Eräitä RSA-salauksen haavoittuvuuksia

Helinä Anttila

Matematiikan pro gradu

Jyväskylän yliopisto
Matematiikan ja tilastotieteen laitos
Kevät 2016

Tiivistelmä: Helinä Anttila, *Eräitä RSA-salauksen haavoittuvuuksia*, (engl. *Some vulnerabilities in the RSA cryptosystem*), matematiikan pro gradu -tutkielma, 43 s., Jyväskylän yliopisto, Matematiikan ja tilastotieteen laitos, kevät 2016.

Tämän tutkielman tarkoituksena on tuoda esiin osa RSA-salauksen tunnetuista, mutta harvemmin esiin tulevista, haavoittuvuuksista sekä keinoja niiden välttämiseen salausta luodessa ja käytettäessä.

RSA-salaus on yksi ensimmäisistä edelleen käytössä olevista julkisen avaimen salausjärjestelmistä, joka perustuu suurien lukujen tekijöihin jaon ongelmaan. RSA-salauksessa lähdetään liikkeelle valitsemalla kaksi erisuurta alkulukua p ja q, joita sanotaan RSA-tekijöiksi. Näiden avulla lasketaan RSA-moduli $N = pq$. Tämän jälkeen valitaan julkinen avain e, $1 < e < (p-1)(q-1)$, sekä lasketaan sitä vastaava salainen avain d, $1 < d < (p-1)(q-1)$. Salaisen avaimen laskeminen julkisesta avaimesta onnistuu Eukleideen algoritmin avulla. Julkisen avaimen e ja salaisen avaimen d tulon modulon tulee olla 1 luvun $(p-1)(q-1)$ jäännösluokassa. Julkinen avainpari on (N, e). Viesti m salataan julkisella avaimella e. Salattu viesti $c \equiv m^e \mod N$ puretaan salaisella avaimella d: $c^d \equiv m \mod N$.

Tekijöiden p ja q sekä avainten valintaan liittyy seikkoja, joiden huomiotta jättämisellä salauksen taso voi menetelmän oikeellisuudesta huolimatta olla heikko. Mikäli toinen tekijöistä on pieni, löydetään molemmat helposti kokeilemalla – toisen löytyessä ovat molemmat selvillä. Tekijöitä ei myöskään kannata valita läheltä toisiaan, koska tällöin ne pystytään löytämään suhteellisen helposti käyttäen hyödyksi niiden summan ja erotuksen puolikkaiden neliön summaa. Summa on yhtä suurta RSA-modulin N kanssa. Lukujen ollessa lähellä toisiaan on niiden erotus lähellä nollaa, jolloin kokeilemalla voidaan selvittää neliöitävät luvut ja sitä kautta ratkaista tekijät. Mikäli tekijät pystytään selvittämään, saadaan julkisen avaimen ja yhtälön $de \equiv 1 \mod N$ avulla salainen avain helposti selville.

Myös avainten valinta tulee tehdä harkiten. Paitsi avainten koko, myös julkisen avaimen kertaluku jäännösluokkaryhmässä $\mathbb{Z}_{(p-1)(q-1)}$ on syytä huomioida. Jos julkisen avaimen kertaluku on pieni, voidaan salaus murtaa yksinkertaisesti kokeilemalla korottaa salattu viesti potenssiin $k = 1, 2, 3, \ldots \mod N$ ja tulkitsemalla tulosta. Salaisen avaimen kohdalla avaimen suuruudella on merkitystä. Mikäli salainen avain $d < \frac{1}{3}N^{\frac{1}{4}}$, voidaan se selvittää käyttäen ketjumurtolukujen ominaisuuksia hyödyntävää Wienerin algoritmia ja siihen liittyvää testiä avaimen oikeellisuudesta.

Huolellinen tekijöiden valinta ja avainten konstruointi ei aina yksistään riitä. Myös käyttöön on kiinnitettävä huomiota. Salauksen murtaminen helpottuu jos useassa viestissä on käytetty samaa RSA-modulia, vaikka jokaisella käyttäjällä olisi oma julkinen avainpari (N, e_i). Kukin käyttäjä pystyy oman salaisen avaimensa avulla selvittämään RSA-tekijät ja sitä kautta laskemaan kaikki salaiset avaimet julkisen avaimen avulla. Salattujen viestien ollessa samat salaus voidaan murtaa myös viestejä kaappaamalla. Tämä on mahdollista jo kahden julkisen avainparin avulla. Ongelman välttämiseksi ei riitä pelkän RSA-modulin vaihtamien, sillä käytettäessä samaa julkista avainta e salaus on mahdollista murtaa ratkaisemalla viesteistä syntyvä kongruenssiyhtälöryhmä esimerkiksi kiinalaisen jäännöslauseen avulla.

Sisältö

Johdanto

Nykyisen lukuteorian perustajana pidetään ranskalaista Pierre de Fermat'ta (1601-1665), joka ei elinaikanaan julkaissut juuri mitään. [**2**, s. 489-501]. Lukuteoria näyttelee suurta roolia nykyajan tietoyhteiskunnassa erilaisten tietojärjestelmien taustalla. Jatkuvasti vaihdettavat sähköiset viestit sisältävät paitsi päivittäisiä asioita, myös salassa pidettäviä tietoja. Laskentatehon kasvu mahdollistaa toimimisen entistä tehokkaammin ja suurempien lukujen parissa. Kaikkea ei kuitenkaan pystytä nykytiedoinkaan tekemään tehokkaasti. Esimerkkinä tästä suurien lukujen tekijöihin jakaminen.

Tässä tutkielmassa käydään läpi Ron Rivestin, Adi Shamirin ja Len Adlemanin ensimmäisen kerran vuonna 1977 julkaistun, yhä käytössä olevan, RSA-salausmenetelmän eräiden yksinkertaisimpien tunnettujen haavoittuvuuksien taustalla olevaa matematiikkaa. Samalla esitetään keinoja niiden välttämiseen salausta muodostettaessa. Lisää olemassa olevista haavoittuvuuksista voi lukea esimerkiksi Bonehin artikkelista [**1**]. Lukijalta oletetaan matematiikan perusteiden yleistä tuntemusta. Lisäksi lukijalla on hyvä olla hieman pohjatietoa kokonaislukujen lukuteoriasta ja algebrasta.

Tutkielman ensimmäisissä luvuissa käydään läpi tarvittavat tiedot myöhemmin käsiteltävien heikkouksien läpikäymiseen. Tutkielman pääasiallisena lähteenä ovat toimineet Buchmanin [**3**] ja Hoffstein ym. [**6**] teokset. RSA-salauksen haavoittuvuuksia käsittelevässä luvussa on lisänä käytetty paljon Bonehin [**1**] ja Wienerin [**11**] artikkeleita. Ketjumurtolukujen kohdalla pääasiallisena lähteenä ovat toimineet Kuritun [**7**] luentomoniste sekä Hardyn & Wrightin [**5**] teos. Tutkielmaa kirjoitettaessa on hyödynnetty Ari Lehtosen pohjaa pro-gradu tutkielmalle.

LUKU 1

Yleistä

Tässä luvussa käydään lyhyesti läpi kokonaislukujen lukuteoriaa. Luku ei suinkaan ole kaiken kattava esitys kyseisistä alueista vaan pikemminkin pintaraapaisu muistin virkistämiseksi, joka antaa pohjan myöhemmin käsiteltävien asioiden läpikäymiseen. Jatkossa puhuttaessa luonnollisista ei luvun 0 katsota kuuluvan luonnollisten lukujen joukkoon.

1.1. Modulaarimatematiikkaa

LAUSE 1.1 (Jakoyhtälö). *Olkoot $a, b \in \mathbb{Z}$ ja niille voimassa $a > b$ ja $b \neq 0$. Tällöin on olemassa yksikäsitteiset luvut q ja $r \in \mathbb{Z}$ siten, että*

$$a = qb + r \quad ja \quad 0 \leq r < b.$$

Lukua r sanotaan jakojäännökseksi.

Sanotaan luvun a olevan jaollinen luvulla b, jos $a = qb + 0$. Vastaavasti luku a ei ole jaollinen luvulla b, jos $a = qb + r, r \neq 0$. Yhtäpitävästi voidaan myös sanoa, että luku b jakaa tai ei jaa lukua a. Merkintä $b \mid a$ tarkoittaa luvun b jakavan luvun a. Mikäli b ei jaa lukua a, merkitään $b \nmid a$.

MÄÄRITELMÄ 1.2 (Suurin yhteinen tekijä). Kahden kokonaisluvun $a, b \neq 0$ *suurin yhteinen tekijä* on suurin kokonaisluku d, joka jakaa molemmat luvut a ja b. Tälle käytetään merkintää $\text{syt}(a, b) = d$.

HUOMAUTUS 1.3. Kahden *keskenään jaottoman luvun* a ja b suurin yhteinen tekijä on 1. Tällöin puhutaan myös *suhteellisista alkuluvuista*.

MÄÄRITELMÄ 1.4. Kokonaisluvut a ja r ovat *kongruentteja* modulo m, $m \in \mathbb{N}$, kun $a - r = km$ jollakin $k \in \mathbb{Z}$. Tällöin merkitään

$$a \equiv r \mod m, m \geq 2.$$

Jakoyhtälön mukaisesti jokaiselle luvulle $l \in \mathbb{Z}$ löytyy luku r, $0 \leq r < m$ siten, että $l = km + r$, toisin sanoen $l \equiv r \bmod m$. Keskenään kongruenteista luvuista saadaan *jäännösluokat*. Jäännösluokille mod m käytetään merkintää

$$[r]_m .$$

Poikkeuksena tästä, huonona tapana on, että erilaisten salausjärjestelmien yhteydessä jäännösluokkia käsiteltäessä, voidaan jäännösluokan merkintätapaa supistaa. Tällöin puhutaan jäännösluokasta, mutta jätetään sulkeet ja alaindeksi merkitsemättä.

ESIMERKKI 1.5. Luvuille $2, 12, 22$ pätee $22 \equiv 12 \equiv 2 \mod 10$, joten ne kuuluvat samaan jäännösluokkaan $[2]_{10}$.

Tarkemmin tarkasteltuna jäännösluokat ovat *renkaita*. Tämä on algebraan liittyvä käsite ja edellyttää tiettyjä ominaisuuksia *ryhmältä*. Nämä käydään lyhyesti läpi myöhemmin.

1.2. Nopea potenssilasku

Laskettaessa potenssilaskua a^n perinteiseen tapaan tehdään $n-1$ kappaletta laskutoimituksia. Tämä määrä on huomattava suurilla n:n arvoilla. Nopea potenssilasku on tapa vähentää laskutoimitusten määrää tehokkaasti.

Lasketaan nopealla potenssilaskulla $a^n, n \in \mathbb{Z}_+$ Kirjoitetaan luku n binäärimuodossa:

$$n = \sum_{i=0}^{k} n_i 2^i, \quad n_i \in \{0, 1\}.$$

Tällöin alkuperäinen potenssi saadaan esitettyä muodossa

$$a^n = a^{\sum_{i=0}^{k} n_i 2^i} = \prod_{i=0}^{k} (a^{2^i})^{n_i} = \prod_{0 \le i \le k, n_i = 1} a^{2^i}. \tag{1.1}$$

Laskutoimitusten määrän väheneminen ei kuitenkaan muuta itse lopputulosta, joka suurilla eksponenteilla on jättimäinen. Nopean potenssilaskun käyttökelpoisuus korostuu laskettaessa *jäännösluokkia*. Luvun ollessa kirjoitettuna yhtälön (1.1) mukaisena tulona, saadaan seuraava tulontekijä, $a^{2^{i+1}}$, neliöimällä tulontekijän a^{2^i} jäännösluokan edustaja. Tämä on mahdollista, sillä potenssin laskusääntöjen mukaan $a^{2^{i+1}} = a^{2^i \cdot 2} = (a^{2^i})^2$. Tällä tavoin kunkin yksittäisen tekijän suuruus on itseisarvoltaan korkeintaan puolet jäännösluokan modulin suuruudesta. Otetaan tästä esimerkki.

ESIMERKKI 1.6. Lasketaan $8^{57} \mod 100$ käyttäen hyväksi nopeaa potenssilaskua. Muutetaan ensin luku 57 binäärimuotoon: $57 = 2^0 + 2^3 + 2^4 + 2^5$. Tämän avulla saadaan 8^{57} esitettyä muodossa $8^{57} = 8^{2^0+2^3+2^4+2^5} = 8^{2^0} \cdot 8^{2^3} \cdot 8^{2^4} \cdot 8^{2^5}$. Lasketaan seuraavaksi ensimmäiset kolme neliötä hyödyntäen kunkin neliön kohdalla edellisen neliön jäännösluokkaa sekä potenssin laskusääntöjä:

$$8^{2^0} \equiv 8 \mod 100$$

$$8^{2^1} \equiv 8^2 = 64 \mod 100$$

$$8^{2^2} \equiv 64^2 = 4096 \equiv -4 \mod 100$$

Seuraavana laskettavana on $8^{2^3} \mod 100$. Tässä nopean potenssilaskun hyöty tulee hyvin näkyviin. Edellinen neliö on $8^{2^2} = 4096$, mutta kun kyseessä on jäännösluokka modulo 100, saadaan tulos kätevästi käyttäen luvun -4 jäännösluokkaa. Tällöin

laskettavaksi jää 4096^2 sijaan $(-4)^2$. Lasketaan vielä loputkin tarvittavista neliöistä:

$$8^{2^3} \equiv (-4)^2 = 16 \mod 100$$
$$8^{2^4} \equiv 16^2 = 256 \equiv -44 \mod 100$$
$$8^{2^5} \equiv (-44)^2 = 1936 \equiv 36 \mod 100$$

Alkuperäinen lasku, $8^{57} \mod 100$ saadaan nyt nopean potenssilaskun avulla laskettua neliöiden tulona seuraavasti:

$$8^{57} \equiv 8^{2^0} \cdot 8^{2^3} \cdot 8^{2^4} \cdot 8^{2^5} \equiv 8 \cdot 16 \cdot (-44) \cdot 36 \equiv 48 \mod 100.$$

1.3. Eukleideen algoritmi

Kahden luvun suurimman yhteisen tekijän selvittäminen onnistuu Eukleideen algoritmin avulla, jossa ideana on toistaa jakoyhtälöä luvulle b_i kunnes jakojäännös r on nolla. Otetaan yksinkertainen esimerkki ennen algoritmin kulun tarkempaa läpikäyntiä.

Esimerkki 1.7. Määritetään lukujen 258 ja 102 suurin yhteinen tekijä Eukleideen algoritmia käyttäen. Katsotaan, kuinka monta kertaa pienempi luku 102 sisältyy suurempaan lukuun 258 ja mitä tällöin jää jakojäännökseksi:

$$258 = 2 \cdot 102 + 54$$

Jakojäännökseksi jää 54. Jatketaan sitten seuraavaan vaiheeseen. Edellä jakajana toiminut luku 102 on mahdollista esittää yksikäsitteisesti käyttäen jakajana saatua jakojäännöstä:

$$102 = 1 \cdot 54 + 48$$

Nyt jakojäännökseksi jää 48, jonka avulla luku 54 voidaan esittää. Toistetaan toimenpidettä, kunnes jakojäännökseksi jää 0:

$$54 = 1 \cdot 48 + 6$$
$$48 = 8 \cdot 6 + 0$$

Viimeisellä rivillä jakojäännökseksi jää 0. Suurin yhteinen tekijä on tätä edeltävän rivin jakojäännös. Tässä tapauksessa lukujen 258 ja 102 suurin yhteinen tekijä on luku 6.

Lause 1.8 (Eukleideen algoritmi). *Olkoot $a, b \in \mathbb{Z}$, $a \geq b > 0$. Asetetaan $r_0 = a$ ja $r_1 = b$. Toistamalla nyt jakoyhtälöä saadaan $r_{i-1} = r_i q_{i+1} + r_{i+1}$, jossa $0 < r_{i+1} < r_i$ kaikilla $1 \leq i < n$, kun $i, n \in \mathbb{N}$ ja $r_{n+1} = 0$. Tällöin* $\operatorname{syt}(a, b) = r_n$.

TODISTUS. Eukleideen algoritmissa jakojäännösten jono $(r_i)_{i\geq 1}$ on aidosti vähenevä ja saavuttaa nollan äärellisessä ajassa. Yhtälöstä $r_{i-1} = r_i q_{i+1} + r_{i+1}$ nähdään, että jos jokin luku $c \in \mathbb{Z}$ on lukujen r_{i-1} ja r_i tekijä, niin

$$r_{i+1} = r_{i-1} - r_i q_i = ck - clq_i = c(k - lq_i)$$

joillekin $l, k \in \mathbb{Z}$. Siten luku c on myös luvun r_{i+1} tekijä. Vastaavasti jokainen lukujen r_i ja r_{i+1} yhteinen tekijä on myös luvun r_{i-1} tekijä. Tämän seurauksena on voimassa

$$\text{syt}(r_{i-1}, r_i) = \text{syt}(r_i, r_{i+1}). \tag{1.2}$$

Koska jono (r_i) on vähenevä, päädytään jossain vaiheessa tilanteeseen, jossa $r_i = 0$. Olkoon $r_{n+1} = 0$. Tällöin $r_{n-1} = r_n q_n + 0$ ja $r_n = \text{syt}(r_{n-1}, r_n) = \text{syt}(r_n q_n, r_n)$. Nyt yhtälön (1.2) mukaan on voimassa

$$r_n = \text{syt}(r_{n-1}, r_n) = \text{syt}(r_0, r_1) = \text{syt}(a, b).$$

Näin ollen Eukleideen algoritmi todella antaa lukujen a ja b suurimman yhteisen tekijän. □

Paitsi että Eukleiden algoritmi antaa lukujen a ja b suurimman yhteisen tekijän, niin lisäksi algoritmia hyödyntämällä löydetään ratkaisu yhtälölle $\text{syt}(a, b) = ax + by$. Tämä tapahtuu ”peruuttamalla” lopputuloksesta alkuun. Esimerkissä 1.7 laskettiin $\text{syt}(258, 102) = 6$. Seuraavassa etsitään ratkaisu yhtälölle $6 = 258x + 102y$.

ESIMERKKI 1.9. Tässä esimerkissä ”peruutetaan” Eukleideen algoritmia ja ratkaistaan yhtälö $6 = 258x + 102y$. Luvuille löydettiin suurin yhteinen tekijä esimerkissä 1.7 Eukleideen algoritmin avulla.

Laskettaessa takaperin lähdetään liikkeelle riviltä, jolla suurin yhteinen tekijä on löydetty. Esimerkin 1.7 tapauksessa rivin sisältö on:

$$54 = 1 \cdot 48 + 6.$$

Kirjoitetaan tästä suurin yhteinen tekijä jakojäännöksen ja jakajan lineaarikombinaationa:

$$6 = 54 - 1 \cdot 48.$$

Jatketaan sitten takaperin etenemistä. Luku 48 on esimerkin 1.7 rivin $102 = 1 \cdot 54 + 48$ jakojäännös ja se voidaan esittää lukujen 54 ja 102 lineaarikombinaationa. Näin suurin yhteinen tekijä saadaan muotoon:

$$\begin{aligned} 6 &= 54 - 1 \cdot 48 \\ &= 54 - 1(102 - 54) \\ &= -102 + 2 \cdot 54. \end{aligned}$$

Esimerkin 1.7 ensimmäisellä rivillä, $258 = 2 \cdot 102 + 54$, jakojäännöksenä on 54, jolle on olemassa esitys lukujen 102 ja 258 lineaarikombinaationa. Tämän myötä suurin

yhteinen tekijä on esitettynä lukujen 102 ja 258 lineaarikombinaationa. Samalla alkuperäiselle yhtälölle on löydetty ratkaisu. Alla vielä koko prosessi tiivistettynä. Rivien lopussa on suluissa esimerkin 1.7 Eukleideen algoritmin rivi, jota on käytetty seuraavan vaiheen muodostamisessa.

Yhtälön $6 = 258x + 102y$ ratkaiseminen Eukleideen algoritmin avulla peruuttamalla:

$$\begin{aligned}
& && (54 = 1 \cdot 48 + 6) \\
6 &= 54 - 1 \cdot 48 && (102 = 1 \cdot 54 + 48) \\
&= 54 - 1(102 - 54) \\
&= -102 + 2 \cdot 54 \\
&= -102 + 2(258 - 2 \cdot 102) && (258 = 2 \cdot 102 + 54) \\
&= 2 \cdot 258 - 5 \cdot 102
\end{aligned}$$

Yhtälölle $6 = 258x + 102y$ saadaan siten ratkaisuksi $x = 2$ ja $y = -5$.

Pienillä luvuilla yhtälön $\text{syt}(a, b) = ax + by$ ratkaiseminen edellä esitetyllä tavalla ei vaikuta erityisen työläältä. Operaatioiden määrä on kuitenkin kaksinkertainen Eukleideen algoritmin operaatioiden määrään verrattuna, sillä jokainen rivi käydään läpi kahteen kertaan. Käsiteltäessä huomattavan suuria lukuja kaksinkertaistumisella on merkittävä ero algoritmin tehokkuuteen ja resurssivaatimuksiin.

Algoritmien yhteydessä puhutaan erilaisista resursseista ja valittaessa käytettäviä algoritmeja pohditaan eri resurssien merkittävyyttä. Yleensä tarkasteltava resurssi on algoritmin toteutuksessa kuluva suoritusaika. Se voisi olla myös jokin muu, kuten käytettävän muistin määrä. Tarkasteltavan resurssin kulutusta vertailemalla vertaillaan eri algoritmeja keskenään pyrkimyksenä löytää kuhunkin tilanteeseen sopivin ja tehokkain algoritmi.

Eukleideen algoritmilla saadaan tehokkaasti selville kahden luvun, a ja b, suurin yhteinen tekijä. Algoritmi on hyvin tehokas suurimman yhteisen tekijän selvittämisessä – suurtenkin lukujen kanssa. Suurilla luvuilla operaatioiden määrät kasvavat, mutta operaatiot itsessään ovat kevyitä suorittaa. Mikäli tarkoituksena on löytää sekä suurin yhteinen tekijä, että ratkaisu yhtälölle $\text{syt}(a, b) = ax + by$, tulisi perinteisen Eukleiden algoritmin kaikki vaiheet tallettaa muistiin myöhempää takaperin laskemista varten. Tämä vie turhaa kapasiteettia käytössä olevalta koneelta. Tässä kohtaa onkin hyödyllistä siirtyä käyttämään *laajennettua Eukleideen algoritmia*. Laajennetussa Eukleideen algoritmissa laskuvaiheiden läpi mukana kulkevat käsiteltävän vaiheen lisäksi vain kahden edellisen vaiheen tiedot sekä kahden apumuuttujan tiedot kustakin vaiheesta. Näiden avulla algoritmin lopussa on selvillä suoraan $\text{syt}(a, b)$ sekä x ja y ilman takaperin laskemista – eli huomattavasti pienemmällä muistikapasiteetilla verrattuna perinteiseen Eukleideen algoritmiin. Operaatioiden määräkin on apumuuttujien tallentamista vaille sama kuin perinteisessä Eukleideen algoritmissa.

Lause 1.10 (Laajennettu Eukleideen algoritmi). *Olkoot luvut r_i, q_i ja n kuten Eukleideen algoritmissa (Lause 1.8). Asettamalla*

$$\begin{cases} x_0 = 1, \quad y_0 = 0 \\ x_1 = 0, \quad y_1 = 1 \\ r_i = r_{i-2} - q_i r_{i-1} \\ x_i = x_{i-2} - q_i x_{i-1} \\ y_i = y_{i-2} - q_i y_{i-1} \end{cases}$$

saadaan ratkaisu $x = x_n$, *ja* $y = y_n$ *yhtälölle* $\text{syt}(a, b) = ax + by$.

TODISTUS. Olkoon luvut r_i, q_i ja n kuten Eukleideen algoritmissa (Lause 1.8). Oletetaan sitten, että on olemassa luvut x_i ja y_i joilla $x_i a + y_i b = r_i$. Eukleideen algoritmista saadaan esimerkin 1.9 tavoin palautusta käyttäen yhtälö jakojäännökselle r_i seuraavasti:

$$\begin{aligned} r_i &= r_{i-2} - q_i r_{i-1} \\ &= x_{i-2}a + y_{i-2}b - q_i(x_{i-1}a + y_{i-1}b) \\ &= x_{i-2}a + y_{i-2}b - q_i x_{i-1}a - q_i y_{i-1}b \\ &= (x_{i-2} - q_i x_{i-1})a + (y_{i-2} - q_i y_{i-1})b. \end{aligned}$$

Toisaalta oletuksen mukaan $r_i = x_i a + y_i b$. Valitsemalla nyt $x_i = x_{i-2} - q_i x_{i-1}$ ja $y_i = y_{i-2} - q_i y_{i-1}$ ollaan löydetty palautuskaavan avulla yhtälölle $x_i a + y_i b = r_i$ kertoimet x_i ja y_i indeksille $i \geq 2$. Mikäli löydetään sopivat alkuarvot indekseille $i = 0$ ja $i = 1$ voidaan todeta, että tällä tavoin löytyy sellaiset luvut a ja b joiden lineaarikombinaationa suurin yhteinen tekijä voidaan esittää. Sopivat luvut alkuarvoiksi ovat

$$x_0 = 1, y_0 = 0, x_1 = 0, y_1 = 1,$$

sillä $r_0 = 1 \cdot a + 0 \cdot b = a$ ja $r_1 = 0 \cdot a + 1 \cdot b = b$.

□

ESIMERKKI 1.11. Etsitään ratkaisu yhtälölle $356x + 124y = \text{syt}(124, 356)$. Ratkaisemalla $\text{syt}(124, 356)$ laajennetun Eukleideen algoritmin avulla saadaan luvut x ja y selville. Taulukoidaan luvut x_i, y_i, r_i ja q_i käyttäen yhtälöitä

$$\begin{cases} r_i = r_{i-2} - q_i r_{i-1} \\ x_i = x_{i-2} - q_i x_{i-1} \\ y_i = y_{i-2} - q_i y_{i-1} \end{cases}$$

Alkuvaiheessa taulukko näyttää seuraavalta:

i	r_i	x_i	y_i	q_i
0	356	1	0	-
1	124	0	1	-

Tämän jälkeen selvitetään q_2 katsomalla montako kertaa 124 menee 356, jonka jälkeen käytetään yllä annettuja yhtälöitä. Vastaavasti jatketaan, kunnes $r_i = 0$.

i	r_i	x_i	y_i	q_i
0	356	1	0	-
1	124	0	1	-
2	108	1	-2	2
3	16	-1	3	1
4	12	7	-20	6
5	4	-8	23	1
6	0	31	-89	3

TAULUKKO 1.1

Taulukon 1.1 riviltä $i = 5$ nähdään, että eräs ratkaisu yhtälölle $356x + 124y = \text{syt}(124, 356) = 4$ on $x = -8$ ja $y = 23$. Vastaavasti riviltä $i = 6$ katsottuna $356 \cdot 31 + 124 \cdot (-89) = 0$.

1.4. Kiinalainen jäännöslause

Lukuteoriassa esiintyy paljon erilaisia algoritmeja. Yksi esimerkki, Eukleideen algoritmi, käytiinkin jo läpi. Eräs toinen tunnettu algoritmi, *Kiinalainen jäännöslause*, ja sen johdannaiset ovat myös laajalti käytössä lukuteorian eri sovelluksissa sekä muissa matematiikan haaroissa [**6**, s. 82]. Kiinalaisen jäännöslauseen avulla löydetään ratkaisu kongruenssiryhmälle. Otetaan ensin esimerkki kongruenssiyhtälön ratkaisusta.

ESIMERKKI 1.12. Etsitään ratkaisua yhtälöryhmälle

$$\begin{cases} x \equiv 5 \mod 7 \\ x \equiv 2 \mod 11 \end{cases}.$$

Huomataan, että ensimmäiselle yhtälölle löytyy triviaaliratkaisu $x_1 = 5$. Yhtälön toteuttavat myös kaikki luvut x, joille $x = 5 + 7k,\ k \in \mathbb{Z}$. Sijoittamalla löydetty ratkaisu toiseen yhtälöön saadaan

$$\begin{aligned} 5 + 7k &\equiv 2 \mod 11 \\ \Rightarrow 7k &\equiv -3 \mod 11 \\ \Rightarrow 7k &\equiv 8 \mod 11. \end{aligned}$$

Näin saadusta yhtälöstä voidaan ratkaista k kertomalla yhtälöä puolittain luvun 7 käänteisluvulla mod 11. Onko tällainen luku olemassa? Koska $\text{syt}(7, 11) = 1$, on luku olemassa. Kokeilemalla huomataan käänteisluvun olevan 8, sillä $7 \cdot 8 = 56 \equiv 1 \mod 11$. Näin ollen

$$k \equiv 8 \cdot 8 = 64 \equiv 9 \mod 11.$$

Yhtälöparin ratkaisu on siis $x = 5 + 7k = 5 + 7 \cdot 9 = 68$. Tarkistetaan saatu ratkaisu sijoittamalla se alkuperäiseen yhtälöön:

$$\begin{cases} 68 \equiv 5 \mod 7 \\ 68 \equiv 2 \mod 11 \end{cases}.$$

Yhtälöpari pitää paikkansa, joten löydetty ratkaisu on oikea. Ratkaisu ei kuitenkaan ole yksikäsitteinen, sillä esimerkiksi -9 toteuttaa yhtälöparin myös.

Esimerkissä 1.12 on yksi huomionarvoinen asia, nimittäin $\text{syt}(7, 11) = 1$. Tämä on Kiinalaisen jäännöslauseen oletuksena; kongruenssiyhtälöiden modulien tulee olla keskenään jaottomia.

LAUSE 1.13 (Kiinalainen jäännöslause). *Olkoot $m_1, m_2, \ldots, m_n$ keskenään pareittain jaottomia, toisin sanoen $\text{syt}(m_i, m_j) = 1$ kaikilla $i \neq j$ ja $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Tällöin kongruenssiryhmällä*

$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \\ \vdots \\ x \equiv a_n \mod m_n \end{cases}$$

on ratkaisu $x = c$.
Lisäksi jos $x = c$ ja $x = c'$ ovat molemmat ratkaisuja, niin $c \equiv c' \mod m_1 m_2 \ldots m_n$.

Kiinalaisen jäännöslauseen todistaminen onnistuu esimerkiksi induktion avulla. Tämä tapahtuu osoittamalla ensin esimerkin tavoin, että on olemassa ratkaisu kahdelle ensimmäiselle yhtälölle ja näyttämällä tämä sitten lopuille yhtälöille. Ongelmia syntyy, mikäli $\text{syt}(m_i, m_j) \neq 1$. Lopullinen ratkaisu saa itse asiassa muodon $x = c_1 + m_1 m_2 \ldots m_n k$, kun $c_i + k m_i$ on yksittäisen yhtälön $x \equiv a_i \mod m_i$ ratkaisu. Tämän kaltainen todistus löytyy Rajalan luentomonisteesta [**10**, s. 25]. Hieman eri tavalla todistus löytyy myös Buchmannin [**3**, s.51] tai Hoffstein ym. [**6**, s.83] teoksista.

LUKU 2

Algebraa

Kokonaislukujen lukuteoriaa on hankala käsitellä törmäämättä algebran peruskäsitteisiin. Yksi tällainen on *ryhmä*. Aiemmin mainittiin jäännösluokat ja jäännösluokkarenkaat. Rengas on myös algebrallinen käsite, joka liittyy vahvasti ryhmään. Seuraavassa määritellään ryhmä ja rengas.

MÄÄRITELMÄ 2.1 (Ryhmä). Olkoon G epätyhjä joukko. Paria $(G, \circ)$ sanotaan ryhmäksi, jos se täyttää seuraavat ehdot (1) - (4):

(1) $\circ$ on joukossa G määritelty laskutoimitus, toisin sanoen $a \circ b \in G$ kaikilla $a, b \in G$

(2) $(a \circ b) \circ c = a \circ (b \circ c)$ kaikilla $a, b, c \in G$

(3) on olemassa *neutraalialkio* $e \in G$, jolle

$$e \circ a = a \circ e = a \text{ kaikilla } a \in G$$

(4) jokaiselle alkiolle $a \in G$ on olemassa käänteisalkio a^{-1} jolle pätee

$$a \circ a^{-1} = a^{-1} \circ a = e.$$

Ryhmän sanotaan olevan *kommutatiivinen ryhmä* tai *Abelin ryhmä*, mikäli ehtojen (1)-(4) lisäksi laskutoimitus $\circ$ on kommutatiivinen eli seuraava ehto on voimassa:

(5) $a \circ b = b \circ a$ kaikilla $a, b \in G$.

Ryhmästä $(G, \circ)$ sanotaan, että G on ryhmä. Tällöin G on ryhmä laskutoimituksen $\circ$ suhteen, mutta tämä jätetään monesti erikseen mainitsematta.

ESIMERKKI 2.2. $(\mathbb{Z}, +)$ on ryhmä. Ryhmässä määritelty laskutoimitus on yhteenlasku. Liitäntälaki, ehto (2), on voimassa kokonaislukujen yhteenlaskulle. Neutraalialkiona on luku 0 ja käänteisalkiona luvun vastaluku. Koska yhteenlasku on kommutatiivinen, on $(\mathbb{Z}, +)$ Abelin ryhmä.

Sen sijaan $(\mathbb{Z}_+, +)$ ei ole ryhmä, sillä joukon $\mathbb{Z}_+$ alkioille ei ole olemassa käänteisalkioita joukossa $\mathbb{Z}_+$. Vastaavasti myöskään $(\mathbb{Z}_-, +)$ ei ole ryhmä.

Kokonaislukujen jäännösluokat $\mathbb{Z}_N$ varustettuna yhteenlaskulla ovat Abelin ryhmiä. Olkoot $[a]_N$ ja $[b]_N \in \mathbb{Z}_N$. Tällöin myös $[a]_N + [b]_N = [a+b]_N \in \mathbb{Z}_n$, joten ryhmän ehto 1 pätee. Liitäntälaki, ehto 2, on myös voimassa kaikilla alkioilla $[a]_N \in \mathbb{Z}_N$. Neutraalialkio on $[0]_N$, ja se sisältyy kaikkien kokonaislukujen jäännösluokkiin. Jokaiselle alkiolle löytyy myös käänteisalkio sillä: $[1]_N$ käänteisalkio on $[m]_N$, $[2]_N$ käänteisalkio on $[m-1]_N$ ja niin edelleen kun m on parillinen. Parittoman kokonaisluvun määräämään

jäännösluokan tapauksessa suuruusjärjestyksessä keskimmäisen alkion käänteisalkio on alkio itse. Lisäksi yhteenlasku on mokkutatiivinen kaikilla $[a]_N \in \mathbb{Z}_N$.

Ryhmä on siis systeemi, jossa on määritelty yksi laskutoimitus. Jäännösluokkien sanottiin olevan renkaita. Mitä nämä renkaat sitten ovat?

Rengas R on joukko, jossa on määritelty kaksi laskutoimitusta, jotka toteuttavat niille asetetut ehdot.

MÄÄRITELMÄ 2.3 (Rengas). Kolmikkoa $(R, +, \cdot)$ sanotaan *renkaaksi*, jos sille pätee

(1) $(R, +)$ on Abelin ryhmä

(2) kertolasku $\cdot$ on joukossa R määritelty laskutoimitus

(3) $a(bc) = (ab)c$ kaikilla $a, b, c \in R$

(4) joukossa R on *ykkösalkio* 1, jolle

$$a \cdot 1 = 1 \cdot a = a \text{ kaikilla } a \in R$$

(5) $a(b + c) = ab + ac, (a + b)c = ac + bc$ kaikilla $a, b, c \in R$.

Rengas on *kommutatiivinen rengas*, jos kertolasku on kommutatiivinen, toisin sanoen $ab = ba$ kaikilla $a, b \in R$.

Ryhmään liittyy oleellisesti myös käsite *kertaluku*. Ryhmän G kertaluku on ryhmän alkioiden lukumäärä ja sille käytetään merkintää $\#G$. Huomioitavaa on, että kertaluku ei välttämättä ole äärellinen, esimerkkinä kokonaislukujen muodostama ryhmä. Rajoitutaan nyt kuitenkin tarkastelemaan vain äärellisiä ryhmiä.

Äärellisen ryhmän *alkion kertaluku* on puolestaan pienin sellainen luku, jonka potenssiin alkio korotettuna tuottaa ryhmän neutraalialkion, ts. ryhmän G alkion g kertaluku $d = \min\{k \in \mathbb{N} \mid g^k = e\}$, missä e on ryhmän G neutraalialkio. Ryhmän kertaluvuilla on lukuisia ominaisuuksia, joita hyödynnetään erilaisissa tilanteissa.

LAUSE 2.4. *Olkoon $g \in G$ ja $s \in \mathbb{Z}$ ja e ryhmän G neutraalialkio. Tällöin*

$$g^s = e \text{ jos ja vain jos } s \text{ on jaollinen } g\text{:n kertaluvulla ryhmässä } G.$$

TODISTUS. Olkoon n alkion g kertaluku ryhmässä G. Tällöin pätee $g^n = e$. Jos $s = kn \in \mathbb{Z}$, niin

$$g^s = g^{nk} = (g^n)^k = e^k = e.$$

Oletetaan sitten, että $g^s = e$. Jakoyhtälön nojalla on olemassa kokonaisluvut q ja r siten, että $s = qn + r$ ja $0 \leq r < n$. Siten

$$e = g^s = g^{qn+r} = (g^n)^q g^r = e \cdot g^r = g^r.$$

Kertaluvun määritelmän mukaan n on pienin sellainen alkio, jolla $g^n = e$. Edelleen jakoyhtälön mukaan $r < n$. Siten on oltava $r = 0$, jolloin $s = qn$. Näin ollen s on jaollinen kertaluvulla n. □

ESIMERKKI 2.5. Kokonaislukujen jäännösluokat $\mathbb{Z}_N$ muodostavat kommutatiivisen renkaan. Käydään läpi renkaan ehdot:

(1) $(\mathbb{Z}_N, +)$ on Abelin ryhmä. Tämä on osoitettu edellisessä esimerkissä.

(2) Kertolasku on joukossa $\mathbb{Z}_N$ on kommutatiivinen ja kaikilla $a, b \in \mathbb{Z}_N$ on voimassa $ab = ba \in \mathbb{Z}_N$.

(3) Ok, sillä $a(bc) = (ab)c$ pätee kaikille $a, b, c \in \mathbb{Z}_N$.

(4) Ykkösalkio kertolaskun suhteen joukossa $\mathbb{Z}_N$ on $[1]_N$.

(5) Ok, sillä $a(b + c) = ab + ac, (a + b)c = ac + bc$ pätee kaikilla $a, b, c \in \mathbb{Z}_N$.

Jäännösluokkarenkaan $\mathbb{Z}_N$ alkio $[a]_N$ on kääntyvä jos ja vain jos $\text{syt}(a, N) = 1$ [**3**, s. 36]. Kääntyvien alkioiden ryhmälle käytetään merkintää $\mathbb{Z}_N^*$.

2.1. Eulerin φ-funktio

Määritellään Eulerin φ-funktio seuraavalla tavalla:

MÄÄRITELMÄ 2.6 (Eulerin φ -funktio.). Olkoon $n \in \mathbb{N}$ ja $\Phi_n = \{k \in \mathbb{N} \mid \text{syt}(k, n) = 1, k \leq n\}$. Asetetaan $\varphi(n) = \#\Phi_n$.

Yllä olevan määritelmän mukaan funktio $\varphi(n)$ antaa lukua n pienempien suhteellisten alkulukujen lukumäärän luonnollisten lukujen joukossa.

Eulerin φ -funktiolle on olemassa eräitä tunnettuja laskutapoja. Määritelmästä johtuen funktion arvoista voidaan varmuudella sanoa $1 \leq \varphi(n) \leq n$. Alkuluvuille puolestaan pätee $\varphi(p) = p-1$. Tämä sen vuoksi, että alkuluvulle p on voimassa $\text{syt}(p, p) = p$ ja $\text{syt}(k, p) = 1$ kaikilla $0 < k \leq p - 1$. Näin ollen joukon Φ_p alkioiden lukumäärä on $p - 1$.

Läheskään kaikki luvut eivät ole alkulukuja. Siitä huolimatta Eulerin φ-funktiolle saadaan laskettua arvo. Itse arvon laskemiseksi tarvitsee vain jakaa luku n alkutekijöihin, jonka jälkeen seuraavaa lausetta soveltamalla saadaan $\varphi(n)$ laskettua.

LAUSE 2.7. *Jos $n > 1$, niin*

$$\varphi(n) = n \prod_{p_i | n} \Big(1 - \frac{1}{p_i}\Big),$$

missä luvut p_i ovat alkulukuja, jotka jakavat luvun n. Kun $n = 1$ on $\varphi(n) = \varphi(1) = 1$.

TODISTUS. Tarkoituksena on selvittää niiden lukujen $k < n$ lukumäärä, joille $\text{syt}(k, n) = 1$. Lauseen ensimmäinen kohta, $\varphi(1) = 1$ on selvä. Oletetaan nyt, että $n > 1$ ja tekijöihin jaettuna $n = p_1^{a_1} \dots p_r^{a_r}$. Tällöin $\text{syt}(m, n) > 1$ jos ja vain jos vähintään yhdelle p_i, $1 \leq i \leq r$, on voimassa $p_i \mid m$. Toisin sanoen luvuilla m ja n on vähintään yksi yhteinen tekijä p_i. Olkoon $P = p_1 p_2 p_3 \dots p_r$. Siten $\text{syt}(m, n) > 1$ jos ja vain jos $\text{syt}(m, P) > 1$, sillä lukujen P ja n alkutekijät ovat samat.

Oletetaan sitten, että jollakin $t < n$ pätee $t \mid n$. Tällöin luvun t lukua n pienempien monikertojen lukumäärä on $\frac{n}{t} < n$. Monikerrat ovat $1t, 2t, \ldots, t(\frac{n}{t})$.

Sellaisille alkioille $k < n$, joille $\operatorname{syt}(k, n) = 1$ pätee $p_i \nmid k$ kaikilla i ja niiden lukumäärä saadaan kombinatoriikan (joukko-opin) inkluusio-eksluusio -periaatteen [**8**, luku 10] avulla. Haettava joukko on juuri se joukko, jonka alkioiden lukumäärän $\varphi(n)$ kertoo. Toisaalta poistettavien alkioiden joukko on yhdiste kaikista joukoista, joiden alkiot ovat jaollisia jollain p_i tai sen monikerralla. Näin haettavat joukot voidaan kirjoittaa auki käyttämällä inkluusio-eksluusio -teoreemaa seuraavasti:

$$\varphi(n) = n - \sum_i \big(\frac{n}{p_i}\big) + \sum_{i<j} \big(\frac{n}{p_i p_j}\big) - \sum_{i<j<k} \big(\frac{n}{p_i p_j p_k}\big) + \cdots + (-1)^r \big(\frac{n}{p_i p_2 \ldots p_r}\big).$$

Ottamalla tästä n yhteiseksi tekijäksi ja sieventämällä lauseketta päästään haluttuun tulokseen seuraavasti:

$$\begin{aligned}
\varphi(n) &= n\Big[1 - \sum_i \big(\frac{1}{p_i}\big) + \sum_{i<j} \big(\frac{1}{p_i p_j}\big) - \sum_{i<j<k} \big(\frac{1}{p_i p_j p_k}\big) + \cdots + (-1)^r \big(\frac{1}{p_i p_2 \ldots p_r}\big)\Big] \\
&= n\big(1 - \frac{1}{p_1}\big)\big(1 - \frac{1}{p_2}\big) \ldots \big(1 - \frac{1}{p_r}\big) \\
&= n \prod_{p \mid n} \Big(1 - \frac{1}{p}\Big).
\end{aligned}$$

□

Lauseen 2.7 seurauksena saadaan huomattavasti yksinkertaisempi tapa laskea Eulerin φ-funktiolle arvo kun kyseessä on kahden suhteellisen alkuluvun tulo.

Seuraus 2.8. *Jos* $\operatorname{syt}(p, q) = 1$*, niin* $\varphi(pq) = \varphi(p)\varphi(q)$.

Todistus. Olkoot lukujen m ja n alkutekijöihin jaot seuraavanlaiset:

$$m = p_1 p_2 \ldots p_r \qquad \text{ja} \qquad n = q_1 q_2 \ldots q_s.$$

Koska $\operatorname{syt}(m, n) = 1$, niin kaikille i, j pätee $p_i \neq q_j$. Siten

$$\begin{aligned}
\varphi(mn) &= mn \prod_{p|mn} \big(1 - \frac{1}{p}\big) \\
&= mn \prod_{\substack{p|m \\ q|n}} \big(1 - \frac{1}{p}\big)\big(1 - \frac{1}{q}\big) \\
&= \Big[m \prod_{p|m} \big(1 - \frac{1}{p}\big)\Big]\Big[n \prod_{q|n} \big(1 - \frac{1}{q}\big)\Big] \\
&= \varphi(m)\varphi(n).
\end{aligned}$$

□

LUKU 3

Ketjumurtoluvut

Poiketen muista luvuista on tässä luvussa käytetty pääasiallisina lähteinä Lassi Kuritun luentomonistetta ketjumurtoluvuista [**7**] sekä Hardyn ja Wrightin teoksen [**5**, luku 10] lukua ketjumurtoluvuista.

Ketjumurtoluku α on muotoa

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ldots \cfrac{1}{a_n}}}}.$$

Käytännöllisyyden vuoksi käytetään α:n ketjumurtolukuesityksen merkitsemisessä muotoa

$$\alpha = [a_0, a_1, a_2, \ldots, a_n],$$

missä $a_i \in \mathbb{Z}$ ja $a_i > 0$ kaikilla $i \geq 1$. Luku $\alpha_k = [a_0, a_1, \cdots, a_k], k \leq n$, on ketjumurtoluvun α k:s *konvergentti* ja kokonaisluku a_i on ketjumurtoluvun α i:s *ketjutekijä*.

Positiiviselle rationaaliluvulle α ketjumurtolukuesitys saadaan muodostettua osamäärämuodosta ottamalla ensin kokonaisosa lattiafunktiolla, mikä on ketjumurtoluvun ketjutekijä $a_0 = \lfloor \alpha \rfloor$. Kun rationaaliluvusta α vähennetään ketjutekijä a_0, jää jäljelle ketjutekijää vastaava *jäännösosa* $r_0 = \alpha - a_0$. Seuraava ketjutekijä, a_1, saadaan ottamalla kokonaisosa edellisen ketjutekijän jäännösosan käänteisluvusta $a_1 = \lfloor \frac{1}{r_0} \rfloor$. Tätä vastaava jäännösosa $r_1 = \frac{1}{r_0} - a_1$. Toistamalla seuraavia toimenpiteitä kunnes jäännösosaksi jää 0 saadaan rationaaliluvun α ketjumurtolukuesitys:

> Otetaan jäännösosan $r_i, i \in \mathbb{N}$ käänteisluku $\frac{1}{r_i}$. Tämän kokonaisosa on ketjutekijä $a_{i+1} = \lfloor \frac{1}{r_i} \rfloor$.
>
> Ketjutekijää a_{i+1} vastaava jäännösosa on $r_{i+1} = \frac{1}{r_i} - a_{i+1}$.

Esimerkki 3.1. Esimerkissä 1.11 selvitettiin lukujen 356 ja 124 suurinta yhteistä tekijää. Muodostetaan luvun $\frac{124}{356}$ *ketjumurtolukuesitys*:

Rationaaliluku $\frac{124}{356}$ on osamäärämuodossa ja sen kokonaisosa on $a_0 = \lfloor \frac{124}{356} \rfloor = 0$.

Ketjutekijää a_0 vastaava jäännösosa $r_0 = \frac{124}{356} - a_0 = \frac{124}{356}$. Ketjutekijä a_1 saadaan ottamalla kokonaisosa jäännösosan käänteisluvusta r_0: $a_1 = \lfloor \frac{356}{124} \rfloor = 2$. Tätä vastaava

jäännösosa $r_1 = \frac{356}{124} - 2 = \frac{108}{124}$. Jatketaan vastaavasti:

$$a_2 = \left\lfloor \frac{1}{r_1} \right\rfloor = \left\lfloor \frac{124}{108} \right\rfloor = 1 \qquad r_2 = \frac{1}{r_1} - 1 = \frac{16}{108}$$
$$a_3 = \left\lfloor \frac{1}{r_2} \right\rfloor = \left\lfloor \frac{16}{108} \right\rfloor = 6 \qquad r_3 = \frac{1}{r_2} - 6 = \frac{12}{16}$$
$$a_4 = \left\lfloor \frac{1}{r_3} \right\rfloor = \left\lfloor \frac{16}{12} \right\rfloor = 1 \qquad r_4 = \frac{1}{r_3} - 1 = \frac{4}{12}$$
$$a_5 = \left\lfloor \frac{1}{r_4} \right\rfloor = \left\lfloor \frac{12}{4} \right\rfloor = 3 \qquad r_5 = \frac{1}{r_4} - 3 = 0$$

Jäännösosaksi jäi 0, joten ketjumurtolukuesitys on valmis. Ketjumurtolukuesitys on $\frac{124}{356} = [0, 2, 1, 6, 1, 3]$. Ketjumurtolukuesitys voidaan myös muodostaa pitämällä yhtäsuuruus koko ajan voimassa. Tällöin näkyviin kirjoitetaan kaikki ketjutekijät ja niiden jäännösosat kuten alla on tehty:

$$\frac{124}{356} = \frac{1}{\frac{356}{124}} = \frac{1}{2 + \frac{108}{124}} = \frac{1}{2 + \frac{1}{\frac{124}{108}}} = \frac{1}{2 + \frac{1}{1 + \frac{16}{108}}} = \ldots = \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{6 + \cfrac{1}{1 + \frac{1}{3}}}}}$$

Verrattaessa saatuja ketjutekijöitä esimerkin 1.11 taulukossa 1.1 oleviin q_i:n arvoihin, voidaan huomata yhtenevyyttä. Seuraava lause antaa keinon määritellä konvergentit rekursiivisesti.

Edellä esitetyssä esimerkissä konstruointi saadaan päätökseen ja kyseessä on niin sanottu *päättyvä ketjumurtoluku*. Rationaalilukujen ketjumurtolukukehitelmät ovat päättyviä [**5**, s. 135, Theorem 161]. Rajoitetaan jatkossa rationaalilukujen osalta ketjumurtolukuesityksen tarkastelu siihen asti, kun sellainen on olemassa. Ketjumurtoluvut eivät suinkaan aina ole päättyviä. Tällöin puhutaan päättymättömistä ketjumurtoluvuista. Tällaisia ovat esimerkiksi irrationaalilukujen ketjumurtolukukehitelmät. Jokasella irrationaaliluvulla on yksikäsitteinen ketjumurtolukuesitys. [**5**, s.140, Theorem 170.] Osoittajana voi olla myös jokin muu luku kuin yksi, mutta jätetään nämä tämän tutkielman tarkastelun ulkopuolelle.

LAUSE 3.2. *Olkoot* $p_n, q_n, n \in \mathbb{N} \cup \{0\}, q_n \neq 0$ *ja* a_n *ketjutekijöitä siten, että*

$$p_0 = a_0, \qquad p_1 = a_1 a_0 + 1 \qquad p_n = a_n p_{n-1} + p_{n-2}, \quad \textit{kun } n \geq 2$$
$$q_0 = 1, \qquad q_1 = a_1 \qquad q_n = a_n q_{n-1} + q_{n-2}, \quad \textit{kun } n \geq 2.$$

Tällöin $[a_0, a_1, \cdots, a_n] = \frac{p_n}{q_n}$.

TODISTUS. Lauseen todistus on suoraviivainen induktio, joka jätetään tässä kirjoittamatta. Sekä lause, että todistus, löytyy mm. Hardyn ja Wrightin teoksesta [**5**, s. 130]. □

3.1. Ketjumurtolukujen ominaisuuksia

Ketjumurtoluvuilla on mielenkiintoisia ominaisuuksia, joista on hyötyä esimerkiksi lukuja arvioitaessa. Eräs ominaisuus on, että ketjumurtoluvut ovat aina supistetussa muodossa. Toinen ominaisuus liittyy konvergenttien muodostamiin jonoihin. Indeksöinnin alkaessa nollasta jokainen parittoman indeksin omaava konvergentti, a_{2k+1}, on parillista konvergenttia, a_{2k}, suurempi [**5**, Theorem 153]. Lisäksi parittomien konvergenttien jono lähestyy lukua α ylhäältä päin ja vastaavasti parillisten konvergenttien jono lähestyy lukua α alhaalta päin. Tämä voidaan näyttää osoittamalla molempien jonojen raja-arvojen olevan samat, mikä puolestaan nähdään arvioimalla konvergenttien $\frac{p_{2n+1}}{q_{2n+1}}$ ja $\frac{p_{2n}}{q_{2n}}$ välistä etäisyyttä. Etäisyys saadaan lähestymään lukua 0 annettaessa n:n kasvaa rajatta käyttäen hyväksi arviota $q_n \geq \sqrt{2^{n-1}}$. Konvergenteille siis pätee

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \cdots < \frac{p_{2n}}{q_{2n}} < \frac{p_{2n+2}}{q_{2n+2}} < \cdots < \frac{p_{2n+3}}{q_{2n+3}} < \frac{p_{2n+1}}{q_{2n+1}} < \cdots < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$

Jatkossa oletamme, että indeksointi alkaa luvusta nolla. Seuraava lemma esittelee erään paljon käytetyn ketjumurtolukujen ominaisuuden, jota hyödynnämme mm. konvergenttien etäisyyksien tarkastelussa.

LEMMA 3.3. *Olkoot luvut p_n, q_n määritelty kuten lauseessa 3.2. Tällöin*

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}.$$

TODISTUS. Todistetaan lemma induktiolla. Kun $n = 1$ saadaan lauseen 3.2 määritelmien $p_0 = a_0,\ p_1 = a_1 a_0 + 1,\ q_0 = 1$ ja $q_1 = a_1$ avulla:

$$p_1 q_0 - p_0 q_1 = a_1 a_0 + 1 - a_0 a_1 = 1 = (-1)^{1-1},$$

eli väite pätee. Oletetaan seuraavaksi, että väite pätee, kun $n = k$ jolloin

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}.$$

Osoitetaan väite todeksi n:n arvolla $k + 1$:

$$\begin{aligned} p_{k+1} q_k - p_k q_{k+1} &= (a_{k+1} p_k + p_{k-1}) q_k - p_k (a_{k+1} q_k + q_{k-1}) \\ &= a_{k+1} p_k q_k + p_{k-1} q_k - a_{k+1} p_k q_k - p_k q_{k-1} \\ &= -(p_k q_{k-1} - p_{k-1} q_k) \\ &= -(-1)^{k-1} = (-1)^{k+1-1}. \end{aligned}$$

Näin ollen induktioperiaatteen nojalla väite pätee. □

Tarkastellaan seuraavaksi hieman konvergenttien etäisyyksiä. Kahden peräkkäisen konvergentin erotukselle saadaan lemman 3.3 tulosta hyväksi käyttäen

$$\frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}} = \frac{p_{2n+1} q_{2n} - p_{2n} q_{2n+1}}{q_{2n+1} q_{2n}} = \frac{(-1)^{2n+1-1}}{q_{2n+1} q_{2n}} = \frac{1}{q_{2n+1} q_{2n}}.$$

Aiemmin todettiin, että konvergentit muodostavat suppenevan jonon sekä parillisilla että parittomilla indekseillä ja jonot suppenevat kohti arvoa α. Lisäksi indeksiltään pariton konvergentti on indeksiltään parillista konvergenttia suurempi. Toisin sanoen

$$\frac{p_{2n}}{q_{2n}} \leq \alpha \leq \frac{p_{2n+1}}{q_{2n+1}}. \tag{3.1}$$

Tarkastellaan seuraavaksi konvergenttien etäisyyttä luvusta α. Kun n on parillinen, niin vähentämällä yhtälöstä (3.1) puolittain $\frac{p_{2n}}{q_{2n}}$ saadaan

$$0 \leq \alpha - \frac{p_{2n}}{q_{2n}} \leq \frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}} = \frac{1}{q_{2n+1}q_{2n}}.$$

Parittomien indeksien tapauksessa käytetään parillisena indeksinä $2n+2$. Tällä merkinnällä siis $\frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n+2}}{q_{2n+2}} = \frac{1}{q_{2n+1}q_{2n+2}}$ ja yhtälö (3.1) saa muodon $\frac{p_{2n+2}}{q_{2n+2}} \leq \alpha \leq \frac{p_{2n+1}}{q_{2n+1}}$. Vähentämällä tästä puolittain $\frac{p_{2n+1}}{q_{2n+1}}$ saadaan

$$\frac{p_{2n+2}}{q_{2n+2}} - \frac{p_{2n+1}}{q_{2n+1}} \leq \alpha - \frac{p_{2n+1}}{q_{2n+1}} \leq 0$$

Yhtälön kaikki termit ovat suuruudeltaan pienempiä tai korkeintaan yhtä suuria kuin nolla. Kirjoitetaan yhtälön vasen puoli siten, että pääsemme hyödyntämään lemman 3.3 tulosta esityksessä. Tämä tapahtuu ottamalla ensin -1 yhteiseksi tekijäksi vasemmalla puolella ja sen jälkeen laventamalla luvut saman nimisiksi:

$$\begin{aligned} -\left(\frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n+2}}{q_{2n+2}}\right) &\leq \alpha - \frac{p_{2n+1}}{q_{2n+1}} \\ -\frac{1}{q_{2n+1}q_{2n+2}} &\leq \alpha - \frac{p_{2n+1}}{q_{2n+1}}. \end{aligned}$$

Kun vielä muistetaan molempien puolien olevan suuruudeltaan korkeintaan 0, pätee termien keskinäiselle suuruusjärjestykselle seuraava:

$$\left|\alpha - \frac{p_{2n+1}}{q_{2n+1}}\right| \leq \frac{1}{q_{2n+1}q_{2n+2}}.$$

Yhteenvetona saadaan näytettyä, että seuraavassa lemmassa esitetty väittämä konvergentin etäisyydelle luvusta α indeksin parittomuudesta riippumatta pätee.

Lemma 3.4. *Konvergentin etäisyydelle luvusta α pätee*

$$\left|\alpha - \frac{p_n}{q_n}\right| \leq \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}.$$

Todistus. Lemman ensimmäinen epäyhtälö seuraa suoraan lemmaa edeltävästä päättelystä. Jälkimmäinen epäyhtälö seuraa jonon (q_i) kasvamisesta, minkä vuoksi $q_{i+1} > q_i$ kaikilla $i \in \mathbb{N} \cup \{0\}$. □

Lemma 3.4 on voimassa, kun tiedetään jonkin luvun olevan α:n konvergentti. Mahtaako kyseinen lemma päteä toiseen suuntaan? Ihan sellaisenaan toinen suunta ei päde. Voidaan kuitenkin osoittaa, että mikäli $|\frac{p}{q} - \alpha| < \frac{1}{2q^2}$, niin $\frac{p}{q}$ on jokin α:n konvergenteista. Tämä on mielenkiintoinen tulos mm. siksi, että lukujen α ja q ollessa tiedossa, luvun p päätteleminen ei liene järin vaikeaa – riittää, että muodostetaan α:n konvergentteja. Tätä puolestaan käytetään hyväksi jatkossa pohdittaessa RSA-salauksen murtamista tietyillä lähtökohdilla. Tuloksen todistamista varten käydään läpi aputulos:

LEMMA 3.5. *Olkoot* $\frac{p_n}{q_n}$, $n > 1$ *luvun* α *konvergentteja. Olkoon* $\frac{p}{q} \in \mathbb{Q}$ *siten, että* $\frac{p}{q} \neq \frac{p_n}{q_n}$ *ja* $0 < q \leq q_n$. *Tällöin*

$$|p_n - q_n\alpha| < |p - q\alpha|$$

kun $n > 1$. [**5**, s.151, Theorem 182]

TODISTUS. Voidaan olettaa, että $\frac{p}{q}$ on supistetussa muodossa. Riittää todistaa väite oletuksella $q_{n-1} < q \leq q_n$, sillä lemman 3.4 seurauksena saadaan epäyhtälö $|p_n - q_n\alpha| < |p_{n-1} - q_{n-1}\alpha|$ jolloin alkuperäisen väitteen todistus saadaan induktiolla.

Tarkastellaan ensin tilannetta, jossa $q = q_n$. Tällöin on voimassa

$$\left|\frac{p_n}{q_n} - \frac{p}{q_n}\right| \geq \frac{1}{q_n} \text{ jos } p \neq p_n, \tag{3.2}$$

sillä kahden konvergentin etäisyys toisistaan on vähintään $\frac{1}{q_n}$.

Kuitenkin lemman 3.4 mukaan

$$\left|\frac{p_n}{q_n} - \alpha\right| \leq \frac{1}{q_n q_{n+1}} < \frac{1}{2q_n},$$

sillä jono $(q)_n$ on kasvava. Jos nyt olisi voimassa antiteesi

$$\left|\frac{p_n}{q_n} - \alpha\right| \geq \left|\frac{p}{q_n} - \alpha\right|,$$

niin kolmioepäyhtälön avulla saataisiin yhtälölle (3.2):

$$\left|\frac{p_n}{q_n} - \frac{p}{q_n}\right| \leq \left|\frac{p_n}{q_n} - \alpha\right| + \left|\frac{p}{q_n} - \alpha\right|,$$

josta antiteesin avulla saadaan

$$\begin{aligned}\left|\frac{p_n}{q_n} - \frac{p}{q_n}\right| &\leq 2\left|\frac{p_n}{q_n} - \alpha\right| \\ &< 2 \cdot \frac{1}{2q_n} = \frac{1}{q_n},\end{aligned}$$

mikä on mahdotonta. Siten on oltava $\left|\frac{p_n}{q_n} - \alpha\right| < \left|\frac{p}{q_n} - \alpha\right| \Leftrightarrow |p_n - q_n\alpha| < |p - q_n\alpha|$ ja näin ollen alkuperäinen väite pätee kun $q = q_n$.

Oletetaan sitten, että $q_{n-1} < q < q_n$ ja $\frac{p}{q} \neq \frac{p_{n-1}}{q_{n-1}}, \frac{p_n}{q_n}$. Kirjoitetaan p ja q lineaarikombinaatioina seuraavasti:

$$\mu p_n + \nu p_{n-1} = p \qquad \Rightarrow \mu = \frac{p - \nu p_{n-1}}{p_n} \tag{3.3}$$

$$\mu q_n + \nu q_{n-1} = q \qquad \Rightarrow \nu = \frac{q - \mu q_n}{q_{n-1}}. \tag{3.4}$$

Sijoittamalla saatu ν:n arvo yhtälöön (3.3)

$$\begin{aligned} \mu p_n + \frac{q - \mu q_n}{q_{n-1}} p_{n-1} &= p \\ \mu p_n q_{n-1} + (q - \mu q_n) p_{n-1} &= p q_{n-1} \\ \mu(p_n q_{n-1} - p_{n-1} q_n) &= p q_{n-1} - p_{n-1} q \end{aligned}$$

josta saadaan Lemman 3.3 tulosta hyväksi käyttäen

$$\mu = \pm(p q_{n-1} - p_{n-1} q).$$

Edellä siis $\mu, \nu \in \mathbb{Z} \setminus \{0\}$. Vastaavalla tavalla saadaan myös $\nu = \pm(p q_n - q p_n)$. Alkuperäisen oletuksen mukaisesti $\mu q_n + \nu q_{n-1} = q < q_n$, joten μ ja ν täytyy olla keskenään erimerkkiset. Koska parittomien konvergenttien jono lähestyy lukua α ylhäältä päin ja parittomien alhaalta, luvut $p_n - q_n\alpha$ ja $p_{n-1} - q_{n-1}\alpha$ ovat keskenään erimerkkiset. Näin ollen $\mu(p_n - q_n\alpha)$ ja $\nu(p_{n-1} - q_{n-1}\alpha)$ ovat saman merkkiset. Toisaalta yhtälöiden (3.3) ja (3.4) mukaan on voimassa:

$$\begin{aligned} p - q\alpha &= \mu p_n + \nu p_{n-1} - (\mu q_n + \nu q_{n-1})\alpha \\ &= \mu(p_n - q_n\alpha) + \nu(p_{n-1} - q_{n-1}\alpha). \end{aligned}$$

Tämän vuoksi on oltava

$$|p - q\alpha| > |p_n - q_n\alpha|.$$

Toisin sanoen alkuperäinen väite pätee.

Todistus pätee myös tapauksille $n = 1$ kun vain $q_2 = q_{n+1} \neq 2$. Rajottava tapaus on mahdollista vain, jos $a_1 = a_2 = 1$.

□

Lause 3.6. [**5**, Theorem 184] *Jos*

$$\left|\frac{p}{q} - \alpha\right| < \frac{1}{2q^2}$$

niin $\frac{p}{q}$ *on jokin* α*:n konvergentti.*

Todistus. Olkoot $\frac{p_n}{q_n}$, $n \geq 0$ α:n konvergentit. Määritelmän mukaan $q_0 = 1$ ja $q_n \to \infty$. Voidaan valita sellainen $n \geq 0$, jolle $q_n \leq q \leq q_{n+1}$. Jos nyt $q_n = q$ tai $q_{n+1} = q$, niin väite on selvä.

Oletetaan, että $q \neq q_n, q_{n+1}$. Tällöin Lemman 3.5 mukaan pätee $|q_n\alpha - p_n| < |q\alpha - p|$, jolloin

$$\left|\frac{p_n}{q_n} - \alpha\right| = \frac{1}{q_n}\left|p_n - q_n\alpha\right| < \frac{1}{q_n}\left|q\alpha - p\right| = \frac{q}{q_n}\left|\alpha - \frac{p}{q}\right| < \frac{q}{q_n} \cdot \frac{1}{2q^2} = \frac{1}{2qq_n} \tag{3.5}$$

Jolloin saadaan

$$\left|\frac{p}{q} - \frac{p_n}{q_n}\right| \leq \left|\frac{p}{q} - \alpha\right| + \left|\alpha - \frac{p_n}{q_n}\right| < \left|\frac{p}{q} - \alpha\right| + \frac{1}{2qq_n} < \frac{1}{2q^2} + \frac{1}{2qq_n} \leq \frac{1}{qq_n}.$$

Tässä ensimmäinen epäyhtälö seuraa kolmioepäyhtälöstä, toinen ehdosta (3.5), kolmas oletuksesta ja neljäs oletuksesta $q_n \leq q$. Muotoilemalla tulosta saadaan

$$\left|\frac{p}{q} - \frac{p_n}{q_n}\right| = \left|\frac{pq_n - p_nq}{qq_n}\right| < \frac{1}{qq_n} \Leftrightarrow |pq_n - p_nq| < 1.$$

Huomataan, että $|pq_n - p_nq|$ on kokonaisluku. Lisäksi pätee $|pq_n - p_nq| < 1$, joten on oltava $|pq_n - p_nq| = 0$. Tällöin $\frac{p}{q} = \frac{p_n}{q_n}$ ja edelleen $\frac{p}{q}$ on α:n konvergentti. [**7**, s. 47] $\square$

LUKU 4

RSA

Salausjärjestelmistä puhuttaessa mainitaan usein julkisen ja symmetrisen avaimen salausjärjestelmät. Näistä jälkimmäisellä tarkoitetaan salausmekanismia, jossa viestin salaus ja avaus tapahtuvat samaa avainta käyttäen. Tällöin sekä viestin lähettäjällä, Lassella, että vastaanottajalla, Liisalla, tulee olla tiedossa tarvittava avain. Mikäli avain joutuu jossain vaiheessa vääriin käsiin, pystyy vihollinen, Erkki, sen avulla purkamaan salauksen vaikeuksitta. Symmetristä avainta käytettäessä ongelmakohtana on avaimen vaihto. Liisan ja Lassen pitää pystyä tapaamaan tai olla suojatun linjan kautta yhteydessä toisiinsa saadakseen suoritettua avaimen vaihto turvallisesti.

Liisan ja Lassen ollessa kykenemättömiä kommunikoimaan suojatusti päättää Liisa vuokrata kaupungilta postilokeron, jonne kuka tahansa voi jättää viestin, mutta johon vain Liisalla on avain. Tällöin Lassen ei tarvitse vaihtaa avainta Liisan kanssa, vaan hän voi jättää salaisen viestin Liisan lokeroon. Liisa puolestaan voi noutaa Lassen viestin ja lukea sen. Tämä järjestelmä on turvallinen aina siihen saakka, kunnes Erkki hakee rautakangen ja murtaa laatikon saadakseen Lassen viestin. Liisalla on kuitenkin mahdollisuus kasvattaa suojauksen tasoa esimerkiksi vahvistamalla lokeron rakenteita. Karrikoiden tällä periaatteella toimivat julkisen avaimen salausjärjestelmät.

Matemaattisessa mielessä salausjärjestelmän määritelmä on viiden joukon P, C, K, E ja D kokelma niin, että seuraavat ehdot toteutuvat:

- joukon P alkioita ovat selväkieliset viestit
- joukon C alkioita ovat salakirjoitetut viestit
- joukon K alkioita kutsutaan avaimiksi
- joukko $E = \{E_k \mid k \in K\}$ on kokoelma funktioita selväkielisten viestien joukolta salakirjoitettujen viestien joukolle. Alkioita kutsutaan salausfunktioiksi.
- joukko $D = \{D_k \mid k \in K\}$ on kokoelma funktioita salakirjoitettujen viestien joukolta selväkielisten viestien joukolle. Alkioita kutsutaan avausfunktioiksi.
- jokaiselle $e \in K$ on olemassa $d \in K$ siten, että $D_d(E_e(p)) = p$ kaikille $p \in P$.

Viimeisen ehdon nojalla jokaisen salausfunktion tulee olla injektio.

Yksi ensimmäisistä julkisen avaimen salausjärjestelmistä on Ron Rivestin, Adi Shamirin ja Len Adlemanin kehittämä RSA [**3**]. Kyseinen menetelmä on edelleen laajassa käytössä. Sen salaus perustuu suurien lukujen tekijöihin jaon ongelmaan. Tässä kappaleessa kerrotaan, miten avainten muodostus tapahtuu. Esitellään kuitenkin tähän

liittyen ensin yksi lukuteoriassa usein esiintyvä lause, jota myös RSA-menetelmässä käytetään hyväksi.

4.1. Fermat'n pieni lause

Fermat'n pienestä lauseesta näkee muutamiakin eri muotoja, ja se on laajalti käytössä lukuteorian saralla. Yksi yleisesti käytetty lauseen sovellus on Fermat'n alkulukutesti.

LAUSE 4.1 (Fermat'n pieni lause). *Olkoot p alkuluku ja $a \in \mathbb{Z}$. Tällöin*

$$a^{p-1} = \begin{cases} 1 \mod p, & \text{jos } p \nmid a \\ 0 \mod p, & \text{jos } p \mid a \end{cases}.$$

TODISTUS. Jos $p \mid a$, niin selvästikin jokainen a:n potenssi on myös jaollinen luvulla p. Näin ollen riittää tarkastella tilannetta, jossa $p \nmid a$. Tarkastellaan luvun p jäännösluokkia

$$a, 2a, 3a, 4a, \ldots, (p-1)a.$$

Listalla on kaiken kaikkiaan $p-1$ kappaletta eri jäännösluokkien edustajia. Osoitetaan ensin, että jokainen jäännösluokan edustaja eri. Otetaan jäännösluokkien edustajat, la ja ka, $l \neq k$, ja oletetaan niiden olevan samat. Tällöin

$$la \equiv ka \mod p$$

ja edelleen $(l-k)a \equiv 0 \mod p$. Tästä huomataan, että $p \mid (l-k)$ sillä oletuksen mukaan $p \nmid a$. Toisaalta luvuille l ja k on voimassa

$$1 \leq l \text{ ja } k \leq p-1,$$

joten niiden erotukselle pätee

$$-(p-2) \leq l-k \leq p-2.$$

Välillä $[-(p-2), p-2]$ on vain yksi luku, joka on jaollinen luvulla p – nolla. Näin ollen täytyy olla $l-k=0$, jolloin $l=k$. Siispä jäännösluokat $a, 2a, 3a, 4a, \ldots, (p-1)a$ ovat kaikki eri luokkia ja väliltä $[1, p-1]$.

Tarkastellaan seuraavaksi jäännösluokkien $a, 2a, 3a, 4a, \ldots, (p-1)a$ tulon kongruenssiyhtälöä modulo p:

$$a \cdot 2a \cdot \cdots \cdot (p-1)a \equiv 1 \cdot 2 \cdot \ldots (p-1) \mod p.$$

Yhtälön vasemmalla puolella on $p-1$ kappaletta lukua a. Tämän vuoksi yhtälö voidaan kirjoittaa yhtäpitävästi muodossa

$$a^{p-1}(p-1)! \equiv (p-1)! \mod p.$$

Koska $\text{syt}(p, k) = 1$ kaikilla $k = 1, \ldots, p-1$, voidaan yhtälö jakaa puolittain termillä $(p-1)!$ jolloin saadaan

$$a^{p-1} \equiv 1 \mod p.$$

□

HUOMAUTUS 4.2. Fermat'n pieni lause voidaan muotoilla myös seuraavasti:

$$\text{Jos } \text{syt}(a, m) = 1, \text{ niin } a^{\varphi(m)} \equiv 1 \mod m.$$

Huomautuksessa 4.2 on kyseessä Eulerin yleistys Fermat'n pienelle lauseelle. Fermat ei itse koskaan todistanut pientä lausettaan, vaan ensimmäisenä sen todisti Euler vuonna 1736. Myöhemmin Euler todisti tämän huomautuksen yleisemmän muodon Fermat'n pienestä lauseesta käyttäen apunaan φ-funktiota. [**2**, s. 642].

4.2. RSA avainten muodostus

Implementointinsa puolesta RSA on suoraviivainen. Lasse haluaa lähettää Liisalle viestin m käyttäen RSA-salausta. Salaukseen tarvitaan *julkinen avain*, pari (N, e) sekä *salainen avain d*. Liisa valitsee aluksi suuret *alkuluvut* p ja q, $p \neq q$. Nämä ovat *RSA-tekijät*, joiden avulla saadaan laskettua *RSA-moduli* $N = pq$. Tämän lisäksi Liisa valitsee luvun e, *salauseksponentin*, siten, että $1 < e < \varphi(N) = (p-1)(q-1)$ ja $\text{syt}(e, \varphi(N)) = 1$. Seuraavaksi Liisa laskee salaisen avaimen d, *avausekponentin*, jolle $1 < d < \varphi(N)$ ja $de \equiv 1 \mod \varphi(N)$. Avaimen d laskeminen käy kätevästi Eukleideen laajennetun algoritmin avulla, sillä $\text{syt}(e, \varphi(N)) = 1$. Liisa lähettää Lasselle julkisen avaimen (N, e).

Lasse salaa viestinsä m käyttäen julkista avainta. Viestin m tulee olla väliltä $[0, N-1]$, jotta se saadaan yksikäsitteisesti salattua ja purettua. *Salattu viesti* on $c = m^e \mod N$, jonka Lasse lähettää Liisalle. Liisa saa alkuperäisen viestin selville käyttäen salaista avaintaan d Lassen lähettämään viestiin, sillä $m \equiv c^d \mod N$.

Taulukossa 4.1 [**6**, s. 119] on esitetty pelkistetysti RSA salauksen vaiheet. Vaiheita on vain muutama, mutta silti viestin väitetään välittyvän salattuna. Käydään seuraavassa läpi hieman perusteita tälle.

Alkuluvut p ja q ovat vapaasti valittavissa. Mikäli salauksen halutaan kestävän myös lähitulevaisuudessa, tulisi RSA-modulin olla nykyarvioiden mukaan minimissään lyhyellä aikavälillä suuruusluokkaa 3072 bittiä ja pidemmällä aikavälillä jopa 15360 bitin suuruusluokkaa [**4**, s. 32-37]. Tämä vaikuttaa osaltaan lukujen p ja q valintaan. Julkisen avaimen salauseksponentin e on oltava pariton, sillä $\varphi(N) = (p-1)(q-1)$ on aina parillinen. Siten pienin $e = 1$, jolloin myös $d = 1$, minkä seurauksena salattu viesti on sama kuin alkuperäinen – salausta ei edes tapahdu! Näin ollen pienin käyttökelpoinen salauseksponentti on $e = 3$. Valinnalla $e = 2^{16}+1 = 65537$ pystytään välttämään eräitä hyökkäyksiä menettämättä kuitenkaan laskennallista etua pienestä eksponentista. Salauseksponentin e valinnan jälkeen saadaan salainen avain d laskettua. Myöhemmin

Liisa	Lasse
Avaimen muodostus	
Valitsee salaiset alkuluvut p ja q. Valitsee salausekseponentin e. Julkaisee avainparin $N = pq$ ja e.	
	Valitsee viestin m. Käyttää Liisan julkista avainta (N, e) ja laskee $c \equiv m^e \bmod N$. Lähettää salatun viestin c Liisalle.
Laskee salaisen avaimen d jolle $ed \equiv 1 \bmod \varphi(N)$. Laskee $m' \equiv c^d \bmod N$. Saa selville alkuperäisen viestin, $m' = m$.	

TAULUKKO 4.1. RSA salauksen kulku

tullaan kertomaan miksi on turvallisempaa valita pieni salausekseponentti e ja suuri avausekseponentti d eikä päinvastoin.

Viestiä m salattaessa suoritetaan toimenpide $c = m^e \bmod N$. Miksi avaus onnistuu avausekseponentilla d? Tähän saadaan vastaus seuraavasta lauseesta.

LAUSE 4.3. *Olkoon (e, N) julkinen RSA avain ja d sitä vastaava salainen avain. Tällöin*

$$(m^e)^d \mod N = m$$

kaikille kokonaisluvuille m, joille $0 \leq m < N$.

TODISTUS. [**3**, s.145] Luvuille e ja d on voimassa $ed \equiv 1 \bmod \varphi(N)$. Siten on olemassa kokonaisluku l, jolle $ed = 1 + l\varphi(N)$. Ja näin ollen

$$(m^e)^d = m^{ed} = m^{1+l\varphi(N)} = m(m^{\varphi(N)})^l.$$

Muistettaessa että $\varphi(N) = (p-1)(q-1)$ saadaan

$$(m^e)^d \equiv m\Big((m^{p-1})^{q-1}\Big)^l \equiv m \mod p. \tag{4.1}$$

Jos p ei jaa lukua m, niin yhtälö (4.1) tulee Fermat'n pienen lauseen 4.1 nojalla. Mikäli p puolestaan jakaa luvun m, niin ovat yhtälön (4.1) molemmat puolet kongruentteja luvun 0 kanssa mod p. Vastaavalla tavalla saadaan

$$(m^e)^d \equiv m \mod q$$

Koska p ja q ovat keskenään jaottomia, $\text{syt}(p, q) = 1$, niin

$$(m^e)^d \equiv m \mod N$$

kun $0 < m < N$. □

Yllä oleva näyttää myös sen, että RSA-menetelmä todellakin on salaus salauksen määritelmän mukaan. Menetelmän salaavuus nojaa vahvasti salaisen avaimen d tuntemattomuuteen ja sen selvittämiseen. Tämä on yhtä hankalaa kuin tekijöiden p ja q selvittäminen RSA-modulista. Tekijöiden selvittäminen puolestaan on tunnettu matemaattinen ongelma, joka nykyisillä tiedoilla on huomattavan hankalaa suurien lukujen tapauksessa. Mikäli tekijöiden selvittämiseen löydetään jokin tehokas tapa, nujertaa se samalla RSA-salauksen.

LUKU 5

RSA-salauksen haavoittuvuuksia

RSA on julkaistu ensimmäisen kerran vuonna 1977 [**1**]. Näin ollen sen heikkouksia on tutkittu jo pitkään — löytämättä selkeää Akilleen kantapäätä. Aikojen saatossa RSA-menetelmästä on kuitenkin löydetty aukkoja, joita pystytään välttämään kiinnittämällä huomiota salauksessa käytettyjen lukujen valintaan. Käytettävissä olevan laskukoneiston tehon kasvaminen näkyy suoraan julkisen avaimen suuruudessa.

5.1. Tekijöiden p ja q valinta

Alkuluvut p ja q ovat RSA-salauksen toimivuuden kannalta vapaasti valittavissa. Kuitenkin on suositeltavaa, että molemmat luvut ovat samaa suuruusluokkaa, koska toisen ollessa suuri on toinen väistämättä pieni RSA-avaimen N pysyessä samana. Pieneen lukuun pääsee kohtalaisessa ajassa käsiksi kokeilemalla pieniä alkulukuja järjestyksessä — toisen luvun löytyessä ovat molemmat löytyneet.

Toisaalta, luvut eivät saa olla myöskään ”liian lähellä” toisiaan, koska silloinkin niiden löytäminen on helpohkoa. Tähän liittyy seuraava yhtälö:

$$\left(\frac{p+q}{2}\right)^2 + \left(\frac{p-q}{2}\right)^2 = N.$$

Määritellään kokonaisluvut $t := \frac{p+q}{2}$ ja $k := \frac{p-q}{2}$ jolloin edellä esitetty yhtälö saa muodon $N-k^2 = t^2$. Mikäli p ja q ovat lähellä toisiaan, on k lähellä nollaa. Tällöin k:n arvo saadaan selville yksinkertaisesti kokeilemalla arvoja $k = 1, 2, 3, \ldots, k_i$ ja katsomalla milloin $N - k_i^2$ antaa jonkin luvun neliön. Tämän testaaminen on nykyisin käytössä olevalla laskentakapasiteetilla ja aiemmin esiteltyä nopeaa potenssilaskua hyödyntäen nopea lasku, vaikka kyseessä saattavatkin olla suuret luvut. Neliön löytyessä saadaan tekijät p ja q selville.

5.2. Tekijöiden p ja q selvittäminen avauseksponentin d avulla

Aiemmin mainittiin, että salaisen avaimen d tuntemattomuus ja sen selvittäminen on yhtä hankalaa kuin tekijöiden p ja q selvittäminen RSA-modulista. Seuraavassa käydään tätä hieman läpi. Mikäli tekijät p ja q ovat tiedossa, saadaan salainen avain d selville julkisen avaimen salauseksponentin ja yhtälön $de \equiv 1 \mod \varphi(N)$ avulla. Toisaalta, mikäli d on tiedossa, saadaan sen avulla RSA-modulin tekijät p ja q hyvällä todennäköisyydellä selville yksinkertaisen algoritmin avulla.

Määritellään jatkoa varten luku k seuraavanlaisesti:

MÄÄRITELMÄ 5.1. Olkoon $s = \max\{t \in \mathbb{N} : 2^t \text{ jakaa luvun } ed-1\}$ ja

$$k = \frac{ed-1}{2^s}.$$

Määritelmässä 5.1 päädytään itse asiassa supistettuun muotoon luvusta k. Osoittajana oleva luku $ed-1$ on aina parillinen, sillä luvut e ja d ovat parittomia johtuen RSA-salauksessa käytetystä menetelmästä. Jaetaan lukua $ed-1$ luvulla 2 kunnes osoittajaan jää pariton luku. Jakojen lukumäärän kertoo nimittäjän eksponentti s. Tällä tavalla saatu luku on määritelmän mukainen k.

Seuraavaksi esitellään aputulos lauseelle ja itse lause, johon tekijöiden p ja q selvittämiseen käytetty algoritmi pohjautuu.

LEMMA 5.2. *Jokaiselle a, jolle $\text{syt}(a, N) = 1$, jäännösluokan $[a^k]_N$ kertaluku jäännösluokkaryhmässä $\mathbb{Z}_N^*$ on muotoa 2^i, missä $0 \leq i \leq s$ ja s on määritelmän 5.1 mukainen.*

TODISTUS. [**3**, s.147] Olkoot $a \in \mathbb{Z}$ ja RSA-moduli N keskenään jaottomia. Lauseen 4.3 mukaan

$$[a]^{ed-1} = [a]^{ed} \cdot [a]^{-1} = [a] \cdot [a]^{-1} = 1 \in \mathbb{Z}.$$

Tämä voidaan esittää muodossa $[a^k]^{2^s} = 1$, sillä k:n määritelmän 5.1 mukaan $ed-1 = k2^s$. Näin ollen Lauseen 2.4 nojalla $[a]^k$:n kertaluku jäännösluokkaryhmässä $\mathbb{Z}_{\mathbb{N}}^*$ jakaa luvun 2^s ja 2^s:n jokainen tekijä on muotoa $2^i, i \leq s$. □

LAUSE 5.3. *Olkoon $a \in \mathbb{Z}$, jolle $\text{syt}(a, N) = 1$. Jos luvulla a on eri kertaluvut* mod p *ja* mod q, *niin $1 < \text{syt}(a^{2^t k} - 1, N) < N$ jollakin $t \in \{0, 1, 2, \ldots, s-1\}$.*

TODISTUS. Lemman 5.2 ja lauseen 2.4 mukaan a^k:n kertaluvut mod p ja mod q kuuluvat joukkoon $\{2^i : 0 \leq i \leq s\}$. Olkoon 2^l luvun a^k kertaluku mod p ja 2^t luvun a^k kertaluku mod q. Oletetaan lisäksi, että $2^t < 2^l$. Tämä voidaan olettaa, sillä luvut ovat erisuuria alkuperäisen oletuksen mukaan. Tällöin $t < s$ ja $a^{2^t k} \equiv 1 \mod q$, mutta $a^{2^t k} \not\equiv 1 \mod p$. Siten $\text{syt}(a^{2^t k} - 1, N) = q$. □

Algoritmi, jota käyttäen tekijät p ja q yritetään selvittää, kun tiedossa on salainen avain d, löytyy Buchmannin teoksesta [**3**, s. 147] ja on seuraavanlainen:

(1) Valitaan kokonaisluku a joukosta $\{1, \ldots, N-1\}$.

(2) Lasketaan $g = \text{syt}(a, N)$.

(3) Lasketaan, ellei ole jo laskettu, $k = \frac{ed-1}{2^s}$, missä $s = \max\{t \in \mathbb{N} : 2^t \text{ jakaa luvun } ed-1\}$.

(4) Jos $g = 1$, lasketaan $g = \text{syt}(a^{2^t k} \mod N, N)$ järjestyksessä $t = s-1, s-2, \ldots$ jatkaen kunnes $g > 1$ tai $t = 0$.

(5) Mikäli $g > 1$, niin $g = p$ tai $g = q$. Tällöin RSA-modulin N tekijät on löydetty ja algoritmi loppuu. Muussa tapauksessa algoritmi ei toiminut kyseisellä alkuarvolla a.

Salaista avainta d tarvitaan oleellisesti luvun k määrittämiseen. Luku k puolestaan on oleellisessa osassa koko algoritmissa. Mikäli algoritmi ei mene ensimmäisellä valitulla luvulla a_1 läpi, suoritetaan se toiselle luvulle $a_2 \neq a_1$. Läpikäynti on nopeaa, sillä suoritettavia laskutoimituksia ovat neliöinti, sekä suurimman yhteisen tekijän selvittäminen.

Miten monta kertaa algoritmia joudutaan toistamaan? Todennäköisyys sille, että algoritmi onnistuu on vähintään $\frac{1}{2}$ [**3**, s. 147]. Mikäli algoritmia joudutaan toistamaan r kertaa, on onnistumistodennäköisyys vähintään $1 - \frac{1}{2^r}$, eli varsin hyvä. Näin ollen voidaan sanoa, että salaisen avaimen d tai tekijöiden p ja q tunteminen ovat saman arvoiset. Toisen avulla saa toisen selville.

5.3. Yhteinen moduli

Oletetaan, että RSA-salauksen avaimet luo ja jakaa jokin luotettava taho. Tämä taho on laskenut RSA-modulin N ja antaa käyttäjälle i avaimet (e_i, N) ja d_i. Kertaalleen laskettua modulia hyödyntäen annetaan seuraavalle käyttäjälle j avaimet (e_j, N) ja d_j. Selvästikään käyttäjä i ei saa selville käyttäjän j avaimella salattua viestiä $c_j = m^{e_j}$ käyttämällä omaa salaista avaintaan d_i.

Salaus näyttäisi olevan kunnossa. Kuten on näytetty, salaisen avaimen d selvittäminen on yhtä vaikeaa kuin RSA-modulin N tekijöihin jakaminen. Käytettäessä samaa modulia usealla eri avaimella saa käyttäjä i salaus- ja avauseksponenttiensa d_i ja e_i avulla RSA-modulin N tekijät selville. Tämän jälkeen käyttäjä i saa salaisen avaimen d_j selville julkisen avainparin e_j:n avulla.

Vastaava ongelma piilee myös lähetettäessä viesti useaan kertaan käyttäen samaa RSA-modulia ja salauseksponentteja e_i ja e_j, $i \neq j$. Oletetaan, että Erkki nappaa salatut viestit $c_i = m^{e_i}$ ja $c_j = m^{e_j}$ Lassen lähettäessä näitä eri vastaanottajille. Jos Erkillä on lisäksi tiedossa salauseksponentit e_i ja e_j pystyy hän selvittämään kokonaisluvut u ja v yhtälöstä

$$e_i u + e_j v = \mathrm{syt}(e_i, e_j)$$

esimerkiksi laajennetulla Eukleideen algoritmilla. Edelleen Erkki voi käyttää saamaansa tietoa hyväkseen ja laskea

$$c_i^u \cdot c_j^v \equiv (m^{e_i})^u \cdot (m^{e_j})^v \equiv m^{e_i u + e_j v} \equiv m^{\mathrm{syt}(e_i, e_j)} \mod N.$$

Jos $\mathrm{syt}(e_i, e_j) = 1$ saa Erkki alkuperäisen viestin $m = m^{\mathrm{syt}(e_i, e_j)}$ selville suoraan selvittämättä salaista avainta tai RSA-modulin tekijöitä.

Entäpä jos käytetään samaa salauseksponenttia e mutta eri RSA-modulia? Saman viestin lähettämisessä on tällöinkin omat vaaransa. Mikäli Erkki on tietoinen, että

viestit ovat samat, saa hän kiinalaisen jäännöslauseen (Lause 1.13) avulla alkuperäisen viestin selville. Tämän edellytyksenä toki on, että RSA-modulit ovat keskenään jaottomia. Saadakseen viestin tällä tavoin varmasti selville, tarvitsee Erkki e kappaletta viestejä. Toisin sanoen, jos salauseksponentti e on pieni, riittää Erkille pieni määrä viestejä. Tämän vuoksi ei ole kannattavaa käyttää salauseksponenttina pientä lukua, vaikka se ei muutoin salausta merkittävästi heikentäisikään.

5.4. Pieni salainen avain d

Pienentääkseen salauksen purkamiseen kuluvaa aikaa houkutus pieneen avauseksponenttiin d on suuri. Erityisesti pieni salainen avain houkuttelee mikäli kyseessä on jokin laskentateholtaan pienehkö laite, kuten älykortti. Valitettavasti tähän tilanteeseen on olemassa tehokas hyökkäys, jonka avulla salaus saadaan murrettua. Kyseisen hyökkäyksen estämiseksi riittää tarkistaa, että avauseksponentti $d \geq \frac{1}{3}N^{\frac{1}{4}}$. Ennen ehdon riittävyyteen perehtymistä esitellään M. Wienerin ketjumurtolukujen ominaisuuksia hyödyntävä algoritmi, joka antaa keinon konvergentin arvaamiseen.

5.4.1. Wienerin algoritmi. Wienerin algoritmi itsessään ei anna varmuutta löydetyn luvun oikeellisuudesta vaan tarvitsee aina testin tuloksen soveltuvuuden varmistamiseksi. Algoritmin avulla on kuitenkin mahdollista muodostaa arvaus, joka onnistuu osuessaan riittävän lähelle.

Olkoon α' arvio alhaaltapäin luvulle α jollakin virheellä $\delta \geq 0$:

$$\alpha' = \alpha(1 - \delta).$$

Olkoot a_i, r_i ja a'_i, r'_i ketjumurtolukujen α ja α' i:nnet ketjutekijät ja niitä vastaavat jäännösosat. Virheen δ ollessa tarpeeksi pieni, voidaan luvun α osamäärämuoto löytää toistamalla seuraavaa algoritmia kunnes α löydetään. Algoritmi lähtee liikkeelle arvosta $i = 0$.

(1) Etsitään i:s ketjutekijä a'_i luvun α' ketjumurtolukuesitykseen.

(2) Konstruoidaan konvergentin α_i murtolukuesitys seuraavasti

$$\alpha_i = [a'_0, a'_1, \ldots, a'_i + 1] \text{ jos } i \text{ on parillinen,}$$

$$\alpha_i = [a'_0, a'_1, \ldots, a'_i] \text{ jos } i \text{ on pariton.}$$

(3) Testataan onko saatu konvergentti $[a'_0, a'_1, \ldots, a'_i]$ yhtenevä haetun luvun f kanssa.

Syy, jonka vuoksi algoritmin kohdassa (2) indeksiltään parillisien konvergenttien ketjutekijään lisätään 1 on se, että arvattavan luvun α tulee olla suurempi, kuin arvauksen α'. Parilliset konvergentit ovat itsessään aina lukua α pienempiä. Aiemmin mainittiin, että arvaus onnistuu osuessaan riittävän lähelle. Riittävän lähellä ollaan mikäli

$$[a_0, a_1, \ldots, a_{m-1}, a_m - 1] < \alpha' \leq [a_0, a_1, \ldots, a_{m-1}, a_m - 1], m \text{ parillinen}$$

$$[a_0, a_1, \ldots, a_{m-1}, a_m + 1] < \alpha' \leq [a_0, a_1, \ldots, a_{m-1}, a_m - 1], m \text{ pariton.}$$

Siitä, miksi tämä on riittävän lähellä, voi lukea lisää M. Wienerin artikkelista [**11**, s. 554]

Palataan sitten tarkastelemaan sitä, miksi salaisen avaimen d rajaksi käy $\frac{1}{3}N^{\frac{1}{4}}$, missä $N = pq$. Olkoon $d < \frac{1}{3}N^{\frac{1}{4}}$. Oletetaan lisäksi, että $q < p < 2q$. Tämä on järkevä oletus, sillä RSA-salauksen toimivuuden vuoksi lukujen p ja q tulisi olla suuruudeltaan lähellä toisiaan, mutta samalla myös mahdollisimman etäällä toisistaan. Käytettäessä suuria lukuja, ero lukujen q ja $2q$ välillä on suuri, jolloin periaate ei toteudu ellei $q < p < 2q$.

RSA-salauksessa $de = 1 \mod \varphi(N)$, joten on olemassa kokonaisluku K siten, että $de - K\varphi(N) = 1$. Jakamalla yhtälö puolittain luvulla $d\varphi(N)$ saadaan

$$\Big|\frac{e}{\varphi(N)} - \frac{K}{d}\Big| = \frac{1}{d\varphi(N)}. \tag{5.1}$$

Yhtälössä (5.1) sanotaan luvun $\frac{K}{d}$ olevan likiarvo luvulle $\frac{e}{\varphi(N)}$ tarkkuudella $\frac{1}{d\varphi(N)}$. Lähdetään tutkimaan arvion tarkkuutta.

Kirjoitetaan aluksi yhtälö (5.1) arvioiden lukua $\varphi(N)$ luvulla N sekä tiedon $1 = de - K\varphi(N)$ avulla seuraavasti:

$$\Big|\frac{e}{N} - \frac{K}{d}\Big| = \Big|\frac{de - KN}{dN}\Big|.$$

Lisätään sitten oikealle puolelle osoittajaan 0 muodossa $K\varphi(N) - K\varphi(N)$ ja otetaan näin saadusta osoittajasta $de - KN + K\varphi(N) - K\varphi(N)$ termeille $-KN$ ja $K\varphi(N)$ luku $-K$ yhteiseksi tekijäksi saaden

$$\Big|\frac{e}{N} - \frac{K}{d}\Big| = \Big|\frac{de - K\varphi(N) - K(N - \varphi(N))}{dN}\Big|. \tag{5.2}$$

Tutkitaan seuraavaksi lukujen N ja $\varphi(N)$ erotusta. Tekijöiden p ja q valinnan oletuksesta $q < p < 2q$ seuraa $q^2 < pq < p^2 < 4q^2$. Käyttämällä Eulerin φ-funktion laskukaavaa $\varphi(N) = (p-1)(q-1) = N-p-q+1$ sekä esitettyä arviota saadaan

$$N - \varphi(N) = p + q - 1 < p + \sqrt{pq} - 1, \tag{5.3}$$

sillä epäyhtälön $q^2 < pq$ seurauksena $0 < q < \sqrt{pq}$.

Keskitytään sitten luvun p arviointiin oletuksen $q < p < 2q$ avulla. Koska $p < 2q$, niin kertomalla tämä puolittain luvulla p saadaan $p^2 < 2pq$. Tämän seurauksena on edelleen voimassa $p < \sqrt{2pq} < 2\sqrt{pq}$. Soveltamalla tätä yhtälöön (5.3) saadaan

$$\begin{aligned} N - \varphi(N) &< p + \sqrt{pq} - 1 \\ &< 2\sqrt{pq} + \sqrt{pq} - 1 \\ &< 3\sqrt{pq} = 3\sqrt{N}. \end{aligned} \tag{5.4}$$

Yhtälössä (5.2) on oikealla puolella osoittajan loppuosassa esillä termi $N - \varphi(N)$, johon voidaan käyttää kohdan (5.4) arviota. Käyttämällä lisäksi osoittajan alkuosaan

tietoa $de - K\varphi(N) = 1$ saadaan yhtälöstä (5.2) seuraavan näköinen:

$$\left|\frac{e}{N} - \frac{K}{d}\right| < \left|\frac{1 - K3\sqrt{N}}{dN}\right| \leq \frac{3K\sqrt{N}}{dN}. \tag{5.5}$$

Toisaalta $K\varphi(N) = de - 1 < de$ ja $e < \varphi(N)$. Tällöin $K < d$, joten oletuksia hyväksi käyttäen saadaan $K < d < \frac{1}{3}N^{\frac{1}{4}}$. Näin ollen termin $\frac{e}{\varphi(N)}$ arvion tarkkuudelle luvulla $\frac{K}{d}$ saadaan lopulta seuraavaa:

$$\left|\frac{e}{N} - \frac{K}{d}\right| \leq \frac{3K}{d\sqrt{N}} \leq \frac{1}{dN^{\frac{1}{4}}} < \frac{1}{2d^2}.$$

Tämä arvio on merkittävä sen vuoksi, että mikäli $\left|x - \frac{a}{b}\right| < \frac{1}{2b^2}$, niin luku $\frac{a}{b}$ on luvun x konvergentti [**5**, Th. 184]. Toisin sanoen $\frac{K}{d}$ saadaan luvun $\frac{e}{N}$ konvergenttina edellyttäen, että $\frac{K}{d}$ on supistetussa muodossa. Luvun arvaamisessa hyödynnetään M. Wienerin algoritmia. Sitä ennen pitää kuitenkin vielä huomioida konvergenttien supistettu muoto.

Konvergentit ovat aina supistetussa muodossa. Luvun d selvittämiseksi täytyy varmistua, että konvergenttina haettava luku on supistetussa muodossa. Edellä olevan arvion luku $\frac{K}{d}$ ei sitä välttämättä ole. Esitetään se hieman eri muodossa. Koska $de \equiv 1 \bmod \varphi(N)$ ja $\varphi(N) = (p-1)(q-1)$ on tulon de jäännösluokka 1 myös lukujen $p-1$ ja $q-1$ pienimmän yhteisen jaettavan suhteen, $de \equiv 1 \bmod \text{pyj}(p-1, q-1)$. Näin ollen on olemassa K', jolle

$$de = K' \cdot \text{pyj}(p-1, q-1) + 1.$$

Olkoot G lukujen $p-1$ ja $q-1$ suurin yhteinen tekijä, $G = \text{syt}(p-1, q-1)$. Kahden luvun suurimmalle yhteiselle tekijälle ja pienimmälle yhteiselle jaettavalle on voimassa $\text{pyj}(p-1, q-1) = \frac{(p-1)(q-1)}{\text{syt}(p-1,q-1)}$, jolloin saadaan seuraavaa:

$$\begin{aligned} de &= K' \frac{(p-1)(q-1)}{\text{syt}(p-1, q-1)} + 1 \\ &= \frac{K'}{G}(p-1)(q-1) + 1. \end{aligned}$$

Vielä ei kuitenkaan ole varmaa, että $\frac{K'}{G}$ olisi supistetussa muodossa. Määritellään luvut $k = \frac{K'}{\text{syt}(K', G)}$ ja $g = \frac{G}{\text{syt}(K', G)}$, jolloin $\frac{k}{g}$ on luvun $\frac{K'}{G}$ supistettu muoto ja

$$de = \frac{k}{g}(p-1)(q-1) + 1. \tag{5.6}$$

Jakamalla tämä vielä puolittain luvulla dpq saadaan

$$\frac{e}{pq} = \frac{k}{dg}(1 - \delta) \text{ , missä } \delta = \frac{p + q - 1 - \frac{q}{k}}{pq}.$$

Ollaan tilanteessa, jossa Wienerin algoritmia voidaan hyödyntää, sillä $\frac{e}{pq}$ koostuu täysin julkisista avaimista ja δ on suuruusluokaltaan pieni [**11**, s.556]. Sovellettaessa Wienerin algoritmia RSA-salaukseen, etsitään arvoa luvulle $\frac{k}{dg}$ käyttäen arviona lukua $\frac{e}{N}$. Huomioitavaa algoritmissa on, että haetun luvun löytämistä varten on oltava olemassa testi, jolla luvun sopivuus testataan. Luvun $\frac{k}{dg}$ testauksessa käydään läpi seuraavat kuusi vaihetta:

(1) Muodostetaan luku edg. Tästä dg on tutkittavan konvergentin nimittäjä ja salauseksponentti e on julkinen tieto. Kerrottaessa yhtälöä (5.6) luvulla g saadaan $deg = k(p-1)(q-1) + g$.

(2) Muodostetaan luku $(p-1)(q-1) = \lfloor \frac{deg}{k} \rfloor$. Jakamalla edellisessä kohdassa saatu yhtälö puolittain luvulla k saaden $\frac{deg}{k} = (p-1)(q-1) + \frac{g}{k}$. Tästä nähdään luvun $(p-1)(q-1)$ olevan luvun $\frac{deg}{k}$ kokonaisosa ja $\frac{g}{k}$ jakojäännös, kun k on suurempi kuin g.

Mikäli tässä kohtaa luvuksi $(p-1)(q-1)$ saadaan 0, on testiä turha jatkaa. Jatkettaessa tulokseksi saataisiin $p = 1$ ja $q = pq$.

(3) Muodostetaan luku g. Koska luvun $(p-1)(q-1)$ kokonaisosa on $\frac{deg}{k}$ ja jakojäännös $\frac{g}{k}$, niin $g = deg \mod k$.

(4) Muodostetaan luku $\frac{p+q}{2} = \frac{pq-(p-1)(q-1)+1}{2}$ käyttäen hyväksi kohdan (2) tulosta. Mikäli $\frac{p+q}{2}$ ei ole kokonaisluku on luku $\frac{k}{dg}$ väärin ja testiä on turha jatkaa.

(5) Muodostetaan luku $(\frac{p-q}{2})^2 = (\frac{p+q}{2})^2 - pq$. Mikäli luku $(\frac{p-q}{2})^2$ on jonkin kokonaisluvun neliö, on luku $\frac{k}{dg}$ oikea.

(6) Muodostetaan salainen eksponentti $d = \frac{dg}{g}$.

Esimerkki 5.4. Käytetään ketjumurtolukuja hyödyntävää algoritmia salaisen avaimen d selvittämiseen, kun $N = 8927$ ja $e = 2621$. Julkinen avain sisältää sekä RSA-modulin N että salauseksponentin e, joten nämä ovat täysin julkista tietoa.

Kun $N = pq = 8927$ ja $e = 2621$, niin $\frac{e}{pq} = \frac{2621}{8927}$. Aloitetaan hakemalla tälle ketjumurtolukuesitys:

$$\frac{2621}{8927} = \frac{1}{\frac{8927}{2621}} = \frac{1}{3 + \frac{1}{\frac{2621}{1064}}} = \frac{1}{3 + \frac{1}{2 + \frac{493}{1064}}} = \cdots = [0, 3, 2, 2, 6, 3, 8, 3]$$

Taulukoidaan sitten muutama ensimmäinen konvergentti. Näiden muodostaminen onnistuu kätevästi lauseen (3.2) avulla. Tällöin alkuarvojen jälkeen $s_n = a_n s_{n-1} + s_{n-2}$ ja $b_n = a_n b_{n-1} + b_{n-2}$ ja tarvittavat ketjutekijöiden a_i arvot saadaan edellä esitetystä ketjumurtolukuesityksestä.

Nyt tarvittavat lähtötiedot Wienerin algoritmiin ovat laskettuna. Lähdetään tutkimaan tapausta $i = 0$. Tällöin konvergentti $\alpha_0' = \frac{s_0}{b_0} = \frac{0}{1}$. Nolla käsitellään parillisen

i	a_i	s_i	b_i
0	0	alkuarvo: $s_0 = a_0 = 0$	alkuarvo: $b_0 = 1$
1	3	alkuarvo: $s_1 = 3 \cdot 0 + 1 = 1$	alkuarvo: $b_1 = a_1 = 3$
2	2	$2 \cdot 1 + 0 = 2$	$2 \cdot 3 + 1 = 7$
3	2	$2 \cdot 2 + 1 = 5$	$2 \cdot 7 + 3 = 17$

TAULUKKO 5.1. Ensimmäisten konvergenttien muodostus luvulle $\frac{2621}{8927}$

luvun tavoin Wienerin algoritmissa, joten konvergentin arvausta muodostettaessa lukujen s_i ja b_i laskemisessa käytetään taulukossa 5.1 esitetyn $a_0 = 0$ arvon tilalla arvoa $a_0' = a_0 + 1 = 1$ ja näin ollen arvaus konvergentiksi on $\frac{k}{dg} = \frac{1}{1}$. Muodostetaan seuraavaksi luku edg. Termi $dg = 1$ löytyy konvergentin nimittäjästä ja e on julkinen eksponentti. Näin saadaan $edg = 2621 \cdot 1 = 2621$. Koska konvergentin osoittaja on 1, niin myös arvaus tulolle $(p-1)(q-1) = 2621$, sillä se muodostuu lattiafunktiolla termistä $\frac{edg}{k}$ ja $k = 1$. Seuraavaksi lasketaan arvaus luvulle $g = edg \bmod k$ eli $2621 \bmod 1 = 0$.

Käydään sitten läpi testauksen vaiheet (4) ja (5). Muodostetaan aluksi haluttu luku $\frac{p+q}{2} = \frac{pq-(p-1)(q-1)+1}{2}$. Näistä $pq = N$ on tiedossa ja tulolle $(p-1)(q-1)$ saatiin arvaus aiemmin. Näin ollen haluttu luku on $\frac{p+q}{2} = \frac{8927-2621+1}{2} = \frac{6307}{2} = 3153,5$. Saatu luku ei ole kokonaisluku, joten testiä on turha jatkaa.

Otetaan seuraavaksi käsittelyyn tapaus $i = 1$. Koska i on pariton, saadaan arvaus konvergentille $\frac{k}{dg}$ suoraan taulukon 5.1 konvergentista. Muutoin arvaukset saadaan vastaavalla tavalla kuin tapauksessa $i = 0$. Saadut luvut ovat esillä taulukossa 5.2. Tälläkin arvauksella testi tyssää luvun $\frac{p+q}{2}$ arvaukseen – tuloksena ei ole kokonaisluku.

Siirrytään sitten seuraavaan arvaukseen ja toistetaan toimenpiteet kun $i = 2$. Nyt kyseessä on parillinen i, joten muodostettaessa arvausta konvergentille käytetään taulukossa 5.1 esitetyn arvon $a_2 = 2$ sijaan arvoa $a_2' = a_2 + 1 = 3$ jolloin saadaan $\frac{k}{dg} = \frac{3}{10}$. Muodostetaan sitten edellisten kohtein tapaan arvaukset, jotka löytyvät taulukosta 5.2. Tällä kertaa laskettaessa lukua $\frac{p+q}{2}$ tulokseksi tulee kokonaisluku, $\frac{p+q}{2} = \frac{8927-8736+1}{2} = 96$. Siirrytään sitten viimeiseen vaiheeseen ja muodostetaan luku $(\frac{p-q}{2})^2 = (\frac{p+q}{2})^2 - pq = 96^2 - 8927 = 9216 - 8927 = 289$. Huomataan, että kyseessä on luvun 17 neliö ja sitä kautta voidaan todeta, että arvaus osuu oikeaan. Näin ollen salainen avain d saadaan selville suorittamalla vielä jakolasku $\frac{dg}{g} = \frac{10}{2} = 5$.

Salaisen avaimen d selvittämisessä käydyt vaiheet ovat tiivistettynä taulukossa 5.2. Tuloksena saadaan $d = 5$.

5.5. Salauseksponentista e

Edellä kerrottiin, miksi avauseksponentti d tulee valita tarpeeksi suureksi. Tämä saattaa herättää kysymyksen salauseksponentin kokoon liittyen. RSA-menetelmän esittelyn yhteydessä salauseksponentin valinnalle annettiin kaksi ehtoa, $1 < e < \varphi(N)$ ja $\text{syt}(e, \varphi(N)) = 1$. Nämä ehdot rajaavat vain pienen osan käytettävistä luvuista

Laskettava luku	Miten tulee	$i=0$	$i=1$	$i=2$
a'_i		0	3	2
$\frac{s'_i}{b'_i}$	i:s konvergentti	$\frac{0}{1}$	$\frac{1}{3}$	$\frac{2}{7}$
Arvaus $\frac{k}{dg}$	$[a'_0,\ldots,a'_i+1]$ jos i parill. $[a'_0,\ldots,a'_i]$ jos i pariton	$\frac{1}{1}$	$\frac{1}{3}$	$\frac{3}{10}$
Arvaus egd	$e\cdot dg$	2621	7863	26210
Arvaus $(p-1)(q-1)$	$\lfloor\frac{edg}{k}\rfloor$	2621	7863	8736
Arvaus g	$edg \mod k$	0	0	2
Arvaus $\frac{p+q}{2}$	Testaus vaihe (4)	3153.5 (lopetetaan)	532.5 (lopetetaan)	96
Arvaus $(\frac{p-q}{2})^2$	Testaus vaihe (5)			$289=17^2$
d	$\frac{dg}{g}$			5

Taulukko 5.2. Esim 5.4

pois. Kun otetaan lisäksi huomioon, että avauseksponentin d tulee olla tarpeeksi iso, saadaan sopivien lukujen joukkoa jälleen supistettua. Näiden ohjeiden lisäksi on vielä hyvä tarkistaa joitakin asioita valintaa tehtäessä. Yksi tällainen on salauseksponentin e kertaluku jäännösluokkaryhmässä $\mathbb{Z}^*_{\varphi(N)}$. Seuraavassa näytetään esimerkin avulla miksi pieni kertaluku on salaukselle turmiollinen.

Esimerkki 5.5. Lasse haluaa lähettää Liisalle viestin käyttäen RSA-salausta. Lassen viesti m on numeeriseksi muutettuna $m = 080509001209091901$. Liisa valitsee alkuluvut, $p = 149$ ja $q = 181$, ja muodostaa näiden avulla RSA-salauksessa tarvittavat avaimet. Lukujen valinnan seurauksena $N = 26969$. Liisa valitsee salauseksponentiksi $e = 179$ jolloin avauseksponentiksi tulee $d = 7739$. Tämän jälkeen Liisa lähettää Lasselle avainparin (N, e) jonka avulla Lasse salaa viestinsä.

Lasse jakaa viestinsä m neljän numeron lohkoihin, jolloin jokaiselle viestille pätee varmasti $m_i < N$. Lasse on muodostanut viestin muuttamalla kirjaimet numeroiksi aakkosten järjestyksen mukaan. Tällöin siis A = 01, B = 02, C = 03, D = 04, ..., Å = 27, Ä = 28, Ö = 29. Välimerkkinä Lasse käyttää numeroa 00, jonka hän myös lisää viestin loppuun saadakseen neljän numeron lohkoja. Lasse salaa viestissään jokaisen lohkon erikseen ja lähettää nämä Liisalle erillisinä viesteinä. Liisa avaa viestit käyttämällä avauseksponenttia, $c_i^d \mod N = m_i \mod N$.

Lasse onnistui lähettämään viestin kokonaisuudessaan Liisalle ongelmitta. Kumpikaan ei kuitenkaan huomaa, että Erkki saa napattua matkalta sekä Lassen lähettämät viestit että Liisan lähettämän julkisen avainparin. Erkillä on siis hallussaan (N, e) ja

Viestit

i	1	2	3	4	5
m_i	0805	0900	1209	0919	0100
c_i	6011	5466	8223	15217	2496

Taulukko 5.3. Esim 5.5

c_i, joiden avulla hän koittaa saada selville alkuperäiset viestit m_i. Erkki arvaa Lassen käyttäneen kirjainten muuttamista numeroiksi aakkosten mukaan. Erkin menetelmä viestin selvittämiseen on yksinkertainen; hän korottaa kunkin salatun viestin c_i järjestään potenssiin $k = 1, 2, 3, \ldots \bmod N$ ja katsoo tuleeko mitään ymmärrettävää. Taulukkoon 5.4 on kirjattu Erkin yritykset.

k		c_1^k	c_2^k	c_3^k	c_4^k	c_5^k
1	Numeerinen muoto	4244	22077	4286	6711	20191
	Kirjaimin modulo 29	MO	VS tai QS	MÄ	IK	TQ tai ÅD
2	Numeerinen muoto	23206	10896	4784	9787	25483
	Kirjaimin modulo 29	WC tai _F	JZ tai UI	RZ	J_	YS tai VY
3	Numeerinen muoto	805	900	1209	919	100
	Kirjaimin modulo 29	HE	I_	LI	IS	A_

TAULUKKO 5.4. Erkin purkuyritykset

Korottaessaan kolmanteen potenssiin viestit Erkki huomaa, että viestistä tulee ymmärrettävää tekstiä: hei Liisa. Tämän jälkeen Erkin ei tarvitse enää koittaa muita eksponentteja, vaan Erkki saa kaikki Lassen kyseisellä avaimella salaamat viestit selville korottamalle ne kolmanteen potenssiin mod N. Miksi näin?

Erkin ei tarvinnut jakaa RSA-modulia N tekijöihin missään vaiheessa, eikä Erkki edes yrittänyt selvittää salaista avainta d. Ennen esimerkkiä mainittiin salauseksponentin e kertaluku jäännösluokkaryhmässä $\mathbb{Z}_{\varphi(N)}$. Esimerkin tapauksessa salauseksponentin kertaluku on neljä, minkä seurauksena Erkki saa viestin selville nopeasti yksinkertaisesti kokeilemalla ja tulkitsemalla tulosta. Liisa olisi voinut välttää tilanteen tarkistamalla salauseksponentin kertaluvun. Minkä vuoksi kertaluku sitten paljastaa alkuperäisen viestin? Taustalla on sama syy, kuin RSA-menetelmän avausmekanismin yhteydessä käytiin läpi.

Olkoon k salauseksponentin e kertaluku jäännösluokkaryhmässä $\mathbb{Z}^*_{\varphi(N)}$, jolloin $e^k \equiv 1 \bmod \varphi(N)$. Tällöin on olemassa kokonaisluku l jolla $e^k = l\varphi(N) + 1$. Näin ollen

$$c^{e^{k-1}} = (m^e)^{e^{k-1}} = m^{ee^{k-1}} = m^{e^k},$$

ja edelleen $m^{e^k} \equiv m \mod N$, sillä $m^{e^k} = m^{l\varphi(N)+1}$. Eulerin lausetta käyttäen saadaan $m^{l\varphi(N)}m \equiv m \mod N$, kun $\text{syt}(m, N) = 1$.

LUKU 6

RSA digitaalisissa allekirjoituksissa

Salaukset, oli kyseessä sitten symmetrinen tai epäsymmetrinen salaus, ovat ratkaisseet ongelman nykyisessä tietoverkossa allekirjoitusten kohdalla. Monin paikoin mustekynällä tehdyt allekirjoitukset ovat korvautuneet digitaalisilla allekirjoituksilla. Digitaalisella allekirjoituksella tarkoitetaan tässä viestiin liitettyä allekirjoitusta, joka osoittaa viestin tulleen tietyltä taholta. Digitaalista allekirjoitusta voi verrata vanhanaikaiseen sinettiin. Jokainen, joka näkee sinetöidyn kirjekuoren, on vakuuttunut kuoren tulleen juuri sinetöijältä. Vain sinetin omistaja voi kuoren kyseisellä tavalla sinetöidä. Tällaista allekirjoitusta voidaan käyttää esimerkiksi varmistettaessa ohjelmien ja verkkosivustojen latauskohdetta – latautuuko ohjelma varmasti valmistajan kautta eikä jostakin tuntemattomalta palvelimelta, onko kyseessä virallinen verkkosivu vai huijausmielessä tehty oikean kaltainen sisäänkirjautumissivu – tai kun halutaan varmentua siitä, kuka toimintamääräysten takana on esimerkiksi verkkopankissa tunnistautumalla. Väärissä käsissä voidaan pankkitunnuksilla tunnistautua valheellisesti toisen nimissä ja solmia taloudellisestikin merkittäviä sopimuksia, sekä ohjata niiden avulla saadut varat muualle.

Salauksen ja digitaalisen allekirjoituksen perusperiaatteet ovat hyvin pitkälti saman kaltaiset. Tämän vuoksi digitaalisten allekirjoitusten ongelmana onkin vääriin käsiin joutumisen lisäksi myös se, että ne voidaan murtaa. Toki, puhuttaessa esimerkiksi verkkopankkitunnuksista, murtaminen ei ole kovin yksinkertaista. On kuitenkin muistettava, että yleisessä sähköpostissa tai erilaisissa tietokannoissa turvallisuustaso voi olla huomattavasti heikompi.

Käytettäessä RSA-menetelmää allekirjoituksessa, oleellisin ero salatun viestin lähettämiseen verrattuna on, että allekirjoittaja sekä julkaisee julkisen avainparin että allekirjoittaa, ”salaa”, salaisella *singeerausekseponentillaan* dokumentin. Yleensä salaus koskee vain dokumentin ”allekirjoitusosaa”. Dokumentti itsessään tai valtaosa sen sisällöstä eivät ole salaisia, vaan tarkoituksena on varmistaa dokumentin alkuperä. Tämän jälkeen viestin vastaanottaja käyttää julkisen avainparin *varmennuseksponenttia* varmentaakseen viestin tulleen oikealta taholta. RSA-salauksessa puolestaan viestin vastaanottaja ainoastaan loi julkisen avainparin ja viestin lähettäjä käytti jo luotua avainparia salatakseen viestin.

Taulukossa 6.1 on esitettynä allekirjoituksen vaiheet. RSA-salauksen implementointia käyttäen singeerauseksponentti s vastaa salaista avainta d ja varmennuseksponentti v julkista avainta e. Alkulukujen p ja q valintaa koskevat samat periaatteet kuin salauksessakin.

Saara	Santtu
Viestin allekirjoitus	
Valitsee salaiset alkuluvut p ja q. Valitsee varmennuseksponentin v. Julkaisee avainparin $N = pq$ ja v.	
Laskee singeerauseksponentin s jolle $sv \equiv 1 \mod \varphi(N)$. Liittää dokumenttiin allekirjoituksen m laskemalla $S \equiv m^s \mod N$. Lähettää selkokielisen dokumentin, jossa salattu allekirjoitus S.	
	Käyttää Saaran julkista avainparia (N, v) ja laskee $S^v \mod N$ sekä vertaa tulosta allekirjoitukseen m.

TAULUKKO 6.1. RSA digitaalisessa allekirjoituksessa

Allekirjoittaakseen dokumenttinsa Saara valitsee kaksi alkulukua p ja q. Näiden tulo $N = pq$ toimii julkisen avainparin toisena osana. Saara laskee alkulukujensa avulla singeerauseksponentin s ja varmennuseksponentin v, joille

$$sv \equiv 1 \mod \varphi(N).$$

Saara julkaisee avainparin (N, v). Lähettämäänsä dokumenttiin Saara liittää salatun allekirjoituksen $S \equiv m^s \mod N$. Oletuksena tässä on, että $0 < m < N$.

Santtu saa Saaran allekirjoituksella S varustetun dokumentin ja laskee siitä $S^v \mod N$. Tuloksen ollessa yhtäpitävä allekirjoituksen m kanssa, Santtu varmistuu viestin tulleen Saaralta.

Minkä takia allekirjoitus toimii? Taustalla oleva matematiikka on käsitelty RSA-salauksen yhteydessä kerrottaessa RSA-avainten muodostuksesta kappaleessa 4.2.

Kirjallisuutta

[1] Dan Boneh: Twenty years of attacks on the RSA cryptosystem *Notices of the American Mathematical Society (AMS)*, 46(2): 203-213, 1999.

[2] Carl Boyer: *Matematiikan historia osa II.* Englanninkielinen alkuperäisteos 2. painos toim. Uta C. Merzbach 1991 suomentanut Kimmo Pietiläinen. WSOY:n graafiset laitokset, Juva, 1994.

[3] Johannes A. Buchmann: *Introduction to cryptography.* Springer-Verlag New York, 2001.

[4] European Union Agency for Network and Information Security (ENISA): Algorithms, Key Sizes and Parameters Report 2014 recommendations, 2014. https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-size-and-parameters-report-2014, Katsottu 21.3.2016.

[5] G. H. Hardy, E. M. Wright: *An introduction to the theory of numbers.* 4th edition, Oxford University Press London, 1968.

[6] Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman: *An introduction to mathematical cryptography.* Springer Sciene+Business Media LCC New York, 2008.

[7] Lassi Kurittu: Ketjumurtoluvut – luentomoniste, 2013. http://users.jyu.fi/∼lkurittu/ketjumurtoluvut.pdf Katsottu 21.3.2015.

[8] J. H. van Lint, R. M. Wilson: *A course in combinatorics.* Cambridge University Press, 1992.

[9] Tauno Metsänkylä, Marjatta Näätänen: *Algebra.* Limes Ry, Helsinki, 2003.

[10] Tapio Rajala: Lukuteoria – luentomoniste, 2010.

[11] Michael L. Wiener: Cryptanalysis of short RSA secret exponents *IEEE Trans. Inform. Theory*, 36(3): 553-558, 1990.