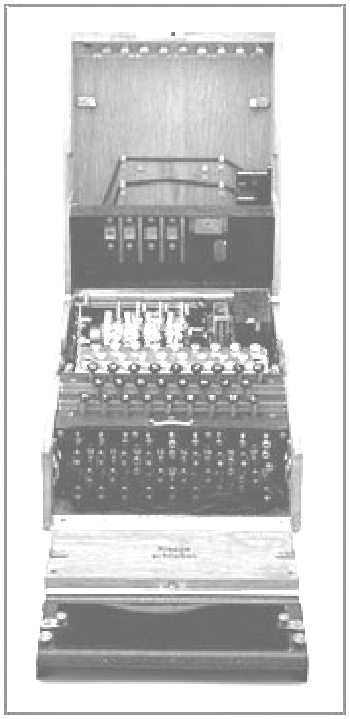
Teksti: SJA Sihvola



Toiminta

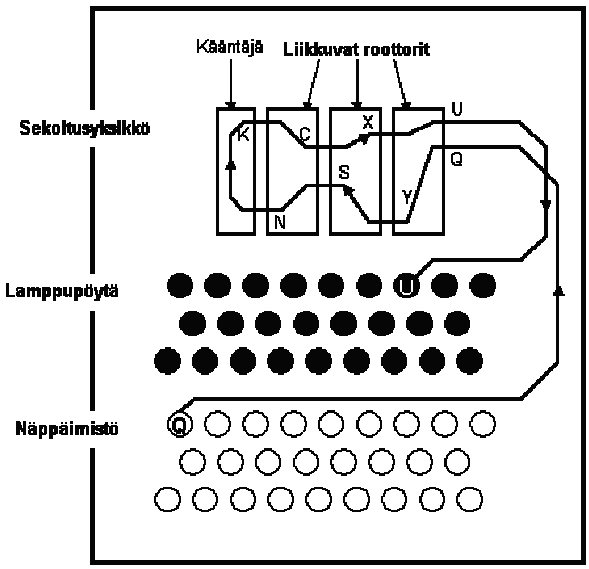
Enigma-laite sai alkunsa vuonna 1918 *Arthur Scherbiuksen* patentoimana kaupallisena tuotteena. Laite oli helppokäyttöinen: Näppäintä painettaessa syttyi valotauluun kirjaimen salakielinen vastine. Käyttäjä vain kirjoitti selväkielisen viestinsä ja merkitsi joka kirjaimen salakielisen vastineen ylös..

Jokainen näppäinpainallus avaa yhden 26:sta mahdollisesta ”kirjainpiiristä”. Virta kulkeutuu roottoreiden läpi, joista jokainen muuttaa kirjaimen toiseksi. Näin kirjaimen salaus on suoritettu. Koneen kytkentä muuttuu joka kirjaimen jälkeen, ensimmäisen roottorin pyörähtäessä 1/26 kierrosta (toinen pyörähtää aina joka 26:nen kirjaimen jälkeen jne.), joten samalle selväkieliselle kirjaimelle ei tule usein samaa salakielistä vastinetta.

Tärkeä ominaisuus Enigman suunnittelussa oli sen helppo käyttö.

Enigma saksalaisten käytössä

Kaupallinen Enigma ilmestyi markkinoille vuonna 1923, ja Saksan armeija kiinnostui laiteesta nopeasti - vaikka *Scherbius* oli tarjonnut samaa laitetta heille jo vuonna 1918 huonoin tuloksin. Tästä oli tuloksena laiteen vetäminen markkinoilta ja sen valmistuksen ja kehityksen jatkuminen sotilaallisiin tarkoituksiin.



Tärkein kehitys kaupalliseen versioon nähden oli liitinpöydän (*Stecker*) lisääminen. Tämä sisälsi 26 liitintä, joiden avulla oli mahdollista ristikytkeä kirjainpareja keskenään näppäimistön ja roottorien välissä, täten monimutkaistaen salausta. Jos esimerkiksi ”A” ristikytkettiin ”Z”:n kanssa, myös ”Z” vaihtui ”A”:han. Yleensä liitinpöydän avulla vaihdet-

tiin kuusi kirjainparia. Tämä säilytti laitteen helppokäyttöisyyden sekä myös laitteen suurimman heikkouden: mikään kirjain ei voinut koodatussa viestissä merkitä itseään. Uuden menetelmän käyttöönotto nosti erilaisten vaihtoehtojen määrän 10 kvadriljoonaan (10^{15}). Nyt saksalaiset olivat varmoja, että heidän salaustaan oli mahdotonta purkaa.

Toisen maailmasodan syttyessä Enigma oli levinnyt Saksan armeijan jokaiseen aselajiin, etulinjan joukoista yliesikuntaan. Laitetta oli käytössä arviolta 40 000 kpl. Se oli pieni, helposti kuljetettavissa ja helppokäytöinen. Tämä teki siitä täydellisen työkalun salamasotaan, jossa esim. panssarien ja ilmavoimien välinen kommunikaatio oli oltava nopeaa ja varmaa.

Eräs olennainen sähköinen taistelukenttä, jossa Enigma näytteli keskeistä osaa, oli taistelu Atlantilla. Saksalaisilla U-veneillä oli Enigma-laitteet, joiden avulla he lähettivät tilannetiedostukset ja saattuehavainnot esikuntaan. Saattueiden tarkat sijainnit olivat tärkeitä susilaumataktiikassa, jotta paljon U-veneitä voitiin keskittää juuri oikeaan paikkaan oikeaan aikaan, ja näin moninkertaistaa upotusmäärät. Samoin Liittoutuneille oli tärkeää saada tietää U-veneiden sijainnit, jotta saattueiden reitit pystyttäisiin muuttamaan tarpeeksi ajoissa. Kriegsmarinen Enigman sanomien purkaminen oli tärkeää varsinkin Englannille, jonka olemassaolo riippui saattueiden perilletulosta.

Saksalaiset käyttivät eri taajuuksia ja avaimia eri yksiköille. Tästä oli se etu, että esimerkiksi Luftwaffen radisti huomasi heti, jos viesti ei ollut tarkoitettu ilmavoimille, ja hänen ei tarvinnut suotta alkaa purkamaan sitä. Menetelmä takasi myös sen, että huippusalaiset viestit eivät olleet asiattomien luettavissa.

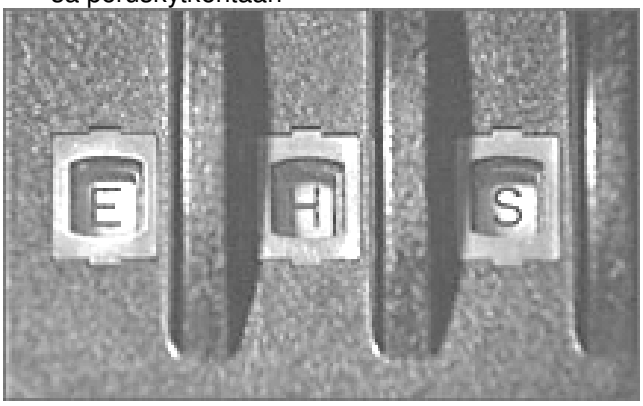
Enigman käyttö

Saksalaiset pitivät Enigman salausta mahdottomana purkaa. Tässä he olivat väärässä. Laite itsessään sekä sen käyttötapa sisälsivät heikkoja kohtia, jotka Saksan vastustajat huomasivat ja näin pääsivät tulkitsemaan saksalaisten viestiliikennettä. Ensimmäinen virhe salauksessa on luulo, että viestejä on mahdotonta purkaa.

Jokainen minkään arvoinen salausväline on suunniteltu siten, että vaikka vihollinen on täysin selvillä menetelmän toiminnasta ja rakentaa salauslaitteen kaksoiskappaleita, ei se saa viestejä puretuksi. Enigman tehokkuus perustui siihen, että se pystyttiin asettamaan valtamaan määrään erilaisia asetuksia (tiloja):

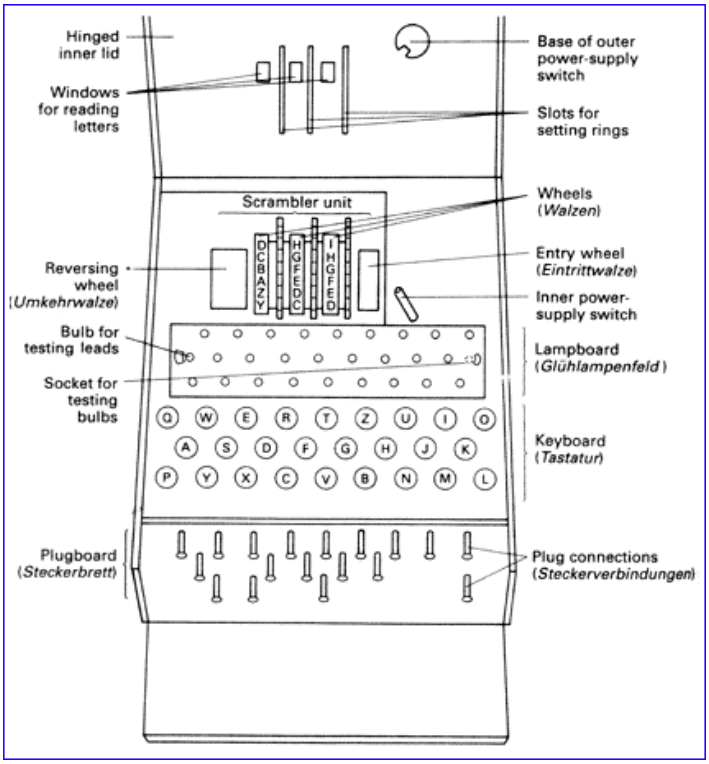
- Kolme roottoria voitiin asettaa mihin järjestykseen tahansa
- Jokaisella roottorilla on 26 eri aloitusasentoa

- Roottorien kirjainrenkaita voitiin siirtää suhteessa peruskytkentään



- Liitinpöydän kytkentöjä voitiin muuttaa

Viestit pyrittiin myös pitämään mahdollisimman lyhyinä, koska mitä pitempi viesti oli, sitä helpompi se olisi purkaa. Jos lähetettävänä oli liian pitkä viesti, se lähetettiin monessa osassa.



Pääosa laitteen asetuksista pääteltiin koodikirjasta, jossa oli joka päivälle omat säätönsä. Kuitenkin oli eräs tekijä, jonka oli määrä olla erilainen joka viestissä – nimittäin kirjaimet, jotka ilmaisivat lähettäjän roottorien asennon viestin alussa. Lähettäjä valitsi kolme kirjainta umpimähkään ja sen jälkeen asetti laitteen päivän perusasetuksille. Seuraavaksi hän lähetti tämän kolmen kirjaimen sarjan kahdesti. Toisto oli tarkoitettu vähentämään viestiyhteyksistä aiheutuvia virheitä, mutta se olikin päävoitto koodinpurkajille, jotka pystyivät päättelemään Enigman perusasetukset ja täten purkamaan koko päivän liikenteen. Radistien heikosta koulutuksesta johtuen myös kirjainvalinnat olivat usein huonoja.

Laivasto oli paremmin järjestänyt asian: vain upseereilla oli oikeus koodata Enigmalla. Viestin alkukirjaimet olivat määrättyjä ja tarkoin valittuja, jotta koodattu viesti olisi mahdollisimman vaikea purkaa. Koodilistat oli painettu veteen liukenevalla musteella ja ne pidettiin lukkojen takana kaiken aikaa. Kriegsmarinen turvatoimet kannattivat: laivaston koodi pysyi purkamattomana vielä kaksi vuotta sen jälkeen, kun muiden aselajien viestejä pystyttiin avaamaan.

Oman koodauksenkaan etevyys ei aina auta: tammikuussa 1941 Luftwaffen kenraali *Jeschonnekilla* oli sukulainen palvelemassa taistelulaiva *Bismarckilla* ja hän lähetti tiedustelun aluksen olinpaikasta. Laivaston koodilla kirjoitettu viesti muutettiin maissa Luftwaffen koodiksi, jota englantilaiset pystyivät lukemaan. Näin englantilaiset, joilta taistelulaiva oli kadonnut, saivat selville sen sijainnin, ja *HMS Ark Royalilta* lähetettiin lentokoneita pommittamaan laivaa. Tämä johti myöhemmin taistelulaivan upotukseen.

Sanomien purku ennen sotaa

Ensimmäiset viestien purkajat olivat puolalaisia. He huomasivat vuonna 1926, että Kriegsmarinen viestit muuttuivat mahdottomiksi purkaa. Sama tapahtui vuonna 1928 Reichswehrin viesteille - saksalaiset olivat ottaneet käyttöön hieman muunnellun version kaupallisesta Enigmasta. Puolalaiset kokeilivat purkaa koodia ostamalla kaupallisen Enigman, mutta tästä ei ollut heille mitään hyötyä. Puolan salakirjoitusyksikön Saksan osasto, *BS4* (*Biuro Szyffrow, osasto 4*), sai varsinaisen onnenpotkun vuonna 1928, kun saksalaiset lähettivät yhden Enigma-laitteen Varsovan lähetystöönsä tavallisen postin kautta. Huomatessaan virheensä, saksalaiset alkoivat kysellä pakettinsa perään, joka hälytti Puolan tulliviranomaiset. Tästä oli tuloksena, että puolalaisilla oli viikonloppu aikaa tutkia laitetta, kunnes he toimittivat sen maanantaina perille.

Kesäkuussa 1930 saksalaiset ottivat käyttöön M1 Enigman, joka oli jo merkittävästi erilainen kuin kaupallinen versio.

Hans Thilo-Schmidt, saksalainen aatelinen, oli joutunut kovien aikojen kolhimaksi. Hän suostutteli viestijoukoissa palvelevan veljensä hankkimaan hänelle töitä. Yksi Hansin tehtävistä oli tuhota vanhoja Enigman koodikirjoja puolustusministeriön salakirjoitusosastolla ja tällöin hän pääsi käsiksi tietoihin, jotka hän päätti myydä ranskalaisille. Hän toimitti marraskuussa 1931 Ranskan tiedustelupalvelulle *(Servic de Renseignement - S.R.F*) ohjekirjan Enigman asetusten muuttamisesta. Ranskalaiset tutkivat saamiaan tietoja ja olivat englantilaisten kanssa samaa mieltä, että saaduista tiedoista ei ollut mitään käytännön hyötyä, koska koodia on mahdoton purkaa. Tämän jälkeen ranskalaiset tarjosivat tietojaan puolalaisille, jotka olivat ikionnellisia edes tästä pienestä johtolangasta Enigman salaisuuksiin. *BS4:sen* tutkijaryhmä, johon kuuluivat mm. *M.Rejewski, J.Rozycki ja H.Zygalski*, esitti samalla pyynnön, että olisiko mahdollisista saada vanhoja Enigman koodeja. Ranskalaiset esittivät pyynnön edelleen *Schmidtille* (ammuttiin maanpetoksesta 1943), joka sitten toimitti vanhoja koodikirjoja Puolaan.

Puolalaisilla oli nyt hallussaan:

- Selväkielisiä viestejä
- Nämä koodattuna
- Avaimet, jonka avulla viestit oli koodattu

Ainoa, jota ei tiedetty oli roottorien kirjainpiirien kytkentä eli miten roottorien molemminpuolin sijaitsevat 26 johdinta oli kytketty toisiinsa (kuva). *Rejewski* kehitti neljän muuttujan kaavan, josta kolme muuttujaa oli tunnettua, oikeapuoleisen, nopeimmin pyörivän, roottorin kirjainpiirin kytkentöjen laskemiseen vuonna 1932.

Roottorien sijoituspaikkaa Enigmassa muutettiin säännöllisesti kolmen kuukauden välein. Aina uuden roottorin tullessa laitteessa ensimmäiseksi, sen kytkentä laskettiin ja viimein saatiin selville kaikkien roottorien kytkennät.

Puolalaiset olivat rakentaneet kaupallisesta Enigmasta version, jossa roottorien kytkentäpiirit olivat saksalaisten M1:ssä käyttämien kaltaisia. He laittoivat laitteen asetukset oikeiksi ja syöttivät koodatun viestin laitteeseen – tuloksena siansaksaa. *Rejewski* tarkisti laskelmansa moneen kertaan pääsemättä tuloksiin ja oli jo aikeissa lopettaa, kun hänen päähänsä pälkähti kokeilla erilaista näppäimistön ja sekoitusosan välistä johdotusta. Laite viritettiin, ja tuloksena oli selväkielinen teksti. Oli joulukuu 1932 ja puolalaisilla oli nyt toimiva Enigman kopio, jonka avulla Reichwehrin koodit saatiin puretuksi.

Vuoden 1934 puoliväliin mennessä oli rakennettu jo 15 täydellistä kopiota saksalaisten käyttämästä Enigmasta. Näitä rakennettiin kaikkiaan 70 kpl ennen sodan syttymistä.

Toimiva laite oli vasta puolet salaukseen purkuun tarvittavasta systeemistä. Tarvittiin myös ”luntteja” (*cribs*), jotka olivat pala selväkielistä tekstiä, jonka tiedettiin vastaavan koodatun viestin tiettyä kohtaa. Saksalaiset olivat näiden toimittamisessa hyvin avuliaita. Monet heidän viestinsä alkoivat kirjainyhdistelmällä *”anx”* (”an” -lle ja x oli sanaerotin). Saksalaiset radistit auttoivat myös valitsemalla viestien alussa olevat roottorien alkuasennon ilmoittavat kirjainsarjat, viestiavaimet, helpoiksi arvata, kuten *”AAA”, ”ZZZ”* jne.

Puolalaiset rakensivat myös kortiston, jonka avulla saatiin 20 minuutissa selville koodikirjan mukainen päivän perusasetus. Kortistossa oli kortti jokaiselle 105 456:lle roottorien alkuasentovaihtoehdolle. Kuitenkin marraskuussa 1937 saksalaiset muuttivat kääntäjäroottorin kytkentöjä – ja kortisto oli hyödytön.

Puolalaiset kasasivat uuden kortiston alle vuodessa, mutta syyskuussa 1938 saksalaiset muuttivat viestiavaimen muodostusta. Uusi menetelmä oli monimutkaisempi kuin vanha, mutta se sisälsi vieläkin tämän kolmen kirjaimen ryhmän kaksoislähetyksen. Puolalaiset murtautuivat tähän ilmaisumenetelmään etsimällä tilanteita, jolloin Enigma koodasi kaksi samaksi tunnettua kirjainta (toistosta) samalla tavalla. Eli tässä kuuden kirjaimen ryhmässä muodostivat parin kirjaimet 1,4 tai 2,5 tai 3,6. Tätä ilmiötä kutsuttiin avaimeksi ja se antoi koodinpurkajille tärkeää tietoa laitteen perusasetuksista.

Listaamalla avainten esiintymisiä eri asetuksilla ja tutkimalla monia viestejä samalta päivältä, Enigman perusasetus pystyttiin määrittelemään. Tämä menetelmä perustui rei’itettyihin *”Zygalskin lakanoihin”*, joita oli kymmenen sarjaa (jokaisessa 26 isoa paperiarkkia jokaiselle hitaimman roottorin asennoille) eli yksi jokaiselle roottorien sijaintipaikalle laitteessa. Näitä rei’itettyjä papereita aseteltiin valaisevalle alustalle päällekkäin, kunnes reiät sattuivat samoille kohdille, jolloin oli löydetty mahdollinen avain. Tätä sitten kokeiltiin Enigma-kopiolla. 10. toukokuuta 1940 saksalaiset luopuivat toistosta, ja roottorien asennon ilmaisevat kolme kirjainta lähetettiin vain kerran.

Puolalaiset kehittivät myös toisen menetelmän ilmaisusysteemin purkamiseksi. Tämä vaati myöskin avaimia, mutta paljon vähemmän kuin aikaisempi menetelmä. Käsityön asemesta, puolalaiset rakensivat vuonna 1938 sähkömekaanisen laitteen nimeltä *Bomba*, jossa oli samankaltaiset virtapiirit kuin Enigmassa, mutta se pystyi käymään läpi roottorien eri asennot löytääkseen huomatut avaimet. Koneita tarvittiin kuusi kappaletta eli yksi jokaista roottorien järjestysvaihtoehtoa varten. Koneen nimi on tullut todennäköisesti sen tikittävästä äänestä, josta muistuttaa aikapommia. *Bomban* avulla pystyttiin nyt avaamaan myös Luftwaffen viestit.

Puolalaiset olivat erityisen kiinnostuneita saksalaisten radioliikenteestä Venäjällä, jossa he harjoittelivat kiertääkseen Versaillesin rauhansopimuksen ehtoja. Puolalaiset eivät koskaan antaneet saamiaan tietojaan eteenpäin ranskalaisille, koska he pelkäsivät saksalaisten saavan selville koodiensa paljastumisen. Saksalaiset olisivat muuttaneet viestiensä salaamista ja puolalaisten aherrus olisi mennyt hukkaan. Ranskalaiset kuitenkin jatkoivat vanhojen koodikirjojen toimittamista puolalaisille, vaikka ihmettelivätkin mikseivät puolalaiset toimittaneet heille mitään tietoja. Puolalaisten aloittaessa viestien purkamisen saksalaiset käyttivät Enigmassa vain kolmea roottoria. Ja vaikka Puolaan toimitetut koodikirjat olivat vanhentuneita, saatiin viestit purettua, kuitenkin viiveellä.

Joulukuussa 1938 saksalaiset ottivat käyttöön kaksi uutta roottoria, joista Enigmassa käytettiin kolmea kerrallaan. Puolalaisilla ei ollut resursseja nyt tarvittavien 60 *Bomban* (350 000$ kpl) tai 60 Zygalskin lakanasarjan tekemiseen.

Puolalaisten jäävät työttömiksi

Resurssien puutteesta ja saatuaan selville puretuista viesteistä maansa tulevasta valloituksesta, puolalaiset tapasivat heinäkuussa 1939 Englannin ja Ranskan tiedustelupalvelujen edustajat ja tyrmistyttivät nämä tiedoillaan Saksan viestien salauksesta. Tämän tapaamisen seurauksena Englannin Salakirjoituskoulu *(GC&CS)* alkoi hyökkäyksensä Enigmaa vastaan. Englantilaisten suurempien resurssien ansiosta oli mahdollista valmistaa nuo 60 paperiarkkisarjaa, jotka toimitettiin Ranskaan paenneille puolalaisille koodinpurkajille.

Saksalaisten miehittäessä loput Ranskasta vuoden 1942 alussa, puolalaiset yrittivät paeta Englantiin. Vain osa heistä pääsi perille, suurimman osan jäädessä kiinni Pyreneillä yrittäessään Espanjaan.

Koska oli puolalaisten ansiota, että englantilaiset pystyivät lukemaan saksalaisten viestejä, on ihmeellistä, että heitä ei otettu mukaan yritettäessä purkaa Kriegsmarinen *Schlüssel-M* –salausta, joka saatiin purettua vasta kun roottorit nro. VI ja VII saatiin haltuun.

Koodinpurkamista Bletchley Parkissa

Kuuluisa matemaatikko ja ensimmäisen tietokoneen keksijä *Alan Turing* alkoi työskennellä parannellun *Bomban, Bomben* parissa. Englantilaisten *Bombe* oli kehittyneempi kuin edeltäjänsä: se toimi nopeammin ja se ei tarvinnut määrättyä perusasetusta. Ensimmäinen *Bombe* otettiin käyttöön toukokuussa 1940.

Brittien koodinpurkaus perustui koodatun viestin sisällön ja sen sisältämien sanojen ”arvaamiseen”, koska viestit alkoivat usein samoilla sanoilla. Tämän menetelmän käyttöä avusti se seikka, että koodatussa viestissä ei mikään kirjain koskaan merkinnyt itseään. Joten oli helppoa asettaa selväkieliset arvaukset ja koodattu viesti vierekkäin ja tarkistaa ettei mikään kirjain vastannut.

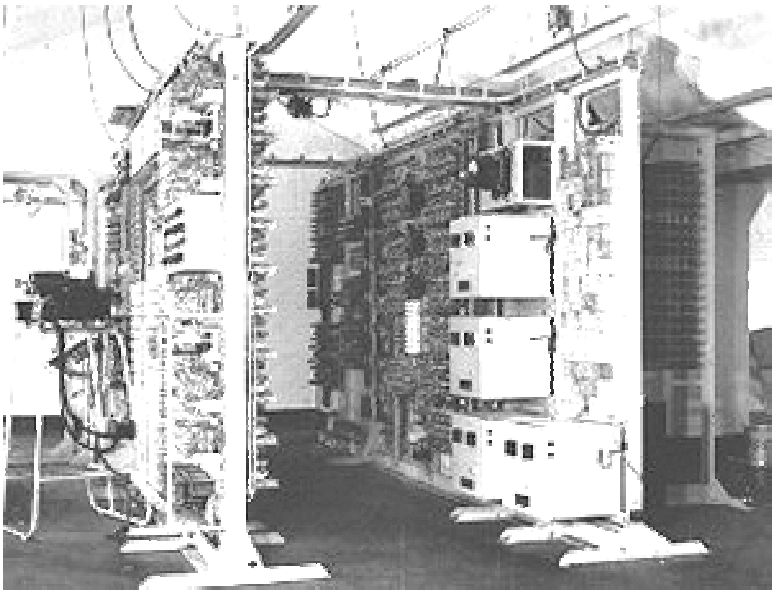
Kun oli löydetty viesti, josta oli voitu ”arvata” tarpeeksi paljon, saatiin selvyys mahdollisista Enigman asetuksista, jotka ohjelmoitiin *Bombeen. Bombe* kytkettiin päälle etsimään näistä asetuksista oikea.

Bomben avulla pystyttiin purkamaan mm. seuraavat salausavaimet: joulukuussa 1940 SS:n yleisavain *Orange I*, tammikuussa 1941 *Afrika Korpsin* operaatioavain, kesäkuussa 1941 Itärintaman avain *Vulture I*, joulukuussa 1941 *Abwehrin* avain.

Vuonna 1943 saatiin avuksi *Colossus*, maailman ensimmäinen ohjelmoitava digitaalinen tietokone, jota pidettiin niin salaisena, että sen piirustukset hävitettiin ja sen olemassaolo paljastettiin vasta vuonna 1976. Tietokone oli huoneen kokoinen, 5 m pitkä, 3 m leveä ja 2,5 m korkea. Se oli rakennettu pääasiassa postitoimistojen puhelin- ja lennätintarvikkeista. *Colossus* luki valosähköön perustuen lennätinnauhasta koodatun viestin 5 000 kirjaimen sekuntinopeudella. Tietokone tarkisti koodatulle viestille kaikki yhdistelmät ja tulosti nauhalle toteamansa Enigman asetukset.

Colossuksesta kehitettiin myös kehittyneempi malli, Mark 2. Näitä rakennettiin kymmenen kappaletta ja ne pystyivät avaamaan Enigman viestejä sekä monimutkaisempia salauksia, kuten saksalaisten 12-roottorisen salauslaitteen viestejä.

Yksi tekijä *Bletchley Parkin* menestyksen takana oli organisaation suuruus. Enigma-viestejä tuli valtava määrä, noin 3 000 kpl päivässä, ja yksi viesti oli vain pieni osa koodin purkamista. Selvitäkseen tästä englantilaiset jakoivat analysoijat ryhmiin eri viestityyppien mukaan. Näiden ryhmien tulokset ohjattiin seuraavalle ryhmälle, joka kokosi tiedoista suuren tietokannan, jonka avulla viestejä purettiin. Sodan



lopussa *Bletchley Parkissa* työskenteli 10 000 henkilöä vuoroissa ympäri vuorokauden.

Enigmaa ja sen salauksen purkamista pidettiin niin salaisena asiana, että vasta 70-luvun puolivälissä englantilaiset ja amerikkalaiset alkoivat julkistaa tietoja siitä, miten he pystyivät lukemaan saksalaisten viestiliikennettä sodan aikana. Ja kaikkia tietoja tiedustelusta ei ole julkistettu vieläkään. Osaltaan tätä salaisenapitämistä selittää myös se, että ainakin britit ”jakoivat” *Enigmoita* liittolaisilleen sodan jälkeen, kehuen sen salauksen laatua. Tietenkin he jättivät mainitsematta, että pystyivät itse purkamaan salauksen ja näin seuraamaan liittolaistensa viesti-

liikennettä. Britit ja amerikkalaiset käyttivät myös itse *Enigmaa* sodan aikana lähettäessään erittäin salaisia viestejä toisilleen.

Kriegsmarinen Enigmat

Vaikka englantilaiset pystyivät säännönmukaisesti lukemaan esim. Luftwaffen viestit, kaikkein tärkeimmät eli Kriegsmarinen viestit olivat mahdottomia purkaa. Enigmaa varten oli kahdeksan eri roottoria. Näistä kuitenkin kolmea, numeroita VI, VII ja VIII, käytti vain laivasto *M3 Enigmassaan*. Laivasto käytti myös koodeja lyhentääkseen viestejä, näin vaikeuttaen koodien purkamista ja lyhentääkseen viestitysaikaa, jotta Liittoutuneet eivät olisi pystyneet paikallistamaan aluksia lähetysten perusteella. Tärkeimmät koodit olivat *Kurzsignalheft* saattueilmoituksiin ja *Wetterkurzschlüsse*l sääraportteihin.

Laivasto käytti useita erilaisia koodeja, jolla jokaisella oli oma päivittäinen avaimensa (roottorien järjestys, niiden alkuasennot ja ristikytkennät). Peruskoodi oli *Heimisch* (*Heimische Gewässer* – englantilaisten nimitys *Dolphin*) lähivesille, johon kuului myöskin Atlantti. Ainakin 14:ää muuta koodia käytettiin sodan aikana.

Useimmissa koodeissa oli *Allgemein-* (yleinen) ja *Offizier-* (virallinen) avain. Offizier-viestit viestit koodattiin ensin ristikytkennän avulla kuukauden listan mukaan. Koko viesti koodattiin sen jälkeen uudestaan Allgemein-avaimella. Joissain viesteissä oli myös *Stab-* (esikunta) avain. Offizier-viestien purkamiseen englantilaisilla meni yleensä viikko tai enemmänkin.

Ensimmäiset kaappaukset

Helmikuussa 1940 miinanraivaaja *HMS Gleaner* pakotti pintaan saksalaisen *U-33:n*. Enigman roottorit annettiin miehistön eri jäsenille heitettäväksi mereen. Eräs sukellusvenemies kuitenkin unohti tämän ja häneltä löydettiin kolme roottoria. Roottorit nro:t VI ja VII löydettiin tässä välikohtauksessa, mutta ilman roottoria nro VIII englantilaiset eivät saaneet purettua *Dönitzin* viestejä sukellusveneille.

Huhtikuussa 1940 englantilainen merimies pelasti merestä saksalaisesta aluksesta paetessa heitetyn kassin, joka sisälsi asiakirjoja Kriegsmarinen viestiliikenteestä. Tämä johti siihen, että toukokuussa englantilaiset pystyivät purkamaan Kriegsmarinen koko huhtikuun viestit.

Elokuussa 1940 englantilaiset saivat haltuunsa roottorin nro. VIII.

9. toukokuuta 1941 saksalainen tyyppiä IXB oleva *U-110* hyökkäsi Islannin lähellä saattueen kimppuun. Eräs saattueen hävittäjistä, *HMS Aubretia*, sai syvyyspommein pakotettua veneen pintaan. Hävittäjän kapteeni aikoi ajaa sukellusveneen upoksiin, mutta tuli toisiin aatoksiin huomatessaan, että voisi saada kaapattua toimivan U-veneen. Sukellusveneen miehistön asettamat upotuspanokset eivät lauenneet ja englantilaiset valtasivat veneen. U-veneen radisti ei tehnyt mitään tuhotakseen Enigma-laitetta tai sen roottoreita, koska hän luuli veneen uppoavan hetkenä minä hyvänsä ja luullessaan, ettei viholliselle olisi mitään hyötyä laitteen saamisesta haltuunsa. Englantilaisilla oli nyt hallussaan Kriegsmarinen Enigma roottoreineen, koodikirja touko- ja kesäkuulle asti ja sukellusveneiden sijaintipaikkakoodit.

Oli kohtalon ivaa, että *U-110:n* itsemurhan tehnyt päällikkö oli kapteeniluutnantti *Fritz-Julius Lemp*, sama mies, joka oli upottanut englantilaisen matkustajalaiva *Athenian* vuonna 1939.

Englantilaiset yrittivät hinata sukellusveneen maihin, mutta se upposi seuraavana päivänä. Tämä oli kuitenkin onni, koska nyt *Dönitzillä* ei ollut mitään syytä epäillä, etteikö *U-110* olisi uponnut Enigman salaisuudet mukanaan. Käyttäessään haltuunsa saamiaan huhti-, touko- ja kesäkuun koodeja, englantilaiset saivat paikannettua ja upotettua monia rahtilaivoja ja tankkereita, jotka huolsivat U-veneitä eteläisellä Atlantilla.

Englantilaisilla oli myös hallussaan heinäkuun koodit, jotka oli saatu kaapattua säälaivoilta *München* ja *Lauenburg*. Elokuusta 1941 eteenpäin laivaston *Heimisch* -koodatut viestit pystyttiin purkamaan ilman koodikirjoja 36:ssa tunnissa *Bomben* avulla, joka pystyi laskemaan päivän asetuksen (jota vaihdettiin vain joka toinen päivä) vain noin 20 minuutissa.

Saksalaiset parantavat menetelmiään

Englantilaisille tuli mittava takaisku helmikuussa 1942, kun saksalaiset ottivat käyttöön *M4 Enigman* ja alkoivat käyttämään siinä edellisen vuoden syyskuussa tullutta *Triton* -salausta (englantilaisten nimitys *Shark*) Atlantilla ja Välimerellä toimivilla sukellusveneillään. Samoihin aikoihin otettiin myös käyttöön paranneltu versio *Wetterkurzschlüssel:istä*, jonka seurauksena englantilaiset eivät enää saaneet luntteja sääilmoituksista. Kaikki nämä yhdessä estivät koodien purkamisen seuraavan 10 kuukauden ajaksi. Englantilaisten onneksi *M4:n* neljäs roottori (beta) ei ollut vaihtokelpoinen roottorien I ja VIII kanssa. Beta lisäsi *M4:n* tehoa edeltäjäänsä verrattuna 26-kertaiseksi, mutta edellämainitusta seikasta johtuen roottorit pystyttiin sijoittamaan ”vain” 336 eri tavalla – ei 3 024:lla, kuten olisi ollut, jos kaikki roottorit olisivat olleet vaihtokelpoisia keskenään.

Oikealla beta-roottorin asennolla *M4* jäljitteli *M3:a*, mikä oli *M4:n* suurin vika. Englantilaisen hävittäjä *HMS Petardin* kolme miehistön jäsentä sai haltuunsa parannellun *Wetterkurzschlüsselin* koodikirjan *U-559:ltä* 30. lokakuuta 1942, ennen kuin se upposi *Port Saidin* edustalla. Englantilaiset saivat taas ”luntteja”, joita he voivat ajaa kolmiroottorisessa *Bombessaan*. U-veneet käyttivät *M4:sta M3:na* lähettäessään sääraportteja, joten *Bombella* meni vain 17 tuntia käydessään läpi kaikki 60 eri roottorien sijoitusvaihtoehtoa. Jos *M4:sta* käytettiin ”täydellä teholla”, englantilaisilla meni 442 tuntia (18 päivää) saadakseen roottorien sijoitusjärjestyksen selville.

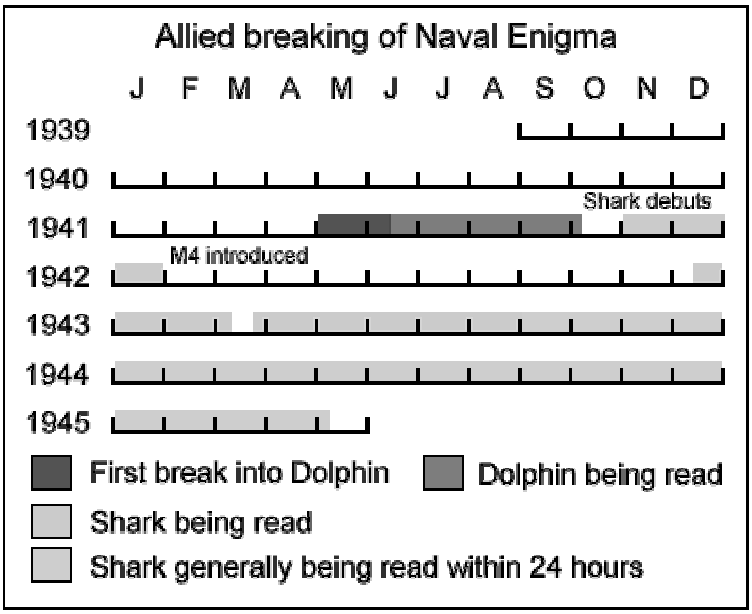
Joulukuun 13. päivä englantilaiset saivat selville 12 Atlantilla toimivan sukellusveneen sijainnit 5. ja 7. päivän välillä. Vaikka puretuista viesteistä saatiin tietoja välillä pitkälläkin viiveellä, se auttoi Liittoutuneita merkittävästi taistelussa Atlantista. On arveltu, että puretuista koodeista saatujen tietojen avulla säästettiin 500 000 – 750 000 tonnin edestä laivoja pelkästään joulukuun 1942 ja tammikuun 1943 välisenä aikana.

Wetterkurzschlüsselin käyttö *Tritonia* vastaan oli lyhytikäinen. Koodin kolmas versio otettiin käyttöön maaliskuussa 1943, ja näin estettiin englantilaisia saamasta arvokkaita ”luntteja” koodien purkamista varten. Mutta englantilaiset keksivät alkaa käyttää sukellusveneiden *Kurzsignalheft*-koodattuja saattueilmoituksia ”lunttien” etsimiseen. *Tritoniin* päästiin käsiksi jälleen 19. maaliskuuta ja koodaus murrettiin 90:nä päivänä 112:sta kesäkuun 30:een päivään mennessä. Myös *Kurzsignalheftissä M4:sta* käytettiin *M3:na* – ja senkin koodikirja oli saatu haltuun *U-559:stä*.

Työ siirtyy USA:lle

Britit ottivat käyttöön neliroottorisen *Bomben* kesäkuussa 1943 ja USA:n laivasto elokuussa, mutta jotkut heinä- ja elokuun koodaukset saatiin purettua vasta jopa 26 päivän viiveellä. Syyskuusta lähtien laivaston salaus saatiin purettua yleensä 24 tunnin sisällä. Vuoden 1943 lopussa *Triton-koodin* purkaminen siirtyi USA:n laivastolle *Washington DC:hin*, koska heillä oli yli 50 *Bombea* käytössään.

Kriegsmarinen salauksen purkamista käytettiin hyväksi pääasiassa saattueiden reittien suunnittelussa ja muutoksissa, mutta siitä oli hyötyä muillakin tavoin. USA:n laivasto käytti saamiaan tietoja hyväkseen vuosina 1943 ja 1944 upottaakseen monia huoltosukellusveneitä (tyypit *XB* ja *XIV*, kuten esim. *U-118, U-233 ja U-460*), jotka huolsivat U-veneitä merillä.



Ilman kolmen miehen rohkeutta U-559:n koodikirjojen kaappauksessa Tritonia ei olisi pystytty purkamaan ennen neliroottorisen Bomben valmistumista kesällä 1943, jos silloinkaan. Tässä tapauksessa Liittoutuneet eivät olisi pystyneet saavuttamaan meriherruutta Atlantilla kuin aikaisintaan vuoden 1943 toisella puoliskolla. Tämä olisi todennäköisesti siirtänyt Normandian maihinnousun vuoteen 1945. Harvoin on kolmen miehen rohkeus saanut niin kauaskantavat seuraukset.