Rabinin salausjärjestelmä

LuK-tutkielma
Suvi Takalahti
Matemaattisten tieteiden laitos
Oulun yliopisto
Kevät 2022

Sisällys

Johdanto

Rabinin salausjärjetelmä on epäsymmetrinen salausjärjestelmä, eli siinä valitaan käyttöön kaksi avainta, joista julkista avainta käytetään tekstin salaamiseen ja salaista avainta viestin avaamiseen. Rabinin salausjärjestelmässä tekstin salaaminen perustuu vain yhteen neliöön korotukseen ja on näin ollen hyvin tehokasta. Viestin avaamiseen tarvitaan useampia askeleita ja ongelmaksi muodostuu, ettei avattaessa saada yksiselitteistä vastausta, vaan vastauksia saadaan aina neljä. Järjestelmän merkittävänä etuna on sen turvallisuus, sillä sen murtamisen voidaan todistaa olevan yhtä vaikeaa kuin suurten lukujen alkulukutekijöihin jakaminen.

Tässä tutkielmassa esitellään Rabinin salausjärjestelmän toimintaperiaatteet ja todistetaan muutamia niihin liittyviä lauseita. Lukijalla on hyvä olla peruskäsitys lukuteorian ja algebran peruskäsitteistä, erityisesti kongruenssista. Kappaleessa 1 määritellään käsitteitä ja esitetään lauseita, joita tarvitaan myöhemmin Rabinin salausjärjestelmän ymmärtämiseen. Kappaleessa 2 esitellään salausjärjestelmän toimintaperiaatteet ja ratkaisuja edellä mainittuun neljän vastauksen ongelmaan. Lopuksi todistetaan, että Rabinin salausjärjestelmän murtaminen on yhtä vaikeaa kuin suurten lukujen alkulukutekijöihinjako. Kappaleessa 3 esitellään eräs Rabinin salausjärjestelmän laajennus.

Tutkielmassa on käytetty lähteenä pääasiassa R. Oppligerin teosta *Contemporary cryptography* [1] ja S.D. Galbraithin teosta *Mathematics of public key cryptography* [2]. Lisäksi viimeisessä kappaleessa on hyödynnetty L.M. Battenin ja H.C. Williamsin artikkelia *Unique Rabin-Williams Signature Scheme Decryption* [3].

1 Esitietoja

Tässä kappaleessa määritellään käsitteitä ja esitetään lauseita, joita tarvitaan Rabinin salausjärjestelmän ymmärtämiseen ja siihen liittyvien lauseiden todistukseen. Lopuksi määriteltävää Jacobin symbolia ja siihen liittyviä lauseita tarvitaan Rabin-Williams salausjärjestelmän rakentamiseen. Suurin osa lauseista esitetään ilman todistusta. Todistukset voi löytää kappaleen pääasiallisena lähteenä käytetystä teoksesta [1].

Lause 1.1 (Kiinalainen jäännöslause)**.** *Olkoot luvut $n_1, n_2, \ldots, n_k$ keskenään pareittain jaottomia, positiivisia kokonaislukuja ja luvut $a_1, a_2, \ldots, a_k$ kokonaislukuja. Lisäksi olkoon näille luvuille voimassa kongruenssiyhtälöryhmä*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k}. \end{aligned}$$

Tällöin edeltävälle kongruenssiyhtälöryhmälle on olemassa yksiselitteinen ratkaisu $x \in \mathbb{Z}_n$, missä $n = \prod_{n=1}^{k} n_i$.

Erityisesti x voidaan laskea seuraavasti:

$$x = \sum_{i=1}^{k} a_i m_i y_i \pmod{n},$$

missä $m_i = \frac{n}{n_i}$ kaikille $i = 1, \ldots, k$ ja $y_i = m_i^{-1} \pmod{n_i}$ on luvun m_i käänteisalkio kertolaskuoperaation suhteen jäännösluokkarenkaassa $(\mathbb{Z}_{n_i}, +, \cdot)$.

Lause 1.2 (Eukleideen algoritmi)**.** *Olkoot a ja b positiivisia kokonaislukuja ja lisäksi $a \neq 0$, $b \neq 0$ ja $|a| > |b|$. Tällöin*

$$\begin{aligned} a &= bq_1 + r_1, \text{missä } 0 < r_1 < b \\ b &= r_1 q_2 + r_2, \text{missä } 0 < r_2 < r_1 \\ r_1 &= r_2 q_3 + r_3, \text{missä } 0 < r_3 < r_2 \\ &\vdots \\ r_{k-3} &= r_{k-2} q_{k-1} + r_{k-1}, \text{missä } 0 < r_{k-1} < r_{k-2} \\ r_{k-2} &= r_{k-1} q_k. \end{aligned}$$

Kaikki luvut q_i ja r_i, $i = 1, ..., k$ ovat positiivisia kokonaislukuja. Nyt luku r_{k-1} on lukujen a ja b suurin yhteinen tekijä.

Seuraus 1.3. *Eukleideen algoritmin avulla voidaan löytää x ja y siten, että*

$$xa + yb = \text{syt}(a, b).$$

Lause 1.4. *Olkoon luku a alkio jäännösluokkien joukossa modulo n. Tällöin luvulla a on käänteisalkio kertolaskuoperaation suhteen jäännösluokkarenkaassa $(\mathbb{Z}_n, +, \cdot)$ jos ja vain jos* $\text{syt}(a, n) = 1$.

Huomautus 1.5. Jos $\text{syt}(a, n) = 1$, niin luvun a käänteisalkio a^{-1} jäännösluokkarenkaassa $(\mathbb{Z}_n, +, \cdot)$ voidaan löytää Eukleideen algoritmin avulla, sillä nyt Seurauksen 1.3 nojalla

$$1 = \text{syt}(a, n) = xa + yn,$$

josta seuraa, että $xa \equiv 1 \pmod{n}$. Koska luku 1 on neutraalialkio kertolaskuoperaation suhteen jäännösluokkarenkaassa $(\mathbb{Z}_n, +, \cdot)$, niin $x = a^{-1}$.

Määritelmä 1.6 (Blumin kokonaisluku)**.** Olkoot p ja q alkulukuja ja lisäksi $p \equiv 3 \pmod{4}$ ja $q \equiv 3 \pmod{4}$. Luku n on *Blumin kokonaisluku*, jos se on muotoa $n = pq$.

Lause 1.7. *Olkoot n Blumin kokonaisluku ja luvut x ja y alkioita jäännösluokkien joukossa modulo n siten, että $x \equiv y^2 \pmod{n}$. Tällöin luvulla x on tasan neljä neliöjuurta jäännösluokkarenkaassa $(\mathbb{Z}_n, +, \cdot)$.*

Määritelmä 1.8 (Eulerin φ-funktio)**.** Olkoon m positiivinen kokonaisluku. Nyt funktio $\varphi : \mathbb{Z}_+ \to \mathbb{Z}_+, \varphi(m) = |\mathbb{Z}_m^*|$ kertoo sellaisten, lukua m pienempien, positiivisten kokonaislukujen määrän, joille suurin yhteinen tekijä luvun m kanssa on 1, eli

$$\varphi(m) = |\{a \in \{0, \ldots, m-1\} : \ \text{syt}(a, m) = 1\}|.$$

Lause 1.9. *Jos p on alkuluku, niin*

$$\varphi(p) = p - 1.$$

Todistus. Nyt alkuluvun määritelmän nojalla $\text{syt}(a, p) = 1$ kaikille positiivisille kokonaisluvuille a, jotka ovat pienempiä kuin p. Siispä kaikki luvut $0 \leq a < p$ toteuttavat Eulerin φ-funktion ehdon ja on oltava $\varphi(p) = p-1$. □

Lause 1.10 (Eulerin teoreema)**.** *Jos* $\text{syt}(a, n) = 1$*, niin*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Määritelmä 1.11 (Legendren symboli)**.** Olkoot p alkuluku ja x kokonaisluku. Nyt *Legendren symboli* kertoo, onko luku x neliöjäännös modulo p, eli onko olemassa jokin kokonaisluku y siten, että $y^2 \equiv x \pmod{p}$. Luvun x *Legendren symboli* modulo p määritellään seuraavasti:

$$\left(\frac{x}{p}\right) = \begin{cases} 1, & \text{jos } x \text{ on neliöjäännös modulo } p, \\ -1, & \text{muulloin.} \end{cases}$$

Lause 1.12. *Olkoon p alkuluku ja x kokonaisluku. Tällöin luvun x Legendren symboli modulo p voidaan laskea seuraavasti:*

$$\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \pmod{p}.$$

Määritelmä 1.13 (Jacobin symboli)**.** *Jacobin symboli* on Legendren symbolin yleistys. Se ottaa huomioon myös tapaukset, joissa moduloluku n ei ole alkuluku. Erityisesti tapauksessa, jossa p ja q ovat alkulukuja ja luku n on muotoa $n = pq$, kokonaisluvun x *Jacobin symboli* modulo n määritellään luvun x Legendren symbolien modulo p ja modulo q tulona, eli

$$\left(\frac{x}{n}\right) = \left(\frac{x}{p}\right) \cdot \left(\frac{x}{q}\right).$$

Lause 1.14. *Olkoot x, y ja n kokonaislukuja. Jos $x \equiv y \pmod{n}$, niin*

$$\left(\frac{x}{n}\right) = \left(\frac{y}{n}\right).$$

Lause 1.15. *Olkoot x, y ja n kokonaislukuja. Tällöin*

$$\left(\frac{xy}{n}\right) = \left(\frac{x}{n}\right) \cdot \left(\frac{y}{n}\right).$$

Lause 1.16. *Olkoon n kokonaisluku. Tällöin*

$$\left(\frac{-1}{n}\right) = n^{\frac{n-1}{2}} = \begin{cases} 1, & \textit{jos } n \equiv 1 \pmod{4}, \\ -1, & \textit{jos } n \equiv 3 \pmod{4}. \end{cases}$$

Lause 1.17. *Olkoon n kokonaisluku. Tällöin*

$$\left(\frac{2}{n}\right) = n^{\frac{n^2-1}{8}} = \begin{cases} 1, & \textit{jos } n \equiv 1 \textit{ tai } n \equiv 7 \pmod{8}, \\ -1, & \textit{jos } n \equiv 3 \textit{ tai } n \equiv 5 \pmod{8}. \end{cases}$$

2 Rabinin salausjärjestelmä

Tässä kappaleessa esitellään Rabinin salausjärjestelmän avaimen valintaan ja viestin salaukseen sekä avaukseen käytetyt algoritmit sekä käsitellään neljän neliöjuuren ongelman ratkaisuja. Lopuksi käsitellään tarkemmin järjestelmän turvallisuutta. Kappaleissa 2.1, 2.2 ja 2.4 on käytetty pääasiallisena lähteenä teosta [1] ja Kappaleessa 2.3 teosta [2].

2.1 Avaimen valinta ja tekstin salaus

Valitaan kaksi suurta alkulukua p ja q, joille pätee $p \equiv 3 \pmod 4$ ja $q \equiv 3 \pmod 4$. Lasketaan sitten luku $n = pq$. Valitaan julkiseksi avaimeksi luku n ja salaiseksi avaimeksi lukupari (p, q).

Rabinin salausjärjestelmää voidaan käyttää salaamaan tekstejä, jotka ovat muotoa $m \in \mathbb{Z}_n = \{0, \ldots, n-1\}$, eli salattavan tekstin m tulee olla alkio jäännösluokkien joukossa modulo n. Salattu viesti c muodostetaan korottamalla salattava teksti m toiseen potenssiin modulo n, eli

$$c \equiv m^2 \pmod n. \tag{1}$$

Siispä Rabinin salausjärjestelmä perustuu funktioon $f : \mathbb{Z}_n \to \mathbb{Z}_n, f(x) = x^2 \pmod n$, missä luku n on Blumin kokonaisluku. Funktio f on niin sanottu salaovifunktio, jonka tarkempi määritelmä annetaan Määritelmässä 2.2. Sitä ennen on kuitenkin määriteltävä yksisuuntainen funktio.

Määritelmä 2.1 (Yksisuuntainen funktio)**.** Funktio $f : X \to Y$ on *yksisuuntainen funktio*, jos sen arvo $f(x)$ on helppo määrittää kaikille lähtöjoukon alkioille x, mutta sen käänteisfunktion arvo $f^{-1}(y)$, mielivaltaiselle maalijoukon alkiolle y, on vaikea määrittää.

Määritelmä 2.2 (Salaovifunktio)**.** Yksisuuntainen funktio $f : X \to Y$ on *salaovifunktio*, jos on olemassa jotain sellaista ylimääräistä informaatiota, jonka avulla sen käänteisfunktion arvo $f^{-1}(y)$, mielivaltaiselle maalijoukon alkiolle y, on helppo määrittää. Tätä ylimääräistä informaatiota kutsutaan *salaoveksi*.

Funktio $f : \mathbb{Z}_n \to \mathbb{Z}_n, f(x) = x^2 \pmod n$, on siis salaovifunktio: Funktion arvo $f(x) = x^2 \pmod n$ on helppo määrittää kaikille lähtöjoukon $\mathbb{Z}_n$ alkioille x, mutta, kuten tullaan näkemään Kappaleessa 2.2, tarvitaan käänteisfunktion arvon $f^{-1}(y) = \sqrt{y} \pmod n$ määrittämiseen, moduloluvun n alkulukutekijöitä p ja q. Siispä Rabinin salausjärjestelmässä tekstin salaaminen vastaa salaovifunktion arvon määrittämistä tekstiä vastaavalle luvulle m ja viestin avaaminen taas vastaa salaovifunktion käänteisfunktion arvon

määrittämistä luvulle c, joka vastaa salattua viestiä. Järjestelmän salainen avain (p, q) toimii salaovena. Tekstin salaaminen Rabinin salausjärjestelmässä on erittäin tehokasta, sillä kuten edellä nähtiin, se perustuu vain yhteen neliöön korotukseen. Tämä onkin salausjärjestelmän merkittävimpiä etuja.

Esimerkki 2.3 (Avaimen valinta ja salaus)**.** Muodostetaan esimerkki Rabinin salausjärjestelmän käytöstä. Valitaan salaiseksi avaimeksi alkuluvut $p = 19$ ja $q = 31$. Nyt $19 \equiv 31 \equiv 3 \pmod 4$. Lasketaan sitten luku $n = 19 \cdot 31 = 589$ ja käytetään tätä lukua järjestelmämme julkisena avaimena. Julkinen avain 589 voidaan julkaista ja salainen avain $(19, 31)$ pidetään vain viestin lähettäjän ja vastaanottajan tiedossa.

Salausärjestelmää voidaan käyttää salaamaan viestejä m, jotka ovat muotoa $m \in \mathbb{Z}_{589} = \{0, \ldots 588\}$. Oletetaan, että lähettäjä haluaa lähettää viestin $m = 58$. Hän salaa viestin ja saa salatun tekstin

$$c \equiv 58^2 \equiv 3364 \equiv 419 \pmod{589}.$$

Salattu viesti $c = 419$ lähetetään vastaanottajalle, jolla on tiedossa järjestelmän salainen avain.

2.2 Viestin avaus

Salatun viestin c avaamiseksi viestin vastaanottajan tulee löytää luvun c neliöjuuri modulo n. Neliöjuuren löytämiseksi vastaanottaja käyttää salaista avainta (p, q), eli moduloluvun n alkulukutekijöitä. Koska luku n on Blumin kokonaisluku, niin Lauseen 1.7 nojalla luvulle c löydetään itseasiassa neljä neliöjuurta modulo n. Tämä onkin eräs Rabinin salausjärjestelmän heikkouksista, sillä vastaanottajan on mahdotonta, ilman ylimääräistä informaatiota, tietää mikä näistä neljästä neliöjuuresta edustaa oikeaa alkuperäistä tekstiä.

Koska n on Blumin kokonaisluku, se on muotoa $n = pq$. Tästä seuraa, että Lauseen 1.1 nojalla jos löydetään luvut m_p ja m_q, jotka toteuttavat seuraavat kongruenssiyhtälöt

$$\begin{aligned} \sqrt{c} &\equiv m_p \pmod p \\ \sqrt{c} &\equiv m_q \pmod q, \end{aligned}$$

niin löydetään jokin m_x, joka on alkio jäännösluokkien joukossa modulo n ja toteuttaa yhtälön $\sqrt{c} \equiv m_x \pmod n$. Siispä näin löydetään etsitty neliöjuuri ja saadaan avattua viesti c. Kuten edellä todettiin, viestiä avatessa saadaan todellisuudessa neljä vastausta, joten on myös muodostettava neljä edellisentyyppistä kongruenssiyhtälöryhmää. Nimetään näiden vastaukset m_1, m_2, m_3 ja m_4.

Aloitetaan siis viestin avaaminen etsimällä luvut m_p ja m_q siten, että $m_p^2 \equiv c \pmod{p}$ ja $m_q^2 \equiv c \pmod{q}$. Ne voidaan laskea seuraavan lauseen osoittamalla tavalla.

Lause 2.4. *Olkoot p alkuluku ja n Blumin kokonaisluku, jonka toinen tekijä on p. Lisäksi olkoot m alkio jäännösluokkien joukossa modulo n ja $c \equiv m^2 \pmod{n}$. Tällöin luku m_p, jolle pätee $m_p^2 \equiv c \pmod{p}$, voidaan muodostaa seuraavalla tavalla:*

$$m_p \equiv c^{\frac{p+1}{4}} \pmod{p}.$$

Todistus. Asetetaan $m_p \equiv c^{\frac{p+1}{4}} \pmod{p}$ ja osoitetaan, että tästä seuraa, että $m_p^2 \equiv c \pmod{p}$.

Oletuksen nojalla

$$m_p^2 \equiv (c^{\frac{p+1}{4}})^2 \equiv c^{\frac{p+1}{2}} \equiv (c^{\frac{1}{2}})^{p+1} \equiv m^{p+1} \pmod{p}.$$

Koska p on alkuluku, on oltava $\text{syt}(m, p) = 1$ tai $\text{syt}(m, p) = p$.

Tutkitaan ensin tilannetta, jossa $\text{syt}(m, p) = 1$: Nyt

$$m^{p+1} \equiv m^{(p-1)+2} \equiv m^{p-1}m^2 \pmod{p}$$

ja Lauseen 1.9 nojalla $\varphi(p) = p - 1$, joten

$$m^{p-1}m^2 \equiv m^{\varphi(p)}m^2 \pmod{p}.$$

Edelleen Lauseen 1.10 nojalla

$$m^{\varphi(p)} \equiv 1 \pmod{p},$$

joten

$$m^{\varphi(p)}m^2 \equiv m^2 \equiv c \pmod{p}.$$

Tutkitaan sitten tilannetta, jossa $\text{syt}(m, p) = p$: Nyt luku p jakaa luvun m, joten $m \equiv 0 \pmod{p}$ ja edelleen $m^x \equiv 0 \pmod{p}$ kaikille positiivisille kokonaisluvuille x. Siispä

$$m^{p+1} \equiv 0 \equiv m^2 \pmod{p}.$$

Siispä on osoitettu, että

$$m_p^2 \equiv c \pmod{p}.$$

□

Lauseen 2.4 nojalla $m_p \equiv c^{\frac{p+1}{4}} \pmod{p}$ ja $m_q \equiv c^{\frac{q+1}{4}} \pmod{q}$. Nyt luvun c kaksi neliöjuurta modulo p ovat $\pm m_p$ ja vastaavasti luvun c kaksi neliöjuurta modulo q ovat $\pm m_q$. Luvut $\pm m_p$ ja $\pm m_q$ voidaan yhdistää kaikkiaan neljällä tavalla. Näistä neljästä tavasta saadaan seuraavat kongruenssiyhtälöryhmät:

$$
\begin{aligned}
&1) && m_1 \equiv +m_p \pmod{p} \\
& && m_1 \equiv +m_q \pmod{q} \\
&2) && m_2 \equiv -m_p \pmod{p} \\
& && m_2 \equiv -m_q \pmod{q} \\
&3) && m_3 \equiv +m_p \pmod{p} \\
& && m_3 \equiv -m_q \pmod{q} \\
&4) && m_4 \equiv -m_p \pmod{p} \\
& && m_4 \equiv +m_q \pmod{q}.
\end{aligned}
$$

Kaikkien neljän yhtälöryhmän ratkaisuksi saadaan eräs luvun c neliöjuuri modulo n. Yksi näistä ratkaisuista m_1, m_2, m_3 tai m_4 vastaa alkuperäistä tekstiä m.

Lauseen 1.1 nojalla yllä olevista kongruenssiyhtälöryhmistä saadaan vastaukset

$$
\begin{aligned}
&1) && m_1 = m_p q y_q + m_q p y_p \pmod{n} \\
&2) && m_2 = -m_p q y_q - m_q p y_p \pmod{n} \\
&3) && m_3 = m_p q y_q - m_q p y_p \pmod{n} \\
&4) && m_4 = -m_p q y_q + m_q p y_p \pmod{n},
\end{aligned}
$$

missä $y_p \equiv p^{-1} \pmod{q}$ ja $y_q \equiv q^{-1} \pmod{p}$. Koska luvut p ja q ovat alkulukuja, niin $\text{syt}(p, q) = 1$ ja näin ollen Lauseen 1.4 nojalla luvulla p on käänteisalkio p^{-1} kertolaskuoperaation suhteen jäännösluokkarenkaassa $(\mathbb{Z}_q, +, \cdot)$. Samoin luvulla q on käänteisalkio q^{-1} kertolaskuoperaation suhteen jäännösluokkarenkaassa $(\mathbb{Z}_p, +, \cdot)$. Siispä luvut y_p ja y_q ovat olemassa ja ne voidaan löytää Eukleideen algoritmin avulla, kuten on esitetty Lauseessa 1.2. Luvut y_p ja y_q eivät riipu alkuperäisestä tekstistä m tai salatusta viestistä c, joten ne voidaan laskea kerran ja niitä voidaan käyttää avaamaan kaikkia viestejä,

jotka on salattu käyttäen Rabinin salausjärjestelmää samoilla avaimilla (p, q) ja $n = pq$.

Huomataan, että $m_2 = -m_1 \pmod{n}$ ja $m_4 = -m_3 \pmod{n}$. Siispä vastaanottaja voi laskea vain luvut r ja s seuraavasti:

$$r = m_p q y_q + m_q p y_p \pmod{n}$$

ja

$$s = m_p q y_q - m_q p y_p \pmod{n}.$$

Luvun c neljä neliöjuurta modulo n ovat $r, -r, s$ ja $-s$ ja jokin näistä neliöjuurista vastaa alkuperäistä tekstiä m. Kappaleessa 2.3 esitellään keinoja, joiden avulla voidaan varmistaa, että viestin vastaanottaja voi tunnistaa oikean alkuperäisen tekstin.

Esimerkki 2.5 (Avaus)**.** Jatketaan aikaisemmin Esimerkissä 2.3 luodun salausjärjestelmän tutkimista. Järjestelmämme salainen avain on lukupari $(p, q) = (19, 31)$ ja julkinen avain luku $n = 589$.

Vastaanottaja saa salatun viestin $c = 419$ ja avaa sen käyttäen salaista avainta $(19, 31)$. Hän laskee ensin avaamiseen tarvittavat luvut $y_p \equiv p^{-1} \pmod{q}$ ja $y_q \equiv q^{-1} \pmod{p}$ käyttäen Eukleideen algoritmia ja saa $y_p = 18$ ja $y_q = 8$. Sitten hän laskee neliöjuuret m_p ja m_q seuraavasti.

$$m_p \equiv 419^{\frac{19+1}{4}} \equiv 419^5 \equiv 1 \pmod{19}$$

ja

$$m_q \equiv 419^{\frac{31+1}{4}} \equiv 419^8 \equiv 4 \pmod{31}.$$

Näiden lukujen avulla vastaanottaja laskee luvut

$$r \equiv 1 \cdot 31 \cdot 8 + 4 \cdot 19 \cdot 18 \equiv 1616 \equiv 438 \pmod{589}$$

ja

$$s \equiv 1 \cdot 31 \cdot 8 - 4 \cdot 19 \cdot 18 \equiv 58 \pmod{589}$$

sekä edelleen luvut $-r \equiv -438 \equiv 151 \pmod{589}$ ja $-s \equiv -58 \equiv 531 \pmod{589}$.

Siispä viestin vastaanottaja saa avauksen tulokseksi luvut $58, 151, 438$ ja 531. Nämä ovat luvun 419 neliöjuuret modulo 589 ja yksi näistä luvuista edustaa alkuperäistä tekstiä m.

2.3 Ratkaisuja neljän neliöjuuren ongelmaan

Kuten nähtiin Kappaleessa 2.2, Rabinin salausjärjestelmän eräs heikkous on se, että salattua viestiä avatessa saadaan neljä mahdollista lopputulosta, joista ei voida, ilman ylimääräistä informaatiota, tietää, mikä edustaa alkuperäistä tekstiä. Viestin lähettäjän on siis lähetettävä viestin mukana jotain ylimääräistä informaatiota, jonka avulla vastaanottaja voi viestin avattuaan päätellä, mikä saaduista lopputuloksista vastaa alkuperäistä tekstiä.

Eräs keino lähettää ylimääräistä informaatiota on lisätä alkuperäiseen tekstiin jotain sellaista, josta se voidaan tunnistaa neljän neliöjuuren joukosta. Tämä ylimääräisyys voi olla esimerkiksi tietty bittijärjestys alkuperäisen tekstin binäärilukuesityksen vähiten merkitsevinä bitteinä. Voidaan esimerkiksi vaatia, että alkuperäinen teksti on sellaista muotoa, että tietty määrä sen vähiten merkitseviä bittejä ovat kaikki ykkösiä. Viesti salataan normaaliin tapaan ja kun vastaanottaja avaa sen, voi hän helposti tunnistaa oikean alkuperäisen tekstin neljän neliöjuuren joukosta, sillä suurella todennäköisyydellä vain yksi neliöjuurista sisältää vaaditun bittijärjestyksen vähiten merkitsevinä bitteinään. On kuitenkin olemassa pieni todennäköisyys, että jokin toinenkin lasketuista neliöjuurista sisältää samalla kaavalla bittejä. Esimerkissä 2.6 lasketaan tämä todennäköisyys.

Esimerkki 2.6. Olkoon l positiivinen kokonaisluku. Meillä on käytössä Rabinin salausjärjestelmä ja lisäksi vaaditaan, että järjestelmällä salattavat tekstit ovat sellaista muotoa, että niiden binääriesityksen l vähiten merkitsevää bittiä ovat kaikki ykkösiä. Halutaan laskea todennäköisyys, jolla alkuperäisen tekstin tunnistaminen neljän neliöjuuren joukosta ei onnistu. Siispä lasketaan todennäköisyys, jolla viestiä avatessa saaduista neljästä neliöjuuresta useampi kuin yksi sisältää l kappaletta ykkösiä vähiten merkitsevinä bitteinään.

Olkoot viestiä avatessa ratkaistut neljä neliöjuurta luvut $\pm r$ ja $\pm s$. Vastatkoon r oikeaa alkuperäistä tekstiä ja näin ollen sen viimeiset l bittiä ovat ykkösiä. Nyt koska n on kahden parittoman luvun tulo, on se itsekin pariton. Koska n on pariton, niin luvuista x ja $-x \equiv n - x \pmod{n}$, toinen on aina parillinen ja toinen pariton kaikille luvuille $x \in \mathbb{Z}_n$. Koska parillisen luvun viimeinen bitti on aina nolla ja parittoman yksi, niin voidaan todeta, että lukujen r ja $-r$ viimeinen bitti on eri ja täten myös l vähiten merkitsevän bitin joukko eroaa toisistaan. Siispä luvulle $-r$ viimeiset l bittiä eivät voi olla kaikki ykkösiä. Tarkastellaan seuraavaksi lukuja s ja $-s$. Jos ajatellaan, että nämä luvut ovat sattumanvaraisesti valittuja, todennäköisyys sille, että toisen l viimeistä bittiä ovat kaikki ykkösiä, on $\left(\frac{1}{2}\right)^l = \frac{1}{2^l}$. Edelleen todennäköisyys sille, että toisen tai molempien näistä luvuista l viimeistä bittiä ovat kaikki ykkösiä on $\frac{1}{2^l} + \frac{1}{2^l} = \frac{2}{2^l} = \frac{1}{2^{l-1}}$.

Toinen tapa varmistaa, että viestin vastaanottaja pystyy tunnistamaan oikean alkuperäisen tekstin neljän neliöjuuren joukosta on lähettää vastaanottajalle itsenäistä, ylimääräistä informaatiota. Näin voidaan saavuttaa jopa tilanne, jossa alkuperäinen teksti tunnistetaan todennäköisyydellä 1, mutta tämä lisää aina sekä lähetättävää datamäärää että vaadittavien askelten, eli matemaattisten operaatioiden, määrää ja näin ollen heikentää salausjärejstelmän tehokkuutta.

Rabinin salausjärjestelmälle on kehitetty myös laajennuksia, joissa varmistetaan, että vastaanottaja saa selville alkuperäisen tekstin salatun viestin avattuaan. Tällaiset laajennukset muistuttavat usein toiminnaltaan huomattavasti Rabinin salausjärjestelmää, mutta niihin on mahdollisesti lisätty joitain askelia salaukseen tai avaukseen tai joitain lisävaatimuksia esimerkiksi avaimelle. Eräs tällainen laajennus on Rabin-Williams salausjärjestelmä, joka esitellään Kappaleessa 3.

2.4 Turvallisuus

Rabinin salausjärjestelmä perustuu salausfunktioon $f(x) = x^2 \pmod{n}$, missä luku n on Blumin kokonaisluku. Osoitetaan seuraavaksi, että tämän salaovifunktion, ja näin ollen myös Rabinin salausjärjestelmän, murtaminen on yhtä vaikeaa kuin luvun n jakaminen alkulukutekijöihin.

Lause 2.7. *Rabinin salausjärjestelmän murtaminen on yhtä vaikeaa kuin moduloluvun n alkulukutekijöiden p ja q löytäminen.*

Todistus. Osoitetaan, että

1. jos osataan jakaa luku n alkulukutekijöihin, voidaan murtaa Rabinin salausjärjestelmä ja

2. jos voidaan murtaa Rabinin salausjärjestelmä, osataan jakaa luku n alkulukutekijöihin.

Nyt suunta 1. käy ilmi Kappaleessa 2.2, jossa esitellään, miten Rabinin salausjärjestelmällä salattu viesti c avataan julkisen avaimen n alkulukutekijöiden p ja q avulla. Luvut p ja q toimivat järjestelmän salaisena avaimena, joten on selvää, että näiden lukujen avulla voidaan avata järjestelmällä salattuja viestejä ja näin ollen henkilö, joka osaa jakaa julkisen avaimen n sen alkulukutekijöihin p ja q, voi myös murtaa Rabinin salausjärjestelmän.

Todistetaan suunta 2. Nyt tulee osoittaa, että jos osataan salatun viestin c avulla saada selville sen neliöjuuret modulo n, osataan myös jakaa moduloluku n sen alkulukutekijöihin p ja q. Todellisuudessa riittää, että salatun

viestin c avulla saadaan selville joku sen neljästä neliöjuuresta modulo n. Oletetaan siis, että on käytössä laite O^{Rabin} joka osaa avata Rabinin salausjärjestelmällä salattuja viestejä. Laite ottaa sisäänsä salatun viestin c ja palauttaa yhden sen neliöjuurista modulo n, eli mahdollisen alkuperäisen tekstin.

Valitaan satunnaisesti luku $x \in \mathbb{Z}_n$. Luku n on Blumin kokonaisluku, joten se on muotoa $n = pq$, missä p ja q ovat alkulukuja. Lisäksi $x < n$, joten on oltava $\text{syt}(x, n) = 1$, $\text{syt}(x, n) = p$ tai $\text{syt}(x, n) = q$. Siispä jos $\text{syt}(x, n) \neq 1$, niin luku x on luvun n alkulukutekijä ja toinen alkulukutekijä on muotoa $\frac{n}{x}$. Näin ollen luvun n alkulukutekijöihin jakaminen on tehty. Oletetaan siis, että $\text{syt}(x, n) = 1$ ja lasketaan

$$c \equiv x^2 \pmod{n}$$

ja

$$m = O^{Rabin}(c).$$

Nyt luku m on yksi luvun c neliöjuurista modulo n, mutta koska näitä neliöjuuria on neljä, niin ei välttämättä ole $x = m \pmod{n}$. Kappaleessa 2.2 viestiä avatessa luotiin neljä kongruenssiyhtälöryhmää, joista jokainen tuotti ratkaisunaan luvun c erään neliöjuuren modulo n. Näistä kongruenssiyhtälöryhmistä nähdään, että lukujen x ja m tulee toteuttaa jokin seuraavista ehdoista. Kussakin vaihtoehdossa tutkitaan lukua $\text{syt}(m - x, n)$.

1. $m \equiv x \pmod{p}$ ja $m \equiv x \pmod{q}$. Tästä seuraa, että $m \equiv x \pmod{n}$ ja koska on valittu $0 \leq x < n$ ja $0 \leq m < n$, niin on oltava $m = x$. Nyt $\text{syt}(m - x, n) = \text{syt}(0, n) = n$. Tätä tietoa ei voida käyttää luvun n alkulukutekijöiden löytämiseen.

2. $m \equiv -x \pmod{p}$ ja $m \equiv -x \pmod{q}$. Tästä seuraa, että $m \equiv -x \pmod{n}$ eli on oltava $m = n - x$. Osoitetaan, että tällöin $\text{syt}(m - x, n) = 1$. Tehdään vastaoletus, että $\text{syt}(m - x, n) \neq 1$. Nyt on oltava $\text{syt}(m-x, n) = p$ tai $syt(m-x, n) = q$. Tutkitaan tilanne, jossa $\text{syt}(m-x, n) = p$. On siis olemassa jokin kokonaisluku l, jolle

   $$m - x = n - 2x = lp.$$

   Tästä seuraa

   $$-2x = lp - n = lp - pq = p(l - q)$$

   ja edelleen

   $$p|2x.$$

   Koska $p > 2$, tästä seuraa $p|x$. Tämä on ristiriita sen kanssa, että $\text{syt}(x, n) = 1$. Tilanne, jossa $\text{syt}(m - x, n) = q$ on vastaava. Siispä on oltava $\text{syt}(m - x, n) = 1$. Tätä tietoa ei voida käyttää luvun n alkulukutekijöiden löytämiseen.

3. $m \equiv x \pmod{p}$ ja $m \equiv -x \pmod{q}$. Tästä seuraa, että luku $m - x$ on jaollinen luvulla p, mutta ei luvulla q. Siispä $\text{syt}(m - x, n) = p$. Suurin yhteinen tekijä voidaan määrittää Eukleideen algoritmin avulla, kuten on esitetty Lauseessa 1.2. Näin ollen luvun n toinen alkulukutekijä löydetään, eli alkulukutekijöihin jako voidaan tehdä.

4. $m \equiv -x \pmod{p}$ ja $m \equiv x \pmod{q}$. Tästä seuraa, että luku $m - x$ ei ole jaollinen luvulla p, mutta on jaollinen luvulla q. Kuten edellisessä kohdassa, tämä tieto on hyödyllistä luvun n alkulukutekijöiden löytämiseksi ja erityisesti $q = \text{syt}(m - x, n)$. Näin ollen luvun n alkulukutekijöihin jako voidaan tehdä myös tässä tapauksessa.

Edellä nähdään, että kahdessa neljästä tapauksesta saadaan selville luvun n alkulukutekijät p ja q. Näin ollen edellisen algoritmin onnistumistodennäköisyys on $\frac{1}{2}$, kun sitä sovelletaan yhden kerran. Mikäli yhdellä yrittämällä ei saada selville luvun n alkulukutekijöitä p ja q, voidaan algoritmi toistaa uudella luvun x arvolla. Kun algoritmi toistetaan k kertaa, luvun n alkulukutekijät löytyvät todennäköisyydellä $1 - (\frac{1}{2})^k$. Nyt luvun k kasvaessa edellinen todennäköisyys lähestyy lukua 1, joten voidaan todeta, että luvun n alkulukutekijät p ja q löytyvät yllä olevalla algoritmilla todennäköisyydellä 1. On siis todistettu, että jos voidaan murtaa Rabinin salausjärjestelmä, osataan jakaa luku n alkulukutekijöihin. □

Esimerkki 2.8. Tutkitaan aiempien esimerkkien avulla, miten Rabinin salausjärjestelmän murtaja voi jakaa moduloluvun n alkulukutekijöihin. Käytetään samoja avaimia kuin Esimerkissä 2.3 ja Esimerkissä 2.5. Murtajalla on siis tiedossaan järjestelmän julkinen avain $n = 589$ ja käytössään laite O^{Rabin}, joka laskee neliöjuuria modulo 589. Hän valitsee luvun $x = 58$. Nyt $\text{syt}(58, 589) = 1$. Sitten murtaja laskee

$$c \equiv x^2 \equiv 58^2 \equiv 419 \pmod{589}.$$

ja

$$m = O^{Rabin}(419).$$

Nyt Esimerkissä 2.5 on määritetty luvun 419 neliöjuuret modulo 589 joten tiedetään, että murtaja saa luvuksi m joko 58, 151, 438 tai 531. Käydään läpi mahdolliset tilanteet. Oletetaan ensin, että murtaja saa $m = 58$. Nyt $m = x$ ja näin ollen

$$\text{syt}(m - x, n) = \text{syt}(58 - 58, 589) = \text{syt}(0, 589) = 589.$$

Siispä murtaja ei onnistu löytämään luvun 589 alkulukutekijöitä. Tarkastellaan sitten tilannetta, jossa $m = 531$. Nyt

$$\text{syt}(m - x, n) = \text{syt}(531 - 58, 589) = 1.$$

Tässäkään tilanteessa murtaja ei löydä luvun 589 alkulukutekijöitä. Olkoon sitten $m = 151$. Nyt

$$\text{syt}(m - x, n) = \text{syt}(151 - 58, 589) = 31.$$

Murtaja saa siis edellisen laskun tulokseksi luvun 589 toisen alkulukutekijän 31 ja sen avulla voi edelleen laskea luvun 589 toisenkin alkulukutekijän $\frac{n}{q} = \frac{589}{31} = 19$. Näin ollen hän on onnistunut jakamaan luvun n alkulukutekijöihinsä. Käydään vielä läpi viimeinen tilanne, eli asetetaan $m = 438$. Nyt

$$\text{syt}(m - x, n) = \text{syt}(438 - 58, 589) = 19.$$

Tässäkin tilanteessa murtaja saa laskun tulokseksi luvun 589 toisen alkulukutekijän 19 ja voi sen avulla laskea $\frac{n}{p} = \frac{589}{19} = 31$ ja on onnistunut jakamaan luvun n alkulukutekijöihin.

Rabinin salausjärjestelmän voidaan sanoa olevan erittäin turvallinen, koska pystytään todistamaan sen murtamisen olevan yhtä vaikeaa, kuin suurten lukujen alkulukutekijöihinjako. Mikäli kuitenkin salausjärjestelmää käytettäessä hyödynnetään jotain Kappaleessa 2.3 esiteltyä keinoa, jolla varmistetaan oikean alkuperäisen tekstin tunnistus, ei välttämättä enää voida todistaa edellä esiteltyä vahvaa ominaisuutta. Jos esimerkiksi alkuperäiseen tekstiin lisätään ylimääräisyyttä Esimerkissä 2.6 esitellyllä tavalla, niin Lause 2.7 ei ole enää voimassa, mikäli oletetaan, että myös murtajalla käytössä oleva laite O^{Rabin}, osaa valita neljän neliöjuuren joukosta oikean alkuperäisen tekstin hyödyntäen sen vaadittua muotoa. Tällöin murtaja päätyy aina Lauseen 2.7 tilanteeseen 1., jossa hän ei saa selville moduloluvun n alkulukutekijöitä. Siispä Rabinin salausjärjestelmän murtaminen ei ole enää yhtä vaikeaa kuin moduloluvun n alkulukutekijöiden löytäminen.

3 Rabin-Williams salausjärjestelmä

Tässä kappaleessa esitellään salausjärjestelmä, joka pohjautuu Rabinin salausjärjestelmään. Rabin-Williams salausjärjestelmä on Rabinin salausjärjestelmän kaltainen, mutta siihen on lisätty uusi vaatimus alkuluvuille p ja q sekä muutama askel tesktin salaukseen ja viestin avaukseen. Näillä lisäyksillä varmistetaan, että viestiä avaava vastaanottaja saa varmasti selville oikean alkuperäisen tekstin. Tämä onkin Rabin-Williams salausjärjestelmän merkittävin etu verrattuna Rabinin salausjärjestelmään. Rabin-Williams salausjärjestelmä kuitenkin vaatii salausaskeleessaan Jacobin symbolin laskemisen ja näin ollen menettää Rabinin salausjärjestelmän tehokkuuden. Kappaleessa on käytetty lähteinä teoksia [2] ja [3].

3.1 Avaimen valinta ja tekstin salaus

Valitaan alkuluvut p ja q siten, että ne toteuttavat Rabinin salausjärjestelmässä vaaditun ehdon $p \equiv q \equiv 3 \pmod 4$ ja lisäksi $p \equiv 3 \pmod 8$ ja $q \equiv 7 \pmod 8$. Käytetään salaisena avaimena lukuparia (p, q) ja julkisena avaimena lukua $n = pq$. Näin muodostettua lukua n kutsutaan *Williamsin kokonaisluvuksi*.

Rabin-Williams salausjärjestelmää voidaan käyttää salaamaan viestejä $m \in \mathbb{Z}_n$, joille pätee $1 \leq m \leq \frac{n}{8} - 1$.

Viestin m salaamista varten halutaan muodostaa luku x, joka on parillinen ja jonka Jacobin symboli modulo n on yksi. Se voidaan tehdä seuraavasti. Lasketaan ensin Jacobin symboli $\left(\frac{2m+1}{n}\right) = b$ Lauseen 1.12 ja Määritelmän 1.13 osoittamalla tavalla. Valitaan sitten

$$x = \begin{cases} 4(2m+1), & \text{jos } b = 1 \\ 2(2m+1), & \text{jos } b = -1. \end{cases}$$

Nyt luku x on molemmissa tapauksissa parillinen. Lisäksi Lauseen 1.17 nojalla $\left(\frac{2}{n}\right) = -1$, sillä $n \equiv 3 \cdot 7 \equiv 5 \pmod 8$. Tästä seuraa, että jos $b = \left(\frac{2m+1}{n}\right) = -1$, niin

$$\left(\frac{2(2m+1)}{n}\right) = \left(\frac{2}{n}\right) \cdot \left(\frac{2m+1}{n}\right) = -1 \cdot (-1) = 1$$

ja jos $b = \left(\frac{2m+1}{n}\right) = 1$, niin

$$\left(\frac{4(2m+1)}{n}\right) = \left(\frac{2}{n}\right) \cdot \left(\frac{2}{n}\right) \cdot \left(\frac{2m+1}{n}\right) = -1 \cdot (-1) \cdot 1 = 1.$$

Näin ollen luku x on aina parillinen ja sen Jacobin symboli on 1.

Tehdään seuraavaksi Rabinin salausjärjestelmän salausaskel eli neliöön korotus luvulle x, eli muodostetaan salattu viesti c seuraavasti:

$$c \equiv x^2 \pmod{n}.$$

Esimerkki 3.1 (Avaimen valinta ja salaus)**.** Muodostetaan esimerkki Rabin-Williams salausjärjestelmän käytöstä. Huomataan, että aiemmin Esimerkeissä 2.3, 2.5 ja 2.8 muodostetussa Rabinin salausjärjestelmässä valitut alkuluvut $p = 19$ ja $q = 31$ toteuttavat myös Rabin-Williams salausjärjestelmän avaimen valinnan ehdot, koska $p \equiv 3 \pmod 8$ ja $q \equiv 7 \pmod 8$. Käytetään siis tässäkin esimerkissä näitä lukuja. Valitaan siis järjestelmämme salaiseksi avaimeksi lukupari $(19, 31)$ ja julkiseksi avaimeksi luku $19 \cdot 31 = 589$.

Salausjärjestelmää voidaan käyttää salaamaan viestejä m, jotka ovat muotoa $1 \leq m \leq 72$. Oletetaan, että lähettäjä haluaa lähettää viestin $m = 58$. Hän laskee Jacobin symbolin

$$b = \left(\frac{2 \cdot 58 + 1}{589}\right) = \left(\frac{117}{589}\right).$$

Laskeakseen luvun 117 Jacobin symbolin modulo 589, vastaanottaja laskee ensin sen Legendren symbolit modulo 19 ja modulo 31 Lauseen 1.12 osoittamalla tavalla ja saa

$$\left(\frac{117}{19}\right) \equiv 117^{\frac{19-1}{2}} \equiv 117^9 \equiv -1 \pmod{19}$$

ja

$$\left(\frac{117}{31}\right) \equiv 117^{\frac{31-1}{2}} \equiv 117^{15} \equiv -1 \pmod{31}.$$

Näiden avulla hän laskee Jacobin symbolin

$$b = \left(\frac{117}{589}\right) = \left(\frac{117}{19}\right) \cdot \left(\frac{117}{31}\right) = -1 \cdot (-1) = 1.$$

Siispä hän laskee luvun $x = 4(2 \cdot 58 + 1) = 468$ ja edelleen salatun viestin

$$c \equiv 468^2 \equiv 505 \pmod{589}.$$

Salattu viesti 505 lähetetään vastaanottajalle.

3.2 Viestin avaus

Salattu viesti c avataan, kuten Rabinin salausjärjestelmässä. Saadaan tulokseksi luvun c neljä neliöjuurta modulo n. Nyt yksi näistä luvuista vastaa tekstin salausvaiheessa valittua lukua x, joka valittiin niin, että se on parillinen ja sen Jacobin symboli modulo n on 1. Itseasiassa voidaan näyttää, että vain yksi neljästä neliöjuuresta toteuttaa nämä ehdot.

Lause 3.2. *Olkoon luku n Williamsin kokonaisluku ja luku c alkio jäännösluokkien joukossa modulo n. Nyt vain yksi alkio x jäännösluokkien joukossa modulo n on sekä luvun c neliöjuuri, että toteuttaa seuraavat ehdot:*

$$2|x \text{ ja } \left(\frac{x}{n}\right) = 1.$$

Todistus. Nyt Kappaleessa 2.2 todettiin, että luvulla c tarkalleen neljä neliöjuurta modulo n ja että nämä neliöjuuret ovat muotoa $r, -r, s$ ja $-s$.

Tutkitaan ensin ehtoa, jonka mukaan $2|x$, eli x on parillinen luku. Luku n on kahden parittoman luvun tulona itsekin pariton luku. Koska n on pariton, niin luvuista r ja $-r \equiv n - r \pmod{n}$, toinen on aina parillinen ja toinen pariton kaikille luvuille $r \in \mathbb{Z}_n$. Siispä tarkalleen kaksi luvun c neljästä neliöjuuresta ovat parillisia. Oletetaan, että nämä kaksi paritonta neliöjuurta ovat r ja s.

Tutkitaan sitten ehtoa, jonka mukaan $\left(\frac{x}{n}\right) = 1$. Nyt

$$c \equiv r^2 \equiv s^2 \pmod{n},$$

josta kongruenssin määritelmän nojalla seuraa

$$n|r^2 - s^2$$

ja edelleen

$$n|(r-s)(r+s).$$

Koska n ei voi jakaa sekä lukua $(r-s)$, että lukua $(r+s)$, tästä seuraa, että

$$p|(r-s) \text{ ja } q|(r+s),$$

mistä kongruenssin määritelmän nojalla seuraa, että

$$r \equiv s \pmod{p} \text{ ja } r \equiv -s \pmod{q}.$$

Lauseen 1.14 nojalla tästä seuraa, että

$$\left(\frac{r}{p}\right) = \left(\frac{s}{p}\right) \text{ ja } \left(\frac{r}{q}\right) = \left(\frac{-s}{q}\right) = \left(\frac{-1}{q}\right) \cdot \left(\frac{s}{q}\right) = -\left(\frac{s}{q}\right),$$

Missä toiseksi viimeinen yhtäsuuruus seuraa Lauseesta 1.15 ja viimeinen yhtäsuuruus seuraa siitä, että Lauseen 1.16 nojalla $\left(\frac{-1}{q}\right) = -1$, sillä $q \equiv 3 \pmod 4$. Edelleen Määritelmän 1.13 nojalla saadaan

$$\left(\frac{r}{n}\right) = -\left(\frac{s}{n}\right).$$

Siispä vain toisen parillisen neliöjuuren Jacobin symboli voi olla 1 ja näin ollen vain yksi luku $x \in \mathbb{Z}_n$ toteuttaa lauseen ehdot. □

Neljästä neliöjuuresta voidaan siis tunnistaa viestin salausvaiheessa muodostettu luku x sulkemalla ensin pois parittomat neliöjuuret ja laskemalla sitten jäljelle jääneen kahden luvun Jacobin symbolit. Luku x on se, jonka Jacobin symboli on 1. Nyt $x = 4(2m+1)$ tai $x = 2(2m+1)$, joten

$$x \equiv 4(2m+1) \equiv 0 \pmod 4$$

tai

$$x \equiv 2(2m+1) \equiv 4m+2 \equiv 2 \pmod 4.$$

Siispä voidaan laskea alkuperäistä tekstiä vastaava luku m seuraavasti.

$$m = \begin{cases} \frac{\frac{x}{4}-1}{2}, & \text{jos } x \equiv 0 \pmod 4, \\ \frac{\frac{x}{2}-1}{2}, & \text{jos } x \equiv 2 \pmod 4. \end{cases}$$

Esimerkki 3.3 (Avaus)**.** Jatketaan aikaisemmin Esimerkissä 3.1 luodun salausjärjestelmän tutkimista. Järjestelmämme salainen avain on lukupari $(p, q) = (19, 31)$ ja julkinen avain luku $n = 589$. Vastaanottaja saa salatun viestin $c = 505$ ja avaa sen kuten Rabinin salausjärjestelmässä. Hän laskee ensin avaamiseen tarvittavat luvut $y_p \equiv p^{-1} \pmod q$ ja $y_q \equiv q^{-1} \pmod p$ käyttäen Eukleideen algoritmia ja saa $y_p = 18$ ja $y_q = 8$. Sitten hän laskee neliöjuuret m_p ja m_q seuraavasti:

$$m_p \equiv 505^{\frac{19+1}{4}} \equiv 505^5 \equiv 7 \pmod{19}$$

ja

$$m_q \equiv 505^{\frac{31+1}{4}} \equiv 505^8 \equiv 28 \pmod{31}.$$

Näiden lukujen avulla vastaanottaja laskee luvut

$$r \equiv 7 \cdot 31 \cdot 8 + 28 \cdot 19 \cdot 18 \equiv 11312 \equiv 121 \pmod{589}$$

ja

$$s \equiv 7 \cdot 31 \cdot 8 - 28 \cdot 19 \cdot 18 \equiv -7840 \equiv 406 \pmod{589}$$

sekä edelleen $-r \equiv -121 \equiv 468 \pmod{589}$ ja $-s \equiv -406 \equiv 183 \pmod{589}$.

Siispä viestin vastaanottaja saa luvun 505 neljäksi neliöjuureksi modulo 589 luvut $121, 183, 406$ ja 468. Vastaanottaja voi hylätä näistä parittomat ja vaihtoehdoiksi jää luvut 406 sekä 468. Seuraavaksi vastaanottaja laskee näiden lukujen Jacobin symbolit modulo 589. Tätä varten hän laskee ensin lukujen Legendren symbolit modulo 19 ja modulo 31 ja saa

$$\left(\frac{406}{19}\right) \equiv 406^{\frac{19-1}{2}} \equiv 406^9 \equiv 1 \pmod{19},$$

$$\left(\frac{406}{31}\right) \equiv 406^{\frac{31-1}{2}} \equiv 406^{15} \equiv -1 \pmod{31},$$

$$\left(\frac{468}{19}\right) \equiv 468^{\frac{19-1}{2}} \equiv 468^9 \equiv -1 \pmod{19},$$

sekä

$$\left(\frac{468}{31}\right) \equiv 468^{\frac{31-1}{2}} \equiv 468^{15} \equiv -1 \pmod{31}.$$

Näiden avulla vastaanottaja laskee Jacobin symbolit

$$\left(\frac{406}{589}\right) = 1 \cdot (-1) = -1 \text{ ja } \left(\frac{468}{589}\right) = -1 \cdot (-1) = 1.$$

Siispä hän valitsee $x = 468$. Lopuksi vastaanottaja toteaa, että $468 \equiv 0 \pmod{4}$ ja tästä johtuen laskee

$$m = \frac{\frac{468}{4} - 1}{2} = 58.$$

Siispä luku 58 vastaa alkuperäistä tekstiä.

Lähdeluettelo

[1] Oppliger, Rolf: *Contemporary cryptography.* Artech House, 2011.

[2] Galbraith, Steven D.: *Mathematics of public key cryptography.* Cambridge University Press, 2012.

[3] Batten, Lynn Margaret; Williams, Hugh Cowie: *Unique Rabin-Williams Signature Scheme Decryption.* Cryptology ePrint Archive, 2019.