hyväksymispäivä arvosana

arvostelija

Enigma - murtamaton

Jani Kirmanen

Helsinki 20.5.2003

Seminaari

HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

Sisältö

1 Johdanto

Salakirjoitustaito on lähes yhtä vanha kuin kirjoitustaito itse. Varsinkin sotilaskäytössä tarve tiedon tehokkaalle salaamiselle on ollut suuri jo muinaisista ajoista lähtien. Tyypillisessä salakirjoituksessa yksittäiset kirjaimet korvataan toisilla koodiavaimen perusteella. Ilman koodiavainta koodin murtaminen on mahdollista vain kokeilemalla; pahimmillaan on kokeiltava kaikki mahdolliset vaihtoehdot, ja siihen kuluva aika voi helposti ylittää saatavilla olevan (esimerkiksi vihollisen tullessa linjojen läpi). Ensimmäisen maailmansodan aikana radiota käytettiin joukkojen väliseen kommunikaatioon. Radioliikenteen kaappaamisen helppouden takia riittävälle salaukselle syntyi jälleen tarve. Saksalaiset ottivat Enigmaksi kutsutun salakirjoituskoneen käyttöön ensimmäisen maailmansodan päätyttyä, ja sitä pidettiin pitkään murtamattomana. Enigman rakenteelliset heikkoudet sekä saksalaisten vankkumaton usko sen murtamattomuuteen synnyttivät yhdessä sen tuhon kipinän. Tässä esitelmässä käsitellään Enigman käyttöä, sen toimintaperiaatetta sekä miten sen murtamiseen käytetty tutkimustyö mahdollisti mekaanisen laskennan kehittymisen lopulta tietokoneeseen asti.

2 Enigman lyhyt historia

Enigman kehitystyön aloitti saksalainen Alfred Scherbius vuonna 1918. Ensimmäinen versio laitteesta oli valmis jo ensimmäisen maailmansodan loppumetreillä, ja sitä tarjottiin Saksan laivaston käyttöön. Laivasto ei kuitenkaan ollut kiinnostunut koneesta ja Scherbius jatkoi koneen jatkokehitystä. Ensimmäisen maailmansodan jälkeen Enigmaa tarjottiin yrityskäyttöön korvaamaan käytössä olleet kömpelöt ja hitaat koodikirjat. Helmikuussa 1926 Saksan laivasto otti käyttöön muunnellun version kaupallisesta Enigmasta. Samoin teki Saksan armeija heinäkuussa 1928. Armeijan ja laivaston käyttöönottamat Enigmat poikkesivat kuitenkin kaupallisesta versiosta niin paljon, ettei kaupallisella versiolla voinut lukea sotilaskäyttöön tarkoitettuja koodeja. Ennen toisen maailmansodan syttymistä Enigmaa paranneltiin ja sen tuottaman koodin kompleksisuus kasvoi. Toisen maailmansodan aikana Enigman kehitys jatkui

ja japanilaiset kehittivät sen pohjalta oman koodauslaitteensa, Purplen. Maailmansodan lähetessä loppuaan liittoutuneet olivat oppineet murtaman Enigman koodin, mitä voidaan pitää vähintäänkin osasyynä Saksan tappioon.

3 Enigman rakenne ja toiminta

Kuva 1: Nelipyöräinen Abwehr-Enigma. [Ham00]

Enigma oli puulaatikkoon sijoitettu salakirjoituskone, jossa oli näppäimistö, pistoketaulu, näppäimiä vastaavat lamput, sekä irrotettavat 26-rattaiset pyörät (kuva 1).

Koko elinkaarensa aikana sen ulkoasu ei muuttunut merkittävästi, sisäinen rakenne sen sijaan paljonkin.

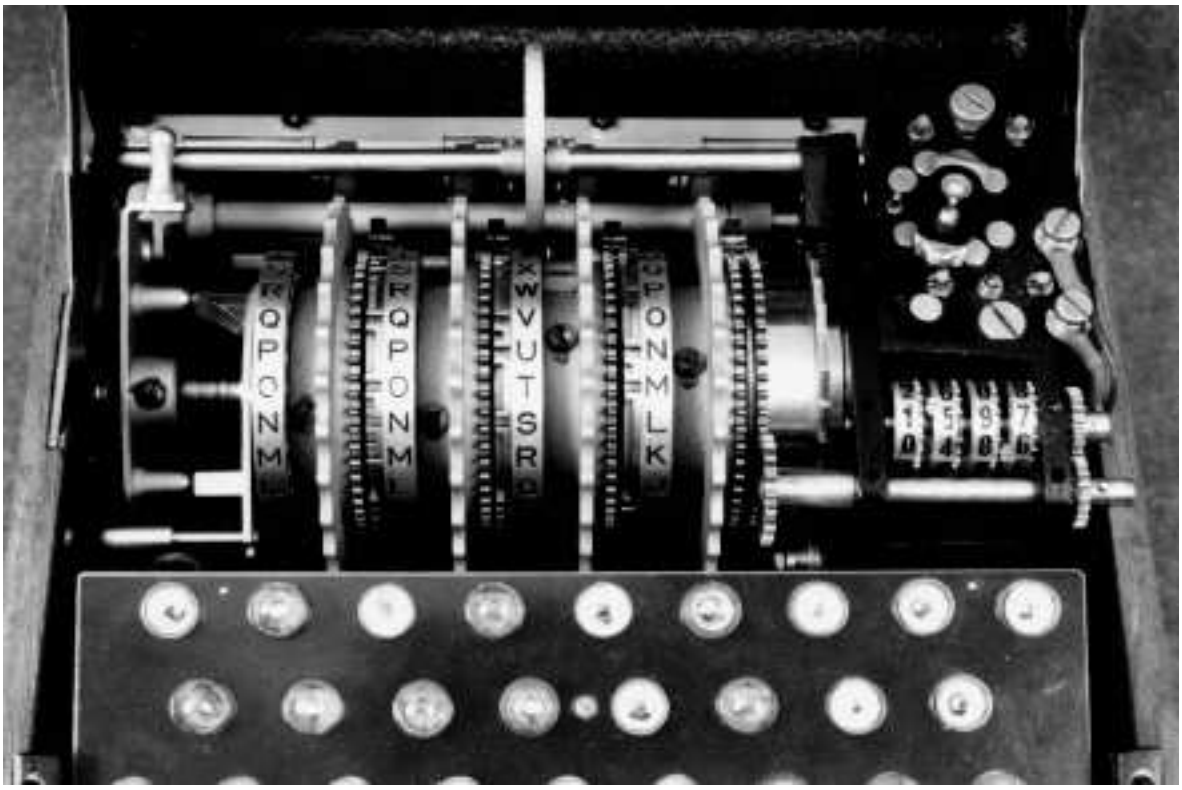
3.1 Näppäimistö ja lamput

Kuva 2: Enigman näppäimistö ja lamput.

Enigma muistutti lähinnä saksalaista kirjoituskonetta. Näppäimistön yläpuolella oli näppäinten järjestyksessä kirjaimilla merkittyjä lamppuja (kuva 2). Kun näppäintä painettiin, syttyi johonkin lamppuun valo. Jos näppäimistöltä syötettiin selväkielistä tekstiä, lampuissa luki sama teksti koodattuna ja päin vastoin. Mikä lamppu kulloinkin syttyi riippui koneen sen hetkisestä tilasta eli pyörien asennoista ja pistokekytkennöistä.

3.2 Pyörät

Enigma sisälsi versiosta riippuen kahdesta neljään 26-rattaista pyörää, jotka oli merkitty roomalaisin numeroin (kuva 3). Pyörät voitiin asettaa koneeseen missä hyvänsä



Kuva 3: Enigman neljä pyörää.[Ham00]

järjestyksessä (esim. III I II). Myöhemmin koneen mukana tuli kolmesta kahdeksaan pyörään, joista siis voitiin valita kulloinkin käytettävät (koneeseen kuitenkin käytti vain kolmea tai neljää pyörää kerrallaan). Pyörät oli koottu siten, että niiden rattaiden lukumäärä vastasi näppäimistön 26 kirjainta ja ne sisälsivät "satunnaisia" kytkentöjä [Sal02].

Jokaisella näppäimistö painalluksella ensimmäinen pyörä kääntyi 1/26 kierrosta ja käännyttyään kokonaisen kierroksen toinen pyörä kääntyi 1/26 kierrosta. Toisen pyörän käännyttyä kokonaisen kierroksen — tai alkuasennosta riippuen tullessaan käännöskohtaan — kolmas pyörä kääntyi jne. Luonnollisesti kaikki kolme pyörää saattoivat kääntyä yhtä aikaa. Pyörien käännöksien riippuminen toisistaan vastaa auton matkamittarin toimintaa.

Enigman tuottama koodi perustui pyörien yhteistoimintaan. Kun operaattori painoi

jotain näppäintä, kulki sähkövirta näppäimestä ensin pistoketauluun ja sieltä ensimmäiseen pyörään. Ensimmäisessä pyörässä sähkövirta "valitsi" jonkin 26 kirjaimesta ja kulki toiseen pyörään. Sama tapahtui toisessa ja kolmannessa pyörässä, jonka jälkeen sähkövirta kulki koodatun kirjaimen osoittavaan lamppuun, joka syttyi. Koska ensimmäinen pyörä kääntyi jokaisella näppäimen painalluksella, samaa kirjainta painettaessa saatiin joka kerta eri koodi, eikä kirjain voinut ikinä koodautua itsekseen.

Kolme 26-rattaista pyörää voi olla $26 * 26 * 26$ eri tilassa, jolloin sen tuottaman koodin selvittäminen kokeilemalla maksimissaan vaatii 17576 yritystä. Kun kolme pyörää voi olla koneessa missä hyvänsä järjestyksessä, se lisää koneen tilojen määrän kuusinkertaiseksi, 105456:een.

Enigman viimeisessä versiossa nk. Abwehr-Enigmassa oli neljä pyörää. Neljäs pyörä ei kääntynyt muiden pyörien tapaan, vaan sen kääntäminen oli operaattorin tehtävä. Neljäs pyörä lisäsi koodin kompleksisuutta, mutta sen ollessa nolla-asennossa kone toimi täsmälleen kuin kolmepyöräinen Enigma.

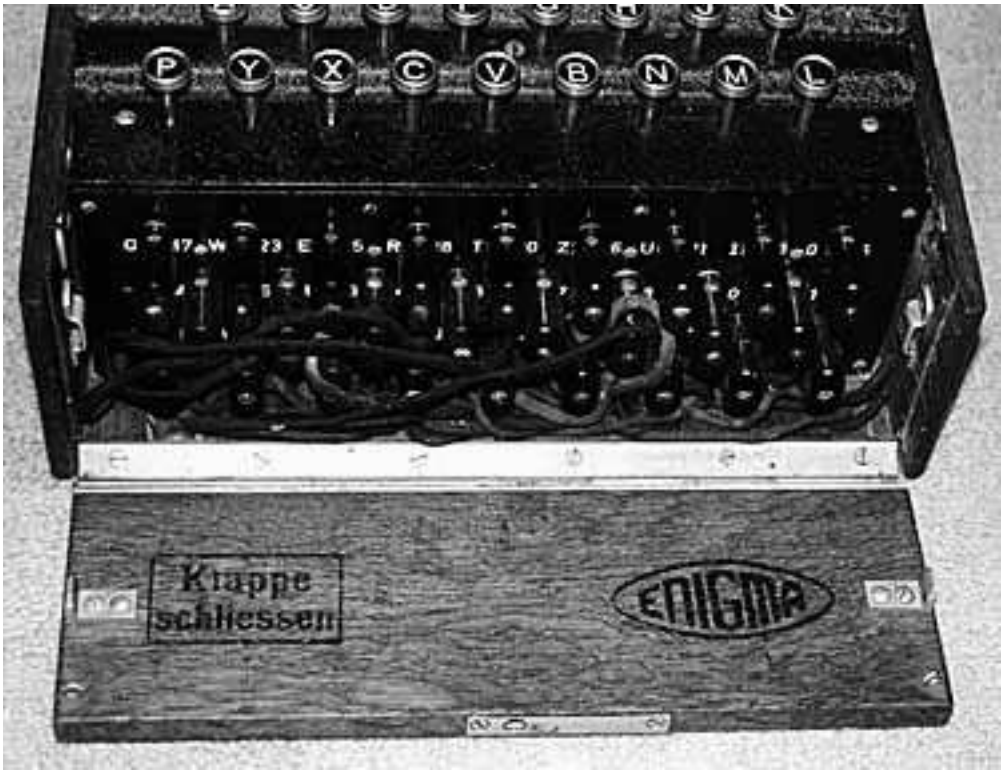
3.3 Heijastinpyörä

Kuva 4: Enigman heijastuspyörä.[Ham00]

Enigmaan lisättiin kolmannen pyörän vasemmalle puolelle erityinen heijastinpyörä, joka ei liikkunut, mutta joka sisälsi kytkentöjä (kuva 4). Heijastinpyörän tarkoitus oli kääntää siihen tulevan sähkövirran suuntaa siten, että se kulki kolmen pyörän läpi eri suuntaan ja lopulta pistoketaulun kautta lamppuihin. Heijastinpyörä aiheutti koneeseen sellaisen ominaisuuden, että sillä voitiin viesti voitiin dekoodata suoraan

näppäilemällä se. Tällöin lamppuihin syttyi selkokielisen viestin kirjaimet. Näin ollen, jos esim. A-kirjain koodautui X:ksi, X koodautui samoilla asetuksilla A-kirjaimeksi.

3.4 Pistoketaulu



Kuva 5: Enigman pistoketaulu.[Per02]

Monimutkaistaakseen koodia saksalaiset lisäsivät Enigman etupaneeliin pistoketaulun, jossa oli 26 pistoketta. Pistokkeet oli merkitty vastaavilla kirjaimilla, ja sen avulla voitiin vaihtaa kahden kirjaimen paikkaa. Esimerkiksi jos johto oli kytketty pistokkeisiin 'E' ja 'L', ja operaattori painoi E-kirjainta, sähkövirta kulkikin johtoa pitkin L-kirjaimeen ja pyörät koodasivat L-kirjainta. Johtojen avulla voitiin vaihtaa kuudesta kymmeneen kirjainparia. Kymmenen kirjainparia voidaan valita 26:sta 150738274937250 eri tavalla, jolloin aiemmin mainittu määrä koneen 105456 eri tilasta kasvoi noin 15 miljoonaan miljoonaan miljoonaan tilaan. Jopa modernilta tietokoneelta kestäisi kuukausia selvittää oikea konfiguraatio pelkästään kokeilemalla.

3.5 Koodiavaimet ja Enigman käyttö

Armeijan esikunta tuotti tarvittavat koodiavaimet, jotka sisälsivät pyörien järjestyksen, niiden alkuasennot sekä pistokkeiden kytkennät. [Sal02] Aluksi koodiavaimia eli koneiden konfiguraatioita vaihdettiin kerran kuukaudessa, mutta sota-aikana konfiguraatiot vaihdettiin päivittäin. Saksan laivasto, maa- ja ilmavoimat käyttivät kaikki eri konfiguraatioita, jolloin laivaston asetuksilla ei voinut lukea ilmavoimille tarkoitettuja viestejä.

Esimerkki Enigman käytöstä[Dea90]: Koneen käyttäjä katsoo ensin kyseisen päivän koodiavaimen eli koneen asetukset.
Pyörien järjestys: II, I, III
Pyörin alkuasennot: ZWD
Pistokekytkennät: EZ, BL, XP, WR, IU, VM, JO

Kun kone on konfiguroitu, operaattori valitsee kolme satunnaista kirjainta FRX ja asettaa pyörät siihen asentoon. Operaattori valitsee jälleen kolme satunnaista kirjainta AGI ja kirjoittaa ne koneella kahdesti — lamput HCA LNU syttyvät. Sen jälkeen pyörät laitetaan AGI-asentoon ja loput tekstistä voidaan kirjoittaa. Operaattorin pari kirjoittaa lamppuihin syttyvän tekstin ylös ja antaa sen radistille morsetettavaksi. Viestin alkuun, joka lähetetään selkokielisenä ,tulevat vastaanottajan nimi, päivämäärä, kellonaika koodatun tekstin pituus sekä viestiavain FRX FRX.

Vastaanottaja purkaa koodin asettamalla pyörät FRX-asentoon, näppäilemällä kuusi ensimmäistä kirjainta (HCA LNU), jolloin lamput AGI AGI syttyvät. Sen jälkeen pyörät asetetaan AGI-asentoon, jonka jälkeen koodattua viestiä näppäiltäessä selkokielinen teksti ilmaantuu lamppuihin, joista pari kirjoittaa sen ylös.

Ennen viestin koodausta ja purkamista Enigma aina konfiguroidaan uudelleen. Näin varmistetaan että sekä vastaanottajan että lähettäjän koneet toimivat identtisesti.

4 Enigman koodin murtaminen

Kun Enigma valmistui sitä pidettiin täysin murtamattomana. Kone saattoi olla koodia tuottaessaan missä hyvänsä sen 150000000000000000 eri tilasta, ja vaikka vihollinen olisikin saanut Enigman käsiinsä, ilman koodiavainta ei koodia voitu murtaa.

4.1 Puola 1928-1939

Puolalaiset aloittivat Enigman koodin murtamistyön jo vuonna 1928, kun Saksan armeija otti sen käyttöön. Puolalaisilla oli hallussaan Enigman kaupallinen versio, mutta sillä ei voinut murtaa laivaston koodeja. Mitään edistystä ei kuitenkaan tapahtunut ennen vuotta 1932, jolloin Puolan tiedustelupalvelu palkkasi kolme Poznanin yliopistosta valmistunutta nuorta matemaatikkoa, Marian Rejewskin, Jerzy Rózyckin ja Henryk Zygalskin. Enigman murtaminen aloitettiin hyödyntämällä matematiikkaa, tilastotiedettä ja hyviä arvauksia. Saksan laivaston viestejä salakuunneltiin ja tallennettiin myöhempää käyttöä varten [Koz03].

4.1.1 Matemaattinen malli

Puolalaisilla oli myös hyvää onnea: Saksalainen Hans Thilo-Schmidt tuhosi työkseen käytöstä poistettuja Enigman koodiavaimia. Hän arveli saavansa ne myytyä ranskalaisille hyvään hintaan. Ranskalaisilla, sen enempää kuin englantilaisillakaan, ei ollut käyttöä koodiavaimilla, joten ne päätyivät pari mutkan kautta Puolaan. Vanhojen avaimien avulla puolalaiset pystyivät lukemaan vanhoja viestejä. Thilo-Schmidt jatkoi koodiavainten hankkimista puolalaisille ja lopulta Enigmasta onnistuttiin muodostamaan matemaattinen malli. Malli oli yhtälö, jossa oli neljä muuttujaa: selkokielinen teksti, koodattu teksti, koodiavain ja pyörien kytkennät. Koska puolalaisilla oli kolme ensimmäistä, saatiin pyörien kytkennät vihdoin selvitettyä. Tämän tiedon avulla puolalaiset pystyivät rakentamaan oman Enigmansa [Mom02].

4.1.2 Syklometri

Toisen maailmansodan häämöttäessä viekä kaukana horisontissa saksalaiset ottivat käyttöön viestiavaimet. Vaikka puolalaisilla olikin oma Enigmansa, ilman viestiavainta purkaminen vaati koneen kaikkien tilojen läpikäymistä. Saksalaiset kuitenkin aloittivat lähes kaikki viestit prepositiolla 'an' (allatiivi), jota seurasi välilyönti 'x', koodin purkaminen aloitettiin rinnastamalla koodatun viestin kolme ensimmäistä kirjainta kirjaimiksi 'anx'. Koska 17576 eri tilan kokeileminen käsin veisi ikuisuuden, puolalaiset kehittivät koneen — syklometrin — tekemään kortiston, josta koneen asetukset löytyisivät koodiavaimen perusteella [Mom02]. Kortiston tekeminen kesti vuoden, mutta sen jälkeen kaapatun viestin purkamiseen tarvittavat asetukset löytyivät parissakymmenessä minuutissa. Lokakuussa 1937 Enigman kytkentöihin tehtiin merkittäviä muutoksia, ja kortisto oli hyödytön. Seuraava kortisto valmistui syyskuuhun 1938 mennessä; samaan aikaan saksalaiset muuttivat viestiavainkäytäntöään, ja kortisto oli hyödytön.

4.1.3 Bomba

Puolalaiset eivät lannistuneet vastoinkäymisistä huolimatta vaan kehittivät uuden tavan hyödyntää saksalaisten tapaa aloittaa viestit tietyllä tavalla. Uusi tapa oli kone nimeltä Bomba, jonka periaatteessa emuloi Enigmaa. Bomballe syötettiin viestin osa, jonka oletettiin tarkoittavan selkokielellä 'anx'. Sen jälkeen kone kokeili järjestyksessä kaikki pyörien asennot, kunnes oikea kombinaatio löytyi. Koska Enigman kolme pyörää saattoivat olla 3! eri asennossa, oli Bomba itseasiassa kuusi konetta[Sal02]. Kone tikitti kuin aikapommi ollessaan käynnissä, mikä lienee sen nimen alkuperä [Mom02]. Bomba valmistui kuitenkin liian myöhään ollakseen enää avuksi puolalaisille: Joulukuussa 1938 saksalaiset ottivat käyttöön pyörät IV ja V, jolloin pyörien asentojen lukumääräksi tuli 3! sijaan 5!/2!. Puolalaisilla ei ollut varaa eikä aikaa rakentaa uutta Bombaa, koska sota näytti olevan syttymässä. Puolalaiset onnistuivat kuitenkin ottamaan yhteyttä englantilaisiin virkaveljiinsä, ja salaisessa tapaamisessa heinäkuussa 1939 kaikki tieto Enigmasta ja sen murtamisesta välitettiin liittoutuneille. Syyskuun

ensimmäisenä päivänä vuonna 1939 Saksa valtasi Puolan ja Enigman murtaminen jäi liittoutuneitten harteille.

4.2 Britannia 1940-1944

Matemaatikko Alan Turingia pidettiin lupaavana koodinmurtajana ja hän vieraili useasti Lontoon Goverment Codes & Cipher Schoolissa kuulemassa mitä alalla oltiin siihen mennessä opittu. Turingin lähtökohta Enigman murtamiseen oli myös puolalaisten käyttämä menetelmä hyödyntää tunnettua selkokielistä tekstinpätkää (esim. 'anx'), jota Bletchley Parkissa kutsuttiin 'luntiksi' [Sal02].

Turing oivalsi, että jos radioliikenneanalyysia voitaisiin käyttää ennustamaan joitain tekstin osia, nopeasti toimiva kone voisi kokeilla onko olemassa sellaista pyörien asentoa, jolla koodista todella löytyy tämä päätelty tekstin osa. Turing myös osoitti matemaattisesti, että kyseisellä tekniikalla löydetään asetukset tehokkaammin kuin vain kokeilemalla [Sal02].

Bletchley Parkissa Alan Turing kehitti Bombaa toimimaan yleisemmin ja sen avulla liittoutuneet onnistuivat myöhemmin murtamaan Enigman koodit versiosta riippumatta. Vuonna 1944 liittoutuneilla oli käytössä Colossus-tietokoneet, joilla pystyttiin purkamaan myös Enigman rinnalle käyttöön otettu nk. Lorentzin koodi, joka perustui binäärilukuihin ja niille tehtäviin logiisiin operaatioihin [Pli98]. Purettavat viestit syötettiin Colossukselle monta metriä pitkinä paperinauhoina, joita käsiteltiin 5000 merkkiä minuutissa.

Sekä puolalaisia että liittoutuneita auttoivat eniten — tahattomasti kylläkin —- Enigman käyttäjät [Pli98]. Huolimattomasti valitut tai usein toistuvat viestiavaimet auttoivat löytämään asetukset nopeasti, samoin kuin tismalleen saman viestin lähettäminen eri koodeilla.

Enigman rakennekin sisälsi ongelmia. Heijastinpyörän takia kirjain ei ikinä voinut esiintyä samalla paikalla sekä selkokielisessä että koodatussa viestissä. Lisäksi kaikkien kolmen pyörän yhtäaikainen kääntyminen helpotti suuresti koodin murtamista

[Nic96].

5 Yhteenveto

Ilmestyessään Enigman uskottiin ratkaisseen kaikki salaamiseen liittyvät ongelmat kertaheitolla. Koneen toimintaperiaate oli yksinkertaisen nerokas ja sen tuottaman koodin murtaminen kokeilemalla oli käytännössä mahdotonta ilman mekaanisen laskennan apua. Pelkkä laskentateho ei kuitenkaan riittänyt koodin murtamiseen, vaan apuna tarvittiin oivallusta, henkistä nujerrusta koneen käyttäjästä. Enigma onnistuttiin murtamaan ensimmäisen kerran jo 1930-luvulla. Tuolloin asialla olivat puolalaiset matemaatikot, jotka olivat muodostaneet koneesta matemaattisen mallin, ja jotka osasivat hyödyntää saksalaisten operaattorien huolimattomuusvirheitä sekä koneen käyttötavan heikkouksia. Huomattuaan tämän saksalaiset jatkoivat Enigman kehittämistä ja lisäsivät siihen osia, jotka entuudestaan lisäsivät sen koodin kompleksisuutta. Saksalaiset kuitenkin luottivat liikaa laskennallisen koodinmurtamisen mahdottomuuteen ja niinpä kohtalokaat virheet olivatkin — kuten aina — ihmisten tekemiä.

Puolalaiset valoivat perustan Enigman murtamiselle mekaanisen laskennan keinoin ja brittiläiset jatkoivat työtä. Toisen maailmansodan yksi suurimmista salaisuuksista oli brittien Enigman murtamiseen käyttämät tietokoneet. Varmuudella ei voida sanoa johtuiko Saksan tappio nimenomaan Enigman koodin murtamisesta, vai nopeuttiko se vain väistämätöntä tuhoa. Se kuitenkin on varmaa, että modernin tietokoneen synty olisi viivästynyt, ellei Enigman kaltaista laitetta olisi tarvinnut murtaa mekaanisen laskennan keinoin.

Lähteet

Dea90 Deavours, C.A., Kruh L.:"The Turing Bombe: Was it Enough?", Cryptologia, XIV, No. 4, s. 342, 1990

Ham00 Hamer, D.:"G-312: An Abwehr Enigma", Cryptologia, XXIV, No.1, s. 41–54, 2000

Koz03 Kozaczuk, W.:The Origins of the Enigma, http://home.us.net/∼encore/Enigma/text.html (20.5.2003), 2003

Mom02 Momsen, B.:Codebreaking and secret weapons in world war II, Nautical Brass, http://home.earthlink.net/∼nbrass1/enigma.htm (17.1.2003), 2002

Nic96 Nichols R.:Classical Cryptography Course, Volume I, Aegean Park Press, 1996

Per02 Perera T.: W1TP Telegraph and scientific instrument museums http://w1tp.com (17.1.2003), 2002

Pli98 Plimmer, B.:Machines invented for WW II code breaking, ACM SIGCSE Bulletinm, Volume 30, Issue 4 (December 1998), s.37–40, 1998

Sal02 Sale, T.:The Enigma cipher machine, http://www.codesandciphers.co.uk/enigma/ (17.1.2003), 2002