RSA-salausmenetelmä ja sopivien alkulukujen valitseminen

LuK-tutkielma
Juulia Kehus
2428389
Matemaattisten tieteiden laitos
Oulun yliopisto
Kevät 2021

Sisältö

1 Johdanto **2**

2 RSA-salausmenetelmä **3**
2.1 Määritelmiä ja lauseita 3
2.2 RSA-salausmenetelmän käyttäminen 9
2.2.1 Avaimen luominen 9
2.2.2 Viestin salaaminen 9
2.2.3 Viestin allekirjoittaminen 10
2.2.4 Viestin lähettäminen 10
2.2.5 Viestin vastaanottaminen ja avaaminen 10
2.2.6 Avainkirjan julkinen tieto ja käyttäjän yksityinen tieto 11
2.3 Esimerkki RSA-salausmenetelmän käyttämisestä 11
2.3.1 Käyttäjän A avainten luominen 11
2.3.2 Käyttäjän B avainten luominen 12
2.3.3 Käyttäjä A lähettää viestin käyttäjälle B 12
2.3.4 Käyttäjä B vastaanottaa ja avaa salatun viestin 13
2.4 Esimerkki viestin allekirjoittamisesta 13

3 RSA ja alkuluvut **15**
3.1 Alkuluvut 15
3.2 Alkulukujen valitseminen 15
3.3 Määritelmiä ja lauseita 15

4 Alkulukujen testaaminen **18**
4.1 Millerin ja Rabinin testi 18
4.2 Millerin ja Rabinin testin käyttäminen 19

Lähdeluettelo **23**

1 Johdanto

RSA-salaus on yksi julkisen avaimen salakirjoitusmenetelmä, joka pohjautuu lukuteorian tunnettuun ongelmaan: kuinka saadaan jaettua annettu, suuri luku N alkutekijöihinsä. Sen kehitti vuonna 1978 tutkijakolmikko Ron Rivest, Adi Shamir ja Leonard Adleman.

Julkisen avaimen salakirjoitusmenetelmillä on etunsa verrattuna perinteisiin yksinkertaisiin salakirjoitusmenetelmiin. Niissä ei nimittäin ole perinteisten salakirjoitusmenetelmien ongelmia. Tällaisia ovat avaimista sopimiseen ja niiden välittämiseen liittyvät hankaluudet sekä allekirjoitusongelma.

Julkisen avaimen salauskirjoitusmenetelmässä kunkin käyttäjän salausavain on kaikille nähtävillä julkisessa avainkirjassa, joten niiden välittäminen on helppoa, eikä sitä tarvitse tehdä salassa. Lisäksi avaimista ei tarvitse sopia keskenään, sillä viestin lähettäjä käyttää viestin salaamiseen aina avainkirjasta löytyvää viestin vastaanottajalle ominaista salausavainta, siitä ei siis tarvitse sopia erikseen.

Julkisen avaimen järjestelmässä selväkielinen viestiyksikkö on usein sama kaikilla käyttäjillä ja se on sama kuin salakirjoitettu viestiyksikkö. Niinpä tarvitaan keinoja viestin allekirjoittamiseksi, jotta tiedetään, kuka viestin on kulloinkin kirjoittanut. Toisaalta allekirjoitus myös takaa sen, ettei kukaan käyttäjistä voi jälkikäteen kieltää lähettämäänsä viestiä.

RSA-salaus perustuu siis hankaluuteen ratkaista kongruenssi, jonka moduloluokka tiedetään, mutta sitä ei osata jakaa tekijöihinsä. Ratkaiseminen on helppoa viestin vastaanottajalle, koska hän tietää modulon alkulukutekijät ja dekryptauseksponentin, mutta haastavaa urkkijalle. Mikäli urkkija saa tietoonsa joitain lisätietoja, voikin moduluksen ratkaiseminen muuttua yllättävän helpoksi. Käytettävän moduluksen on siis oltava mahdollisimman suurten alkulukujen tulo.

Tarvitaan siis keinoja, jotta voidaan selvittää onko jokin luku alkuluku vai ei, että saataisiin käytettyä julkisen avaimen salauskirjoitusmenetelmää, RSA-salausta, joka pohjautuu hankaluuteen ratkaista kongruenssiyhtälöä ilman tietoa julkisen avaimen muodostavista tekijöistä.

Tässä työssä tutustutaan RSA-salausmenetelmän toimintaan ja periaatteisiin sekä salausmenetelmän käyttöa varten tarvittaviin alkulukuihin ja niiden tutkimiseen. Työssä käydään läpi eräs alkulukutesti nimeltään Millerin ja Rabinin alkulukutesti. Sen avulla voidaan tutkia valituista suurista luvuista, ovatko ne RSA-salauksen avainten laskemiseen tarvittavia alkulukuja vai paljastuvatko ne yhdistetyiksi luvuiksi.

Työssä on käytetty pääasiallisena lähteenä teosta Undergraduate texts in mathematics; An introduction to Mathematical Cryptography (2008) [1].

2 RSA-salausmenetelmä

RSA-salauksessa kukin käyttäjä U julkaisee oman salausmenettelynsä E_U julkisesti näkyvissä olevassa avainkirjassa, mutta pitää avausmenettelynsä D_U pelkästään omana tietonaan. Kun halutaan lähettää viesti tietylle henkilölle, lähetettäessä katsotaan avainkirjasta kohdehenkilön salausmenettely, jota käytetään viestin salaaamiseen. Näin ollen viestin saa avattua vain henkilö, joka tietää avausmenettelyn, eikä kukaan ulkopuolinen urkkija pysty avaamaan salattua viestiä [2].

Menettely on toimiva ja pitää viestin salaisena, mikäli sekä E_U, että D_U ovat nopeita, eivätkä tarvitse paljoa muistia. Turvallisuuden vuoksi on lisäksi oltava siten, että menettelyn E_U avulla on miltei mahdotonta määrittää menettelyä D_U, jotta urkkija ei pysty avaamaan sieppaamaansa viestiä [2].

2.1 Määritelmiä ja lauseita

Lause 2.1 (Eulerin lause)**.** *Olkoon $p, q \in \mathbb{P}, p \neq q$ erisuuria alkulukuja ja olkoon*

$$g = \text{syt}((p-1),(q-1)).$$

Tällöin

$$a^{(p-1)(q-1)/g} \equiv 1 \pmod{pq},$$

kaikilla a, joille $\text{syt}(a, pq) = 1$.

Erityisesti, mikäli p ja q ovat parittomia alkulukuja, niin

$$a^{(p-1)(q-1)/2} \equiv 1 \pmod{pq},$$

kaikilla a, joille $\text{syt}(a, pq) = 1$.

Todistus. Oletuksen mukaan $p \nmid a$ ja $g \mid q-1$. Muokataan potenssissa oleva tulo potenssin potenssiksi

$$a^{(p-1)(q-1)/g} = (a^{p-1})^{(q-1)/g}.$$

Myöhemmin esitettävän Fermat'n pienen Lauseen 3.3 perusteella $a^{(p-1)} \equiv 1 \pmod{p}$ ja kaikille potensseille pätee, että luvun 1 potenssi on aina 1 eli $1^{(q-1)/g} = 1$, joten

$$\begin{aligned} a^{(p-1)(q-1)/g} &= (a^{p-1})^{(q-1)/g} \\ &\equiv 1^{(q-1)/g} \pmod{p} \\ &\equiv 1 \pmod{p}. \end{aligned}$$

Suoritetaan sama laskutoimitus vaihtaen lukujen p ja q paikat toisinpäin ja saadaan

$$a^{(p-1)(q-1)/g} \equiv 1 \pmod{q}.$$

Tämä osoittaa, että $a^{(p-1)(q-1)/g} - 1$ on jaollinen kummallakin luvulla p ja q, joten se on myös jaollinen niiden tulolla pq.

Oletuksen perusteella $p \nmid a$. Mikäli p ja q ovat parittomia alkulukuja, niin $p-1$ ja $q-1$ ovat parillisia. Tällöin $2 \mid (p-1)$ ja $2 \mid (q-1)$. Edelleen Fermat'n pienen Lauseen 3.3 perusteella $a^{(p-1)} \equiv 1 \pmod{p}$ ja koska luvun 1 potenssi on aina 1 niin $1^{(q-1)/2} = 1$. Saadaan

$$\begin{aligned} a^{(p-1)(q-1)/2} &= (a^{p-1})^{(q-1)/2} \\ &\equiv 1^{(q-1)/2} \pmod{p} \\ &\equiv 1 \pmod{p} \end{aligned}$$

ja vaihtamalla luvut p ja q toisinpäin saadaan

$$a^{(p-1)(q-1)/2} \equiv 1 \pmod{q},$$

joten $a^{(p-1)(q-1)/2} - 1$ on jaollinen sekä luvulla p että luvulla q, joten se on jaollinen myös niiden tulolla pq.

Siispä

$$a^{(p-1)(q-1)/2} \equiv 1 \pmod{pq}$$

kaikilla a, joille $\text{syt}(a, pq) = 1$. □

Määritelmä 2.2. Funktiota f kutsutaan *yksisuuntaiseksi funktioksi* (one-way function), mikäli sen arvojen laskeminen on helppoa, mutta olemassa olevan käänteisfunktion f^{-1} määrittäminen on hyvin haasteellista. *Salaovifunktio* on yksisuuntainen funktio, jonka käänteisfunktion määrääminen muuttuu helpoksi jonkin lisätiedon avulla. Tätä lisätietoa kutsutaan *salaoveksi* (trapdoor).

RSA-salauksessa yksisuuntainen funktio pohjautuu siihen, että annettujen alkulukujen p ja q tulo N on helppoa laskea, mutta tulon tekijöiden löytäminen on haastavaa ja liian aikaa vievää.

Määritelmä 2.3. Funktio $E(x) = x^e$, $E : \mathbb{Z}_n \to \mathbb{Z}_n$ on RSA-*kryptausfunktio*, missä e on *kryptauseksponentti* (julkinen avain) ja $D(y) = y^d$, $D\colon \mathbb{Z}_n \to \mathbb{Z}_n$ on RSA-*dekryptausfunktio*, missä d on *dekryptauseksponentti* (salainen avain).

RSA-salausmenetelmässä on siis hankalaa laskea kongruensseja

$$x^e \equiv c \pmod{N},$$

kun tunnetaan ainoastaan luvut e, c ja N. On siis vaikeaa ratkaista luvun x asteen e ratkaisuja modulo N.

Lause 2.4. *Olkoon $p \in \mathbb{P}$ alkuluku ja olkoon sellainen luku $e \geq 1$, että* $\text{syt}(e, p-1) = 1$. *Luvulla e on käänteisalkio d*

$$de \equiv 1 \pmod{(p-1)}.$$

Kongruenssin

$$x^e \equiv c \pmod{p}$$

ainoa ratkaisu on $x \equiv c^d \pmod{p}$.

Todistus. Jos $c \equiv 0 \pmod{p}$, niin $x \equiv 0 \pmod{p}$ on tämä ainoa ratkaisu. Oletetaan siis, että $c \not\equiv 0 \pmod{p}$. Kongruenssi $de \equiv 1 \pmod{(p-1)}$ tarkoittaa, että on olemassa luku k siten, että

$$de \equiv 1 + k(p-1).$$

Tarkistetaan, että luku c^d on kongruenssin $x^e \equiv c \pmod{p}$ ratkaisu. Eksponenttien laskusääntöjen, yhtäsuuruuden $de = 1 + k(p-1)$ ja Fermat'n pienen Lauseen 3.3 vuoksi saadaan

$$\begin{aligned}
(c^d)^e &\equiv c^{de} \pmod{p} \\
&\equiv c^{1+k(p-1)} \pmod{p} \\
&\equiv c \cdot (c^{p-1})^k \pmod{p} \\
&\equiv c \cdot 1^k \pmod{p} \\
&\equiv c \pmod{p}.
\end{aligned}$$

Näin ollen $x = c^d$ on kongruenssin $x^e \equiv c \pmod{p}$ ratkaisu.

Osoitetaan vielä, että ratkaisu on ainoa. Oletetaan, että molemmat x_1 ja x_2 ovat kongruenssin $x^e \equiv c \pmod{p}$ ratkaisuja. Osoitettiin, että $z^{de} \equiv z \pmod{p}$ kaikille nollasta eroaville luvuille z. Huomataan, että

$$x_1 \equiv x_1^{de} \equiv (x_1^e)^d \equiv c^d \equiv (x_2^e)^d \equiv x_2^{de} \equiv x_2 \pmod{p}.$$

Siksi x_1 ja x_2 ovat samat modulo p, joten kongruenssilla $x^e \equiv c \pmod{p}$ on ainoastaan yksi ratkaisu. □

Lause 2.5. *Olkoon p ja $q \in \mathbb{P}, p \neq q$ erisuuria alkulukuja. Olkoon lisäksi $e \geq 1$ siten, että*

$$\text{syt}(e, (p-1)(q-1)) = 1.$$

Luvulla e on käänteisalkio modulo $(p-1)(q-1)$ eli

$$de \equiv 1 \pmod{(p-1)(q-1)}.$$

Näin ollen kongruenssin

$$x^e \equiv c \pmod{pq}$$

ainoa ratkaisu on $x \equiv c^d \pmod{pq}$.

Todistus. Osoitetaan ensin tapaus $\text{syt}(c, pq) = 1$. Käytetään Eulerin lausetta 2.1. Kongruenssi $de \equiv 1 \pmod{(p-1)(q-1)}$ tarkoittaa, että on olemassa kokonaisluku k siten, että

$$de = 1 + k(p-1)(q-1).$$

Varmistetaan, että c^d on kongruenssin $x^e \equiv c \pmod{pq}$ ratkaisu käyttämällä eksponenttien laskusääntöjä, Eulerin lausetta ja ylläolevaa tietoa luvusta de:

$$\begin{aligned}
(c^d)^e &\equiv c^{de} \pmod{pq} \\
&\equiv c^{1+k(p-1)(q-1)} \pmod{pq} \\
&\equiv c \cdot (c^{(p-1)(q-1)})^k \pmod{pq} \\
&\equiv c \cdot 1^k \pmod{pq} \\
&\equiv c \pmod{pq}
\end{aligned}$$

Niinpä $x = c^d$ on kongruenssin $x^e \equiv c \pmod{pq}$ ratkaisu. On vielä osoitettava tämän olevan ainoa ratkaisu. Olkoon $x = u$. Hyödyntämällä tietoa tulosta de, Eulerin lausetta ja oletusta $x = u$ saadaan

$$\begin{aligned}
u &\equiv u^{de-k(p-1)(q-1)} \pmod{pq} \\
&\equiv (u^e)^d \cdot (u^{(p-1)(q-1)})^{-k} \pmod{pq} \\
&\equiv (u^e)^d \cdot 1^{-k} \pmod{pq} \\
&\equiv c^d \pmod{pq}.
\end{aligned}$$

Näin ollen jokainen ratkaisu on yhtäsuuri kuin $c^d \pmod{pq}$, joten tämä on ainoa ratkaisu.

Osoitetaan sitten tapaus $\text{syt}(c, pq) > 1$. Tällöin $p \mid c$ tai $q \mid c$. Oletetaan, että $p \mid c$, jolloin $q \nmid c$. Käytetään Eulerin lausetta 2.1. Kongruenssi $de \equiv 1 \pmod{q}$ tarkoittaa, että on olemassa kokonaisluku k siten, että

$$de = 1 + kq.$$

Tarkistetaan, että c^d on yhtälön $x^e \equiv c \pmod{q}$ ratkaisu käyttämällä eksponenttien laskusääntöjä, Eulerin lausetta ja ylläolevaa tietoa luvusta de:

$$\begin{aligned}(c^d)^e &\equiv c^{de} \pmod{q} \\ &\equiv c^{1+kq} \pmod{q} \\ &\equiv c \cdot (c^q)^k \pmod{q} \\ &\equiv c \cdot 1^k \pmod{q} \\ &\equiv c \pmod{q}.\end{aligned}$$

Yksikäsitteisyyden todistaminen sivuutetaan tässä tapauksessa.

On siis osoitettu, että $c^{de} - c$ on jaollinen luvulla q. Koska $p \mid c$, niin myös $c^{de} - c$ on jaollinen luvulla p. Koska $c^{de} - c$ on jaollinen luvulla p ja luvulla q niin se on jaollinen myös niiden tulolla pq. □

Huomautus 2.6. Lause 2.5 antaa algoritmin, jonka avulla saadaan ratkaistua yhtälö $x^e \equiv c \pmod{pq}$. Ensin ratkaistaan yhtälö

$$de \equiv 1 \pmod{(p-1)(q-1)}$$

ja sitten lasketaan

$$c^d \pmod{pq}.$$

Tämän voi usein tehdä nopeammin käyttämällä pienempää arvoa luvulle d. Olkoon $g = \text{syt}(p-1, q-1)$ ja ratkaistaan kongruenssiyhtälöä

$$de \equiv 1 \pmod{\frac{(p-1)(q-1)}{g}}.$$

Eulerin lauseen mukaan $a^{(p-1)(q-1)/g} \equiv 1 \pmod{pq}$, joten mikäli kirjoitetaan $de = 1 + k(p-1)(q-1)/g$, niin

$$(c^d)^e = c^{de} = c^{1+k(p-1)(q-1)/g} = c \cdot (c^{(p-1)(q-1)/g})^k \equiv c \pmod{pq}.$$

Siispä käyttämällä pienempää arvoa luvulle d saadaan silti, että c^d on ratkaisu yhtälölle $x^e \equiv c \pmod{pq}$.

Esimerkki 2.7. Olkoon $p = 79$ ja 163 alkulukuja ja niiden tulo

$$N = pq = 12877.$$

Saadaan laskettua myös tulo

$$(p-1)(q-1) = (79-1)(163-1) = 78 \cdot 162 = 12636.$$

Valitaan sellainen kryptauseksponentti $e = 1387$, että

$$\text{syt}(e, (p-1)(q-1)) = 1.$$

Olkoon c vastaanotettu salattu viesti eli kryptoteksti $c = 2317$. Ratkaistaan ensiksi luvun e käänteisalkio d yhtälöstä

$$ed \equiv 1 \pmod{(p-1)(q-1)}$$

Eukleideen algoritmin avulla ja saadaan käänteisalkioksi $d = 3799$.

Seuraavaksi ratkaistaan nopealla potenssiinkorotuksella viestin sisältö

$$\begin{aligned} x &\equiv c^d \pmod{pq} \\ x &\equiv 2317^{3799} \equiv 7431 \pmod{12877}. \end{aligned}$$

Huomautuksen 2.6 tapaan voidaan nopeuttaa laskemista selvittämällä

$$g = \text{syt}((p-1), (q-1)) = \text{syt}(79-1), (163-1)) = \text{syt}(78, 162) = 6$$

ja ratkaisemalla d_2 yhtälöstä

$$\begin{aligned} ed_2 &\equiv 1 \pmod{\frac{(p-1)(q-1)}{g}} \\ 1387d_2 &\equiv 1 \pmod{\frac{12636}{6}}. \end{aligned}$$

Eukleideen algoritmilla saadaan käänteisalkioksi $d_2 = 1693$. Seuraavaksi ratkaistaan nopealla potenssiinkorotuksella viestin sisältö

$$\begin{aligned} x &\equiv c^{d_2} \pmod{pq} \\ x &\equiv 2317^{1693} \equiv 7431 \pmod{12877} \end{aligned}$$

ja saadaan sama lopputulos hieman pienemmällä työmäärällä. Mitä isommat luvut ovat kyseessä, sitä hyödyllisempää on käyttää Huomautuksen 2.6 laskutapaa.

2.2 RSA-salausmenetelmän käyttäminen

RSA-menetelmän käyttäminen koostuu eri vaiheista: kunkin käyttäjän julkisen salausavaimen (N_U, e_U) luomisesta, alkuperäisen viestin m salaamisesta, salatun viestin c lähettämisestä julkista kanavaa pitkin, salatun viestin c vastaanottamisesta ja sen avaamisesta henkilökohtaisella salaisella avaimella $((p-1)(q-1), d_U)$ selkotekstiksi m'. Lisäksi viesti usein allekirjoitetaan viestin lähettäjän tunnistamiseksi.

2.2.1 Avaimen luominen

Salausavainta luotaessa kukin käyttäjä U valitsee erisuuret alkuluvut p_U ja q_U sekä laskee luvun

$$N_U = p_U q_U.$$

Lisäksi kukin käyttäjä valitsee oman kryptauseksponetnttinsa e_U siten, että

$$\text{syt}(e_U, (p-1)(q-1)) = 1.$$

Tämän jälkeen käyttäjät julkaisevat oman salausavaimensa $K_U = (N_U, e_U)$ julkisessa avainkirjassa.

2.2.2 Viestin salaaminen

Käyttäjät salaavat toisilleen lähettämiään viestejä valitsemalla selvätekstin m, jonka salaamiseen käytetään viestin vastaanottajan julkista avainparia (N_U, e_U). Selvätekstinen viesti m muutetaan salatekstiksi seuraavasti:

$$c \equiv m^e \pmod{N_U}.$$

Saatu salateksti c lähetetään julkista kanavaa pitkin vastaanottajalle.

Kun käyttäjä A haluaa lähettää salatun viestin käyttäjälle B hänen on siis katsottava ensiksi julkisesta avainkirjasta käyttäjän B julkinen avain, joka on $K_B = (N_B, e_B)$. Sitten hänen on muutettava viesti joukon $\mathbb{Z}_{N_B}$ alkioiksi ja salattava viesti $m \in \mathbb{Z}_{N_B}$. Tämä tapahtuu seuraavasti:

$$E_B(m) = m^{e_b} = c \in \mathbb{Z}_{N_B}.$$

Viesti c lähetetään julkisen kanavan kautta, jossa myös avainkirjan sisältämä informaatio on julkisesti näkyvissä.

2.2.3 Viestin allekirjoittaminen

Jotta käyttäjä B tunnistaa viestin lähettäjän, on käyttäjän A allekirjoitettava viesti. Viestin allekirjoittaminen tapahtuu siten, että käyttäjä A muuttaa viestin j joukon $\mathbb{Z}_{N_B}$ alkioiksi ja allekirjoittaa viestin j omalla salaisella avausfunktiollaan $D_A(j) = j^{d_A} = s$. Allekirjoitettu viesti (j,s) kulkee julkista kanavaa pitkin, samoin kuin käyttäjän A julkinen avain (N_A, e_A). Käyttäjä B pystyy näin ollen tunnistamaan lähettäjän, kun hän avaa viestin $E_A(s) = s^{e_A} = j$. Allekirjoituskin on salattava, sillä muuten allekirjoitettu viesti voidaan avata julkisella avaimella ja tällöin myös viesti paljastuu.

- Käyttäjä A muuttaa viestin j joukon $\mathbb{Z}_{N_A}$ alkioksi. Sitten A salaa viestin $j \in \mathbb{Z}_{N_A}$ käyttäjän B julkisella avaimella ja muuttaa salatun viestin joukon $\mathbb{Z}_{N_B}$ alkioiksi seuraavasti

$$E_B(j) = j^{e_B} = c \in \mathbb{Z}_{N_B}.$$

- Sitten käyttäjä A allekirjoittaa viestin $j \in \mathbb{Z}_{N_A}$ omalla salaisella dekryptasfunktiollaan

$$D_A(j) = j^{d_A} = s$$

ja salaa allekirjoitetun viestin $s \in \mathbb{Z}_{N_B}$ käyttäjän B julkisella kryptausfunktiolla

$$E_B(s) = s^{e_B} = r \in \mathbb{Z}_{N_B}.$$

2.2.4 Viestin lähettäminen

Julkista kanavaa pitkin kulkee salattu, allekirjoitettu viesti (c,r) sekä käyttäjien A ja B kryptausfunktiot

$$E_B(x) = x^{e_A}$$

ja

$$E_B(x) = x^{e_B}.$$

2.2.5 Viestin vastaanottaminen ja avaaminen

Kun käyttäjä B vastaanottaa viestin c, hän avaa sen henkilökohtaisella salaisella avausfunktiollaan. Avausfunktiota varten käyttäjän B täytyy kuitenkin ensiksi selvittää laskemalla dekryptauseksponentti d_B. Tämä tapahtuu seuraavan kaavan avulla

$$d_B = e_B^{-1} \in \mathbb{Z}^*_{(p-1)(q-1)}.$$

Käyttäjä B avaa viestin avausfunktion avulla

$$D_B(c) = c^{d_B} = m^{e_B d_B} = m.$$

Vastaanotettuaan viestin c, käyttäjä B avaa viestin oman salaisen dekryptausfunktionsa avulla

$$D_B(c) = c^{d_B} = j.$$

Sen jälkeen käyttäjä B tarkistaa allekirjoituksesta, että lähettäjä on käyttäjä A.

$$E_A(D_B(r)) = E_A(r^{d_B}) = E_A(s) = s^{e_A} = j.$$

2.2.6 Avainkirjan julkinen tieto ja käyttäjän yksityinen tieto

Avainkirjassa julkaistaan siis kunkin käyttäjän avain $K_U = (N_U, e_U)$, mutta käyttäjät pitävät omana tietonaan salaoven muodostavan luvun d_U, luvut p_U ja q_U sekä luvut $(p-1)$ ja $(q-1)$ ja myös niiden tulon $(p-1)(q-1)$.

2.3 Esimerkki RSA-salausmenetelmän käyttämisestä

2.3.1 Käyttäjän A avainten luominen

Käyttäjä A valitsee haluamansa alkuluvut $p = 11$ ja $q = 19$ ja laskee niiden tulon

$$N_A = pq = 11 \cdot 19 = 209$$

ja lisäksi tulon

$$(p-1)(q-1) = (11-1)(19-1) = 10 \cdot 18 = 180.$$

Sitten hän valitse kryptauseksponentin e_A siten, että

$$\text{syt}(e_A, (p-1)(q-1)) = 1.$$

Koska $syt(7, 180) = 1$, hän voi valita kryptauseksponentikseen $e_A = 7$.

Lopulta hän ilmoittaa julkisessa avainkirjassa julkisen avaimensa

$$K_A = (N_A, e_A) = (209, 7).$$

Lisäksi hän selvittää henkilökohtaisen dekryptauseksponenttinsa d_A ratkaisemalla sen yhtälöstä

$$\begin{aligned} e_A d_A &\equiv 1 \pmod{(p-1)(q-1)} \\ 7d_A &\equiv 1 \pmod{180}. \end{aligned}$$

Eukleideen algoritmia hyödyntäen saadaan yhtälön $7d_A \equiv 1 \pmod{180}$ erääksi ratkaisuksi $d_A \equiv -77 \pmod{180}$. Kaikki ratkaisut ovat muotoa

$$d_A \equiv 103 \pmod{180},$$

josta dekryptauseksponentiksi saadaan $d_A = 103$. Käyttäjä A pitää yksityisen avaimen

$$((p-1)(q-1), d_A) = (180, 103)$$

salassa itsellään.

2.3.2 Käyttäjän B avainten luominen

Käyttäjä B valitsee vastaavasti haluamansa alkuluvut $p = 13$ ja $q = 17$, laskee niiden tulon $N_B = pq = 13 \cdot 17 = 221$ sekä tulon

$$(p-1)(q-1) = (13-1)(17-1) = 12 \cdot 16 = 192$$

ja valitsee kryptauseksponentikseen $e_B = 11$, sillä $\text{syt}(11, 192) = 1$.

Lopulta hänkin ilmoittaa julkisessa avainkirjassa julkisen avaimensa

$$K_B = (N_B, e_B) = (221, 11).$$

Käyttäjä B ratkaisee vielä Eukleideen algoritmia hyödyntäen yhtälöstä

$$\begin{aligned} e_B d_B &\equiv 1 \pmod{(p-1)(q-1)} \\ 11 d_B &\equiv 1 \pmod{192}. \end{aligned}$$

salaisen dektryptauseksponenttinsa d_B. Saaden yhtälön $11d_B \equiv 1 \pmod{192}$ ratkaisuksi $d_B \equiv 35 \pmod{192}$ eli dekryptauseksponentti $d_B = 35$. Käyttäjä B pitää yksityisen avaimen

$$((p-1)(q-1), d_B) = (192, 35)$$

salassa itsellään.

2.3.3 Käyttäjä A lähettää viestin käyttäjälle B

Kun käyttäjä A haluaa lähettää salatun viestin käyttäjälle B, hän katsoo julkisesta avainkirjasta käyttäjän B julkisen avainparin

$$K_B = (N_B, e_B = (221, 11).$$

Käyttäjä A valitsee lähetettävän selvätekstin "HEI", jonka hän esittää kolmena viestiyksikkönä $H = m_1 = 009$, $E = m_2 = 006$ ja $I = m_3 = 010$.

Selväteksti muutetaan kryptotekstiksi käyttäjän B julkisen avainparin avulla seuraavasti

$$\begin{aligned} c_1 &\equiv m_1^{e_B} \pmod{N_B} \\ &\equiv 9^{11} \equiv 185 \pmod{221} \end{aligned}$$

hyödyntäen kryptauseksponentin esittämistä luvun 2 potensseina ja nopeaa potenssiinkorottamista. Vastaavasti saadaan salattua loput viestiyksiköt

$$c_2 \equiv 6^{11} \equiv 141 \pmod{221}$$

ja

$$c_3 = 10^{11} \equiv 173 \pmod{221}.$$

Käyttäjä A lähettää julkista kanavaa pitkin viestin ”185141173” käyttäjälle B.

2.3.4 Käyttäjä B vastaanottaa ja avaa salatun viestin

Käyttäjä B vastaanottaa salatun viestin, jossa $c_1 = 185$, $c_2 = 141$ ja $c_3 = 173$, jonka hän avaa dekryptausfunktiollaan seuraavasti

$$\begin{aligned} m_1 &\equiv c_1^{d_B} \pmod{N_B} \\ &\equiv 185^{35} \equiv 9 \pmod{221} \end{aligned}$$

hyödyntäen nopeaa potenssiinkorotusta. Vastaavasti saadaan avattua

$$m_2 \equiv 141^{35} \equiv 6 \pmod{221}$$

ja

$$m_3 \equiv 173^{35} \equiv 10 \pmod{221},$$

joiden avulla käyttäjä B saa muunnettua sen viestiksi "hei".

2.4 Esimerkki viestin allekirjoittamisesta

Edellisen esimerkin käyttäjä A, jolle $N_A = 209$, $e_A = 7$ ja $d_A = 103$ lähettää käyttäjälle B, jolle $N_B = 221$, $e_B = 11$ ja $d_B = 35$ salatun allekirjoitetun viestin seuraavien vaiheiden mukaisesti. Käyttäjä A esittää viestin ”S” joukon $\mathbb{Z}_{209}$ alkiona $j = 20$ ja salaa sen käyttäjän B julkisella kryptauseksponentilla

$$c = j^{e_B} = 20^{11} \equiv 41 \pmod{221}.$$

Käyttäjä A liittää salaamaansa viestiin allekirjoituksen s käyttäen omaa dekryptauseksponenttiaan

$$s = j^{d_A} = 20^{103} \equiv 58 \pmod{209}.$$

Käyttäjä A salaa allekirjoituksensa käyttäjän B kryptauseksponentilla

$$r = s^{e_B} = 58^{11} \equiv 167 \pmod{221},$$

jonka jälkeen hän lähettää julkista kanavaa pitkin salatun ja allekirjoitetun viestin $(c, r) = (41, 167)$.

Käyttäjä B avaa viestin omalla dekryptauseksponentillaan

$$c^{d_B} = 41^{35} \equiv 20 = j \pmod{221},$$

joka vastaa käyttäjän A lähettämää selkoviestiä. Lisäksi käyttäjä B tarkistaa viestin lähettäjän avaamalla salatun allekirjoituksen omaa dekryptauseksponenttiaan käyttäen

$$r^{d_B} = 167^{35} \equiv 58 \pmod{221}$$

ja varmistaa lähettäjän käyttäjän A julkisella kryptauseksponentilla

$$(r^{d_B})^{e_A} = 58^7 \equiv 20 \pmod{209},$$

joka vastaa lähetettyä viestiä $j = 20$.

3 RSA ja alkuluvut

3.1 Alkuluvut

Määritelmä 3.1. *Alkuluku* on lukua 1 suurempi kokonaisluku, joka on jaollinen vain itsellään ja luvulla yksi. Se ei ole jaollinen millään muilla positiivisilla kokonaisluvuilla.

Määritelmä 3.2. Lukua 1 suurempia kokonaislukuja, jotka eivät ole alkulukuja kutsutaan *yhdistetyiksi luvuiksi.*

3.2 Alkulukujen valitseminen

RSA-salausmenetelmän toimivuuden ja salassapitävyyden kannalta on erityisen tärkeää pystyä valitsemaan alkuluvut hyvin. Niiden on oltava mahdollisimman suuria, mutta kuitenkin riittävän pieniä ja satunnaisia. Lisäksi niiden tulon jakaminen tekijöihinsä on oltava mahdollisimman aikaavievää ja hankalaa.

Alkulukujen pitäisi olla kohtuullisen pieniä, jotta niiden tulo on helppo laskea ja siten niiden avulla salaaminen ja salauksen purkaminen on tehokasta eikä turhan työlästä. Kuitenkaan ne eivät saa olla niin pieniä, että luvun N eli alkulukujen tulon jakaminen tekijöihin kävisi liian helposti ja nopeasti, koska tällöin viestin salauksen purkaminen olisi liian helppoa urkkijalle. RSA-salausmenetelmän käyttämiseksi siis tarvitaan keino selvittää, onko satunnaisesti valitut suuret luvut alkulukuja vai eivät, että luku N olisi kahden mahdollisimman suuren alkuluvun tulo.

RSA-salauksen julkista ja yksityistä avainparia valittaessa on siis tärkeää valita nimenomaan kaksi mahdollisimman suurta alkulukua, eikä vain kahta suurta, mutta mahdollisesti yhdistettyä lukua. Mikäli luvut eivät ole alkulukuja, on vastaanottajan tehtävä niille ensin tekijöihinjako avatakseen lähettäjän viestin, jolloin salauksen avaaminen on liian työlästä. Mikäli alkuluvut taas ovat pieniä, voi mahdollinen urkkija saada suoritettua luvun N tekijöihinjaon, jolloin hän pystyy helposti purkamaan viestin salauksen.

Alkulukujen valitsemiseen liittyy siis ongelma: kuinka voidaan valita kaksi mahdollisimman suurta alkulukua, toisin sanoen mistä voidaan tietää, onko jokin suuri luku alkuluku vai yhdistetty luku. Jotta voidaan valita sopivat alkuluvut RSA-salauksessa käytettäväksi, täytyy selvittää, onko satunnaisesti valittu suuri luku n mahdollisesti alkuluku vai yhdistetty luku.

3.3 Määritelmiä ja lauseita

Lause 3.3 (Fermat'n pieni lause)**.** *Olkoon $p \in \mathbb{P}$ alkuluku. Tällöin*

$$a^{p-1} \equiv 1 \pmod{p}, \ \textit{jos } p \nmid a \in \mathbb{Z}$$

Todistus. Olkoon p alkuluku ja a kokonaisluku siten, että se ei ole jaollinen luvulla p eli $p \in \mathbb{P}, a \in \mathbb{Z}, p \nmid a$. Olkoon

$$A = \{1, 2, 3, \ldots, (p-1)\}$$

positiivisten kokonaislukujen osajoukko.

Koska luku p on alkuluku, joka ei ole luvun a tekijä eikä minkään osajoukon A alkion tekijä, niin se ei myöskään ole joukon

$$A_a = \{(a, 2a, 3a, \ldots, (p-1)a\}$$

tekijä. Joukossa A_a on $(p-1)$ kappaletta lukuja, joiden oletetaan olevan keskenään erisuuria. Tämän osoittamiseksi valitaan satunnaisesti kaksi joukon A_a alkiota $ja \pmod{p}$ ja $ka \pmod{p}$, jotka oletetaan yhtäsuuriksi. Näinollen

$$ja \equiv ka \pmod{p},$$

joten $(j-k)a \equiv 0 \pmod{p}$.

Koska $p \mid (j-k)a$, niin on oltava siten, että $p \mid (j-k)$, sillä oletuksen mukaan $p \nmid a$. Kumpikin luvuista $j \in [1, (p-1)]$ ja $k \in [1, (p-1)]$, joten niiden erotus $j - k \in [-(p-2), (p-2)]$. Lukujen $-(p-2)$ ja $p-2$ välillä on vain yksi luvulla p jaollinen luku ja se on luku nolla. Niinpä lukujen erotus $j - k = 0$, joten $ja = ka$ ja joukon A_a luvut ovat kaikki eri suuria. Ne ovat myös nollasta eroavia, sillä luvut $1, 2, 3, \ldots, p-1$ ja a eivät ole jaollisia luvulla p.

Siispä mitkään luvuista $a, 2a, 3a, \ldots, (p-1)a$ eivät ole kongruentteja keskenään modulo p.

Täten tiedetään, että

$$1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv a \cdot 2a \cdot \ldots \cdot (p-1)a \pmod{p}.$$

Tämä voidaan saattaa kertoman avulla muotoon

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

Jaetaan puolittain luvulla $(p-1)!$, joten yhtälö saadaan muotoon

$$a^{(p-1)} \equiv 1 \pmod{p},$$

joka on Fermat'n pieni lause. □

Lause 3.4 (Fermat'n pieni lause versio 2)**.** *Olkoon $p \in \mathbb{P}$ alkuluku. Tällöin*

$$a^p \equiv a \pmod{p}, \ \forall\ a \in \mathbb{Z}.$$

Todistus. Jos $p \nmid a$, niin ensimmäisestä Fermat'n pienestä lausesta seuraa, että $a^{p-1} \equiv 1 \mod p$. Kerrottaessa tämä puolittain luvulla a saadaan

$$a^p \equiv a \pmod{p},$$

mikä tosoittaa, että Lause 3.3 on totta.

Toisaalta, jos $p \mid a$, niin molemmat puolet ovat $0 \mod p$. □

Määritelmä 3.5. Olkoon n jokin kokonaisluku. Sanotaan, että a on todistaja luvun n *jaollisuudesta* eli luku a on todistaja, että luku n on yhdistetty luku mikäli

$$a^n \not\equiv a \pmod{n}.$$

Esimerkki 3.6. Olkoon $n = 15$ yhdistetty luku, sillä $15 = 3 \cdot 5$. Luku $a = 2$ on todistaja luvun $n = 15$ jaollisuudesta, sillä

$$2^{15} \equiv 13 \neq 2 \pmod{15}.$$

Fermat'n pienen Lauseen 3.4 ja Määritelmän 3.5 avulla voidaan osoittaa ehdottomasti, että jokin luku n on yhdistetty luku. Tätä varten riittää löytää yksikin todistaja a. Fermat'n testin avulla ei kuitenkaan saada varmaa tietoa siitä, onko luku n alkuluku, sillä on olemassa sellaisia yhdistettyjä lukuja, joille ei löydy Määritelmän 3.5 kaltaista todistajaa. Tällaisia lukuja kutsutaan Carmichaelin luvuiksi.

Määritelmä 3.7. *Carmichaelin luvut* ovat sellaisia yhdistettyjä lukuja, joille ei löydy todistajaa a luvun n jaollisuudesta.

Huomautus 3.8. Vaikka todistajaa a etsiessä kokeillaan useilla luvun a eri arvoilla löytämättä todistajaa a, ei voida tehdä päätelmiä siitä, onko luku n alkuluku.

4 Alkulukujen testaaminen

Toimivaa RSA-salausta varten on kyettävä valitsemaan alkuluvut hyvin. Tätä varten tarvitaan keinoja selvittää, onko valittu luku alkuluku vai yhdistetty luku. Alkulukutestaamista on tutkittu jo antiikin Kreikan aikaan, mutta vasta nykytietokoneet ovat mahdollistaneet suurienkin lukujen tekijöihinjakamisen ja alkulukujen testaamisen. On olemassa useita erilaisia alkulukutestejä, joista nyt käsitellään Millerin ja Rabinin testiä yhdistetyille luvuille.

4.1 Millerin ja Rabinin testi

Fermat'n pienen lauseen 3.4 ja Määritelmän 3.5 avulla voidaan selvittää luvun jaollisuutta, mutta niiden avulla ei saada tietoa siitä, onko luku n alkuluku. Millerin ja Rabinin testin avulla pystytään osoittamaan minkä tahansa yhdistetyn luvun jaollisuus ja se perustuu Fermat'n pienen lauseen muunnelmaan.

Lause 4.1. *Olkoon p alkuluku*

$$p - 1 = 2^k q, \text{ missä } q \text{ on pariton.}$$

Jos a on sellainen kokonaisluku, että p ja a ovat keskenään jaottomia eli $p \nmid a$, niin toinen seuraavista väittämistä pätee:

1. $a^q \equiv 1 \pmod{p}$
2. *On olemassa jokin sellainen luku $k \in \{0, 1, \ldots, l-1\}$,*
   missä $l = max\{k \in \mathbb{N} : 2^k \mid p - 1\}$, että

$$a^{2^{k-1}q} \equiv -1 \pmod{p}.$$

Todistus. Fermat'n pienen lauseen mukaan $a^{p-1} \equiv 1 \pmod{p}$. Tutkittaessa jonoa $a^q, a^{2q}, a^{4q}, \ldots, a^{2^{k-1}q}, a^{2^k q}$ tiedetään, että jonon viimeiselle luvulle pätee

$$a^{2^k q} = a^{p-1} \equiv 1 \pmod{p}.$$

Tämän lisäksi jokainen jonon luvuista on edellisen luvun neliö, joten toinen seuraavista ehdoista pätee:

1. Jonon ensimmäinen luku $a^q \equiv 1 \pmod{p}$

2. Kaikki jonon luvuista eivät ole kongruentteja luvun yksi kanssa modulo p, vaan jollekin jonon luvuista b pätee:

$$b \not\equiv 1 \pmod{p}.$$

Kuitenkin luvun b neliölle pätee aina:

$$b^2 \equiv 1 \pmod{p}.$$

Ainoa luku, joka täyttää yhtäaikaisesti molemmat ehdot

$$b \not\equiv 1 \pmod{p} \text{ ja } b^2 \equiv 1 \pmod{p}$$

on luku -1, joten jonossa on oltava sellainen luku c, jolle

$$c \equiv -1 \pmod{p}.$$

□

Määritelmä 4.2 (Millerin ja Rabinin testi yhdistetyille luvuille)**.** Olkoon n positiivinen ja pariton kokonaisluku. Olkoon

$$n - 1 = 2^k q, \text{ missä } q \text{ on pariton.}$$

Lukua a, joka toteuttaa ehdon $\text{syt}(a, n) = 1$ kutsutaan *Miller-Rabinin todistajaksi* luvun n *jaollisuudesta*, mikäli seuraavat ehdot:

1. $a^q \not\equiv 1 \pmod{n}$
2. $a^{2^i q} \not\equiv -1 \pmod{n}$ kaikilla $i = 0, 1, 2, \ldots, k-1$

toteutuvat.

4.2 Millerin ja Rabinin testin käyttäminen

Olkoon luku n positiivinen kokonaisluku, joka on testattavana. Olkoon lisäksi kokonaisluku a mahdollinen todistaja luvun n jaollisuudesta. Millerin ja Rabinin testissä tutkitaan, toteuttaako tutkittava luku n testin ehdot eli löytyykö jokin todistaja a luvun n jaollisuudesta. Mikäli löydetään todistaja a, jolle ovat voimassa ehdot $a^q \not\equiv 1 \pmod{p}$ ja $a^{2^i q} \not\equiv -1 \pmod{n}$, kaikilla $i = 0, 1, 2, \ldots, k-1$, niin luku n paljastuu yhdistetyksi luvuksi. Mikäli se ei toteuta ehtoja tutkittavalla mahdollisella todistajalla, luku n voi olla alkuluku. Toisaalta se voi edelleen olla myös yhdistetty luku, jonka pystyy osoittamaan jollakin sopivalla todistajalla. Millerin ja Rabinin testissä suoritetaan seuraavat vaiheet:

1. Jos n on parillinen tai $1 < \text{syt}(a, n) < n$, niin n on yhdistetty luku eli se ei voi olla alkuluku. Mikäli tämä ehto ei toteudu, luku n voi edelleen olla alkuluku, joten jatketaan testaamista kohdan 2 mukaan.

2. Kirjoitetaan luku n muodossa $n - 1 = 2^k q$, missä q on pariton. Etsitään siis pariton kokonaisluku q jakamalla lukua $n-1$ kahdella, kunnes saadaan luku $n - 1$ muotoon $n - 1 = 2^k q$.

3. Lasketaan a^q.

   - Jos saadaan $a^q \not\equiv 1 \pmod{n}$, jatketaan testiä kohtaan 4.
   - Mikäli saadaan $a \equiv 1 \pmod{n}$, testi epäonnistuu, eikä saada tietoa luvun n jaollisuudesta. Luku n voi siis olla yhdistetty luku tai alkuluku.

4. Lasketaan $a^{2^i q}$, kaikilla $i = 0, 1, 2, ..., k - 1$.

   - Jos saadaan $a^{2^i q} \not\equiv -1 \pmod{n}$, kaikilla $i = 0, 1, 2, ..., k - 1$, jatketaan kohtaan 5.
   - Mikäli saadaan $a^{2^i q} \equiv -1 \pmod{n}$ jollakin $i = 0, 1, 2, ..., k - 1$, testi epäonnistuu, eikä saada tietoa luvun n jaollisuudesta. Luku n voi olla yhdistetty luku tai alkuluku.

5. Mikäli mahdollinen todistaja a toteuttaa molemmat ehdot

   (a) $a^q \not\equiv 1 \pmod{n}$

   (b) $a^{2^i q} \not\equiv -1 \pmod{n}$, kaikilla $i = 0, 1, 2, ..., k - 1$

   on se todistaja luvun n jaollisuudesta ja luvun n on oltava yhdistetty luku. Mikäli vähintään toinen ehdoista ei toteudu, testillä ei saada tietoa luvun n jaollisuudesta todistajalla a, vaan täytyy tutkimus tehdä jollakin toisella mahdollisella todistajalla.

Lause 4.3. *Olkoon n satunnainen jaollinen luku. Tällöin välillä $1, ..., n - 1$ olevista luvuista a ainakin 75 % on Millerin ja Rabinin todistajia luvulle n.*

Todistus. Todistus sivuutetaan. □

Esimerkki 4.4. Tutkitaan paritonta lukua $n = 1105$. Mikäli luku n on yhdistetty luku, se toteuttaa Millerin ja Rabinin testin ehdot. Mikäli se ei toteuta ehtoja, se voi olla alkuluku. Kirjoitetaan Määritelmän 4.2 ja testin kohdan 2 mukaisesti $n - 1$ muotoon $2^k q$, missä q on pariton:

$$n - 1 = 1105 - 1 = 1104 = 2^4 \cdot 69.$$

Nyt siis $k = 4$ ja $q = 69$, q on pariton.

Tutkitaan, onko luku $a = 2$ todistaja luvun $n = 1105$ jaollisuudesta eli onko luku a todistaja, että luku n on yhdistetty luku. Tämä tapahtuu selvittämällä täyttyvätkö ehdot:

$$a^q \not\equiv 1 \pmod{1105} \text{ ja}$$
$$a^{2^i q} \not\equiv -1 \pmod{1105} \text{ kaikilla } i = 0, 1, 2, \ldots, k-1.$$

Mikäli molemmat ehdot täyttyvät, luku n on yhdistetty luku. Mikäli toinen ehdoista ei täyty, testi epäonnistuu. Tällöin ei voida sanoa onko luku yhdistetty luku vai alkuluku ja on kokeiltava etsiä jokin toinen mahdollinen todistaja luvun jaollisuudesta.

Suoritetaan Millerin ja Rabinin testi mahdolliselle todistajalle $a = 2$. Tutkitaan ensiksi toteutuuko ehto $a^q \not\equiv 1 \pmod{1105}$. Nopealla potenssiinkorotuksella lasketaan

$$2^{69} \equiv 967 \equiv -138 \pmod{1105}.$$

Nyt $2^{69} \equiv 967 \equiv -138 \not\equiv 1 \pmod{1105}$ eli $2^{69} \not\equiv 1 \pmod{1105}$.

Tutkitaan seuraavaksi, toteutuuko ehto $a^{2^i q} \not\equiv -1 \pmod{1105}$ kaikilla $i = 0, 1, 2, \ldots, k-1$. Lasketaan nopealla potenssiinkorotuksella

$$2^{2^0 \cdot 69} = 2^{1 \cdot 69} \equiv 967 \pmod{1105},$$
$$2^{2^1 \cdot 69} = 2^{2 \cdot 69} \equiv (967)^2 \equiv 935089 \equiv 259 \pmod{1105},$$
$$2^{2^2 \cdot 69} = 2^{4 \cdot 69} \equiv (259)^2 \equiv 67081 \equiv 781 \equiv -324 \pmod{1105} \text{ ja}$$
$$2^{2^3 \cdot 69} = 2^{8 \cdot 69} \equiv (-324)^2 \equiv 104976 \equiv -1 \pmod{1105}.$$

Kun $i = 3$ saadaan $2^{2^3 \cdot 69} \equiv -1 \pmod{1105}$, joten ehto $a^{2^i q} \not\equiv -1 \pmod{1105}$ kaikilla $i = 0, 1, 2, \ldots, k-1$ ei toteudu. Siispä testi ei anna tulosta luvun n jaollisuudesta, kun todistajaksi kokeiltiin lukua $a = 2$.

Kokeillaan testiä mahdollisella todistajalla $a = 3$. Nopealla potenssiinkorotuksella

$$3^{69} \equiv 1093 \equiv -12 \pmod{1105},$$

joten ehto $a^q \not\equiv 1 \pmod{1105}$ toteutuu.

Lasketaan nopealla potenssiinkorotuksella

$$3^{2^0 \cdot 69} = 3^{1 \cdot 69} \equiv -12 \pmod{1105},$$
$$3^{2^1 \cdot 69} = 3^{2 \cdot 69} \equiv (-12)^2 \equiv 144 \pmod{1105},$$
$$3^{2^2 \cdot 69} = 3^{4 \cdot 69} \equiv (144)^2 \equiv 20736 \equiv 846 \equiv -259 \pmod{1105} \text{ ja}$$
$$3^{2^3 \cdot 69} = 3^{8 \cdot 69} \equiv (-259)^2 \equiv 67081 \equiv 781 \equiv -324 \pmod{1105}.$$

Koska $3^{69} \not\equiv 1 \pmod{1105}$ ja $3^{2^i \cdot 69} \not\equiv -1 \pmod{1105}$, kaikilla $i \in [0, 3]$ luku a on todistaja luvun n jaollisuudesta, joten luku n on yhdistetty luku eikä se siis voi olla alkuluku.

Lähdeluettelo

[1] Hoffstein, J., Pipher, J., and Silverman, J. H.: *Undergraduate texts in mathematics; An Introduction to Mathematical Cryptography*. Springer, New York, 2008.

[2] Leinonen, L., Matala-aho, T., Rinta-aho, T., Törmä, T., Väänänen, K.: *Luentorunko; Salausmenetelmät*. Oulun Yliopisto, Oulu, 2017.