptography [4], också den en tegelsten, 760 sidor tjock. Den är övervägande matematisk till sin karaktär och innehåller ”allt” man kan tänkas behöva veta om kryptoprotokoll, kryptoteknik, kryptoalgoritmer och kryptopolitik. Den innehåller också källkod för nio kryptoalgoritmer, bland andra DES. Referenslistan upptar hela 1653 hänvisningar.

Ordförklaringar

Krypto – Hemlig skrift. Krypto kan också betyda en viss metod för kryptering.

Klartext – Text som kan förstås utan att man behöver använda en hemlig metod och/eller hemlig kryptonyckel.

Kryptera – Översätta en klartext till kryptotext med hjälp av krypto och kryptonyckel.

Kryptotext – Resultat av kryptering. En kryptotext kan man inte förstå utan att den först dekrypteras.

Dekryptera – Återföra en kryptotext till klartext med hjälp av ett krypto och oftast en hemlig kryptonyckel.

Kryptonyckel – Data som styr hur man krypterar och dekrypterar med ett visst krypto.

Steganografi – Metod för att dölja förekomsten av en text, t. ex. genom att använda osynligt bläck.

Substitutionskrypto – Krypto där man vid kryptering ersätter en bokstav eller ett tecken i klartexten med ett annat tecken eller par av tecken.

Transpositionskrypto – Krypto där man vid kryptering ändrar ordningsföljden för bokstäverna i klartexten.

Meddelande – består av namn (och eventuellt även adress) samt den text som man vill att mottagaren skall läsa.

Klartextmeddelande – Meddelande som består av namn m.m. och klartext.

Kryptomeddelande – Meddelande som består av namn m.m. och kryptotext.

Redigering – Åtgärder som görs på en text efter dekryptering för att stor bokstav, mellanslag och skiljetecken skall införas så att texten blir lätt att läsa för mottagaren.

Internationella alfabetet – ABCDEFGHIJKLMNOPQRSTUVWXYZ

Forcering – Att ta fram klartexten som hör till en kryptotext utan att på förhand känna till den använda kryptonyckeln.

Referenser

Huvudreferenser

[1] David Kahn: The Codebreakers, Weidenfeld and Nicolson, London, 1974.

[2] Bengt Beckman: Svenska kryptobedrifter, Albert Bonniers förlag, 1996, pocketutg. 2006.

[3] Simon Singh: Kodboken, Norstedts, 1999.

[4] Bruce Schneier: Applied Cryptography, Second Edition, John Wiley & Sons, 1996.

Rökstenen

[5] Gun Widmark: Varför Varin ristade, Forskning och Framsteg nr 5, 1998, sid. 16 - 22.

[6] Conny L A Petersson: Rökstenen, Varins besvärjelse, Noteria Förlag, Klockrike, 1991

Andra allmänna uppsatser

[7] Yves Gyldén: Chifferbyråernas insatser i världskriget till lands, Militärlitteraturföreningen förlag, 1931.

[8] Juliusz Brzezinski: Om kryptering, Nämnaren nr 4, 2001, sid. 47 - 51. (Artikeln behandlar huvudsakligen öppen-nyckelkryptering, särskilt RSA-kryptot. I artikeln anges felaktigt att Arne Beurling knäckte Enigma-kryptot.)

[9] Johan Håstad: Ett datornät utan chiffer är som en stad med olåsta dörrar, Forskning och Framsteg nr 8, 1995, sid. 22 - 27.

Tidiga uppsatser om datorer och informationsteori

[10] John von Neumann: En allmän och logisk teori för automater, SIGMA vol. VI, sid 2174 - 2202, Forum, 1960.

[11] Allan M. Turing: Kan en maskin tänka? SIGMA vol. VI, sid 2203 - 2227, Forum 1960.

[12] Claude Shannon: En schackspelande maskin, SIGMA vol. VI, sid 2228 - 2236, Forum 1960.

[13] Claude Shannon: A Mathematical Theory of Communication, Bell System Technical Journal, vol. 27, nr 4, 1948, sid. 379 - 423, 623 - 656.

[14] Claude Shannon: Communication Theory of Secrecy Systems, Bell System Technical Journal, vol. 28, nr 4, 1949, sid. 656 - 715.

Öppen nyckel-kryptering

[15] Whitfield Diffie and Martin Hellman: New Directions in Cryptography, IEEE Transactions on Information Theory, vol IT-22, nr 6, Nov 1976, sid. 644 - 654.