

Svenska kryptobedrifter under Andra Världskriget

Det tyska överfallet på Danmark och Norge den 9 april 1940 kom överraskande för alla, inklusive den svenska signalspaningen. Tack vare en bragdardad kryptologisk bedrift blev det i försättningen inte lika lätt för tyskarna att komma oanmälda till Sveriges gränser. Sverige var förhållandevis dåligt rustat och med tyska trupper i grannländerna behövde man all den förvarning man kunde få. Sverige lyckades tappa och knäcka den kryptotrafik på högsta nivå som på förhryda ledningar gick över svenskt territorium.

Maskinen som åstadkom kryptot kallas "Der Geheimschreiber" och mannen som knäckte kryptot hette Arne Beurling.

Omedelbart efter intåget i Norge uppvaktades UD av den tyske ministern i Stockholm. Han hade krav att ställa och ett av dem var att tysk telefon- och teletrafik skulle få fortgå på den s.k. västkust-kabeln som tidigare använts av det norska telegrafverket. Det svenska svaret kom med någon försening men var jakande. Det innehöll dock vissa invändningar för att dölja det faktum att svenskarna ämnade koppla in sig på linjen och syna trafiken. Den 14 april övertog tyskarna formellt de uthyrda ledningarna.

Den tyska trafiken underkastades omedelbart undersökningar av den svenska teletekniker och bara några dagar senare kunde de konstatera att det som sändes var tontelegrafi utnyttjad för 5-kanals teleprintertrafik. En kommunikation som denna var något helt nytt för både den svenska signalspaningen och det svenska telegrafverket. När man insåg att den märkliga trafiken inte var någon tillfällig historia anpassades inhämtningen snabbt till omständigheterna. Sedan mottagnings-apparaturen modifierats var det möjligt att registrera och läsa trafiken på telegrafverkets Creed-teleprinterar. Texten trycktes på pappersremsor.

De tyska operatörerna skrev i klartext om "der Geheimschreiber" eller "G-schreiber" som snart skulle tas i bruk. Och i slutet av april dök mycket riktigt en ny typ av trafik upp samtidigt som de klartexter som varit intressanta försvann. Det visade sig vara teleprintertrafik med möjlighet till simultan kryptering. Två "G-skrivare" - som blev den svenska benämningen för "G-schreiber" - kunde kommunisera i dialog och operatörerna kunde byta från klartext till kryptotext när de behagade. Bytet markerades av fem tvåsiffriga tal följda av ordet "umum" (umschalten) från den sändande parten och "veve" (verstanden) från den mottagande.

För att kunna registrera alla fjärrskriftalfabetets 32 kombinationer byggdes de mottagande teleprinterarna om. Sex av fjärrskriftalfabetets kombinationer är icke-tryckande, d.v.s. de har en funktion men de skriver inga tecken. Det är vagnretur, radmatning, skift till bokstäver, skift till siffror, mellanslag och en noll-funktion. För kryptotextens skull var det nödvändigt att även de här tecknen skrevs ut. På Creed-teleprinterarna kopplade man därför bort funktionerna vagnretur, radmatning etc. och lät motsvarande kombinationer skriva siffrorna 1 till 6 i stället.

Den 21 maj flyttade en nybildad "trådspaningsgrupp" bestående av fem studerande från Tekniska högskolan, som skulle handha mottagarutrustningen, och fem flickor, som skulle klistra upp remsor, in i en ruffig rivningsfastighet med adress Karlaplan 4. De flyttade in i en jungfrukammare belägen två trappor upp i gathuset. Försvarsstabens kryptoavdelning hade redan lokaler i övriga delar av huset. En ström av meddelanden togs nu emot; en del var på klartext men en ökande del sändes på det nya okända kryptosystemet.

Vem skulle kunna tänkas analysera denna för Sverige helt nya form av krypto? Problemet överantvordades till Sveriges mest framstående kryptoanalytiker, Arne Beurling, professor i matematik i Uppsala. Beurling, som redan vid sin värnplikts-tjänstgöring 1930 hade avslöjat sig som "chifferhjärna", hade ställt sig till förfogande som konsult på försvarsstabens kryptoavdelning. Beurling hade för tillfället sin arbetsplats i en villa på Elfviks udde, vilket var en av flera lokaler ute på Lidingö som kryptoavdelningen disponerade. Han avbröt nu det arbete med ryska överchiffererade koder, som han var inkopplad på, för att istället ta itu med detta för Sveriges väl och ve så betydelsefulla arbete.

Och efter bara ett par veckor kunde Beurling - helt sensationellt - presentera klartextfragment. Han använde sig av särskilt gynnsamma material från den 25 och 27 maj. När han studerade textremorna förstod han att operatörerna ofta gjorde misstaget att sända flera meddelanden på samma nyckel. Han kombinerade detta med en analys av hur karakteristiska egenheter i teleprinteralfabetets fembitstecken motsvarade egenheter i chifffertextens tecken. I mitten av juni kunde så Beurling presentera en matematisk modell för G-skrivarens

arbetssätt.

Beurling hade i själva verket knäckt ett teleprinterchiffer konstruerat av den tyska firman Siemens & Halske under 30-talet. Den auteniska beteckningen på maskinen var "T typ 52A/B". Den hade ett otroligt antal möjliga nyckelkonfigurationer. Den hade tio hjul med ett antal positioner - relativt prima - mellan 47 och 73 (a9 och antalet steg till dess en given nyckelinställning återkom var 893 622 318 929 520 950 (jfr 17 576 för Enigma). Varje hjul hade en kamskiva vars profil representerade en slumpmässig binär sekvens (b), som upprepades när hjulet fullbordat ett varv. Hjulen stod i förbindelse med resten av maskinen genom tio kablar (c) som kunde placeras 1 10! eller 3 628 800 olika lägen. Fem bitar erhållna från fem av hjulen förändrade den på tangentbordet tryckta bokstaven (d) genom en binär addition (e). Det så förändrade tecknet ändrades ytterligare en gång genom att de fem bitarna kastades om av fem reläer som styrdes av fem bitar från de återstående hjulen (f). Reläerna kunde placeras på 719 olika sätt (från den 1 april 1942 användes dock endast reläkopplingschema).

I nedanstående figur visas hur den på tangentbordet nedtryckta bokstaven R förvandlas till A. Sedan en tecken chiffererats matades alla hjulen fram ett steg. Därmed skapades nya värden både för den binära additionen (e) som för omkastningen av bitarna (f). Under sommaren 1940 dechiffererades meddelanden manuellt efter Beurlings schema. Det var tidsödande och enahanda arbete och trafiken ökade hela tiden. Det stod tidigt klart att en speciell maskin måste byggas som kunde dechifferera på samma sätt som G-skrivaren. En civilingenjör, Vigo Lindstein, utsågs att enligt Beurlings anvisningar bygga en dylik apparat - en s.k. "app". Under de närmaste två åren byggdes mer än 30 "appar" hos LM Ericsson.

Innan dechiffkering med "appen" kunde ske måste ett inledande kryptologiskt arbete utföras. Varje dag använde tyskarna en ny nyckelinställning för fem av de tio hjulen och varje morgon måste svenska kryptoanalytiker lösa denna inställning. Inställningen * för de övriga fem hjulen gav den tyske operatören själv i telegramingressen. Apparna var kopplade till fjärrskrivare på vars tangentbord man skrev kryptotexten. Texten dechiffererades i appen och resultatet kom tillbaka till fjärrskrivaren och skrevs ut på dess pappersremsa.

Allt fler människor - mest unga flickor - rekryterades för att sköta arbetet med den tyska G-skrivarentrafiken. Man arbetade dygnet runt och trafiken fortsatte öka. Den tyska legationen i Sockholm började använda G-skrivaren på våren 1940 och från och med det tyska anfallet mot Ryssland midsommaren 1941 kom också de tyska kommunikationerna till och från Finland med i trafiken. Forceringsframgångarna nådde sin kulmen i november 1942. Under den månaden överlämnades till Försvarsstaben och UD mer än 10 500 meddelanden. Men trots stor sekretess kring verksamheten fick tyskarna - förmodligen genom sina finska allierade - reda på att Sverige läste deras topphemliga trafik.

Gradvis förstärktes kryptosäkerheten i de tyska maskinerna och kryptorutinerna blev alltmer disciplinerade. Men svenskarna hängde med och kunde även knäcka de förbättrade modellerna T52C (september 42) och T52CA (mars 43). Men i december 1943 introducerades den avsevärt förbättrade modellen T52D med oregelbunden hjulmatning. Den blev för svår för de svenska forcörerna i den alltmer glesnande telegramskörden och i början av 1944 kunde inte längre någon del av trafiken läsas. Men då hade redan 300 000 meddelanden lösts och levererats till ivriga läsare på försvarsstaben och UD.

Underrättelserna som utvanns ur G-skrivarmaterialet var naturligtvis ovärderliga för Sveriges regering och försvarsstab. En huvuduppgift var att följa allt som tydde på tyska anfallsplaner. Man räknade med att man genom tillgången till de tyska meddelandena skulle ha en förvarningstid på åtminstone två veckor före anfall. Sverige gavs en unik möjlighet att noga kartlägga de tyska styrkeförhållandena runt de egna gränserna. De tyska högkvarterets sammanfattningar och orienteringar gav också upplysningar om krigsläget på övriga fronter. Och rapporter till och från den tyska stockholmslegationen gjorde det möjligt att följa de tyska reaktionerna på olika svenska utrikespolitiska initiativ.

Sverige hade vid den här tiden inblick i de allra hemligaste tyska planerna. Ett exempel är Operation Barbarossa (anfallet på Sovjetunionen 1941). Truppkoncentrationer rapporterades i telegrammen och i ett meddelande talades om den dubbla sold som soldaterna skulle få efter inmarschen i Ryssland. Trots att trupprörelser i bl.a. Finland också kunde ha tolkats som en förberedelse för anfall mot Sverige visste man här vad saken gällde och kunde handla i enlighet därmed.

I förhandlingar och diskussioner var det utomordentligt värdefullt att ha tillgång till de instruktioner de tyska förhandlarna fått från Berlin. Ett exempel är det tysk-svenska handelsavtalet för 1942. Sverige kände sålunda i förväg till den kreditränta som tyskarna fått instruktioner om att i yttersta nödfall acceptera. På så sätt kunde Sverige få ett betydligt gynnsammare avtal än man räknat med.

De forcerade telegrammen var också i stort värde för det svenska kontraspionaget. Sverige hade en god inblick i vad Abwehr (tyska militära underrättelsetjänsten) företog sig. Därigenom gavs säkerhetspolisen möjligheter till både ingripanden och förebyggande åtgärder. Stockholm var under kriget en frekventerad spelplats för de krigförande ländernas underrättelseagenter och tyskarna samlade flitigt underrättelser såväl om svenska som om sina fienders förhållanden.

Svenskarna knäckte aldrig Enigman. Det bedömdes utsiktslöst att nå en forceringsframgång utan tillgång till en autentisk maskin och ur svensk synpunkt var det dessutom betydligt viktigare att lösa G-skrivaren. G-skrivaren användes för strategisk kommunikation mellan de högsta instanserna i Berlin och de militära högkvarteren och att läsa den trafiken var av största betydelse för Sverige. Enigma maskinen användes för operativa och taktiska kommunikationer inom vapenslagen. För de allierade styrkorna i fält var det av största värde att den trafiken kunde läsas.

Till sist - hur skall Beurlings insats värderas - förutom att den kom då den som bäst behövdes? Man ska komma ihåg att när Beurling började sitt arbete visste han ingenting om teleprinterar, än mindre om teleprinterchiffer. Studier av tillgänglig litteratur på området - kanske ingick patenthandlingar - men framför allt en skarpsinning analys av egenheter i telegrammaterialet ledde honom fabulöst snabbt till lösningen. Det var en bragd.

Matematikern Arne Beurling betraktas i vika kretsar som ett geni. När han i november 1976 besökte FRA tillfrågades han om vad som lett honom till lösningen av den tyska kryptomaskinen. "En trollkarl avslöjar inte sina tricks" blev svaret. Han är utan tvekan det största namnet bland svenska kryptoanalytiker. Han föddes i Göteborg 1905 och blev professor i Uppsala 1937. Han var en karismatisk och ibland "svår" person. Som lärare var han legendarisk och han gjorde ett djupt intryck på sina elever. Under 30-, 40- och 50-talet var han ett internationellt ledande namn inom den matematiska analysen. År 1948 blev han gästprofessor i Harvard och 1952 fick han en hedrande befattning vid Princeton Institute for Advanced Study, där han stannade till sin död 1986.

Referenser:

Beckman Bengt. "Svenska kryptobedrifter". Stockholm:Bonniers 1996. Författaren är före detta kryptoanalytiker, och boken ger en initierad skildring av svenska kryptobragder under andra världskriget.

Ahlfors Lars. "The Story of a Friendship: Recollections of Arne Beurling". The Mathematical Intelligencer Vol15, No 3, 1993

Davies, Donald D. "The Siemens&Halske T52e Cipher Machine". Cryptologia Vol 6, No 2, 1983

Davies, Donald D. "The early Models of the History of the Siemens&Halske T52 Cipher Machines". Cryptologia Vol 18, No 2 , 1984.

Davies, Donald D. "New information on the History of the Siemens&Halske T52 Cipher Machines". Cryptologia, Vol 18, No 2, 1994

Kahn David. "The codebreaker". New York:Macmillan 1967.

Kjellberg Bo. "Memories of Arne Beurling". The mathematical intelligencer. Vol15,No 3 1993

Mache Wolfgang W. "Der Siemens-Geheimschreiber". Archiv für Deutsche Postgeschichte. Heft 2, 1992

Selmer Ernst S. "The Norwegian Modifications of the Siemens & Halske T52e Cipher Machine". Cryptologia, Vol 18, No 2, 1994

Smith Michael. "Station X". London:Macmillan 1998

Weierud Frode. "Sweden, Cryptographic Superpower. A book review". Cryptologia. Vol22, No 1, 1998

Wermer John. "Recollections of Arne Beurling. The Mathematical Intelligencer". Vol 15, No 3, 1993

© Bengt Beckman 2000

Publicerat 2003-06-05.
Copyright © Försvarets Historiska Telesamlingar