Enigma

Eero Nevalainen

Helsinki 21. huhtikuuta 2004

Tietojenkäsittelytieteen historia-seminaarin esitelmä

HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

Sisältö

1 Johdanto

Modernille sodankäynnille tyypillinen eri aselajien ja joukko-osastojen yhteistoiminnan tarkka koordinointi edellyttää turvattuja ja luotettavia viestiyhteyksiä. Tämä tarve on ollut merkittävä salakirjoitusmenetelmien kehityksen moottori. Yksi varhaisimpia dokumentoituja tähän tarkoitukseen käytettyjä salakirjoitusmenetelmiä on Julius Caesarin rotaatiomenetelmä [WikA].

Toinen maailmansota oli ensimmäinen sota, jossa tämä eri aselajien yhteistoiminta saavutti modernit piirteensä. Erityisesti historiankirjoihin on jäänyt saksalaisten *Blitzkrieg*. Nopeuteen ja yllätykseen pohjautuva taktiikka vaati radion laajamittaista käyttöä, ja sähkötetyn viestiyhteyden suojaamiseksi tarvittiin epätriviaali salakirjoitusmenetelmä, joka kesti tieteenalana orastavan, matematiikkaa yhä suuremmassa määrin hyödyntävän *kryptoanalyysin* hyökkäykset.

Tässä esitelmässä paneudutaan saksalaisten legendaariseen *Enigma*-salakirjoituskoneeseen ja pyrkimyksiin sen murtamiseksi.

2 Enigman rakenne ja kryptauksen toiminta

Tässä luvussa nojataan enimmäkseen tietoihin lähteistä [SalA, alasivut 1 ja 2] sekä [Tur40, luku 1], ellei toisin mainita.

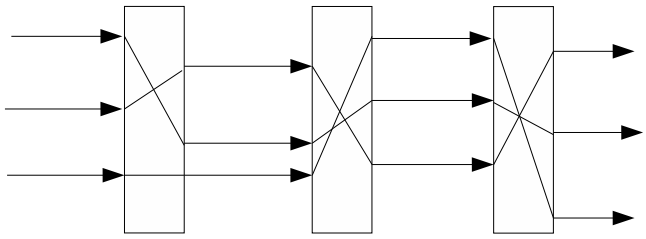
Merkinkorvausmenetelmät ovat yksinkertaisia salakirjoitussysteemejä, joissa selkotekstin merkit korvataan yksi kerrallaan salakirjoitetun tekstin merkeillä. Edellä mainittu Caesarin menetelmä toimii juuri näin. Triviaalin merkinkorvauksen suurimpana heikkoutena on käytetyn korvauskuvauksen löytämisen helppous. Yksinkertaisimmillaan viestin purku onnistuu muutaman onnistuneen arvauksen jälkeen. Arvauksien tekoa helpottaa se, ettei merkinkorvausmenetelmä muuta merkkien tilastollista jakaumaa.

1800-luvulla kehitettiin lukuisia *moniaakkostollisia* salakirjoitusmenetelmiä, joissa salatekstin merkin määrämiseen käytetään monia eri korvausaakkostoja. Käytetty aak-

kosto määräytyy menetelmäkohtaisen säännön mukaan. Seuraavalla vuosisadalla tuli mahdolliseksi toteuttaa merkkien korvaaminen sähköisiä kytkentöjä käyttämällä. Tämä johti lopulta Enigma-koneen kehittämiseen.

Neljä keksijää neljässä eri maassa kehitti Enigman periaatteen toisistaan riippumatta kolmen vuoden sisällä. Kuitenkin Enigman varsinaisina isinä pidetään saksalaisia insinöörejä Arthur Scherbiusta ja E. Ritteriä, jotka ensimmäisenä toivat markkinoille Enigma-koneen vuonna 1918. Yritykset kaupata laitetta Saksan silloiselle keisarilliselle laivastolle ja ulkoministeriölle olivat tuloksettomia; vuodesta 1923 lähtien laite saavutti jonkinasteista kaupallista menestystä. [KrD02]

Enigma on sähkömekaaninen salakirjoituslaite, joka käyttää useaa korvausaakkostoa samanaikaisesti. Korvausaakkosto on oleellisesti aakkoston permutaatio, joka kuvaa selkotekstimerkin salakirjoitusmerkiksi. Tällainen permutaatio voidaan toteuttaa sähköisillä kytkennöillä. Nämä kytkennät on Enigmassa johdotettu joukkoon pyöreitä valsseja eli "roottoreita" siten että jokainen roottori sisältää yhden tällaisen permutaatiokuvauksen johdotuksessaan.



Kuva 1: Enigman periaate

Kuvassa 1 on esitetty yksinkertaistettu malli kolmiroottorisen Enigman toimintaperiaatteesta. Kuvassa laatikot edustavat roottoreita ja nuolet ja viivat sähkön virtausta järjestelmän läpi. Jokaisen roottorin sivupinnalla on joukko kontakteja, joita pitkin sähkö virtaa roottoriin ja toiselta puolelta ulos. Jokaista aakkoston kirjainta varten on oma kontaktinsa. Kytkennät roottorin sisällä yhdistävät kontaktit toisiinsa ja toteuttavat sekoituksen. Sarjassa seuraava roottori toistaa sekoitusprosessin oman kuvauksensa mukaisesti. Koska jokainen Enigman roottori saattoi olla 26 asennossa (Enigman aakkoston koko), saadaan tällä yksinkertaistetulla mallilla tuotettua 26^3

eri korvausaakkostoa.

Roottorit eivät sinällään vielä lisää Enigman kryptauksen vahvuutta suhteessa yksinkertaiseen korvausmenetelmään – itse asiassa staattiset roottorit edustavat sinällään vain yhtä korvausaakkostoa. Enigman merkittävin ero triviaalimetodiin on siinä, että roottorit *pyörivät* syötettä annettaessa. Oikeanpuoleisin roottori pyörähtää kerran jokaisen merkin kohdalla, seuraava roottori sen jälkeen kun ensimmäinen on pyörähtänyt täyden kierroksen ja niin edelleen (vrt. auton matkamittari). Näin käytetty korvausaakkosto *vaihtuu jokaisen merkin kohdalla*. Lopulta aakkosto palautuu samaksi kuin se oli alussa, mutta niin pitkiä viestejä ei käytännössä koskaan lähetetä.

Aakkoston muuttuminen jokaisen merkin kohdalla vaikeuttaa merkittävästi lingvististä analyysiä, joka käyttää salakirjoituksen murtamiseen tietoa merkkien jakaumista selko- ja salatekstissä.

Fyysisenä laitteena Enigma muistuttaa kirjoituskonetta. Siinä on näppäimistö, jolla syöte annetaan ja pienillä sähkölampuilla toteutettu taulu, jolta salakirjoitettu merkki luetaan. Koneen sähköinen osa sytyttää jokaisella näppäimen painalluksella salakirjoitettua merkkiä vastaavan lampun ja mekaaninen osa pyöräyttää koneen roottoreita yhden pykälän verran eteenpäin.

Kuva 2: Enigma [WikB]

Edellä kuvatun lisäksi Enigmassa oli vielä hitaimmin pyörivän roottorin takana niinsanottu *reflektori*. Tämä oli periaatteessa yksipuolinen roottori, joka käänsi virran takaisin siten, että se palasi roottorien läpi jotain toista reittiä ennen kuin se saavutti lopullisen tuloksen ilmoittavan lampun. Versiosta riippuen reflektori saattoi pyöriä muiden roottorien mukana tai olla staattinen.

Reflektorin ansiosta Enigmalla voidaan sekä salakirjoittaa että purkaa salakirjoitus käyttämällä samaa mekanismia, kunhan vain laitteen lähtötila (eli avain) tunnetaan. Näin ollen Enigmassa ei tarvitse olla erillistä purkumoodia.

Myöhemmissä, sotilaskäyttöön tarkoitetuissa Enigmoissa laitteen kompleksisuutta lisättiin kahdella tavalla. Ensimmäisessä menetelmässä Enigman avaimen koko lisättiin käyttämällä eräänlaista kytkentätaulua näppäimistön ja roottorien välissä. Asettamalla johtoja kytkentätauluun voitiin valita korkeintaan 10 paria merkkejä, jotka kuvautuivat toisikseen ennen kuin virta syötettiin roottoreihin. Muunnos suoritettiin sekä ennen sekoittajaroottoreita että niiden jälkeen.

Toinen tapa kasvatti avainta lisäämällä jokaiseen roottoriin aakkostetun renkaan, jonka asema suhteessa roottoriin määräsi lopullisesti sen, mikä roottorin kontakteista vastasi mitä aakkoston kirjainta.

Vaikka Enigman eri versioissa oli eroja, voidaan yleisesti ottaen sanoa, että avain koostuu seuraavista osista:

- Roottorien järjestys. Roottorit voitiin irrottaa ja asettaa koneeseen mielivaltaisessa järjestyksessä. Enigmoissa oli tyypillisesti 3 roottoria, mutta roottori saatettiin valita esimerkiksi viiden tai jopa kahdeksan roottorin joukosta.
- Roottorien ympärillä olevien aakkosrenkaiden asento
- Kytkentätauluun tehdyt kytkennät
- Roottorien asento viestin syötön alussa. Asento luetaan aakkosrenkaasta.

Tyypillinen armeijan käytössä olleen kolmiroottorisen (s.e. roottorit valitaan viidestä mahdollisesta) Enigman alkutilaa kuvaavan avaimen tila-avaruus on siis kooltaan edellisen perusteella laskien (suuruusluokkaa[1]) $5 \times 4 \times 3 \times 2 \times 26^3 \times \binom{26}{10}$.

3 Enigman heikkoudet

Varhaiset kaupalliset Enigmat kyettiin murtamaan jo ennen toisen maailmansodan alkua. Uudelleenjohdotettuinakin ne olivat edelleen heikkoja. Italialaiset käyttivät

[1] Tämä ei ole ihan tarkka luku, sillä kaikkia kytkentätaulun kytkentöjä ei ole pakko tehdä.

laajasti sotaa edeltävää kaupallista Enigman D-versiota, ja tämä johti tappioon Matapanin taistelussa [KrD02].

Enigmalla salakirjoitettujen viestien murtamista helpotti joukko viestien ja itse Enigman ominaisuuksia. Edelliset johtuivat lähinnä koneen käyttäjien proseduraalisista virheistä; jälkimmäiset usein Enigman suunnittelijoiden virheellisestä käsityksestä siitä, mikä salakirjoitusjärjestelmässä luo turvallisuutta.

Merkittävin Engiman puute on, että koneen konstruktiosta seuraa, että selkotekstin merkki ei koskaan kuvaudu itsekseen [Tur40, luku 1, s. 2]. Enigman viestien murtamisessa keskeiseksi menetelmäksi muodostui niin sanottu tunnetun selkotekstin metodi, jossa ennalta tiedetyn selkotekstin ja salatekstin välisistä suhteista voidaan päätellä salakirjoitusavain [Tur40, erit. luvut 4-6]. Edellä olevasta seuraa, että mahdollisia selkotekstin esiintymiskohtia voidaan etsiä salakirjoituksesta löytämällä sellainen viestin ja mahdollisen selkotekstin kohdistus, jossa mitkään vastinmerkit eivät ole samat [SalB]. Mitä pidempi selkotekstin pätkä on, sitä suuremmalla todennäköisyydellä tällaisen ehdon täyttämä kohdistus myös on oikea.

Monissa Enigman malleissa jotkin roottorit pyörähtivät eri vaiheessa kuin muut roottorit, roottorin siirtyminen eteenpäin ei siis tapahtunut täysin samoin periaattein joka roottorin kohdalla. Tämä aiheutti eri roottorivalinnoilla konfiguroitujen koneiden salatekstiin säännönmukaisuuksia, joista voitiin parhaassa tapauksessa päätellä koneeseen valitut roottorit ja niiden järjestys.

Saksalainen täsmällisyys auttoi koodinmurtajia erityisesti yhdistettynä edellä todettuun Enigman salakirjoituskuvauksen rajoitteeseen. Saksalaiset koodasivat Enigmalla lähes kaiken; materiaalia oli siis runsaasti saatavilla. Usein jopa säätiedotukset salakirjoitettiin – säätiedotuksen määrämuotoisuus mahdollisti selkotekstin selvittämisen hyvin helposti. [WikB]

Radioliikenteen ja kielen muut säännönmukaisuudet tarjosivat myös mahdollisuuksia älykkääseen selkotekstin arvaamiseen. Ensimmäisenä kokeiltiin usein sovittaa selkotekstiä ANX viestin alkuun, sillä saksan prepositio “an” esiintyi tyypillisesti tässä kohtaa (esim *an General...*), ja X oli välilyönnin virkaa toimittava merkki. Innokkaimpien

natsien joka viestiin liittämä tervehdys “Heil Hitler” testattiin myös systemaattisesti. [Mom, luku 1]

Jos yleiset selkotekstit eivät tuottaneet tulosta tietyn päivän viesteille, vastustaja voitiin yrittää pakottaa lähettämään ennalta arvattava viesti esimerkiksi levittämällä laivaston reitille miinoja. Tällöin jokin viesteistä luultavasti sisälsi sanan *Minen*. [WikB]

Enigman käytön virheistä oli myös suurta hyötyä. Jotkin näistä virheistä olivat systemaattisia ja liittyivät Enigman ohjesäännön mukaiseen käyttötapaan.

Saksalaisten ennen syyskuuta 1938 käyttämä n.s. *indikaattorijärjestelmä* oli perusteiltaan virheellinen. Tässä systeemissä Enigma-operaattoreilla oli käytössään jokaiselle päivälle ennalta sovittu koneen konfiguraatio roottorien alkuasentoa lukuunottamatta. Operaattori valitsi mielivaltaisen roottorien alkuasennon ja lähetti sen selkotekstinä. Tämän jälkeen hän valitsi kolmikirjaimisen *viestiavaimen* ja salakirjoitti sen Enigmalla *kahteen kertaan*. Tämän jälkeen roottorit käännettiin viestiavaimen osoittamaan asentoon ja loppu viestistä salakirjoitettiin. Viestiavaimen lähettäminen kahteen kertaan oli eräänlainen virheenkorjauksen muoto, mutta se lisäsi viestiin redundanttia informaatiota, josta oli myöhemmin hyötyä puolalaisille koodinpurkajille. [2] [SalA, alasivu 3]

Toisenlaiset operaattorin virheet liittyivät operaattorin laiskuuteen tai tietämättömyyteen. Yhteyttä testatessaan operaattori saattoi lähettää pitkän sarjan yhtä ja samaa kirjainta. Tämä tietysti näkyi salaviestissä pitkänä jaksona, jossa ei esiinny tätä tiettyä aakkosta. Tästä viestin purkaja saa pitkän, varman selkotekstin.

Eräs radisti käytti viestiavaimena aina tyttöystävänsä nimen ensimmäisiä kirjaimia *CIL*. Brittien keskuudessa tällaiset triviaalit avaimet tulivat tunnetuiksi nimellä *cillies*.

[2] Eri lähteet ovat eri mieltä siitä, millainen ennen syksyä 1938 käytetty metodi tarkalleen oli. Tässä on valittu Tony Salen esitys asiasta.

4 Puolalaisten rooli

Ehkä unohdetuin osa Enigman tarinaa on puolalaisten koodinmurtajien työ ennen toisen maailmansodan alkua. Puolalla oli kaksi erityistä edellytystä olla Enigman murtajien eturintamassa: välitön huoli Saksan 1930-luvun sisäpoliittisesta kehityksestä ja tästä johtuva pakko tietää naapurin aikomukset ja Puolassa 20- ja 30-luvuilla vallinnut matematiikan kukoistuskausi.

Puolalaiset olivat siepanneet saksalaisten Enigma-viestejä vuodesta 1928, jolloin Saksan armeija otti koneen käyttöönsä. Samana vuonna puolalaisia kohtasi onnenpotku saksalaisten unohtaessa lähettää Varsovan lähetystöön matkalla olleen Enigman sinetöidyssä diplomaattipostissa. Puolalaisilla oli viikonlopun verran aikaa tutkia konetta, kun saksalaiset olivat ensin herättäneet heidän mielenkiintonsa vaatimalla juuri erään tietyn lähetyksen välitöntä palauttamista. [Har99] [3]

Kuva 3: Marian Rejewski

Laitteesta saatuja tietoja ryhdyttiin kuitenkin toden teolla hyödyntämään vasta vuonna 1932, kun Marian Rejewski (kuva 3)[4], Jerzy Rozycki ja Henryk Zygalski päätyivät töihin Puolan signaalitiedusteluun. Kolmikko oli aiemmin läpäissyt ainoina menestyksellä Poznanin yliopistossa järjestetyn salaisen koodinmurtokurssin. [Koz84]

Rejewski lähestyi Enigmaa puhtaan matemaattisesta suunnasta. Hän muotoili permutaatioihin perustuvia yhtälöitä, joiden ratkaisu jäi kuitenkin puutteelliseksi, sillä armeijan Enigman roottorien johdotusta ja näppäimistön kirjainten järjestystä ei tunnettu. Nämä puutteet korjautuivat pian puolalais-ranskalaisen yhteistyön ja lahjotun saksalaisen upseerin avustuksella [Kah83, Koz84]. Tämän jälkeen puolalaisilla oli käytössään toimiva Enigman teoreettinen malli.

Rejewskin suurin saavutus oli sen havaitseminen, että indikaattorijärjestelmän mukaisesti lähetetyn viestiavaimen toisto kahteen kertaan sisälsi tietoa koneen koko avai-

[3] Tässä luvussa käytetyt lähteet [Har99], [Kah83] ja [Koz84] eivät ole olleet kirjoittajan käytössä; niiden oikeellisuudessa luotetaan lähteeseen [Wes].

[4] Lähde: http://home.us.net/ encore/Enigma/enigma.html

mesta. Koska viestin otsakkeen ensimmäinen ja neljäs, toinen ja viides sekä kolmas ja kuudes kirjain olivat selkotekstissä aina samat, tietty salateksti saattoi syntyä vain tietyissä konfiguraatioissa olevissa Enigmoissa. [SalC]

Voidaan sanoa, että jokainen Enigman roottorien konfiguraatio aiheuttaa kuuteen otsakkeen merkkiin tiettyjä karakteristisia ominaisuuksia, jotka ovat *riippumattomia kytkentätaulun asetuksista*. Nämä karakteristiikat voidaan generoida taulukkoon, kun koneen roottorien johdotukset ovat tunnettuja. Generointia varten puolalaiset kehittivät *syklometriksi* kutsumansa koneen. Syklometri taulukoi kuuden merkin joukon karakteristiikat jokaiselle mahdolliselle 26^3:lle roottorien alkuasennolle. Koodinpurkajan tarvitsi tämän jälkeen vain vertailla päivän radioliikennettä näihin taulukoihin. Toisen vastaavan menetelmän kehitti Zygalski: hänen päällekkäin aseteltavat lävistetyt paperiarkkinsa eliminoivat niitä viestiavaimia, jotka eivät voineet tuottaa havaittuja salakirjoitettuja viestiavainpareja. [SalC]

Vuoden 1938 jälkipuoliskolla saksalaiset tekivät joukon muutoksia Enigmaan – syyskussa muuttui indikaattorimekanismi ja joulukuussa lisättiin entisten kolmen roottorin joukkoon neljäs ja viides roottori. Nämä muutokset lisäsivät Enigman kompleksisuutta siinä määrin, että puolalaisten koodinmurtajien resurssit loppuivat. Heidän menetelmänsä olivat sinällään vielä käyttökelpoisia, mutta Puolalla ei ollut rahaa eikä aikaa rakentaa suuria määriä Rejewskin kehittämää uutta koodinmurtokone *bombaa*. Toisen maailmansodan syttymisen alla puolalaiset luovuttivat Enigmaa koskevan tietämyksensä länsiliittoutuneille. [Wes]

5 Bletchley Park ja Turingin Bombe

Puolan valloituksen jälkeen Enigman murtamisponnistukset keskittyivät Englantiin Bletchley Parkin kartanon alueelle. Aikanaan paikka tunnettiin koodinimellä *Station X* alueella sijainneen radioaseman mukaan.

Bletchley Parkin rakennustyöt aloitettiin 1882. Vuonna 1938 se siirtyi brittihallituksen omistukseen, ja sitä alettiin käyttää signaalitiedustelun päämajana.

Toiminta Bletchley Parkissa oli organisoitu joukkoon mökkejä, joissa eri alojen spesialistit hoitivat tehtäviään. Tehtävät oli tarkkaan rajattu ja kaikilla asiaan osallisilla oli käytössään vain se tieto, mikä ehdottomasti tarvittiin sen suorittamiseksi. Mökkejä pidettiin käytännössä karanteenissa siten, että niissä työskentelevät ihmiset eivät olleet tekemisissä toistensa kanssa, ja tieto niiden välillä kuljetettiin turvallisia kanavia pitkin (esim. sinetöitynä kuriirin välityksellä). Tietovuossa osallisina olleet viestien murtajat, kääntäjät ja tiedusteluanalyytikot pyrittiin eristämään toisistaan. Salailu vietiin niin pitkälle, että edes Bletchley Parkista tiedustelutietoja saava rajoitettu joukko – muun muassa aselajien komentajat – eivät koskaan tienneet, että Enigma oli onnistuttu murtamaan! Tiukat varotoimet onnistuivat pitämään Bletchley Parkin salaisena koko sodan ajan ja vielä pitkään sodan jälkeenkin. [SalE, SalF]

Mökissä 8 työskenteli Alan Turing. Hänen johdollaan ja englantilaisten puolalaisia suuremmilla resursseilla Enigman murtamisesta voitiin tehdä likipitäen teollista toimintaa. Sodan loppuvaiheissa Bletchley Parkissa työskenteli yli 10000 ihmistä. Turing kehitti Rejewskin *bomba*-konetta edelleen ja tästä syntyi kone, jonka nimi oli englantilaisittain *Bombe* [SalD].

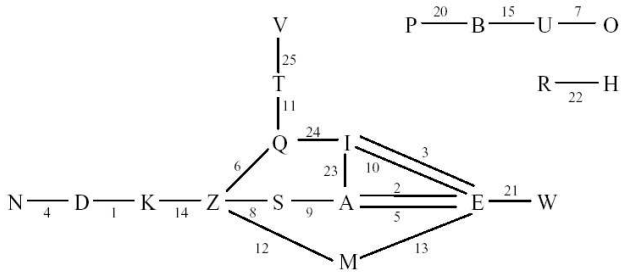
Bombe oli merkittävä parannus verrattuna puolalaisten syklometriin siinä, että sillä kyettiin etsimään missä tahansa kohtaa viestissä esiintyvän todennäköisen selkotekstin avulla mekaanisesti ja automaattisesti mahdollisia Enigman asetuksia [Tur40, luku 6]. Syklometrihän generoi vain taulukkoa eri asetusten tuottamista viestin otsakkeen kuuden ensimmäisen kirjaimen karakteristisista ominaisuuksista.

Muistutetaan mieliin tässä vaiheessa, että Enigman salakirjoituskuvauksessa $X \to Y \Leftrightarrow Y \to X$. Turing tarkasteli salatekstin ja selkotekstin jossain kohdistuksessa esiintyviä samoja merkkipareja.

Jos jossain kohdistuksen positiossa esiintyy merkkipari ja sama pari esiintyy myöhemmin, voidaan mahdollisia tällaisen tilanteen tuottavia asetuksia hakea kahdella sarjaan kytketyllä Enigmalla. Enigmat kytketään peräkkäin siten, että jälkimmäinen Enigma on niin monta askelta edellä ensimmäistä, kuin merkkiparien esiintymien ero on tarkasteltavassa kohdistuksessa (engl. *crib*). Enigmoja kytketään peräkkäin niin

monta kuin esiintymiä on. Tällaista konstruktiota kutsutaan *Letchworth-Enigmaksi*. Nyt Enigmoja voidaan pyörittää eteenpäin kunnes virta kulkee systeemin läpi ensimmäisestä kontaktista X jälkimmäisen ulostuloon Y. Tällöin Enigmat ovat mahdollisesti viestin kirjoittamiseen käytetyissä asetuksissa. Asetukset voidaan periaatteessa tarkistaa käsin Enigmaa käyttäen, joskin tällä tavoin mahdollisuuksia on vielä hyvin monta. [SalB]

Merkkipareihin pohjautuvaa menetelmää voi laajentaa merkeistä muodostuvien syklien tarkasteluun. Jos selkoteksti on esimerkiksi *SPRUCHNUMMERXEINS* ja salateksti *JYCQRPRYDEMCJMRSR*, merkit positioissa 7, 16 ja 17 muodostavat syklin $R \rightarrow N$, $N \rightarrow S$, $S \rightarrow R$. Tämä voidaan kytkeä Letchworth-Enigmaksi. [SalB]



Kuva 4: Esimerkki menusta [Tur40, luku 6, s. 3]

Bletchley Parkissa edellä olevan kaltaisia syklejä kuvattiin verkon kaltaisella graafisella esityksellä, jota kutsuttiin *menuksi*. Kuvassa 4 on annettu tällaisesta esimerkki. Merkit on yhdistetty kaarella, jos ne esiintyvät syklissä, ja kaaren numero on parin ensiintymispositio kohdistuksessa.

Enigman kytkentätaulu estää edellä esitetyn kaltaisen lähestymistavan suoraviivaisen käytön. Turing keksi kuitenkin tavan kiertää ongelman. Turingin ratkaisussa Letchworth-Enigman ulostulot kytketään takaisin syötekontakteihin. Tarkastelemalla systeemin läpi muodostuvia virtapiirejä voitiin tehdä päätelmiä eri kirjainten pareista kyktentätaulussa. Erityisesti jos syklin (ABC) kirjainten parit kytkentätaulussa ovat S_1, S_2 ja S_3 ja roottorien järjestys ja asento on oikea, systeemi stabiloituu tilaan jossa virta kulkee Letchworth-Enigman komponenttien välillä ainoastaan kontaktien S_1, S_2 ja S_3 kautta [SalB]. Vastaavan kaltaisten ehtojen avulla voitiin myös nopeasti

hylätä vääriä hypoteeseja Enigman asetuksista.

Turingin Bombe oli kone, joka teki näitä tarkistuksia mekaanisesti [Tur40, luku 6]. Siinä oli joukko menun mukaan Letchworth-Enigmoiksi johdotettuja rumpuja, joita moottorit pyörittivät, kunnes järjestelmän läpi muodostuvat virtapiirit olivat tilassa, joka osoitti mahdollisen avaimen löytyneen. Yhdessä Bombessa Letchworth-Enigmoja oli 60 kappaletta – yksi kohden jokaista tapaa valita Enigman kolme roottoria viidestä mahdollisesta. Kaikki roottorivalinnat voitiin siis testata samanaikaisesti ja yhdellä menu-ohjelmoinnilla. [SalB, SalD]

Bomben ja siihen myöhemmin tehtyjen parannusten avulla Bletchley Park pystyi jo vuoden 1942 tienoilla purkamaan suuren osan Saksan armeijan Enigma-viestiliikenteestä. Sodan lähestyessä loppuaan lähes kaikki viestit olivat luettavissa [WikB].

Alkuperäisiä Turingin Bombeja ei enää ole olemassa, koska ne ja lähes kaikki niihin liittyvä materiaali tuhottiin Winston Churchillin käskystä sodan päätyttyä.

6 Lopuksi

Enigman viestien purkamisella oli suuri merkitys erityisesti Atlantin taistelulle. Voitaneen olettaa, että ellei Enigman viestejä olisi voitu edes rajoitetusti lukea, Englannin ja Yhdysvaltain laivastot olisivat hyvinkin saattaneet kärsiä kestämättömiä tappioita saksalaisille sukellusveneille.

Ison-Britannian hallitus on pitänyt monia Enigmaan liittyviä seikkoja salaisina aina viime vuosiin asti. Esimerkiksi tieto Enigman murtamisesta tuli julkiseksi vasta 1960-luvulla, ja itse asiassa länsiliittoutuneet vakoilivat Enigmaa käyttäviä valtioita aina tietokonesalakirjoituksen yleistymiseen asti [WikB].

Puolalaisten pioneerien rooli ei ole historiankirjoituksessa saanut ansaitsemaansa asemaa. Rejewskille ja kumppaneille myönnettiin kuitenkin taannoin postuumisti korkein puolalainen kunniamerkki.

Koska Enigmaan liittyvä salailuoperaatio oli niin laaja, paljon jää luultavasti ikuisesti

arvoitukseksi. Historialliset tosiasiat hämärtyvät entisestään fiktiivisen kirjallisuuden käsittelyssä. Voitaneen kuitenkin todeta, että Bletchley Parkin tapahtumat ansaitsevat tunnuksen viime vuosisadan merkittävimpinä tietojenkäsittelytieteellisenä sankaritekona.

Lähteet

Har99 Harper, S.: *Capturing Enigma: How HMS Petard Seized the German Naval Codes.* Sutton Publishing (1999).

Kah83 Kahn, D.: *Kahn on Code.* MacMillan (1983).

Koz84 Kozaczuk, W.: *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two.* University Publications of America (1984).

KrD02 Kruh, L., Deavours, C.: *The Commercial Enigma: Beginnings of Machine Cryptography.* Cryptologia vol. XXVI (3), 2002.

Mom Momsen, B.: *Codebreaking and Secret Weapons in World War II.* Nautical Brass. `http://home.earthlink.net/~nbrass1/enigma.htm` (12.4.2004).

SalA Sale, T.: *WWII Codes and Ciphers: The Enigma Cipher Machine.* `http://www.codesandciphers.org.uk/enigma/` (24.2.2004).

SalB Sale, T.: *Alan Turing at Bletchley Park in World War II.* Julkaistu teoksessa *Alan Turing: Life and Legacy of a Great Thinker*, s. 441-462. Toim. Christof Teuscher. Springer Verlag (2003).

SalC Sale, T.: *The Breaking of Enigma by the Polish Mathematicians.* `http://www.codesandciphers.org.uk/virtualbp/poles/poles.htm` (12.4.2004).

SalD Sale, T.: *Alan Turing, the Enigma and the Bombe.* http://www.codesandciphers.org.uk/virtualbp/tbombe/tbombe.htm 12.4.2004.

SalE Sale, T.: *Gordon Welchman: Getting BP Organised.* http://www.codesandciphers.org.uk/virtualbp/gwelchman/gwelch.htm (12.4.2004).

SalF Sale, T.: *Information flow from German ciphers to Intelligence to Allied commanders.* http://www.codesandciphers.org.uk/virtualbp/infoflow/infoflown.htm (12.4.2004).

Tur40 Turing, A.M.: *A treatise on Enigma.* http://frode.home.cern.ch/frode/crypto/Turing/ (24.2.2004).

Wes Wesolkowski, S.: *The Invention of Enigma and How the Polish Broke It Before the Start of WWII.* University of Waterloo. http://www.ieee.org/organizations/history_center/cht_papers/wesolkowski.pdf (16.3.2004).

WikA Wikipedia: *The Caesar Cipher.* http://en.wikipedia.org/wiki/Caesar_cipher (24.2.2004).

WikB Wikipedia: *Enigma.* http://en.wikipedia.org/wiki/Enigma (24.2.2004).