Matti Wihuri och krypteringsnyckeln Allu

Sakari Pajunen, ex OH2WQ (Översättning: Thomas Anderssén, OH6NT)

Reino Hallamaa värvade Matti Wihuri för tjänst inom signalspaningen redan under de extra repetitionsövningarna (ER) 1939. Han fick i uppdrag att skola radister för Högkvarterets fjärrpatruller och planera sådana metoder för fjärrpatrullernas radiosamband som inte skulle uppdaga att det var frågan om finsk militär radiotrafik. Samtidigt höll man först nu på med utvecklingen av de första egna patrullradioapparaterna ”Kyynel” och ”Töpö” (”Tåren” och ”Stumpen”). En fjärrpatrull som verkade i Lappland sände ändå redan under vinterkriget uppgifter om fiendens rörelser med hjälp av en tysk agentsändare.

Som den radioamatör han var, valde Wihuri den internationella radiotrafikens metoder och förkortningar till grund för fjärrpatrullernas signaltrafik. Som krypteringsmetod valdes ett ersättningsförfarande, där varje tecken ersattes med ett av det engelska alfabetets 26 tecken. Under fortsättningskriget användes en blandad version av Tritheims tabell. Den var tryckt på ett A5-ark, och under bokstäverna för klartext, som var i bokstavsordning, hade man 25 rader med bokstäver, vilka bestod av samma bokstäver, blandade i godtycklig ordning, olika för varje rad.

Texten som skulle krypteras delades in i grupper om fem tecken, och ordens mellanrum utelämnades. Klartextens första tecken ersattes med motsvarande tecken från den första radens motsvarande kolumn, den andra bokstaven fick sin motsvarighet från den andra krypteringsraden och så vidare, tills 25 tecken hade krypterats, och man var nere på tabellens sista rad. Då började man om från den första raden, och när meddelandet var färdigkrypterat, fylldes den sista teckengruppen ut till fem tecken med godtyckliga bokstäver.

Under dåtida förhållanden var krypterad text ganska svårforcerad, men i en kall eller våt skog var det inte heller lätt med hjälp av en sådan papperslapp att åstadkomma ett krypterat meddelande. När man dessutom minns att ”tårmannen”, som fjärradisten kallades, verkligen inte var någon kontorist eller inomhusarbetare, utan en vanlig lantgosse som vanligen härdats i skogsarbete, måste man beundra hans ihärdighet och förmåga att sätta sig in i uppgiften så bra, att informationen gick fram tillräckligt noggrant i båda riktningarna.

Krypteringsskivan ”Allu” föddes med gemensamma krafter.

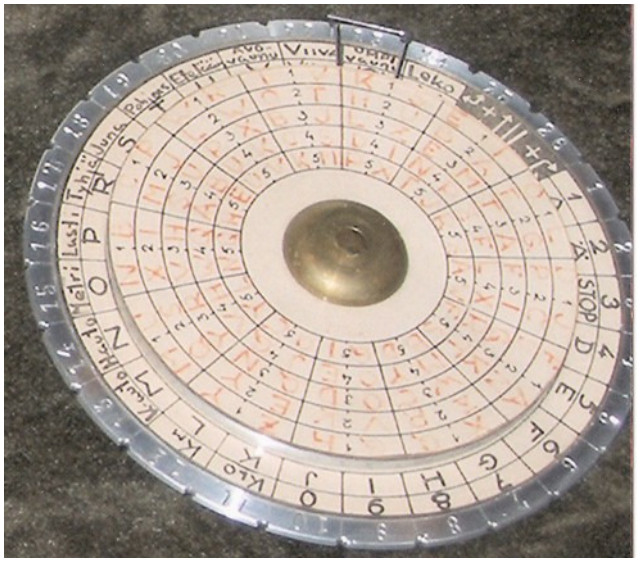
Klottrandet med dessa pappersark var orsak till ständig oro hos Wihuri. Därför utvecklade han tillsammans med militärmästare Alvar Ahonen en idé för en lämpligare metod. Redan innan vinterkriget hade Alvar Ahonen, som även var händig, värvats till signalspaningen som radist. Genom Wihuris och Ahonens gemensamma funderingar utvecklades så småningom en krypteringsskiva, som till Ahonens ära fick namnet ”Allu”

Den var tillverkad av aluminium, och bestod av två koncentriskt lagrade skivor, varav den större hade diametern 12 cm, och den mindre 9 cm. Skivorna var indelade i 26 sektorer och skivorna styrdes inbördes med hjälp av en skåra i den större och en låsfjäder i den mindre skivan. Den synliga cirkeln av den större skivan rymde alla klartextens tecken i två cirklar. I den ena cirkeln fanns alla finska språkets bokstäver, 24 tecken, och två sektorer som användes när man förflyttade sig till klartextens andra cirkel, som för sin del innehöll siffrorna, skiljetecknen, och de vanligaste förkortningarna, såsom km, leko (flygplan, av finskans ”lentokone”), tåg, p-bil osv. Låsfjädern var utformad så, att den omgav numret på

den sektor som för tillfället var i bruk. Den mindre skivan å sin sida innehöll det engelska språkets 26 tecken i fem koncentriska cirkelrader, blandade på olika sätt i varje rad. För att blanda tecknen hade man svarvat 26 st. träkulor med ca, 25 mm diameter, som bokstäverna var ritade på. När dessa bollar blandades i en för ändamålet tillverkad låda, var det lätt att plocka en boll åt gången ur lådan för läsning, och vidare anteckning på motsvarande plats på skivan. När den första krypteringsraden för skivan var klar, blandades bollarna på nytt och arbetet fortsatte.

Av varje kryptoskiva tillverkades två exemplar, av vilka patrullen hade den ena, och den andra fanns vid kompaniets centrala radiostation. Patrullerna hade vanligen två olika nycklar med sig ifall man råkade förlora den ena.

Man har tagit tillvara krypteringsskivorna från ett av Er.P 4:s kompanier vid signalmuseet i Riihimäki. När jag besökte museet, såg jag skivorna i sin förpackning, och förundrades då de krypterade texterna hade så bekant handstil. Först senare kom jag ihåg att det var jag själv som hade textat dem på Wihuris order i St. Michel. Texterna hade gjorts på förtryckta pappersbottnar, och på skivorna var texterna täckta med celluloidskivor, så att de skyddades mot både fukt och nötning.



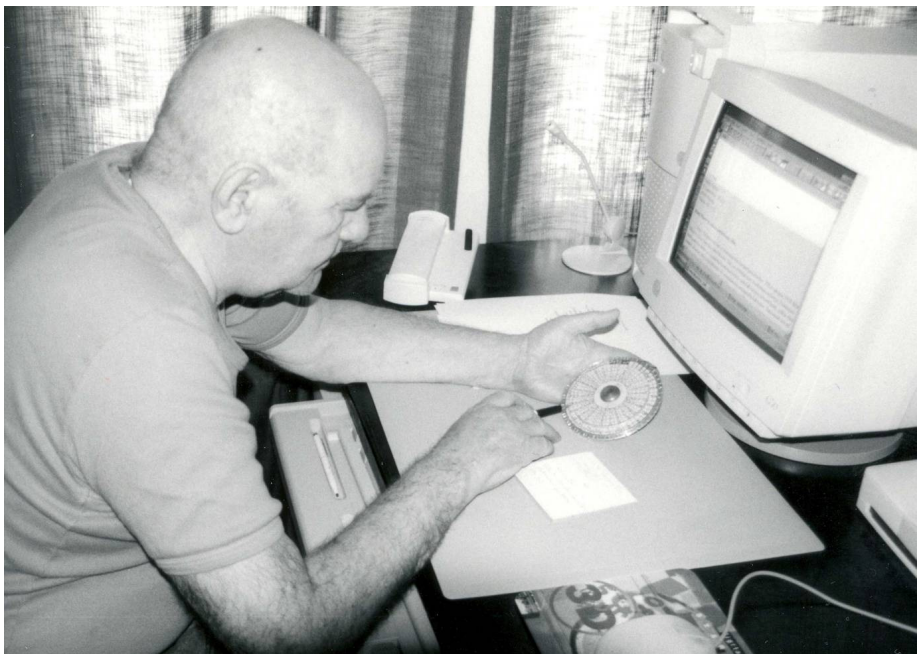
Krypteringsskivan ”Allu” fotograferad i sin vitrin i Finlands Signalmuseum i Riihimäki.
Bild: Timo Ekko.

Krypteringen utfördes så att man började med att ställa in låsfjädern på överenskommen sektor, och de första fem tecknen krypterades med denna inställning, varvid det första tecknet togs från den mindre skivans yttersta cirkel, nästa från den andra cirkeln, det tredje tecknet från tredje osv.

För att kryptera de följande fem tecknen flyttades den inre skivans låsning till följande sektor, och så fortsatte man tills hela meddelandet hade krypterats. Dechiffreringen gick till på motsvarande sätt genom att söka fram klartextens tecken på den yttre skivans cirklar. Förfarandet var enklare än denna beskrivning låter förstå, och en van radist klarade relativt snabbt av att både kryptera och dechiffrera.

I detta sammanhang kan det vara skäl att nämna, att man inte känner till något fall, där fienden skulle ha lyckats forcera krypteringen i fjärrpatrullernas meddelanden. I vissa fall är det skäl att misstänka att fienden med radio försökte störa patrullernas trafik, men även dessa fall var sällsynta.

Skivorna tillverkades av depåkompaniet vid Högkvarterets radiobataljon under ledning av major Ragnvald Lautkari, liksom fjärrpatrullernas radioapparater. När ”Allu” hade fåtts i bruk, blev ”tårmannens” uppgift betydligt lättare, men utan själva ”tårmannen” hade alla dessa rackerier varit förgäves. – Om fjärrpatrullmännen var krigstidens elit, så fanns ”tårmännen” i främsta ledet av denna elit.



Signalspaningsveteranen Sakari Pajunen (1925-2004) ex OH2WQ studerar här krypteringsskivan Allu framför sin dator i augusti 1998.

Bild: R. Janhunen

För signalspaningsverksamheten, som leddes av Reino Hallamaa, skolade Matti Wihuri (1905-1992) redan före vinterkriget fjärrpatrullradister och signallottor. Med hjälp av den livslånga radioamatörhobbyn (OH2OH), var den tidigare signalofficerens radioapparater alltid i brukbart skick.

Bild: R. Janhunen

Denna artikel publicerades första gången i Finlands Radiohistoriska Förenings informationstidning nr. 3/1998.

(10.7.07/rja – 12.7.07/tha)