Enigman matematiikasta

ℝami Luisto*

3. kesäkuuta 2014

Enigma on mahdollisesti historian tunnetuin, ja joissain mielessä merkittävin salkirjoitusmenetelmä. Pelkästään Enigman historiasta, murtamisesta, kryptografisista ominaisuuksista tai vaikutuksesta tietokoneiden historiaan voisi kirjoittaa, ja on kirjoitettukin, kokonaisia kirjoja. Tässä lyhyessä esseessä tarkoituksena on tutustua Enigman perusideaan matemaattisen kryptografian näkökulmasta. Sana Enigma viittaa tarkalleen ottaen isoon kokoelmaan 1900-luvun alkupuoliskolla käytössä olleita elektronis-mekaanisia salakirjoituskoneita, mutta yleensä puhekielessä Enigmalla tarkoitetaan toisen maailmansodan aikana Saksan käytössä ollutta salakirjoituskonetta sekä sen modifikaatioita. Tässä kirjoitelmassa keskitytään erääseen tämän salakirjoituskoneen version tutkimiseen.

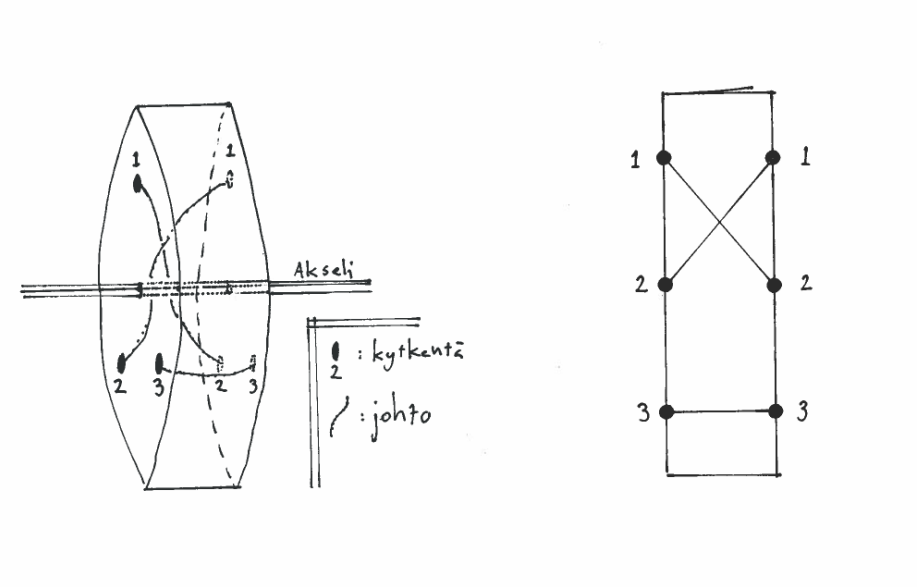
Sisältö

1 Roottorisalaimet

Enigma voidaan luokitella fyysisen rakenteensa perusteella niin sanotuksi roottorisalauslaitteeksi. Roottorisalauslaitteet olivat laajassa käytössä 1900-luvun puolivälissä ennen tietokoneiden kehittymistä ja Enigman rakennetta ymmärtämiseksi tutustutaan nyt niiden johinkin perusideoihin. Roottorisalauslaitteiden ideana oli elektro-mekanisoida salakirjoitusmenetelmissä käytettyjä algoritmeja. Tämä saatiin aikaan *roottoreilla*, jotka realisoivat jonkin aakkoston permutaatioita muodostamalla sopivia suljettuja virtapiirejä. Roottorisalaimen roottori

*Kirjoittaja ottaa mielellään vastaan kommentteja, korjauksia, sekä parannusehdotuksia tekstiin liittyen (etunimi.sukunimi(at)gmail.com). Esseessä ei luetella selkeitä viitteitä, mutta historiaan liittyvät väitteet on poimittu Wikipediasta sekä yleissivistyksestä. Matemaattiset väittämät ja analyysi on puolestaan tuotettu ottamalla kirjoittajan muistista Enigman määritelmä ja miettimällä kovaa. (Alunperin Enigman määritelmä on päätynyt kirjoittajan päähän useista eri lähteistä.)

on käytännössä ohuehko sylinteri, jonka kummallakin pyöreällä sivulla on aakkoston koon verran kytkentöjä. Roottorin sisällä vastakkaisten sivujen kytkentöjen välillä on johtoja, jotka muodostavat kyseisen aakkoston jonkin permutaation. Piirretään jatkossa roottori kuten kuvassa 1.



Kuva 1: Roottori, joka realisoi permutaation (12) aakkostossa $\{1, 2, 3\}$, sekä yksinkertaistettu tapa piirtää roottori.

Roottorisalaimen toiminta perustuu siihen, että se 'laskee' nopeasti yhden tai useamman roottorin realisoimien permutaatioiden kombinaatioita realisoimalla ne virtapiirinä. Näitä permutaatioita voi soveltaa tämän jälkeen aakkostoon esimerkiksi antamalla syötteen kytkimellä ja lukemalla tulosteen syttyvästä lampusta. Havainnoillistetaan ideaa esimerkillä. Oletetaan, että meillä on kolmen merkin aakkosto $S = \{1, 2, 3\}$, sekä salauspermutaatio $\alpha := (12)$. Aiemman kuvan 1 roottori realisoi tämän permutaation, joten roottorin avulla voidaan muodostaa roottorisalain kuten kuvassa 2. Sulkemalla sopiva kytkin ja katsomalla mikä lampuista syttyy, voidaan tällä koneella salakirjoittaa viestejä permutaation α antamalla tavalla. Roottorisalaimen eräs perusominaisuus on se, että kiertämällä roottoria saadaan aikaan uusia salauspermutaatioita. Roottorin kierron voi nimittäin realisoida konjugoimalla roottorin realisoimaa permutaatiota aakkoston syklisellä permutaatiolla $\rho := (123)$. Täten yksinketaisessa roottorisalaimessa syntyvät nyt permutaation $\alpha = (12)$ lisäksi sen konjugaatit $\rho\alpha\rho^{-1} = (23)$ sekä $\rho^2\alpha\rho^{-2} = (13)$, kun roottoria käännetään eri asentoihin kuten kuvassa 3.

Roottorisalainten yksi vahvuuksista perustui siihen, että peräkkäin asetettujen roottorien avulla saatiin mahdollisuus toteuttaa valtava määrä erilaisia aakkoston permutaatioita, jotka oli helppo realisoida. Vaihtamalla salakirjoituksen aikana roottorien asentoja (esimerkiksi joka kirjaimen kohdalla, kuten tullaan Enigmassa näkemään) saatiin aikaan moniaakkostosalauksia[1] joissa oli käytös-

[1]Kirjoittaja ei tiedä sanalle 'polyalphabetic substitution cipher' parempaa suomennosta.

sä valtava määrä erilaisia aakkoston permutaatioita. Koneellisesti toteutettuina näitä, tuohon aikaan hyvin voimakkaita, salausmenetelmiä saattoi käyttää nopeasti ja (mikäli salauskone oli järkevästi toteutettu) varsin vähäisellä koulutuksella[2].

2 Enigma

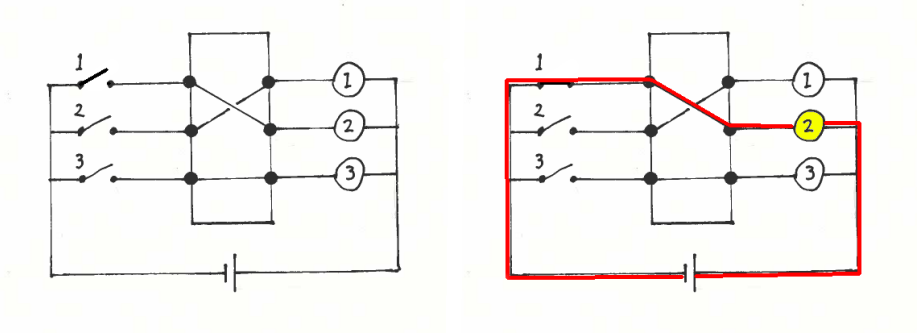
Jo 1900-luvun alkupuolella oli jo havaittu, että vähintään viestin pituisella kerta-avaimella salakirjoitettua viestiä on mahdotonta murtaa. Laajan skaalan viestiliikenteessä (esimerkiksi sotatilanteessa) on kuitenkin työlästä (ja usein epäkäytännöllistä) luoda, kommunikoida ja säilyttää pitkiä kerta-avaimia. Tämän johdosta on hyödyllistä muodostaa jokin algoritmi jolla lyhyempi avainkoodi muokataan hyvin pitkäksi salakirjoitusavaimeksi tavalla, jota on hankala ennustaa tai murtaa. Kuten aiemmin mainittiin, suosittu ratkaisu tähän ongelmaan oli roottorisalain. Esimerkiksi Enigman kohdalla saksalaisten koodikirjat sisälsivät jokaiselle päivälle pariinkymmeneen merkkiin pakatut tiedot Enigman alkuasetuksista. Näistä alkuasetuksista Enigma käytännössä loi noin 16000:n merkin mittaisen 'kerta-avaimen', joka riitti hyvin yksittäisten viestien salakirjoitukseen. Koska kyseessä ei ole aito kerta-avain, ei tämä salaus kuitenkaan ole murtamaton.

2.1 Yksinkertaistettu "pre-Enigma"

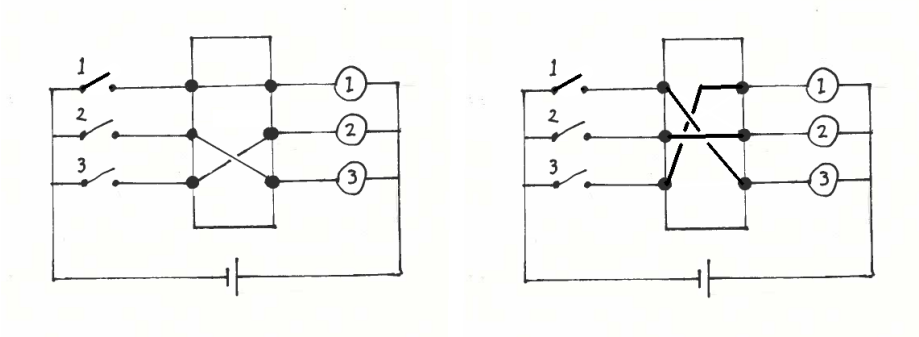
Ennen kuin koko Enigman rakenne avataan esille, tutkitaan yksinkertaistettua "pre-Enigmaa". Yksinkertaistettu pre-Enigma on kuvassa 4 näkyvä roottorisalain, jossa on permutaation (312) realisoiva roottori sekä toinen mekaaninen permutaation $P = (14)(23)$ realisoija jota kutsutaan *peilaajaksi*. Peilaajan sivulla on 4 kosketinta, ja peilaajan sisällä nämä on yhdistetty *pareittain toisiinsa* permutaation P perusteella.

Pre-Enigman käyttöä on havainnoillistettu kuvasarjassa 5, ja se toimii seuraavasti. Aluksi Pre-Enigman roottori asetetaan ennalta sovittuun alkuasen-

[2]Kännykköjen ja nettipankin yleisyys sekä matemaatikkojen koulutusmäärät ja työllistymismarkkinat olisivat varsin erilaisia jos kaikkeen salakirjoitukseen tarvittaisiin käyttäjäksi matematiikan maisteri, toim. huom.



Kuva 2: Kuvan 1 roottorikone, joka realisoi permutaation (12) 'syklikonjugaatteja' aakkostossa $\{1, 2, 3\}$, sekä kirjaimen 1 salaus tällä laitteella.



Kuva 3: Kuvan 2 roottorikone, jonka roottori on käännetty eri asentoihin. tuottaen uusia (konjugaatio)permutaatioita.

toon. Tämän jälkeen Suljetaan ensimmäiseen salattaan kirjaimeen liittyvä kytkin, ja katsotaan mihin kirjaimeen liittyvä lamppu syttyy. Matemaattisesti salauksessa viestin ensimmäistä kirjainta permutoidaan ensin roottorin realisoimalla permutaatiolla R, tämän jälkeen permutaatiolla P ja lopuksi permutaation R käänteispermutaatiolla. Ensimmäinen kirjain x_1 salataan siis kirjaimeksi $R^{-1}PRx_1$. Ennen viestin seuraavan kirjaimen salaamista *roottoria käännetään yhdellä pykälällä*. Roottorin kääntäminen vastaa roottorin konjugoimista syklillä $\rho := (1234)$, joten toinen kirjain x_2 salataan permutaatiolla

$$(\rho R\rho^{-1})^{-1}P(\rho R\rho^{-1})x_2.$$

Tämän jälkeen roottoria käännetään taas, ja yleisesti viestin kirjain numero n salataan permutaatiolla

$$(\rho^n R\rho^{-n})^{-1}P(\rho^n R\rho^{-n})x_n. \tag{1}$$

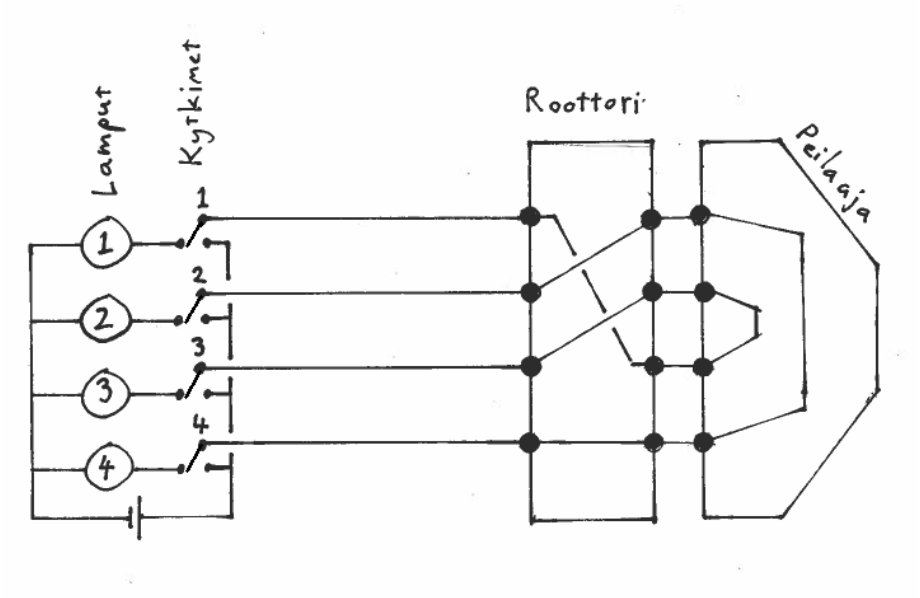
Pre-Enigma tuottaa siis jokaisella alkuasennollaan erilaisen salauksen.

2.2 Vain vähän yksinkertaistettu Enigma

Seuraavaksi tutkitaan Enigman mallia, joka vastaa autenttista Enigmaa lähes[3] täysin. Aakkosto koostuu 26:sta kirjaimesta A-Z. Huomaa, että kuten pre-Enigmassakin, Enigman rakenne vaatii parillisen kokoisen aakkoston. Välilyöntejä ei käytetä, koska ne joko paljastaisivat sanojen pituuksia sekä lauserakenteita ja altistaisivat salauksen tilastollisille hyökkäyksille, tai ne salattaisiin muiden symbolien joukossa, jolloin salatusta tekstistä olisi hankalaa lukea onko tekstissä peräkkäin tai sen lopussa useampi välilyönti. Välilyönnin sijasta saatetaan käyttää kirjainta X. Numeroita ei myöskään salakirjoiteta, vaan ne pitää tavata.

Tässä esseessä käytössä oleva Enigman malli on ikäänkuin laajennettu versio äskeisestä pre-Enigmasta. Ensinnäkin, yhden roottorin sijaan roottoreita on kolme peräkkäin, ja ne saatetaan asettaa mihin tahansa järjestykseen. Kunkin

[3]Kirjoittajan tietojen mukaan ainut yksinkertaistus liittyy siihen, että käytössä olleessa Enigmassa kakkosroottori teki mekaanisen toteutuksensa johdosta tietyssä tilanteessa ns. tuplasiirtymisen. Enigman eri mallien välillä oli tosin myös eroja roottorien siirtymiskäyttäytymisen suhteen. Asiasta löytyy tarkempaa tietoa esimerkiksi englanninkielisestä Wikipediasta.

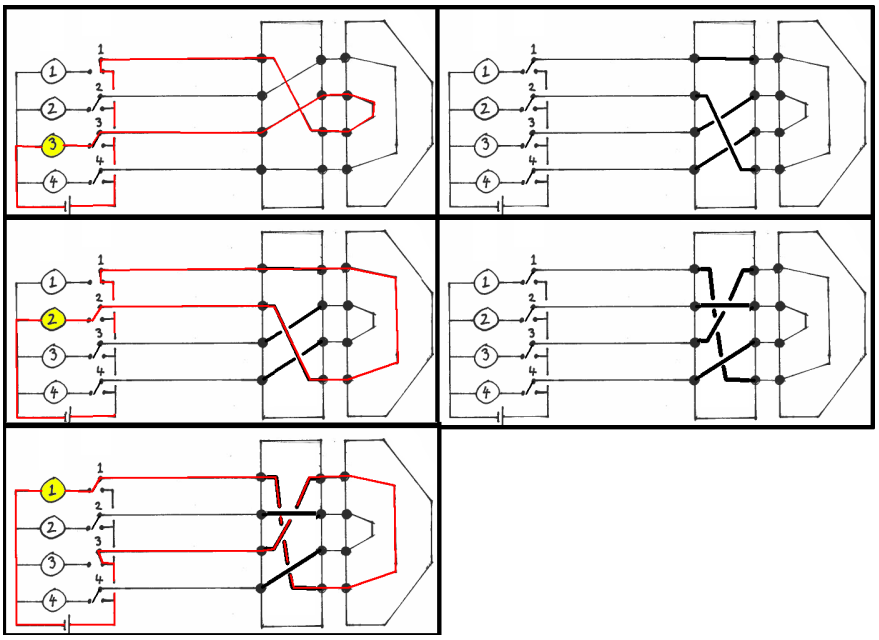


Kuva 4: Pre-Enigman rakenne. Kytkimet ovat kuvan asennossa kunnes niitä painetaan.

roottorin kytkennät on merkitty kirjaimilla A-Z, joista yksi on koneen päällä näkyvissä. Roottorin näkyvissä olevaa kirjainta kutsutaan roottorin sen hetkiseksi *asennoksi*. Enigman alustuksessa kukin roottori asetetaan aluksi ennalta sovittuun asentoon. Jokaisesta roottorista on lisäksi merkitty yksi kirjain, joka määrää milloin seuraavaa roottoria käännetään. Ensimmäinen roottori kääntyy jokaisen kirjaimen jälkeen kuten aiemminkin. Toinen roottori kääntyy silloin, kun ykkösroottorin asento on sama kuin ykkösroottorin merkitty kirjain, ja kolmosroottori silloin kun toisen roottorin asento on sama kuin toisen roottorin merkitty kirjain. Ensimmäinen roottori kääntyy siis joka kirjaimen kohdalla, toinen rottori keskimäärin kerran 26:n merkin välein ja kolmas roottori keskimäärin $26^2 = 676$ merkin välein. Tämän lisäksi ensimmäisen roottorin eteen on asetettu niin kutsuttu *kytkentälevy*. Kytkentälevy realisoi permutaation K, joka koostuu vaihtelevasta määrästä pareittain erillisten kirjainparien vaihdoista. Nämä vaihdot, ja siten permutaatio K on jälleen ennalta sovittu ja ne asetetaan Enigman alustuksen aikana. Kytkentälevy voidaan siis lisätä malliin ykkösroottorin eteen ikään kuin liikkumattomana roottorina, jonka permutaatio asetetaan erikseen salauksen alkaessa. Muodostetaan Enigman kirjaimeen numero n kohdistama salauspermutaatio E_n. Notaatiossa samaistetaan numerot 1-26 sekä aakkoset A-Z luonnollisella tavalla ja viestin kirjainten numerointi aloitetaan nollasta. Kuten aiemminkin, aakkoston siirtoa yhdellä pykälällä eteenpäin merkitään ρ. Roottorin siirtäminen pykälällä realisoituu taas roottorin konjugointina permutaatiolla ρ. Merkitään roottoreiden R_1, R_2 ja R_3 alkuasentoja a_1, a_2 ja a_3, sekä merkittyjä kohtia k_1, k_2 ja k_3. Nyt huomataan, että

(i) Ensimmäistä roottoria käännetään jokaisen kirjaimen kohdalla.

(ii) Toista roottoria käännetään kun salattavaa kirjainta numero n vastaava



Kuva 5: pre-Enigma salaa sanan “113” sanaksi “321”. Kuvasarjassa vasemmalla realisoidaan sen hetkinen permutaatio ja oikealla käännetään roottoria pykälän verran.

roottorin R_1 kohta $n + a_1$ osuu merkityn kirjaimen k_1 kohdalle.

(iii) Kolmatta roottoria käännetään vastaavasti kun roottorin R_2 kirjaimeen n liittyvä kohta osuu merkityn kirjaimen k_2 kohdalle.

Tämän innoittamana määritellään kuvaukset $\alpha, \beta, \gamma \colon \mathbb{N} \to \mathbb{Z}_{26}$, jotka kuvaavat missä asennossa kunkin roottorin kuuluu olla kirjainta n salakirjoitettaessa. Seuraavassa $p_{26} \colon \mathbb{N} \to \mathbb{Z}_{26}$ on projektio $n \mapsto [n] \in \mathbb{Z}_{26}$ ja merkitään

$$h_+ \colon \mathbb{Z} \to \mathbb{N}, \quad h(k) = \begin{cases} 0, & \text{kun } k < 0 \\ k, & \text{kun } k \geq 0. \end{cases}$$

Määritellään

$$\begin{aligned} \alpha &= p_{26} \circ \alpha', \text{ missä } \alpha'(n) = a_1 + n, \\ \beta &= p_{26} \circ \beta', \text{ missä } \beta'(n) = a_2 + \left\lfloor \frac{h_+(\alpha'(n) - k_1)}{26} \right\rfloor \\ \gamma &= p_{26} \circ \gamma', \text{ missä } \gamma'(n) = a_3 + \left\lfloor \frac{h_+(\beta'(n) - k_2)}{26} \right\rfloor . \end{aligned}$$

Nyt voidaan määritellä seuraava permutaatio R_n, joka on Enigman ’roottoriosion’ yhteen suuntaan realisoima permutaatio kirjaimen n kohdalla.

$$R_n := (\rho^{\gamma(n)} R_3 \rho^{-\gamma(n)})(\rho^{\beta(n)} R_2 \rho^{-\beta(n)})(\rho^{\alpha(n)} R_1 \rho^{-\alpha(n)})$$

Täten saadaan kaavaa (1) vastaava, koko Enigman realisoima, viestin kirjaimen numero n liittyvä salauspermutaatio kirjoitettua muotoon:

$$E_n := K^{-1}R_n^{-1}PR_nK, \tag{2}$$

missä K ja P ovat kytkentälevyn ja peilaajan realisoimat permutaatiot.

2.3 Enigman ominaisuuksia

Ilmeisesti (Wikipedia) Enigma oli niin tehokas salausjärjestelmä, että sen murtaminen ei olisi onnistunut toisen maailmansodan aikaisilla menetelmillä, ellei Enigman käytössä olisi tehty paljon virheitä. Kirjoitelmassa ei kuitenkaan puututa historiallisesti Enigman käytössä tehtyihin virheisiin, vaan keskitytään Enigman hyviin ja huonoihin rakenteellisiin ominaisuuksiin. Enigman hieman subjektiivisempi hyvä ominaisuus oli aiemminkin mainittu roottorisalainten helppokäytöisyys, varsinkin kun ottaa huomioon miten raskaan saluksen Enigmalla sai aikaiseksi. Salakirjoitettuja viestejä saattoi lähettää ja vastaanottaa kuka tahansa, joka oli saanut muutaman tunnin koulutuksen Enigman käyttöön.

Toinen Enigmalle hyvin ominainen ominaisuus on sen 'kaksisuuntaisuus'. Tällä tarkoitetaan tässä yhteydessä sitä, että viestin salaaminen ja purkaminen olivat täysin symmetriset operaatiot. Mikäli salatun viestin salakirjoitti uudelleen samoilla alkuasetuksilla, oli tuloksena selväkielinen viesti. Matemaattisesti ilmaistuna kaikilla n on siis voimassa, että $E_nE_n = \mathrm{id}$. Käydään läpi Enigman eri osien merkitystä seuraavaksi erikseen, jotta nähdään mistä tämä ja muut Enigman ominaisuudet johtuvat.

Peilaajan merkitys

Matemaattisesti peilaajan realisoiman permutaation P täytyy toteuttaa seuraavat kaksi ominaisuutta Enigman mekaanisen rakenteen johdosta.

(P1) Kaikilla kirjaimilla ξ pätee, että $P\xi \neq \xi$.

(P2) Permutaatio P koostuu pareittain erillisistä kahden alkion vaihdoista, eli erityisesti $P^2 = P$.

Jälkimmäisestä ominaisuudesta (P2) seuraa aiemmin mainittu huomio, että Enigman toiminta on symmetristä viestin salauksen ja viestin avaamisen suhteen. Tämän näkee myös formaalisti, sillä mikäli kirjaimen n permutaation (2) korottaa toiseen potenssiin, kumoutuvat kaikki termit:

$$\begin{aligned} E_nE_n &= (K^{-1}R_n^{-1}PR_nK)(K^{-1}R_n^{-1}PR_nK) \\ &= K^{-1}R_n^{-1}P^2R_nK \\ &= K^{-1}R_n^{-1}R_nK \\ &= K^{-1}K \\ &= \mathrm{id}\,. \end{aligned}$$

Ehto (P1) on myös historiallisesti tunnettu, ja se usein mainitaan Enigman kryptoanalyysin yhteydessä. Enigman rakenteesta, ja matemaattisesti erityisesti peilaajan realisoiman permutaation ominaisuuksista johtuen Enigma ei ikinä

salakirjoita kirjainta itselleen. Tätä voidaan hyödyntää Enigman kryptoanalyysissä, sillä se esimerkiksi vähentää mahdollisten salauspermutaatioiden määrää.

Miksi sitten Enigmassa käytettiin peilaajaa? Enigman olisi voinut toteuttaa kaksisuuntaisena roottorisalaimena mikäli sen rakenne olisi muistuttanut esimerkiksi kuvassa 2 esiintyvää hyvin yksinkertaista roottorisalainta. Tällöin kuitenkin roottorien yhdessä realisoiman permutaation S_n olisi jokaisen kirjaimen kohdalla täytynyt toteuttaa ehto $S_n S_n = \mathrm{id}$. [4] Ilman lähteitä tai varmaa tietoa, kirjoittajan hypoteesi kysymykseen liittyen on seuraava: Ensinnäkin, laitteen kaksisuuntaisuutta pidettiin niin tärkeänä, että siitä ei haluttu luopua. Täten vaikkakin peilaajan käyttö aiheutti peilaajalle, ja siten koko Enigmalle ominaisuuden (P1) ja täten heikensi Enigman salausta, oli tämä pienempi haitta kuin se, että roottorien permutaatiot olisi jouduttu valitsemaan hyvin rajoitetulla tavalla. Nimittäin kuten seuraavassa kappaleessa huomataan, saatettiin roottorien salaukset valita vapaasti, pitkälti peilaajan ansiosta. Viimeisessä luvussa 'Kysymyksiä' on asiaan liittyviä jatkokysymyksiä.

Roottorien merkitys

Enigman roottorit olivat jossain mielessä 'vapaimmat' permutaatiot mitä koneesta löytyi. Ne saattoivat kuvata kirjaimen itselleen, eikä niiden tarvinut olla itsensä käänteisalkiota. Roottoreihin saatettiin valita realisoitavaksi mikä tahansa bijektio käytössä olevalta aakkostolta itselleen. Enigman haluttu 'kaksisuuntaisuus' säilyy, sillä kirjaimen n salauksessa käytettävä permutaatio E_n sisältää sekä roottorien realisoimat permutaatiot että niiden käänteispermutaatiot, kuten aiemmin huomattiin. Roottorien realisoimat permutaatiot olivat kuitenkin kiinteät, eikä niitä voinut muuttaa vaihtamatta roottoreita. (Roottorien järjestystä tosin vaihdettiin päivittäin ja joissain laivastomalleissa saatettiin käyttää kolmesta viiteen roottoria eri kombinaatioilla.)

Kytkentälevyn merkitys

Kuten mainittiin, matemaattisesti Enigman 'roottoriosan' eteen asetettu kytkentälevyn realisoima permutaatio K lisäsi roottoriosan realisoimaan, kirjaimittain vaihtuvaan salauspermutaatioon R_n kiinteän konjugoinnin $K^{-1} R_n K$, joka asetettiin Enigman alustuksessa ennalta sovittuina pareina. Täten kytkentälevyn realisoimaksi permutaatioksi olisi voinut asettaa minkä tahansa bijektion aakkosten välillä hävittämättä Enigman kaksisuuntaisuutta. Syy 'valinnanvapauteen' on sama kuin roottorien kohdalla: kytkentälevyn realisoima permutaatio esiintyy permutaatio-käänteispermutaatioparina ja nämä kumoavat toisensa kuten osiossa 'Peilaajan merkitys' huomattiin.

Kytkentälevyn realisoima permutaatio ei kuitenkaan ollut ikinä mielivaltainen permutaatio, vaan se toteutti edelleen ehdon $K^2 = \mathrm{id}$, sillä se koostui pareittain erillisistä kahden kirjaimen vaihdoista. (Maksimissaan 13 paria vaihdettiin, historiallisesti vaihtoja oli yleensä 6-10.) Erona peilaajaan realisoimaan permutaatioon saattoi kytkentälevyn permutaatiossa kirjain kuvautua itselleen, sillä kaikkien aakkosten ei tarvinnut sisältyä vaihdettuun pariin. Kirjoittajalla ei ole

[4] Kirjoittaja olisi huolehtinut tästä valitsemalla kunkin roottorin realisoiman permutaation toteuttamaan tämän ehdon $R_i^2 = \mathrm{id}$ erikseen. Harjoitustehtäväksi jää miettiä, onko mahdollista rakentaa roottoreita, jotka eivät toteuta ehtoa $R_i^2 = \mathrm{id}$, mutta joista muodostetttu "peilaajaton Enigma" toteuttaa ehdon $E_n^2 = \mathrm{id}$.

varmaa tietoa tai lähteitä liittyen siihen, että miksi permutaatiota K ei toteutettu mielivaltaiseksi, vaan erillisisten kahden alkion syklien kombinaatioksi, mutta kirjoittaja konjekturoi, että tälle oli seuraavat kaksi pääsyytä:

- Vaikka mahdollisten kytkentälevyn vaihtoehtojen määrä oli pienempi kuin mitä olisi ollut yleisessä tapauksessa mahdollista, oli vaihtoehtoja kumminkin tarpeeksi paljon (yli 10^{12}) jottei niitä kaikkia voitu käydä sen ajan laitteilla lävitse.

- Erillisten kirjainparien vaihtojen elektro-mekaaninen realisointi oli helppo toteuttaa rakenteellisesti, ja Enigman alkuasetusten asettaminen onnistui nopeasti ja yksinkertaisesti. (Maksimissaan kolmentoista kaksipäisen kaapelin kytkeminen annettujen kirjainparien ilmoittamiin pistokkeisiin onnistuu jopa väsyneeltä viestimieheltä.)

Enigma kokonaisuutena

Tarkastellaan seuraavaksi miten äsken mainitut palaset muodostavat kokonaisuudessaan Enigman sekä sen realisoiman permutaation E_n. Kootaan yhteen muutama välittömästi esiin nouseva ominaisuus.

Ensinnäkin, kuten jo todettiin, niin Enigma on kaksisuuntainen järjestelmä, eli $E_n^2 = \mathrm{id}$. Toisaalta peilaajan johdosta Enigman permutaatiolla on kryptoanalyysissä hyödynnettävä ominaisuus, että $E_n\xi \neq \xi$ kaikilla kirjaimilla ξ. (Enigma toimii ilman kiintopisteitä tjsp.) Toisaalta Enigma on, kuten lähes kaikki symmetriset salausjärjestelmät, herkkä alkuasetusten, eli salakirjoitusavaimen paljastumisen suhteen. Enigman alkuasetuksia vaihdettiin kerran vuorokaudessa, joten yksien alkuasetusten paljastuminen mahdollisti koko sen päivän viestiliikenteen lukemisen.

Hyvänä tai suorastaan loistavana Enigman ominaisuutana mainittakoon, että yhden avoin-salattu -viestiparin tunteminen ei riitä muiden viestien murtamiseen. Mikäli tunnetaan esimerkiksi selväkielinen viesti “HEI” ja sen salattu versio “LOL”, niin tästä ei voida (ainakaan a priori) päätellä muuta, kuin että ensimmäistä kirjainta salakirjoitettaessa kirjaimet H ja L vaihtuvat, toista kirjainta salakirjoitettaessa kirjaimet E ja O vaihtuvat ja kolmatta kirjainta salakirjoitettaessa kirjaimet I ja L vaihtuvat. Näillä tiedoilla ei voinut sanoa esimerkiksi salakirjoitetusta viestistä “OLO” muuta, kuin että:

- Ensimmäisellä paikalla ei selväkielisessä viestissä voi olla kirjaimia O, H tai L.

- Toisella paikalla ei selväkielisessä viestissä voi olla kirjaimia E, O tai L.

- Kolmannella paikalla ei selväkielisessä viestissä voi olla kirjaimia I, L tai O.

Kokonaisuus on enemmän kuin osiensa summa

Kirjoittajan mielestä Enigman kauneimpia puolia on sen kaksijakoisuus, jonka muodostavat kytkentälevy ja roottorikoneisto peilaajineen. Pelkän kytkentälevyn käyttö saisi aikaan yksinkertaisen korvaussalakirjoituksen[5] johon voisi

[5]Kirjoittaja ei tunne parempaa suomennosta termille ’substitution cipher.’

soveltaa tunnettuja kryptoanalyyttisiä metodeja, esimerkiksi frekvenssianalyysiä. Myöskin yhden salatun viestin purkaminen helpottaisi valtavasti muiden samalla korvauksella salattujen viestien purkamista.

Toisaalta pelkän roottorimekaniikan käyttö olisi riittämätön salaus, sillä mikäli vastapelaaja saa tutkittavakseen roottorimekaniikan ja saa selville sen rakenteen (kuten toisen maailmansodan aikana Enigman suhteen kävi) voi salauksen purkaa käsin. Kolmiroottorisessa Enigmassa on nimittäin kertaluokkaa 10^5 eri aloitusvaihtoehtoa ja suurvallan tiedusteluorganisaatio pystyy käymään nämä vaihtoehdot käsin lävitse. (Jos esimerkiksi tiedetään yleisesti viestiliikenteessä käytettävä aloitusteksti, voi tämän kaikilla eri metodeilla salaamalla muodostaa 'sanakirjan', jolla käytössä olevia mahdollisuuksia voi rajata. En tiedä onko tällaista metodia historiallisesti käytetty, mutta ennen toista maailmansotaa Enigman kytkentälevytön versio oli käytössä Espanjan sisällissodassa 1930-luvulla, ja Britit saivat purettua[6] käsin salatun viestiliikenteen.)

Yhdessä käytettynä nämä kaksi salausmenetelmää kuitenkin paikkaavat kauniisti toistensa heikkoudet. Kytkentälevyn eri 'alkuasetuksia' on enemmän kuin 10^{12}. (Vaihdettujen kirjainparien määrä vaihteli sodan aikana. Käytettäessä sodan loppupuolen kymmentä vaihtoparia nousee vaihtoehtojen lukumäärä kertaluokkaan 10^{14}.) Tämän johdosta kytketälevyn eri vaihtoehtoja ei voi käydä käsin lävitse. Toisaalta tämän jälkeen sovellettava roottorisalaus muodostaa kytkentälevyn permutaatiosta valtavan määrän erilaisia permutaatioita, joiden käyttö peräkkäisiin kirjaimiin tekee frekvenssianalyysiin tukeutuvista menetelmistä mahdottomia.

Kirjoittaja suosittelee lukijansa miettimään tätä kaksijakoisuutta, ja kahden eri tekniikan yhdistelmän tuomaa lisärakennetta.

3 Kysymyksiä

Muutama kysymys, jota ehdotan mietittäväksi jos haluaa perehtyä aiheeseen. (Ja joihin en ehtinyt itse esseen kirjoituksen aikana paneutua.)

(?1) Enigma luo alkusetuksillaan peräkkäisille kirjaimille eri permutaatiot. Miten kaukana nämä permutaatiot ovat toisistaan? Miten kahden salauspermutaation etäisyyttä kannattaisi mitata?

(?2) Miten 'kauas toisistaan' Enigma salakirjoittaa saman viestin, mikäli alkuasetuksia muuttaa vain hieman? Onko Enigmalle aina edullista salakirjoittaa sama viesti hieman eri alkuasetuksilla hyvin kauas toisistaan, eli onko 'voimakas epäjatkuvuus' jotain tavoittelemisen arvoista tällaisissa salauslaitteissa? Onko Enigman tärkeää olla eräänlainen 'käänteinen hash-funktio'?

(?3) Enigman roottoreiden realisoimat permutaatiot saatettiin valita miksi tahansa permutaatioksi. Niitä ei kannata valita identtisiksi permutaatioiksi, mutta onko olemassa muita rajoitteita siihen, kuinka roottorien permutaatiot kannattaa valita? Onko haittaa jos roottorien realisoimat permutaatiot ovat toistensa käänteispermutaatioita, tai yleisemmin toisistaan lineaarisesti riippuvaisia? Onko haittaa jos yhdeksi roottoriksi valitaan kahden

[6] Lähde: Wikipedia

alkion sykli? Miten voitaisiin valita parhaat roottorit, miten parhautta mitattaisiin ja miltä tällaiset roottorit näyttäisivät?

(?4) Miten Enigma toimisi nykyään? Jos saisit käsiisi toisen maailmansodan aikaista viestiliikennettä, niin pystyisitkö murtamaan Enigman 'Brute force' -menetelmillä ja/tai frekvenssianalyysillä käyttäen vain pöytäkonettasi? Tai kännykkääsi?

(?5) Mikäli lähetät vain lyhyitä viestejä, (enintään kaksikymmentä merkkiä) niin riittäisikö yksiroottorinen Enigma salausmenetelmäksi? Nollaroottorinen aukeaa frekvenssianalyysillä, mutta missä kohtaa yksiroottorinen kone ei enää riitä?

(?6) Kohdassa 'Peilaajan merkitys' pohdittiin, muuttuisiko Enigman muurtaminen helpommaksi mikäli Enigmasta poistetaan peilaaja, mutta roottorien realisoimille permutaatioille pätee $R_i^2 = \mathrm{id}$? Vertaa ensimmäiseen muutamaan kysymykseen, miten roottorien realisoimien permutaatioiden rajoittaminen muuttaa Enigman tuottamien moniaakkostosalauspermutaatioiden joukkoa, pieneneekö esimerkiksi Enigman luomien permutaatioiden joukon halkaisija tai karkea dimensio? Miten edelliset kaksi termiä pitäisi tulkita?

(?7) Edelleen kohdassa 'Peilaajan merkitys' alaviitteessä kysyttiin, voitaisiinko roottorien permutaatiot valita niin, että välttämättä ei päde $R_i^2 = \mathrm{id}$, mutta että näiden avulla toteutettu 'peilaajaton Enigma' realisoisi permutaation S_n, jolle on voimassa $S_n^2 = \mathrm{id}$?