Så knäcktes Z-maskinen

För att knäckadet av ett kryptosystem ska få sitt maximala värde, bör det komma vid rätt tidpunkt och på rätt material. Ett slående exempel är Arne Beurlings insats i början av andra världkriget. Den 9 april 1940 hade Hitlers trupper gått in i Norge och redan i juni hade Arne Beurling åstakommit den historiska bragden att på några få veckor knäcka kryptot i Siemens & Halskens Geheimschrieber, typ T52B. Den användes för kommunikation på allra högsta nivå mellan Hitler och hans överkommando. Den krypterade teleprinttrafiken mellan Berlin och Oslo gick på förhyrda kablar över svenskt territorium där svenskar passade på att "tappa" dem. Den information som utvanns var av utomordentligt värde för den svenska regeringen. Svenskarna löste också snabbt ytterligare två G-skrivarmodeller - T52C och T52CA - som tyskarna satte in 1942, när de genom sina finska vapenbröder fått reda på att svenskarna läste deras topphemliga telegramtrafik.

Men så fanns där ännu en maskin; de tyska opperatörerna kallade den Z-Schreiber och svenskarna kallade den Z-maskinen eller Z-skrivaren och om den visste man ingenting alls. De tyska kommandona i Norge och Finland hade fått order att använda den istället för de maskintyper svenskarna knäckt. Z-maskinen hade varit i bruk sedan 1941 och trots att trafiken från början varit ganska sparsam hade i april 1943 en avsevärd mängd text hunnit samlats.

Maskinen var svårlöst. Först på senare år har det blivit känt att engelsmännen, som hade en betydligt rikligare trafik, använde den berömda datorföregångaren Colossus för att lösa den. Engelsmännen hade tillgång till trafik från linjen Athen - Wien och likaså från förbindelsen mellan Italien och Nordafrika. Den trafik som Sverige hade möjlighet att inhämta var den som gick på kabel genom Sverige eller via radioteleprinter runt Sveriges gränser. Det var förenat med stora tekniska svårigheter att fånga in materialet, särskilt det som förmedlades via radioteleprinter. Från och till hade de svenska kryptoanalytikerna arbetat med telegrammaterial för att hitta några inkörsportar, men det hade hela tiden varit förgäves. Men så i mars 1943 var tiden mogen för svenskarna att efter en koncentrerad insats nedlägga även detta byte.

Det var en mönstergill forcering som de tre kryptoanalytikerna Bo Kjellberg, Carl-Gösta Borelius och Tufve Ljunggren genomförde. Den var i hög grad värd att uppmärksammas men den kom i någon mån vid fel tidpunkt. Den kom i ett skede av kriget då Sveriges läge ej längre kändes lika kritiskt och den kom då den tyska telegramtrafiken hade gått ned både i fråga om kvantitet och kvalitet. Dessutom hamnade de tres kryptobedrift i ett större perspektiv i skuggan av G-skrivar forceringen.

Dokument och arbetspapper från lösandet finns bevarade och här kommer en del tyska operatörskommentarter som bidrog till lösandet och Bo Kjellbergs egen handskrivna rapport i ärendet att återges. Likaså kommer den egenartade maskin som svenskarna byggde för att dechiffrera trafiken att skildras.

Bo Kjellberg var elev till Arne Beurling och handplockades av denne till kryptoanalysjobb på FRA. Han blev sedemera professor i matamatik vid Tekniska Högskolan i Stockholm.

Carl-Gösta Birelius hade 1940 just börjat matematikstudier i Uppsala då han inkallades till värnpliktstjänstgöring. Efter godkännande av Beurling placerades han på Försvarets kryptoavdelning.

Tufve Ljunggren var för tillfället inkallad som värnpliktig och även han hade matematiska studier i bagaget.

Maskinen, som de svenska kryptoanalytikerna kände till under namnet Z-Schreiber, var isjälva verket en kryptotillsats som användes tillsammans med en Standard Elektrik Lorenz tillverkad telereprinter. Kryptoutristningen kallades SZ40 (SZ=SchlŸsselzuzats, i svenska dokument anges också namnet GZ=Geheimkzuzats). En senare variant kallades SZ42.

Trafiken som härörde från Z-maskinen såg i stort sett ut som den som kom från G-skrivaren - dvs T52 maskinerna. De texter man arbetade med innehöll alltså 32 tecken: alfabets 26 bokstäver samtsiffrorna 1-6. Operatören kunde skriva i klartext och övergå till krypto genom att skriva en nyckelangivelse bestående av ordet "QEP" följt av sex bokstavsbigram, dvs en bokstav för inställningen av vart av ett av de tolv hjulen. Därefter skrev operatören "umum" (umschalten). Mottagaren ställde in sin maskin efter den angivna nyckeln och skrev "veve" (verstanden). Därefter följde den krypterade texten.

Med maskinen i klartextläge kommenterade operatörerna ofta sina bekymmer med inställningar och annat. På det sättet gav de oavsiktligt små pusselbitar som var för sig kanske inte sade så mycket, men Bo Kjellberg & Co samlade ihop dem och kunde dra slutsatser. Här återges några exempel på tyska kommentarer. Den tyska texten har lämnats oöversatt men meningen framstår i de flesta fall ganska klar. Tillfogande svenska kommentar återges också. Texten återges såsom den skrevs av i orginal.

1941 26 nov HC RN UZ QF - also bitten gebe Sie mal anderen qep, oder ist Ihr Grundschl. vielleicht heute nicht eingestellt worden?

1941 11 dec Einst. Buchstaben. Na klar, - so den Zahlen geschreiben. Bit noch mal qek qep + qep: KV DR -, ich kan hier nur Zahlen einstellen. Verd., ich habe doch ABZZ verlangt

1941 11 dec Die anderen Fernschreiber sind doch viel besser, kann mich an die anderen Kiste nicht gewöhnen. + Ach so, nur an die Z-Schr. + Ja, na brauch auch kein G-Schr. sein. + Nur die einfache Kiste.

1942 7 jan Wie ist bit die erste Zahl, ich habe zwei Tafeln und weiss nun nicht welche. +21+

1942 20 jan Auf den Z-Schr. ist es doch kein Vergnügen und wenn Sie eine Frage stellen, müssen Sie schön eb bis ich antworte, nun fiel natürlich der Schl. wieder zusammen, weil wir beide schreiben.

1942 5 feb Har först givit en qep med HI som 6:e trupp. Den andre svarar: Die letzte gr. muss HK heissen. + Ja, HK+

1942 8 feb Ist denn Marine-Schreiber (0G-Schr) absolut nicht möglich + Nein, kommt nicht in frage, ich habe Befehl vom ldn (Leider des Nachrichtendienstes) dass mir hbr und Finnland nur auf Z-schreiber gearbeitet wird.

1942 23 feb Ne,ne nicht so schnell ich muss doch erst den Schl. einstellen. (Den andre har givit en qep först).

1942 19 jun Hast du schon den neuen Schl. von heute eingestellt? + Ne, ich glaube noch nicht, + Also der neue Schl. ist eingestellt. Haben Sie alles auf Dat gestellt? (Dat=Datum). Also qauf 19+

1942 28 jul Ich gebe umum und du veve dann aber nicht gleich umschalten sondern bis 15 zählen vd ve und dann erst umschalten.

1942 1 aug In der letzen Gruppe ich rpt - SE - nicht - SD-. Also Wenn das nicht klappt machen wir nur eine Zahl zum einstellen ok? Also ich neu einst.

1942 8 okt - Hier qep ED FU IK OL MB - KK gleich in Zahlen durch ve - Haben Sie schon meine qep erhalten? - Geben Sie gleich in Zahlen durch habe die Tafel im mom nicht zur Hand. - Ist verboten. (Stöd för antagandet att bokstavsqepen översätts till siffer qep med hjälp av substitutionsruta.)

1942 11 okt Qep VB NI CK IJ HG UL + J=I ?? - Rpt mal - Ich hatte gefragt ob J gleich I ? - Ja ja ja.

1942 6 nov (Förmodligen om Z-skrivaren) : Oh Bimbabulla, errette mich von diesem Übel.

1942 7 nov Haben Sie nun auch schon den neuen Schlüssel sonst ist hier C-Schreiber frei geworden.

1942 9 dec Habt ihr schon neuen Tagesschlüssel drin - Hier ist schon neuen Schlüssel, da müssen wir ja leider noch bis 9 Uhr warten.

1942 24 dec (Ger först qep): VV FF GG RR TT HH. Mensch ich bin noch immer da bit rpt qep: SE DR FT GZ HU KI, - Du bist wohl mit deinen gedsnken schon bei heute Abend.

Det fanns mycket att ta fasta på i kommentarerna: otillåtna bokstäver på sista hjulet, sammanfallande bokstäver i substitutionstabellen (I och J), nyckelbyten m.m. Därutöver framgick klart att Z-maskinen var impopulär och att man hellre ville använda G-skrivarna, men att dessa i de flesta fall inte fick användas. Bo Kjellbergs redogörelse för rekonstrueradet av Z- maskinen :

Den 1 mars 1943 gav gruppchefen L.Carlbom i uppdrag åt undertecknade, C-G Borelius, Tufve Ljunggren och Bo Kjellberg, att söka rekonstruktera Z- maskinen. Emedan talrika prov, grundande sig på olika hypoteser, tidigare misslyckats, skulle arbetet denna gång bedrivas på det långsammare men säkrare sättet att systematiskt härleda säkra fakta, vilka i sin tur utnyttjas för ytterligare framstötar. En gynnsam omständighet var att gruppen redan från bšrjan erhöll ett lugnt och avskilt arbetsrum.

Den första veckan ägnades åt noggrann genomläsning av de förefintliga Z-matrealet, en packe telegram av ca. 1,5 meters höjd, anlända under tiden 26.11.41-mars 1943.

Syftet med genomläsningen var dels att uppgöra tillförlitliga QEP-lstor, dels att erhålla upplysningar av värde ur telegrafisternas samtal i klartext.

Då Z-maskinen begagnas, ges en QEP, bestående av 12 bokstäver, uppdelade i tvåställda grupper, t.ex. AB CD FK MN OP QR.

Genomläsningen av telegrambuntarna ledde bl.a. till följande slutsatser:

a Det är icke möjligt att genom något enkelt handgrepp övergå från Z till C eller AB.

b Det finns en "dagsnyckel" och därjämte en "månadsnyckel".

c Apparaten har en "Zusatz", där 12 valsar finns, vilka ställas in efter siffror på valsarnas periferi.

d Bokstavs-QEPEN begagnas så att man med hjälp av en substitutionsruta övergår från siffror til bokstäver och tvärtom.

e Substitutionsrutan byts månatligen. Detta framgick därav att valet av den 12:e (sista) QEP-bokstaven icke är alldeles fritt, på grund av att två bokstäver i alfabetet sakna siffermotsvarighet i substitutionsrutans kolumn för 12:e valsen. Det visade sig, att t.ex. under november 1942 bokstäverna E och K kunde förekomma, men i stället 2 andra bokstäver fattades, t.ex i oktober C och M.

f Emedan i rutan I=J återstå 25-2=23 bokstäver i alfabetet, varav den slutsatsen kunde dragas, att 12:e valsens period är 23.

g Vidare framgick av telegrafistenas samtal, att de 12 hjulen icke samtidigt kunde ställas in genom något handgrepp, utan måste få en mera individuell behandling - ett olidligt besvär för telegrafisterna, som ger anledning till diverse expressiva uttryck.

Till slut måste sägas, att dessa klartextsamtal icke kunna karaktiseras som en vishetens brunn att ösa ur, emedan teknisk obildad personal kan komma med både inkonsekvenser och felaktigheter vid beskrivningen av apparaten.

Efter dessa förberedande undersökningar påbörjades så det egentliga forskningsarbetet.

Z-maskinen åstadkommer en ren överlagring av klartexten.

Redan tidigare hade gjorda forceringar pekat på, att varje vals ständigt hade samma funktion, m.a.o att någon variabel koppling existerade. För att vinna full klarhet i denna sak, genomgingos QEP-listorna, varvid alla QEPER inom samma dag, som liknade varandra, utplockades. Motsvarande material forcerades i största möjliga utsträckning. Resultatet blev, att de 5 första liksom de 5 sista bokstäverna (valsarna i "Zusatzen" hade inflytande i ordning på de 5 raderna i överlagringen. I detta sammanhang erhölls fšr de 4 sista valsarna, 31, 29, 26 och 23.

De tidigare undersökningarna hade lett till förmodandet, att överlagringen alstrade av 5 jämnt frammatade valsar (de 5 sista), samt 5 ojämnt matade (stegmatade) valsar (de 5 första), samt slutligen eventuellt en šverlagrad dagsnyckel av obekant karaktär, möjligen alstrad av gamla G-apparater. Bortsett från dagsnyckeln bestyrktes förmodandet.

Perioderna 29 och 23 hade redan före vår undersökning erhållits ur följande material för den 4.8.42:

AT WU SR GS DB ZE och AT WU SR GS DS ZB

För t.ex. dessa material äro 1:a, 2:a och 4:e raderna i överlagringen lika (samma månadsnyckel, dagsnyckel och QEP-bokstäver), men 3:e och 5:e olika. Additionen av dessa sinsemellan ger remsor med perioderna resp. 29 och 23, vilka alltså ger en bild av motsvarande valsar adderade till sig själva efter vridning ett okänt antal steg.

Forcering av material av denna typ gav ständigt samma periodtal. Att den sista gruppen av valsar matades jämnt, var sålunda fastslaget. En besvikelse var sedan, att de erhållna periodiska summorna i de flesta fall kunde visas härröra från valsar av olika utseende, ehuru perioderna var konstanta. Omstiftning eller rent av ombyte av valsar måste sålunda förutsättas, något som i hög grad försvårade arbetet, emedan gynnsammare jämförelsematrial förekomma mycket sparsamt. Ofta voro också de behövliga forceringarna mödosamma och tidsödande, t.ex. då endast ett telegram finns på en viss nyckel.

Så småningom kunde emellertid några av de jämnt frammatade valsarna rekonstrueras, delvis med hjälp av en egenskap, som framkom, nämligen att telegram med liknande QEPER voro i någon mån jämförbara, icke blott på samma dag, utan även inom samma månad, i det senare fallet dock enbart de första 5-10 bokstäverna. Detta faktum talade tydligt för, att dagsnyckeln hade en annan karaktär än överlagring. I så fall borde efter bortaddition av den enkla överlagringen en remsa uppkomma, som härrörde från en av de 5 första valsarna, matad på ett visst sätt. Sedan forceringar utförts tillräckligt långt, kunde också kvasiperiodiska följder på detta sätt identifieras. Därmed var klart, att dagsnyckeln hade med den ojämna frammatningen att skaffa.

Nästa etapp i undersökningen var nu självskriven, nämligen studium av frammatningsfunktionen. För telegram på en viss nyckel kunde en dag brottstycken av frammatningfunktionen härledas, och det visade sig vara samma funktion. Förmodandet att alla 5 första valsarna hade samma stegmatningsfunktion visade sig riktig, och detta möjliggjorde i sin tur beräkning av såväl de tre återstående "enkla" överlagringsvalsarna som de 5 ojämnt matade. Perioderna befunnos vara:

I II III IV V VI VII VIII IX X XI XII

43 47 51 53 59 ? ? 41 31 29 26 23

Denna kännedom om maskinens konstruktion ledde till att material från olika månader kunde analyseras. "Månadsnyckeln" visade sig bestå i omstiftning av de 10 överlagringsvalsarna.

För att lösa det återstående problemet, hur frammatningsfunktion alstras, forcerades två material från samma dag, där den senare av de mellersta QEP-bokstäverna var gemensam. De båda matningsfunktionerna härleddes och jämfördes. De befunnos vara kvasiperiodiska bilder av en vals med perioden 37 i två olika lägen, i sin tur stegmatad av en vals med perioden 61.

Z-maskinen konstruktion var då röjd, den 9.4.43 kl.17.

Undersökning för olika dagar gav vid handen att dagsnyckeln bestod i omstiftning av de två matningsvalsarna VI och VII. Skiss av Z-apparatens "Zusatz" :

a Vals VII-XII jämn matning.

b Vals VII matar VI, som i sin tur matar gruppen I-V.

Till slut kan nämnas, att hela undersökningen grundat sig på forcering av ett 60-tal dagsmatrerial. Stockholm den 12 april 1943 / C-g Borelius, Tufve Ljunggren och Bo Kjellberg.

Den forcering av 60 dagsmaterial som Kjellberg nämner innebär att man i 60 fall haft så pass många telegram sända på samma nyckel (QEP) under samma dag - 4-8 telegram - att det gått att rekonstruera den underliggande texten samt den överlagringsserie som maskinen producerat. Det var genom analys av den rekostruerade överlagringsserien - av forcörerna noterad som fem rader av ringar och punkter - som maskunens slutliga funktion kunde klarläggas.

Den lyckade forceringen grundade sig på material som hade gått på kabel över svenskt territorium. Men ute på Fiskarudden på Lidingö hade också startats försök att inhämta tysk teleprintertrafik som gick på radio över

Baltikum. Täckbenämningen var "Oskartrafiken". Visserligen hade Telegrafverket i en rapport hävdat att det var omöjligt att ta sådan trafik, men ledaren för "maskinradiospaningen", Berndt Thisell, tyckta att man borde försöka - och visst gick det. Kvaliten var så dålig men i juni kunde i alla fall Lars Carlbom rapportera att man forcerat Z-material på Oskar. Ytterligare något senare - i september - forcerades också en ny version av Z-maskinen. Den skiljde sig från ursprungmaskinen genom annan stegmatning och torde motsvara den maskin som tyskarna kallade SZ42.

Men med sinande trafik och dålig kvalitet gick forceringen allt sämre och i februari 1944 vädjar Åke Rossby, chef för Bearbetningsbyrån, i ett brev till Arne Beurling om att han skulle komma till undsättning - även T52-forceringen gick dåligt. "Carlbom har fått nya svårigheter, och Oskar gör just inga framsteg. Carlbom är otvivelaktig bra, och rätt troligt är väl, att de tekniska betingelserna är otillräckliga; men inga utvägar bör lämnas oförsökta och därför vänder vi oss åter till Dig". Beurling lovar, likaså brevledes, att uppsöka Carlbom på "gamla stället" i början av mars.

Men den här gången kunde inte Beurling göra några trollkonster. Den tyska trafiken blev i stort sett oåtkomligt under resten av kriget.

Något som med i all säkerhet förevisades för Beurling under hans besök på "Karlbo" i mars 1944 var den dechiffreringsmaskin som just byggts. Detta skedde medan det ännu var hopp om att Z-trafiken skulle bli något stort. Men det blev bara en enda maskin och den rapporteras färdig i februari 1944, just då nedgången i användbar trafik blivit påtaglig.

Maskinen, populärt kallad "Cykelkedjemaskinen", är en intressant skapelse. Den var konstruerad av tekniske chefen O.W.Jonsson och byggd av på verkstan anställde Erik Asker. Den har nyligen granskats för att man skall få en uppfattning om hur den var gjord och hur den arbetade. Någon utförligare beskrivning från tillverkningen har inte återfunnits.

Maskinen har en elektromekanisk funktion bestående av tolv modifierade cykelkedjor som simulerar ursprungsmaskinens hjul. Modifieringen är gjord så, att de axlar som håller samman länkarna (och i vilka t.ex. en cykels drevhjul griper in) har borrats ur och ersatts med ett stift av ca, dubbla längden. Dessa stift kan förskjutas genom länkarna, och varje stift kan då ställas så, att det sticker ut åt höger eller vänster. Över varje länkpar har placerats en U-formad "hatt" av plåt, vilken hålls på plats av stifen. På hattarnas ovansida har nummer slagits in med en sifferstans, så att varje stift erhållit ett unikt nummer på respektive kedja. På så sätt kan man - liksom på orginalmaskinen - referera till en viss stiftposition med ett nummer.

Det finns tre grupper av kedjor. Det är "snabba gruppen" som består av kedjorna 7 till 12 och förflyttar sig ett steg för varje teleprinttecken. Förflyttningen åstadkoms av en kraftig elektronmagnet i maskinens nedre högra hörn, vilken påverkar en fjäderbelastad hävstång. När hävstångens undre del dras från sitt viloläge mot magneten, faller dess övre del in i ett urtag på ett drivhjul, och detta drivhjul kommer att stega fram snabba gruppen, då magneten släpper och fjädern drar tillbaka hävstången till viloläget.

Stiften på kedjorna 8 till 12 sluter fjäderkontakten i maskinens övre del, beroende på om de är ställda åt höger eller vänster. Stiften på kedja 7 fungerar som kuggar om de är ställda åt vänster. De påverkar då den högra delen av ett dubbelt kugghjul så att detta drivs framåt ett steg. Dubbelkugghjulets vänstra del matar kedja 6-motorkedjan - då ett vänsterställt stift på kedja 7 påverkar dubbelkugghjulet.

Stiften på motorkedjan (6) sluter en fjäderkontakt i maskinens övre del då de är ställda i ett visst läge. Då kontakten sluts, sluts även en strömkrets, vilken aktiverar ytterligare en elektronmagnet i maskinen nedre vänstra hörn. Denna driver den "långsamma gruppen."

"Långsamma gruppen" består av kedjorna 1 till 5. Precis som kedjorna 8 till 12 sluter dessa kedjors stift fjäderkontakter i maskinens övre del, då stiften är ställda i visst läge.

Snabba gruppens kedjor kan även matas fram med en vev på maskinens högra kortsida och långsamma gruppen kan likaså matas med en vev på den vänstra kortsidan. Möjligt är att denna möjlighet utnyttjas vid forcering av dagens nyckel, vilken bestod i omstiftning av kedja 6 och 7. Genom att mata de bägge grupperna för hand kanske man provade sig fram hur den långsamma gruppen skulle matas för att ge klartext.

Exakt hur maskinen var ansluten till teleprintern är inte klart, men på baksidan av maskinen finns tretton hål för banankontakter, via vilka kommunikationen skett.

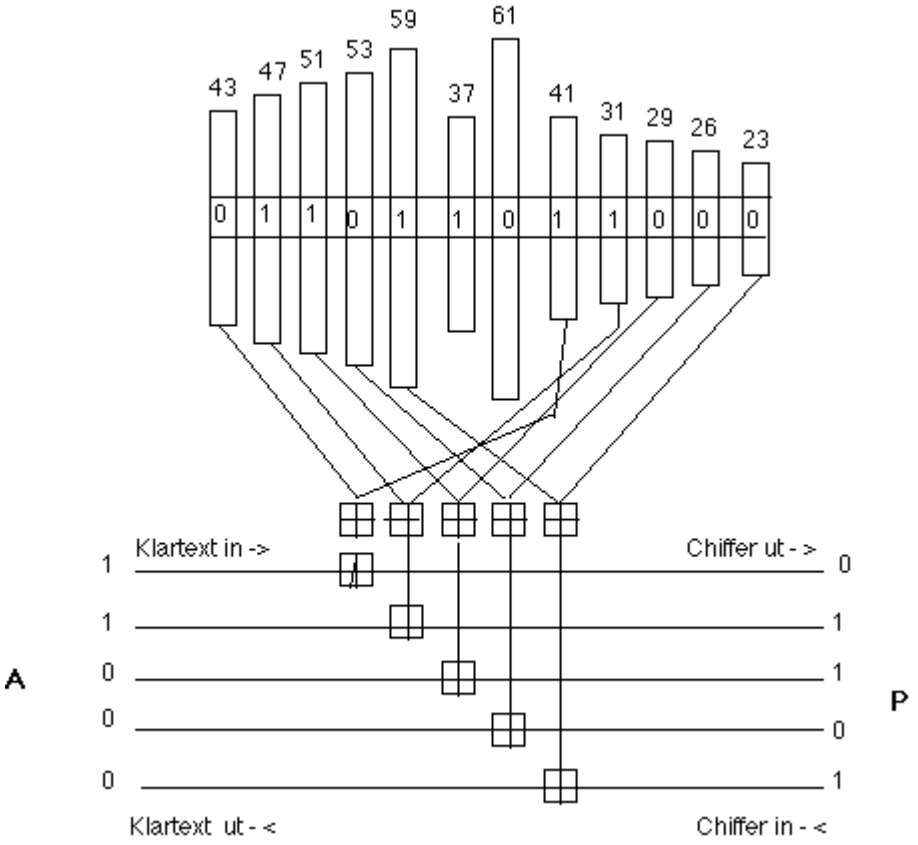
Misstanken om att maskinen måste ha bullrat avsevärt bekräftas av att hela maskineriet är inneslutet i en filtklädd låda.

Engelsmännen

Engelsmännen i Bletchley Park var andra världskrigets mästare på kryptoforcering. De lade också ned stora resurser på området. De teleprinterkrypton som nämnts i det föregående fick det gemensamma täcknamnet "Fish". T52-trafiken kallades "Sturgeon" och SZ40/42-trafiken kallades "Tunny". Båda systemen knäcktes 1942 men engelsmännen prioriterade "Tunny", som innehöll den för dem viktigaste trafiken. Lorenz SZ40/42 var väl också något lättare att forcera än Siemens & Halskes T52.

För att klara den löpande forceringen av Tunnymaterialet byggde de specialmaskiner, betydligt mer avancerade än den svenska cykelkedjemaskinen. De byggde först den maskin som kallades "Heath Robinson" efter den engelske skämttecknare som specialiserat sig på att rita fantastiska maskiner. (Man kan nog kalla den svenska cykelkedjemaskinen för en äkta "Heath Robinson". Därefter byggdes den berömda maskin som kallades "Colossus" och som ansetts vara en dator före datorernas tillkomst. Båda maskinerna byggde på teorier från matematikgeniet Alan Turing. Colossus kunde för vaje nyckelinställning genom en statistisk beräkning fastställa de 12 hjulens startpositioner.

Att maskinen kunde angripas statistiskt var man på det klara med även i Sverige. Lars Carlbom utarbetade en metod, genom vilken man kunde bestämma hjulen med utgångspunkt från en framforcerad överlagringsserie på mer än 400 positioner. Av skäl som nämnts i det föregående kom dock aldrig någon mera löpande forcering igång, än mindre fanns resurser att bygga en svensk Colossus.



* Z-maskinen hade 12 hjul med stift som kunde ställas in i passivt eller aktivt läge. Hjulen 7 till 12 matades regelbundet ett steg för varje sänt tecken. Hjulet 7 påverkade matningen av hjul 6; ett aktivt stift pŒ hjul t gjorde att hjul 6 gick fram ett steg samtidigt med hjul 7 (och med hjulen 8 till 12) medan ett passivt stift gjorde att hjul 6 stod stilla. På samma sätt matades hjulet 6 alla hjulen 1 till 5. Verkan av hjulen 1 till 5 adderades parvis, modulo 2, med verkan av hjulen 8 till 12 och resultatet bildade överlagringsserien.

Publicerat 2003-06-27.