Särtryck ur
Säkerhet&Sekretess nr4 2005
Säkerhet&sekretess

Hitlers gåta:

Enigman var ingen tysk krigshemlighet – den lanserades redan 1922 och konstruktionen var allmänt känd. Men trots att den forcerades redan 1932 kom den att användas kriget ut.

Enigma fortfarande mystisk efter 80 år

Text: Mikael Simovits och Tomas Forsberg Foto: Mikael Simovits och Andreas Eklund Grafik: Ola Rehnberg

■ **Enigman – när utvecklades den, och hur fungerade denna mytomspunna maskin?**
■ **Framför allt: hur forcerade man den – och varför var det över huvud taget möjligt?**
■ **Vad kan vi lära av Enigman, de alliera-des framgångar, och nazisternas misstag?**

Den berömda Enigman har ett grundmurat rykte som kryptomaskin. Vad som är sant och falskt är ibland fortfarande okänt, eftersom ar-kiven bara öppnats delvis. Långt efter kriget fanns det fortfarande skäl att dölja de metoder som använts därför att västmakternas ryska allierade aldrig fick insyn i verksamheten och inte heller skulle få ledtrådar som kunde göra de ryska kryptosystemen säkrare. De ryska kryptomaskinerna skilde sig från de tyska ge-nom ett större antal rotorer, men hade stora likheter. Så direkt efter kriget startade västmak-terna en nedmontering av verksamheten; i stort sett all utrustning förstördes. När information nu börjar bli tillgänglig är den inte komplett, och stora delar av mystiken lever kvar.

1920: Arthur Scherbius uppfinner maskinen

Bakom Enigmamaskinen låg den tyske uppfin-naren Arthur Scherbius. I början av 1920 sålde han sin nya kryptomaskin på mässor, och 1922 tog han ett amerikanskt patent på den. Scher-bius vände sig vid denna tid främst till företag som skulle skydda telegram. Intresset från före-tagen var dock lågt. Men 1926 köpte den tyska krigsmakten sina första exemplar, och 1932 ha-de Enigman blivit den viktigaste tyska krypto-produkten. Scherbius fick själv aldrig uppleva det drama som följde, eftersom han dog 1929.

Enigman fungerar närmast som en kompli-cerad ficklampa med skrivmaskinstangent-bord. Då en tangent trycks ned leds strömmen genom tre eller fyra rotorer fram till en reflek-tor, tillbaka genom rotorerna och genom ett kopplingsbord. Resultat av denna strömkrets avgör vilken lampa som tänds.

Totalt använder Enigman 26 bokstäver och varje rotor innehåller lika många kontaktorer. Inne i rotorn är varje bokstav med hjälp av en ledningstråd omkastad till en annan bokstav. Varje rotor är alltså ett substitutionskrypto, och när dessa ändrar inbördes läge bildas ett poly-alfabetiskt substitutionskrypto. Då ett medde-lande skrivs in flyttas den första rotorn ett steg för varje bokstav och en helt ny översättning uppstår. Då den första rotorn gått ett varv flyttas även nästa rotor fram ett steg.

Förutom rotorerna hade den militära Enig-man ett kopplingsbord på framsidan. Då en sladd sätts in i kopplingsbordet kastas två bok-stäver om en extra gång. Enigman är reciprok, det vill säga den krypterar och dekrypterar på samma sätt.

En ny dag gryr i det tyska kryptolägret

Varje dag ställde den tyske kryptören in en grundinställning. Först valet av rotorer och deras ordning – en viss dag kunde exempelvis rotor 2, 3 och 5 användas i nämnd ordning. Vidare skulle ringställningen ställas in på dessa rotorer, det vill säga den position där de stegar fram nästa rotor ett snäpp, varefter Enigman stängdes och man kopplade sladdarna på fram-sidan enligt vad som gällde för den dagen. Där-efter ställdes startpositionen in, till exempel ”LFU”. Denna position användes enbart för att skicka meddelandenyckeln. Kryptören hittade då själv på en kombination på tre bokstäver och krypterar denna. Mottagaren dekrypterar kombinationen, och därefter ställer både mot-tagare och avsändare rotorerna i det nya läget.

Kryptografiskt säker – men undergrävd

Även om den kryptografiska säkerheten skulle visa sig otillräcklig var antalet kombinationer svindlande – den amerikanska signalspaningen räknande ut att ubåtsversionen av Enigma (med fyra rotorer) hade cirka 2×10^{145}, motsva-rande en kryptonyckel på över 400 bitar. Denna teoretiska nyckellängd förutsatte dock att varje rotors inre konstruktion var okänd, vilket inte var fallet, och konstruktionen ledde till att knäckningen blev en industri där båda sidor använde identiska rotorer.

Grundarbetet gjordes i Polen, före kriget

Polackerna hade tidigt ett stort behov av att för-stå de tyska avsikterna och började därför stu-dera Enigman. Inledningsvis använde tyskarna den kommersiella Enigmamodell som vem som helst kunde köpa. Då de efter hand byggde en egen modell med egna rotorer, egen reflektor och med nytt kopplingsbord blev säkerheten betydligt bättre – men när tyskarna av misstag skickade en Enigma med posten så att den ham-nade i Polen passade polackerna på att mäta upp de rotorer som medföljde.

Före kriget krypterade tyskarna nyckeln två gånger, och polackerna byggde en egen force-ringsmetod som utnyttjade detta faktum. Dess-utom födde polackerna planerna på den maski-nella knäckningen, det vill säga den konstruk-tion som blev känd som *bomben*. Vid krigs-utbrottet flydde de polska kryptoanalytikerna med Marian Rejewski i spetsen till de allierade, och med deras erfarenheter kunde bomberna snabbt färdigställas. Eftersom tyskarna inte längre krypterade meddelandenyckeln två gånger var man dock tvungen att finna en ny lösningsprincip.

Under kriget kunde de allierade helt enkelt ta till våld då matematiken inte räckte till, exem-pelvis plundra tyska väderskepp på kryptout-rustning, kartor och tabeller över kommande nyckelinställningar. De tyska ubåtarna använde ett meddelandesystem där läge angavs efter ett eget rutnät, och när sådana kartor blivit kända kunde man framställa en förmodad klartext som motsvarade de meddelanden en ubåt skickade då den siktat en konvoj och anger dess läge, fart och riktning för att tillkalla andra.

Därför gick Enigman trots allt att knäcka

Tyskarna betraktade sin maskin som omöjlig att forcera, och antalet tänkbara nycklar för en Enigma var närmast oändligt mycket större än nyckellängderna i de kryptosystem som idag anses säkra. Ändå forcerades den. Den enkla förklaringen är att hemligheterna kunde knäck-as bit för bit.

Enigman är i grund och botten sina rotorer och deras inbördes omkastningar av bokstäver. Under hela kriget användes som mest åtta olika

Forts ▷▷

ORDLISTA

- **Reciprok kryptering** – Skriver man in klartexten får man kryptotexten och omvänt (om ett A krypteras till ett L blir ett L till ett A).
- **Ringställning** – Ringställningen markerar den position där varje rotor ska dra fram nästa rotor ett snäpp.
- **Crib** – Korta stycken med en trolig klartext som de allierade kunde gissa. En crib fick aldrig vara längre än ett varv på rotorn och delades normalt in i två halvor. En halva skulle då sannolikt inte ligga över en framstegning av nästa rotor.
- **Meny** – Då en crib och en kryptotext kunde matchas byggde man en meny som visade sambandet mellan de bokstäver som plockats ut. Menyn kunde därefter testas i bomberna.
- **Bomb** – De forceringsmaskiner som de allierade byggde. Varje bomb kunde testa en crib med ett tänkbart val av rotorer. Med flera bomber kunde man testa flera rotorval samtidigt.

rotorer. Flera av dessa var kända sedan före kriget. Nya rotorer tillfördes bara en i taget, och gick då att forcera. Om tyskarna hade bytt ut samtliga rotorer på samma gång hade kryptoanalys inte varit tillräckligt!

Enigman hade dock ett par särdrag som möjliggjorde forceringen. Den princip man valde var att pröva en gissad klartext mot alla tänkbara rotorpositioner. Eftersom Enigman aldrig krypterade en bokstav till sig själv kunde klartexten (som benämndes ”crib”) passas in på ett tänkbart ställe på kryptotexten. Detta innebar en ny risk: de egna kryptörerna måste få aktuell och hemlig information om krigshändelser för att kunna gissa meddelanden. Med hjälp av kryptotext och klartext gällde det sedan att hitta ett antal kopplingar som kunde testas maskinellt.

Rotorerna hade även vissa individuella statistiska kännetecken, vilket gjorde det möjligt att gissa vilken rotor som satt på den snabbast roterande positionen. De nyaste rotorerna saknade dessa särdrag, och tyskarna införde då en regel att minst en av rotorerna 6, 7 eller 8 alltid måste användas.

Rent kryptoanalytiskt var det dagliga arbetet ganska monotont. Så fort ett meddelande grundforcerats visste man rotorerna, kabeldragningen och dagsnyckeln. Någon gång på förmiddagen var detta arbete gjort, och därefter kunde man resten av dagen tolka trafiken lika fort som tyskarna själva.

Många tyska meddelanden var stereotypa och innehöll kända namn, gradbeteckningar eller hälsningar. Ett av de mest kända exemplen var en väderstation som varje dag skickade texten ”vädret i Biscayabukten är idag ...” – följaktligen en hög prioritet för de allierade. En annan vanlig text var ”inget att rapportera”.

Gjorde mycket för att göra maskinen säkrare

Utan kopplingssladdarna hade Enigman varit betydligt lättare att knäcka. Eftersom dessa sladdar kunde byta varje bokstav till en annan bokstav tillförde de vid fullt utnyttjande en komplexitet jämförbar med en extra rotor. Tyskarna tänkte sig att sladdarna skulle minska riskerna med att rotorerna kunde röjas – en röjd rotor kunde ju inte snabbt ersättas under krig, sladdarna däremot kunde kopplas om varje dag.

Det är inte säkert att tyskarna förstod omfattningen av de allierades dekryptering, men de kunde i alla fall gissa sig till att maskiner och rotorer kunde ha förlorats under oklara omständigheter. I slutet av kriget använde tyskarna därför ofta den fullständiga uppsättningen av tretton sladdar.

Och sladdarna *var* ett svårt problem för de allierade, men med bomberna gick det att hitta lösningar. Knäckarna kunde redan innan de bestämde sig för en crib räkna ut hur många falska träffar den kunde generera och hur många sladdar man skulle kunna bestämma med den.

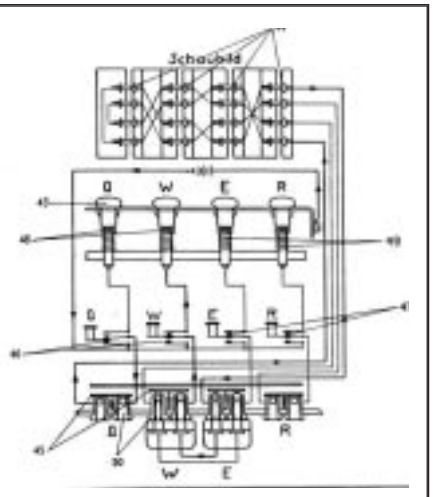
Men givetvis gjorde tyskarna mer för att höja säkerheten. En åtgärd var att öka antalet varianter på Enigmor – förutom tre- och fyrarotorsmaskinerna hade underrättelsetjänsten en modell med fler pinnar för att utöka ringställningen och åstadkomma extra rotationer. Detta minskar chansen att hitta en crib som inte störs av en rotation. Och nästa åtgärd var att öka antalet olika nycklar – varje frontavsnitt kunde ha en egen nyckel, vilket minskade risken med att en nyckel eller ett meddelande kom på avvägar. Detta hade dock en baksida också: om ett meddelande skickades över flera frontavsnitt kunde en tidigare forcering underlätta då samma meddelande dök upp i ett annat sambandsnät.

För att förvilla kunde tyskarna lägga på slumpmässiga ord eller tecken i början av meddelandet – annars visste de allierade att meddelandet inleddes med ANX, det vill säga det tyska ordet *an* för *till* följt av ett X för blanktecken. Ett sådant ord var *Sonnenschein*, som användes vid utbildningen – de tyska kryptörerna var dock inte mer fantasifulla än att de ofta fortsatte använda det.

För att öka säkerheten begränsade man även meddelandelängden till 200–300 tecken. Nyckelförstöring kunde också underlättas – tyska flottan skrev sina nycklar med vattenlösligt rött bläck på rosa papper – och slutligen kunde meddelanden dubbelkrypteras. Detta gjordes främst för personliga meddelanden, som sällan forcerades, eftersom det var svårt att gissa en crib.

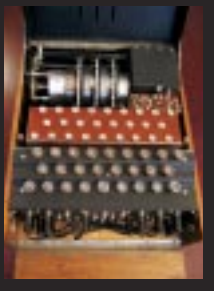
Myckat att lära av nazisternas misstag

Tyskarna hade stor tilltro till sin lösning och förstod aldrig vidden av de allierades ansträngningar. Kombinationen av tiotusentals personer som arbetade med hundratals maskiner var tillräcklig – i kombination med röjda rotorer och stereotypa meddelanden. I praktiken skapade



Kopplingsdiagram över Enigman: När en tangent trycks ned sluts en krets och en lampa lyser som indikerar en bokstav.

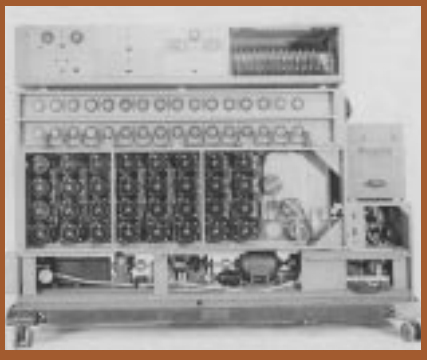
VAD BARA EN TYSK OFFICER FICK SE



Enigman såg helt enkelt ut som en skrivmaskin med en display med lampor. Bilder av Enigman med öppnat lock visar hur rotorerna sitter placerade. Då locket stängts kunde operatören inte längre se vilka rotorer som valts eller deras ringställning. Det var normalt bara en officer som fick öppna locket. För att ytterligare öka säkerheten fanns det en lös lamptillsats som kunde flytta displayen någon meter bort – utom synhåll för den som använde tangentbordet.

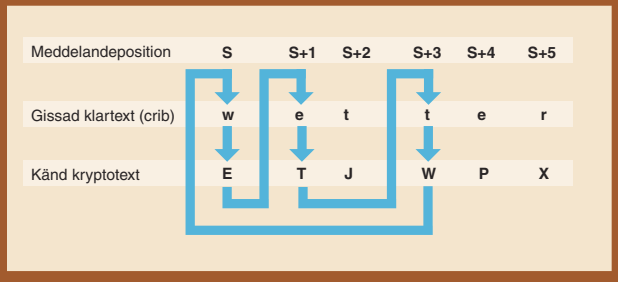
Enigman bestod av ett antal rotorer som kastade om bokstäverna. Någonstans under varvet fanns en pigg som matade fram nästa hjul ett steg. Inställningen av dessa piggar kallades ringställning. I slutet av kriget införde tyskarna en extra pigg och kunde alltså mata fram nästa hjul två gånger per varv. För att ytterligare öka omkastningen användes ett kopplingsbord. Inledningsvis använde tyskarna normalt tre sladdar för att sedan öka till sju, tio och till slut tretton sladdar.

DE ALLIERADES BOMBER



När de allierade forcerade Enigman använde de så kallade ”bomber”. Varje Enigma representerades av en uppsättning rotorer. Bokstäverna i ”criben” (se diagrammet till vänster) testades parallellt, varför den snabbast roterande rotorn var förskjuten en eller flera steg. Grupperna till höger på fotot motsvarade alltså helt enkelt samma Enigma en eller ett par tangenttryckningar in i framtiden.

Jämfört med en Enigmarotor som hade 26 kontaktorer hade en bombrotor 104 kontaktorer och kunde så att säga testa fyra olika saker samtidigt. Då en träff (tänkbar lösning) registrerats hade bomben redan snurrat förbi, varför den automatiskt stannade och sakta backade till lösningen, som skrevs ut. Varje körning tog tjugo minuter, och kunde resultera i en eller ett par träffar som måste kontrolleras för hand.



För att forcera Enigman användes huvudsakligen tänkta klartexter. Med hjälp av aktuella händelser kunde innehållet ofta grovt bestämmas. Då en tänkt klartext bestämts kunde den placeras på kryptotexten med ledning av att Enigman aldrig översatte en bokstav till sig själv. För att medge ett test behövde kombinationen klartext/kryptotext helst innehålla en loop och ett flertal bokstavspar.

I exemplet ovan ser vi hur criben *wetter* placerats på en kryptotext varvid en loop mellan tre bokstäver detekteras (W, E och T). Notera också att positionen S+2 inte säger något utan helt enkelt hoppas över då bomben programmeras.

Enigman grunden för den moderna kryptoanalysen. Både när tyskarna utvecklade tekniken och när de gjorde misstag drev de utvecklingen framåt.

De fel som tyskarna gjorde låg utspridda på flera nivåer. Systemet var kryptografiskt svagt och matematiken var vilseledande. Den maximala nyckellängden var ointressant eftersom de enskilda rotorernas inre kopplingar redan inhämtats. Och det regelverk som användes var ibland direkt olämpligt: en regel sa att samma inbördes placering av rotorerna inte fick återanvändas innevarande månad – allteftersom dagarna gick minskade alltså antalet tester som måste göras. Andra tveksamma regler sa att en rotor inte fick sitta två dagar i rad på samma plats eller att en kopplingskabel inte fick förbinda två intilliggande bokstäver.

En ödesdiger blunder stod den tyska ubåt för som tjuvstartade en sändning med de nya 4-rotorsmaskinerna, uppmärksammade sitt misstag och sände om meddelandet med det gamla systemet. De allierade kunde då få en fullständig klartext genom att forcera det gamla systemet, och med hjälp av denna välja de effektivaste delarna för den maskinella forceringen.

I nästa steg finns samspelet mellan krypto och operationell verklighet. Då en tysk ubåt löpte ut hade den order för den första veckans verksamhet. Om den fick kontakt med en konvoj skickades informationen på ett kort och standardiserat sätt för att försvåra fullständig radiopejling. Då ubåten skickade målinformation kunde de allierade genom pejling fastställa läge och via sin egen kunskap om konvojerna fastställa målets kurs och fart. Ofta räckte den här sortens information för en forcering, speciellt som den upprepades under dagen. De allierade slog normalt inte till mot ubåtar som samlades utan väntade tills ubåten beställde möte för tankning. Om tyskarna förstått riskerna hade de kunnat hålla sig med separata kartsystem för målrapportering och bunkring, och dessutom hade de kunnat omsätta kartsystemen oftare. I så fall hade de haft en lösning som varit rimligt säker även om kryptot forcerats.

Vad betyder historien idag?

Idag, 60 år senare, har vi en stark tilltro till kryptosystem som exempelvis DES (i dess användning som 3DES). I likhet med tyskarna kan vi visa matematiskt att systemen är säkra. Problemet är att vi inte känner till om någon lyckats knäcka systemen utan att berätta det. Vidare har de flesta som använder kryptosystem begränsad kunskap om säker användning.

I DES används så kallade S-boxar för att kasta om en grupp av bitar. Man kan alltså säga att S-boxen är en direkt motsvarighet till rotorn i Enigman, som kastade om en bokstav. Om rotorernas konstruktion hade kunnat hållas hemlig hade de allierade aldrig kunnat forcera meddelandena. En rimlig säkerhetshöjande åtgärd skulle alltså kunna vara att modifiera en S-box. Modifieringar av denna typ är inte helt ovanliga – flera kryptosystem finns i exempelvis en civil och militär variant.

Om man skulle modifiera S-boxarna för DES skulle en motståndare först och främst behöva kunskap om själva modifikationen. Under förutsättning att han byggt speciell hårdvara – antingen det är en kvantdator eller en avancerad ”bomb” – skulle han därefter behöva modifiera sin hårdvara.

Proprietära kryptosystem avfärdas ofta som osäkra. Argumentet är att om inte flera är med och granskar systemet är risken desto större att brister går oupptäckta. Men att Enigmans konstruktion var känd 15 år före kriget hjälpte de allierade. Så historien om Enigman motsäger värdet av öppna kryptografiska system – tvärtom kan proprietär, hemlig kryptografi vara att föredra om man är rädd om sina hemligheter. ■

Mikael Simovits är civilingenjör med inriktning mot kryptosystem — och innehavare till en av två Enigmor i Sverige. Tomas Forsberg är civilingenjör med inriktning mot datateknik och nätverkskommunikation. De arbetar med IT-säkerhetsrelaterade projekt, säkerhetsgranskningar och konsultationer. Vill du kontakta Simovits och Forsberg når du dem på sakerhet@idg.se.

LÄS MER

- **www.nsa.gov/publications/publi00016.cfm** – Den amerikanska beskrivningen av hur forceringen var möjlig.
- **w1tp.com/enigma/ecds.htm** – En innehållsrik beskrivning av själva Enigman.
- **www.codesandciphers.org.uk/virtualbp/tbombe/tbombe.htm** – En mer detaljerad beskrivning av Allan Turings arbete med forceringen av Enigma.
- **www.bletchleypark.org.uk** – Bletchley Parks hemsida, med det brittiska Enigma-museet.
- **www.bletchleypark.org.uk/upload/bombestops.pdf** – Matematisk beräkning av hur många falska lösningar som måste elimineras. Normalt kunde en träff av hundra vara riktig, förutsatt att criben var rätt.