Digitaaliset allekirjoitukset

LuK-tutkielma
Lotta Makkonen
2578161
Matematiikan tutkinto-ohjelma
Oulun yliopisto
Kevät 2021

Sisällys

Johdanto

Tässä tutkielmassa tarkastellaan erilaisia digitaalisia allekirjoitussysteemejä, joita käytetään usein yhdessä julkisen avaimen kryptografian kanssa. Ensimmäisessä luvussa esitellään sekä salaisen, että julkisen avaimen kryptografian perusperiaatteet ja keskeiset eroavaisuudet. Tämän jälkeen käsitellään yleisellä tasolla digitaalisten allekirjoitusten toimintaperiaate, sekä muutamia olennaisia piirteitä, jotka ovat tärkeitä allekirjoituksen luotettavuuden ja turvallisuuden kannalta.

Tutkielmassa esitellään ja todistetaan myös tärkeitä lukuteorian lauseita, joihin digitaalisten allekirjoitusten toiminta perustuu. Erityisesti kongruenssin ja kongruenssiyhtälön määritelmät ovat hyvin olennaisia kryptografisissa menetelmissä. Lukuteorian käsittelyn jälkeen tutkielmassa tarkastellaan yksityiskohtaisesti ja esimerkkien avulla kolmen erilaisen digitaalisen allekirjoitussysteemin toimintaa.

Ensimmäinen tutkielmassa tarkasteltava allekirjoitussysteemi on RSA-allekirjoitus, jonka Rivest, Shamir ja Adleman kehittivät yhtä aikaa RSA-salauksen kanssa vuonna 1978. RSA-systeemit perustuvat suurten kokonaislukujen tekijöihinjaon vaikeuteen ja allekirjoittaminen tapahtuu hyvin samankaltaisesti kuin salaaminenkin. Digitaalisista allekirjoituksista RSA on yleisesti tunnetuin ja yksinkertaisin systeemi, joka on kuitenkin edelleen riittävän suurilla luvuilla turvallinen.

Tutkielmassa tarkastellaan tämän jälkeen ElGamal-allekirjoitusta, joka kehitettiin yhdessä ElGamal-salauksen kanssa vuonna 1985. ElGamal-systeemit perustuvat diskreetin logaritmin ongelmaan, minkä vuoksi siirtyminen salauksesta allekirjoitussysteemiin ei ole aivan yhtä suoraviivaista kuin RSA:n tapauksessa. ElGamal on menetelmänä luotettava ja turvallinen, mutta sillä saadut allekirjoitukset ovat hyvin pitkiä, mikä ei ole useassakaan tapauksessa kovin kätevää. Niinpä vuonna 1991 esiteltiin hieman paranneltu ElGamal-allekirjoituksen versio, DSA-allekirjoitus. Menetelmät toimivat muuten hyvin samankaltaisesti, mutta DSA:ssa laskut tapahtuvat ryhmän sijaan aliryhmässä, mikä mahdollistaa lyhyemmät allekirjoitukset.

Esitellyistä allekirjoituksista DSA on nykyään laajimmin käytössä ja sitä pidetään yleisenä allekirjoitusstandardina. Edellä mainittuihin systeemeihin poiketen DSA:ta ei kuitenkaan voi käyttää pelkkään salaukseen, vaan sillä on mahdollista tuottaa ainoastaan allekirjoituksia.

Tutkielmassa on käytetty päälähteenä J. Hoffsteinin teosta *An introduction to mathematical cryptography* [1], mutta allekirjoitussysteemien esimerkit on keksitty itse.

1 Yleistä kryptografiasta

Kryptografialla tarkoitetaan erilaisia systeemejä ja algoritmeja, joita käyttämällä informaatiota voidaan salata sellaiseen muotoon, että ulkopuoliset henkilöt eivät saa siitä selvää. Menetelmien tarkoitus on siis mahdollistaa luotettava ja salainen informaation siirtäminen henkilöltä toiselle, vaikka kommunikointi olisi mahdollista ainoastaan valvotun kanavan kautta.

Kryptografiset systeemit perustuvat erilaisiin vaikeisiin matemaattisiin ongelmiin. Tällaisia ongelmia ovat esimerkiksi diskreetin logaritmin ongelma, sekä erittäin suurten kokonaislukujen jakaminen alkulukutekijöihin. Hyvät kryptosysteemit perustuvat ongelmiin, jotka ovat aluksi todella hankalia ratkaista, mutta pienellä lisätiedolla ratkaiseminen onnistuukin helposti.

Käytännössä kryptografisissa menetelmissä lähettäjä salaa selväkielisen viestin avaimen avulla salakirjoitukseksi ja lähettää sen vastaanottajalle. Vastaanottaja käyttää salakirjoitukseen avainta, jonka avulla viesti muuttuu takaisin selväkieliseksi. Näin ollen vaikka ulkopuoliset henkilöt näkisivätkin salakirjoitetun viestin, he eivät pysty ilman avainta muuttamaan sitä selväkieliseksi tekstiksi. Alkeellisimpia salausmenetelmiä lukuunottamatta viestin kirjaimet muutetaan salaamisen ajaksi joukon $\mathbb{Z}_n$ alkioiksi.

Tuhansien vuosien ajan salaukset ja koodit perustuivat salaiseen avaimeen, jonka vain tietyt henkilöt tiesivät. Tällaisia menetelmiä kutsutaan salaisen avaimen kryptosysteemeiksi. Systeemeissä lähettäjä salaa viestin käyttämällä salaista avainta ja vastaanottaja avaa viestin samalla avaimella. Käytännössä tällöin avain voi olla esimerkiksi bijektiivinen funktio $E : P \mapsto C$, missä P on selväkielisen tekstin alkioiden joukko ja C on vastaavasti salatun viestin alkioiden joukko. Tällöin viestin avaaminen tapahtuu käänteisfunktiolla $D = E^{-1}$.

Salaisen avaimen kryptografian ohelle kehitettiin 1970-luvulla julkiseen avaimeen perustuvia menetelmiä, joissa kullakin käyttäjällä on käytössään kaksi avainta. Menetelmän käyttäjä valitsee itselleen yksityisen avaimen K^Y, ja pitää sen salassa. Yksityisen avaimensa avulla käyttäjä laskee itselleen julkisen avaimen K^J, joka julkaistaan esimerkiksi avainkirjassa kaikkien nähtäville. Sopivien avainten valinta on erityisen tärkeää, sillä julkisen avaimen tulee olla sellainen, että sen avulla ei ole mahdollista päätellä yksityistä avainta.

Julkisen avaimen krytptosysteemeissä lähettäjä salaa viestinsä käyttämällä vastaanottajan julkista avainta K^J. Kuka tahansa voi siis lähettää kenelle tahansa viestejä. Salauksen jälkeen viesti julkaistaan ja vastaanottaja avaa sen omalla yksityisellä avaimellaan K^Y. Menetelmien toiminta perustuu siihen, että viestin avaamiseen tarvitaan salaamisessa käytettyä julkista avainta K^J vastaava yksityinen avain K^Y, joka on siis vain viestin tarkoite-

tun vastaanottajan tiedossa. Niinpä kukin käyttäjä voi avata vain itselleen tarkoitettuja viestejä.

Salatun avaimen kryptografiaan verrattuna julkisen avaimen systeemien etu on se, että henkilöiden ei tarvitse etukäteen olla suorassa kontaktissa ja vaihtaa avaimiaan salassa. Uusien käyttäjien lisääminen on myös huomattavasti helpompaa kun käytössä on julkisen avaimen menetelmä, sillä tällöin riittää yhden uuden julkisen avaimen lisääminen avainkirjaan. Salaisen avaimen kryptografiaa käytettäessä täytyisi jokaiselle uudelle jäsenelle onnistua aina jakamaan käytössä oleva avain salaisesti ja turvallisesti.

Julkisen avaimen menetelmät ovat kuitenkin jonkun verran salaisen avaimen menetelmiä monimutkaisempia, ja niiden kautta viestiminen on sen vuoksi hitaampaa. Salaisen avaimen menetelmät toimivatkin tehokkaammin pidemmille viesteille. Tämän vuoksi usein käytetään julkisen ja salaisen avaimen kryptosysteemejä yhdessä. Käytännössä ensin hyödynnetään jotakin julkisen avaimen systeemiä salaisen avaimen jakamiseen. Kun avain on saatu jaettua kaikille, käyttäjät voivat viestiä keskenään salaisen avaimen menetelmien kautta.

2 Digitaaliset allekirjoitukset

Koska julkisen avaimen kryptografiassa kaikki voivat lähettää toisillensa viestejä, on hyvin tärkeää lisätä viestiin allekirjoitus. Viestin vastaanottaja pystyy silloin varmistamaan, kuka viestin on lähettänyt ja että viesti ei ole muuttunut tai vaihtunut matkalla. Digitaaliset allekirjoitukset vastaavatkin kynällä fyysisiin dokumentteihin tehtyjä allekirjoituksia. Useissa tapauksissa digitaalinen allekirjoitus on vähintään yhtä tärkeää, kuin itse viestin salaaminen.

Digitaaliset allekirjoitussysteemit muistuttavat paljon julkisen avaimen kryptografisia menetelmiä, sillä kummassakin käyttäjät valitsevat itselleen julkisen avaimen K^J ja yksityisen avaimen K^Y. Avainten lisäksi eri systeemit käyttävät erilaisia allekirjoitus- ja vahvistusalgoritmeja, joiden avulla allekirjoitus ja sen vahvistaminen tapahtuvat.

Tutkitaan esimerkkinä yksinkertaista tapausta, jossa henkilö A haluaa allekirjoittaa digitaalisen dokumentin D ja lähettää sen henkilölle B. A käyttää ensin dokumenttiin D omaa salaista allekirjoitusavaintaan K^Y ja saa allekirjoituksen S. Tämän jälkeen A lähettää dokumentti-allekirjoitusparin (D, S) vastaanottajalle B. Viestin vastaanottaja B haluaa nyt varmistaa lähettäjän oikeellisuuden ja käyttää lähettäjän A julkista vahvistusavainta K^J saamaansa allekirjoitukseen S. Jos tämä operaatio antaa dokumentin D arvon, lähettäjä on ollut A. Jos tällöin saadaan jokin muu kuin D, lähettäjä ei ole ollut A, tai joku on muuttanut viestiä allekirjoittamisen jälkeen.

Allekirjoitussysteemin turvallisuuden kannalta on olennaista, että kenenkään käyttäjän julkisesta avaimesta K^J ei voida selvittää tämän yksityistä avainta K^Y, tai mitään toista avainta, joka tuottaisi samanlaisia allekirjoituksia. Sopivan julkisen avaimen valitseminen onkin menetelmän turvallisuuden ja toimivuuden kannalta erittäin tärkeää. Jos julkinen avain on esimerkiksi jokin kokonaisluku ja yksityinen avain on sen tekijä, kokonaisluvun täytyy olla riittävän suuri, että alkulukutekijöihin jakaminen on vaikeaa ja hidasta.

Toinen tärkeä ehto turvallisuuteen liittyen on, että käyttäjän julkisen avaimen K^J, sekä aiemmin lähetettyjen dokumenttien ja niitä vastaavien allekirjoitusten listojen $D_1, D_2, ..., D_n$ ja $S_1, S_2, ..., S_n$ avulla ei voida päätellä allekirjoitusta sellaiselle dokumentille D, joka ei ole aiemmin lähetettyjen dokumenttien listalla. Toisin sanoen, vaikka jokainen allekirjoitusmenetelmän käyttökerta paljastaakin yhden uuden dokumentti-allekirjoitusparin, mahdollinen hyökkääjä ei saa tästä apua menetelmän murtamiseen.

Koska allekirjoitus riippuu allekirjoitettavasta dokumentista, suurten ja pitkien dokumenttien allekirjoitukset ovat myös pitkiä. Tämän vuoksi allekirjoituksissa käytetään käytännössä usein Hash-funktioita, joiden avulla suuret dokumentit D saadaan tiivistettyä lyhempään muotoon Hash(D). Tällöin allekirjoittaminen on nopeampaa ja allekirjoitus pysyy halutun mittaisena.

3 Lukuteoriaa

Tässä luvussa esitellään tärkeimpiä lukuteorian lauseita ja määritelmiä, joihin tutkielmassa esitetyt digitaaliset allekirjoitukset perustuvat. Suurin osa lauseista on esitelty ja todistettu kursseilla Algebran perusteet [3] ja Algebralliset rakenteet [2]. Lauseet, joita ei ole todistettu edellä mainituilla kursseilla, todistetaan tässä luvussa yksityiskohtaisesti.

Määritelmä 3.1. Olkoon $m \in \mathbb{Z}_+$ ja $a, b \in \mathbb{Z}$. Jos $m \mid a - b$, sanotaan, että kokonaisluvut a ja b ovat *kongruentteja modulo* m. Tällöin merkitään

$$a \equiv b \pmod{m}.$$

Esimerkki 3.2. Kokonaisluvut 13 ja 3 ovat kongruentteja modulo 5, sillä $13 - 3 = 10$ ja $5 \mid 10$. Siis $13 \equiv 3 \pmod{5}$.

Esimerkki 3.3. Kokonaisluvut 13 ja 4 eivät ole kongruentteja modulo 5, sillä $13 - 4 = 9$ ja $5 \nmid 9$. Siis merkitään $13 \not\equiv 4 \pmod{5}$.

Määritelmä 3.4. Kokonaislukujen a ja b *suurin yhteinen tekijä* on suurin sellainen positiivinen kokonaisluku d, jolla $d \mid a$ ja $d \mid b$. Tällöin merkitään $syt(a, b) = d$.

Huomautus 3.5. Ainakin toisen kokonaisluvuista a ja b täytyy olla nollasta poikkeava, että suurin yhteinen tekijä on määritelty.

Esimerkki 3.6. Koska $24 = 2^3 \cdot 3$ ja $18 = 2 \cdot 3^2$, lukujen 24 ja 18 yhteisiä tekijöitä ovat kokonaisluvut $2, 3$ ja 6. Koska luku 6 on yhteisistä tekijöistä suurin, merkitään $syt(24, 18) = 6$.

Lause 3.7. *Olkoon $a, b \in \mathbb{Z}$ ja $m, n \in \mathbb{Z}_+$ siten, että $a \equiv b \pmod{m}$ ja $a \equiv b \pmod{n}$. Jos lisäksi $syt(m, n) = 1$, niin*

$$a \equiv b \pmod{mn}.$$

Lause 3.8. *Kongruenssiyhtälöllä*

$$ax \equiv b \pmod{m}$$

on ratkaisu, jos $syt(a, m) = 1$.

Esimerkki 3.9. Kongruenssiyhtälöllä $7x \equiv 4 \pmod{10}$ on ratkaisu, sillä $syt(7, 10) = 1$. Kokeilemalla nähdään, että eräs ratkaisu on $x = 2$, koska $7 \cdot 2 \equiv 14 \equiv 4 \pmod{10}$. Nyt kaikki muut ratkaisut ovat muotoa $x = 2 + i \cdot 10$, missä $i \in \mathbb{Z}$. Siis kongruenssiyhtälön kaikki ratkaisut ovat $x \equiv 2 \pmod{10}$.

Määritelmä 3.10. Jos $ax \equiv 1 \pmod{m}$, niin sanotaan, että luku x on luvun *a käänteisalkio modulo m.*

Esimerkki 3.11. Luvun 3 käänteisalkio modulo 20 on 7, koska $3 \cdot 7 \equiv 21 \equiv 1 \pmod{20}$.

Lause 3.12. *Jos $a, b \in \mathbb{Z}$ ja $b \neq 0$, niin on olemassa yksikäsitteiset kokonaisluvut q ja r siten, että $a = qb + r$, missä $0 \leq r < |b|$. Yhtälöä $a = qb + r$ sanotaan jakoalgoritmiksi.*

Määritelmä 3.13. Kokonaislukujen joukko $\mathbb{Z}$ jaetaan jakoalgoritmin perusteella *jäännösluokkiin modulo m* sen mukaan, mikä jakojäännös r on jaettaessa luvulla m. Jäännösluokkaan $[a]$ kuuluvat siis kaikki sellaiset kokonaisluvut, joiden jakojäännös jaettaessa luvulla m on a. Jakoalgoritmin nojalla mahdollisia jakojäännöksiä voivat olla vain luvut $0, 1, 2, ..., m-1$. Jäännösluokkien joukosta käytetään merkintää $\mathbb{Z}_m$. Siis

$$\mathbb{Z}_m = \{[0], [1], [2], ..., [m-1]\}.$$

Joukon $\mathbb{Z}_m$ alkioiden lukumäärä eli kertaluku on $|\mathbb{Z}_m| = m$.

Esimerkki 3.14. Kun kokonaislukujen joukko $\mathbb{Z}$ jaetaan jäännösluokkiin modulo 8, saadaan joukko

$$\mathbb{Z}_8 = \{[0], [1], [2], [3], [4], [5], [6], [7]\}.$$

Alkioiden lukumäärä eli joukon $\mathbb{Z}_8$ kertaluku on 8.

Määritelmä 3.15. Mikäli $syt(a, m) = 1$, jäännösluokkaa $[a]$ modulo m sanotaan *alkuluokaksi modulo m*. Alkuluokkien joukosta käytetään merkintää $\mathbb{Z}_m^*$.

Määritelmä 3.16. Eulerin φ-funktio on funktio $\varphi : \mathbb{Z}_+ \mapsto \mathbb{Z}_+$,

$$\varphi(m) = |\mathbb{Z}_m^*|.$$

Funktio siis kertoo alkuluokan $\mathbb{Z}_m^*$ alkioiden lukumäärän.

Lause 3.17. *Jos p on alkuluku, niin*

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

Siis alkuluokan $|\mathbb{Z}_p^*|$ kertaluku eli alkioiden lukumäärä on $p - 1$.

Esimerkki 3.18. Alkuluokkien joukko modulo 7 on

$$\mathbb{Z}_7^* = \{[a] \in \mathbb{Z}_7 \mid syt(a, 7) = 1\} = \{[1], [2], [3], [4], [5], [6]\}.$$

Joukon kertaluku eli alkioiden lukumäärä on 6, mikä saadaan myös Eulerin φ-funktiolla, sillä Lauseen 3.17 nojalla $\varphi(7) = 7 - 1 = 6$.

Määritelmä 3.19. Olkoon $[a]$ ja $[b]$ jäännösluokkia modulo m. Tällöin

$$[a] + [b] = [a + b]$$

ja

$$[a] \cdot [b] = [a \cdot b].$$

Määritelmä 3.20. Olkoon $G \neq \emptyset$ ja $(*)$ joukon G operaatio. Tällöin pari $(G, *)$ on *ryhmä*, mikäli seuraavat ehdot toteutuvat.

1. Operaatio $(*)$ on *binäärinen*, eli $a * b \in G$ aina, kun $a, b \in G$. Lisäksi alkio $a * b$ on yksikäsitteinen.

2. Operaatio $(*)$ on *assosiatiivinen*, eli $(a * b) * c = a * (b * c)$ aina, kun $a, b, c \in G$.

3. Joukossa G on alkio e siten, että $a * e = e * a = a$ aina, kun $a \in G$. Alkio e on tällöin ryhmän G *neutraalialkio.*

4. Kaikille alkioille $a \in G$ on olemassa alkio $a^{-1} \in G$ siten, että $a * a^{-1} = a^{-1} * a = e$. Alkiota a^{-1} sanotaan *alkion a käänteisalkioksi.*

Jos edellä mainittujen ehtojen lisäksi operaatio $(*)$ on *kommutatiivinen* eli $a * b = b * a$ aina, kun $a, b \in G$, ryhmä on *Abelin ryhmä.*

Huomautus 3.21. Abelin ryhmässä $(G, +)$ neutraalialkio on alkio 0_G, jolla pätee $a + 0_G = 0_G + a = a$ aina, kun $a \in G$. Alkiota 0_G sanotaan tällöin *nolla-alkioksi.*

Huomautus 3.22. Abelin ryhmässä $(G, +)$ alkion a käänteisalkio on alkio $-a$, jolla pätee $a + (-a) = -a + a = 0_G$. Alkiota $-a$ sanotaan tällöin alkion a *vasta-alkioksi.*

Lause 3.23. *Pari $(\mathbb{Z}_m, +)$ on Abelin ryhmä, jonka kertaluku eli alkioiden lukumäärä on $|(\mathbb{Z}_m, +)| = m$.*

Lause 3.24. *Pari $(\mathbb{Z}_m^*, \cdot)$ on Abelin ryhmä, jonka kertaluku $|(\mathbb{Z}_m^*, \cdot)| = \varphi(m)$.*

Määritelmä 3.25. Olkoon $(G, *)$ ryhmä ja $H \subseteq G$. Jos nyt myös $(H, *)$ on ryhmä, sitä sanotaan *ryhmän $(G, *)$ aliryhmäksi.*

Lause 3.26. *(Lagrangen lause) Äärellisessä ryhmässä aliryhmän kertaluku jakaa ryhmän kertaluvun.*

Määritelmä 3.27. Olkoon $R \neq \emptyset$ ja $(\cdot)$ joukon R operaatio. Pari $(R, \cdot)$ on *monoidi*, jos operaatio $(\cdot)$ on binäärinen ja assosiatiivinen, sekä joukossa R on operaation $(\cdot)$ suhteen neutraalialkio, eli alkio $1_R \in R$ siten, että $1_R \cdot a = a \cdot 1_R = a$ aina, kun $a \in R$. Alkioa 1_R kutsutaan *ykkösalkioksi*.

Määritelmä 3.28. Olkoon $R \neq \emptyset$ ja $(+)$ sekä $(\cdot)$ joukon R operaatiot. Tällöin kolmikko $(R, +, \cdot)$ on *rengas*, jos seuraavat ehdot toteutuvat.

1. $(R, +)$ on Abelin ryhmä.
2. $(R, \cdot)$ on monoidi.
3. Joukon R alkioilla on voimassa *osittelulait*, eli $a \cdot (b + c) = a \cdot b + a \cdot c$ ja $(a + b) \cdot c = a \cdot c + a \cdot c$ aina, kun $a, b, c \in R$.

Lause 3.29. *Kolmikko $(\mathbb{Z}_m, +, \cdot)$ on rengas.*

Määritelmä 3.30. Rengas $(R, +, \cdot)$ on *kommutatiivinen*, jos operaatio $(\cdot)$ on kommutatiivinen, eli $a \cdot b = b \cdot a$ aina, kun $a, b \in R$.

Määritelmä 3.31. Kommutatiivinen rengas $(K, +, \cdot)$ on *kunta*, jos $(K \setminus \{0_K\}, \cdot)$ on Abelin ryhmä. Tällöin ryhmä $(K \setminus \{0_K\}, \cdot)$ on kunnan K *multiplikatiivinen ryhmä* ja $(K, +)$ on kunnan K *additiivinen ryhmä.*

Lause 3.32. *Jos p on alkuluku, niin jäännösluokkarengas $(\mathbb{Z}_p, +, \cdot)$ on kunta. Tällöin kunnasta käytetään merkintää $\mathbb{F}_p$.*

Lause 3.33. *Kunnan $\mathbb{F}_p$ multiplikatiivinen ryhmä on Abelin ryhmä $(\mathbb{Z}_p^*, \cdot)$. Ryhmästä käytetään merkintää $\mathbb{F}_p^*$.*

Lause 3.34. *Olkoon p alkuluku. Tällöin $\mathbb{F}_p^*$ on syklinen ryhmä, eli on olemassa alkio $g \in \mathbb{F}_p^*$, jonka potensseina saadaan kaikki ryhmän $\mathbb{F}_p^*$ alkiot. Siis*

$$\mathbb{F}_p^* = \{1, g, g^2, g^3, ..., g^{p-2}\}.$$

Tällöin sanotaan, että g on kunnan $\mathbb{F}_p$ primitiivijuuri tai ryhmän $\mathbb{F}_p^*$ generoija. Lauseen 3.17 *nojalla ryhmän $\mathbb{F}_p^*$ alkioiden lukumäärä eli kertaluku on $p - 1$.*

Esimerkki 3.35. Kunnan $\mathbb{F}_7$ eräs primitiivijuuri on luku 3, sillä

$$\mathbb{F}_7^* = \{1, 2, 3, 4, 5, 6\} = \{3^0, 3^2, 3, 3^4, 3^5, 3^3\}.$$

Siis kaikki kunnan $\mathbb{F}_7$ alkiot nollaa lukuunottamatta saadaan luvun 3 potensseina.

Lause 3.36. *Alkion $a \in \mathbb{Z}_m$ kertaluku ord(a) on pienin positiivinen kokonaisluku k, jolla $a^k \equiv 1 \pmod{m}$.*

Huomautus 3.37. Lauseen 3.34 mukainen luku $p-1$ on primitiivijuuren g kertaluku.

Huomautus 3.38. Jos alkuluku p on suuri, äärellisellä kunnalla $\mathbb{F}_p$ on useita primitiivijuuria.

Lause 3.39. *Olkoon G äärellinen ryhmä ja $a \in G$. Tällöin alkion a kertaluku ord(a) jakaa ryhmän G kertaluvun ord(G).*

Todistus. Koska G on ryhmä ja $a \in G$, alkio a generoi nyt aliryhmän, jonka kertaluku on $\mathrm{ord}(a)$. Lagrangen lauseen 3.26 nojalla aliryhmän kertaluku $\mathrm{ord}(a)$ jakaa ryhmän G kertaluvun $\mathrm{ord}(G)$. □

Lause 3.40. *(Eulerin teoreema) Olkoot $a, m \in \mathbb{Z}_+$. Jos nyt $syt(a,m) = 1$, niin*

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

Lause 3.41. *(Fermat'n pieni lause) Olkoon p alkuluku ja a positiivinen kokonaisluku. Tällöin jos $p \nmid a$, niin*

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

Lause 3.42. *Olkoon p alkuluku ja g kunnan $\mathbb{F}_p$ primitiivijuuri. Tällöin jos*

$$a \equiv b \pmod{p-1},$$

niin

$$g^a \equiv g^b \pmod{p}.$$

Todistus. Koska $a \equiv b \pmod{p-1}$, voidaan kongruenssin määritelmän nojalla kirjoittaa $a = i \cdot (p-1) + b$, missä $i \in \mathbb{Z}$. Siis Fermat'n pienen lauseen 3.41 nojalla voidaan laskea

$$g^a \equiv g^{i\cdot(p-1)+b} \equiv (g^{(p-1)})^i \cdot g^b \equiv 1^i \cdot g^b \equiv g^b \pmod{p}.$$

□

Lause 3.43. *Olkoot p ja q alkulukuja siten, että $p \equiv 1 \pmod{q}$. Lisäksi olkoon alkion $g \in \mathbb{F}_p^*$ kertaluku q. Tällöin jos*

$$a \equiv b \pmod{q},$$

niin

$$g^a \equiv g^b \pmod{p}.$$

Todistus. Koska $a \equiv b \pmod{q}$, kongruenssin määritelmän nojalla voidaan kirjoittaa $a = i \cdot q + b$, missä $i \in \mathbb{Z}$. Lisäksi, koska alkion g kertaluku on q, niin $g^q \equiv 1 \pmod{p}$. Tällöin voidaan laskea

$$g^a \equiv g^{i \cdot q + b} \equiv (g^q)^i \cdot g^b \equiv 1^i \cdot g^b \equiv g^b \pmod{p}.$$

□

Lause 3.44. *(Eulerin teoreema luvulle pq) Olkoon p ja q erisuuria alkulukuja ja* $g = syt(p-1, q-1)$. *Tällöin kaikille kokonaisluvuille a, joilla* $syt(a, pq) = 1$, *pätee*

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

Todistus. Nyt voidaan laskea

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

Oletusten nojalla tiedetään, että alkuluku p ei jaa kokonaislukua a, ja että g jakaa luvun $q-1$. Fermat'n pienen lauseen nojalla voidaan nyt kirjoittaa

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

sillä luku 1 korotettuna mihin tahansa kokonaislukupotenssiin on 1. Vastaavasti voidaan laskea

$$a^{(p-1)(q-1)/g} = \left(a^{(q-1)}\right)^{(p-1)/g},$$

jolloin Fermat'n pienen lauseen nojalla saadaan

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

Kongruenssin määritelmän nojalla $a^{(p-1)(q-1)/g} - 1$ on siis jaollinen sekä luvulla p, että luvulla q. Lauseen 3.7 nojalla se on siis jaollinen myös luvulla pq eli

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

□

Seuraus 3.45. *Olkoon p ja q erisuuria alkulukuja. Tällöin kaikille kokonaisluvuille a, joilla* $syt(a, pq) = 1$, *pätee*

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

Todistus. Koska $a^{(p-1)(q-1)/g} \equiv 1 \pmod{pq}$ ja $g = syt(p-1, q-1)$, voidaan kirjoittaa

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

□

Määritelmä 3.46. Olkoon g kunnan $\mathbb{F}_p$ primitiivijuuri ja h nollasta poikkeava kunnan $\mathbb{F}_p$ alkio. *Diskreetin logaritmin ongelmalla* tarkoitetaan sopivan eksponentin x löytämistä siten, että

$$g^x \equiv h \pmod{p}.$$

Eksponenttia x kutsutaan luvun h *diskreetiksi logaritmiksi kannassa* g. Tällöin merkitään $x = \log_g h$.

Huomautus 3.47. Jos diskreetin logaritmin ongelmalla on ratkaisu, niin sillä on äärettömän monta ratkaisua. Jos eräs ratkaisu on luku x, ratkaisuja ovat myös luvut $x + k(p-1)$ kaikilla kokonaislukuarvoilla k, sillä Fermat'n pienen lauseen 3.41 nojalla

$$g^{x+k(p-1)} \equiv g^x \cdot (g^{p-1})^k \equiv g^x \cdot 1^k \equiv g^x \equiv h \pmod{p}.$$

4 RSA-allekirjoitus

RSA-allekirjoituksen idea on hyvin yksinkertainen. Käyttäjä valitsee itselleen kaksi salaista suurta alkulukua p ja q, sekä varmennuseksponentin e niin, että $e \in \mathbb{Z}^*_{(p-1)(q-1)}$. Toisin sanoen Määritelmän 3.15 nojalla varmennuseksponentille e täytyy päteä $syt(e,(p-1)(q-1)) = 1$. Allekirjoittaja laskee tämän jälkeen tulon $N = pq$. RSA-allekirjoituksessa julkinen avain on siis muotoa (N, e).

Salaisena avaimena käytetään allekirjoituseksponenttia d, joka saadaan ratkaisemalla kongruenssiyhtälö

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

Kongruenssiyhtälöllä on aina Lauseen 3.8 nojalla olemassa ratkaisu, sillä varmennuseksponentti e on valittu siten, että $syt(e,(p-1)(q-1)) = 1$.

RSA-allekirjoituksella voidaan allekirjoittaa digitaalisia dokumentteja $D \in \mathbb{Z}$, joille $1 \leq D < N$. Allekirjoittaminen tapahtuu laskemalla

$$S \equiv D^d \pmod{N}.$$

Nyt eteenpäin lähetettävä viesti on siis (D, S).

Viestin vastaanottaja voi vahvistaa allekirjoituksen oikeellisuuden käyttämällä lähettäjän julkista avainta e allekirjoitukseen S. Vastaanottaja laskee siis arvon

$$S^e \pmod{N},$$

ja vertaa sitä dokumentin D arvoon. Jos luvut ovat samat, vastaanottaja tietää, että lähettäjä on oikea.

Varmistusprosessin toiminta voidaan todistaa helposti, kun oletetaan, että dokumentti D ja luku N ovat keskenään jaottomia, eli $syt(D, N) = 1$. Oletus voidaan tehdä, sillä suurilla alkuluvuilla p ja q on hyvin epätodennäköistä, että valitun dokumentin D eräs tekijä sattuisi olemaan juuri p tai q. Käytännössä siis lähes kaikille mahdollisille dokumenteille D pätee $syt(D, N) = 1$. Koska nyt tiedetään, että $de \equiv 1 \pmod{(p-1)(q-1)}$, voidaan kongruenssin määritelmän nojalla kirjoittaa $de = i \cdot (p-1)(q-1) + 1$, missä $i \in \mathbb{Z}$. Seurauksen 3.45 nojalla voidaan siis laskea

$$\begin{aligned} S^e &\equiv (D^d)^e \equiv D^{de} \equiv D^{i\cdot(p-1)(q-1)+1} \\ &\equiv (D^{(p-1)(q-1)})^i \cdot D \equiv 1^i \cdot D \equiv D \pmod{N}. \end{aligned}$$

Haluttu kongruenssiyhtälö $S^e \equiv D \pmod{N}$ pitää kuitenkin paikkansa myös erittäin harvoissa tapauksissa, joissa $syt(D, N) = p$ tai $syt(D, N) = q$. Jos

nyt $syt(D, N) = p$ eli $syt(D, q) = 1$, voidaan Fermat'n pienen lauseen 3.41 nojalla laskea

$$\begin{aligned} S^e &\equiv (D^d)^e \equiv D^{de} \equiv D^{i\cdot(p-1)(q-1)+1} \equiv D \cdot D^{i\cdot(p-1)(q-1)} \\ &\equiv D \cdot (D^{q-1})^{i\cdot(p-1)} \equiv D \cdot 1^{i\cdot(p-1)} \equiv D \pmod{q}. \end{aligned}$$

Lisäksi nyt pätee $D \equiv 0 \pmod{p}$, koska $syt(D, p) = p$. Siis $S^e \equiv D^{de} \equiv 0^{de} \equiv 0 \equiv D \pmod{p}$. Koska nyt $S^e \equiv D \pmod{q}$ ja $S^e \equiv D \pmod{p}$, Lauseen 3.7 nojalla saadaan $S^e \equiv D \pmod{pq}$. Vastaavat laskut voidaan myös suorittaa tapauksessa, jossa $syt(D, N) = q$. Siispä varmistusprosessi toimii kaikille dokumenteille D. Kuitenkin mikäli käytetyt luvut olisivat melko pieniä ja ulkopuolinen henkilö huomaisi, että $syt(D, N) \neq 1$, hän voisi jakaa luvun N helposti tekijöihin ja siten menetelmä saataisiin murrettua. Kuitenkin suurille kokonaisluvuille D ja N luvun $syt(D, N)$ laskeminen on hidasta ja vaikeaa, eivätkä harvat tilanteet, joissa $syt(D, N) \neq 1$ aiheuta todellista turvallisuusuhkaa RSA-allekirjoitukselle.

Esimerkki 4.1. Anna valitsee itselleen kaksi salaista alkulukua $p = 61$ ja $q = 43$, sekä laskee niiden tulon

$$N = p \cdot q = 61 \cdot 43 = 2623.$$

Seuraavaksi Anna laskee tulon $(p-1)(q-1) = 60 \cdot 42 = 2520$ ja valitsee sitten itselleen varmennuseksponentiksi $e = 913$, sillä tällöin pätee

$$syt(e, (p-1)(q-1)) = syt(913, 2520) = 1.$$

Nyt Annan julkinen avain on $(N, e) = (2623, 913)$.

Anna haluaa nyt allekirjoittaa dokumentin $D = 753$, jolle pätee $1 \leq D < N$. Hän laskee salaisen allekirjoituseksponentin d ratkaisemalla kongruenssiyhtälön

$$\begin{aligned} & de \equiv 1 \pmod{(p-1)(q-1)} \\ \Rightarrow \quad & d \cdot 913 \equiv 1 \pmod{2520} \\ \Rightarrow \quad & d \equiv 817 \pmod{2520}. \end{aligned}$$

Dokumentille $D = 753$ saadaan nyt allekirjoitus S laskemalla

$$\begin{aligned} S &\equiv D^d \equiv 753^{817} \\ &\equiv 753^{512} \cdot 753^{256} \cdot 753^{32} \cdot 753^{16} \cdot 753 \\ &\equiv 753^{512} \cdot 753^{256} \cdot 1172^2 \cdot 1172 \cdot 753 \\ &\equiv 753^{512} \cdot (1755^2)^8 \cdot 1755 \cdot 1188 \\ &\equiv 753^{512} \cdot 623^8 \cdot 2278 \\ &\equiv 379^2 \cdot 379 \cdot 2278 \\ &\equiv 1999 \cdot 395 \equiv 82 \pmod{2623}. \end{aligned}$$

Anna julkaisee nyt dokumentti-allekirjoitusparin $(D, S) = (753, 82)$.

Viestin vastaanottaja käyttää allekirjoituksen varmistamisessa Annan julkista avainta $(N, e) = (2623, 913)$ ja laskee

$$\begin{aligned} S^e &\equiv 82^{913} \\ &\equiv 82^{512} \cdot 82^{256} \cdot 82^{128} \cdot 82^{16} \cdot 82 \\ &\equiv 82^{512} \cdot 82^{256} \cdot 82^{128} \cdot 2209 \cdot 82 \\ &\equiv 82^{512} \cdot 962^2 \cdot 962 \cdot 151 \\ &\equiv 82^{512} \cdot 2148 \cdot 997 \\ &\equiv 2148^2 \cdot 1188 \\ &\equiv 47 \cdot 1188 \\ &\equiv 55836 \equiv 753 \pmod{2623}. \end{aligned}$$

Koska nyt $D = S^e$, vastaanottaja tietää, että lähettäjä on ollut Anna.

RSA-allekirjoituksen toiminta perustuu siihen, että vaikka ulkopuoliset henkilöt tietävät käytettävän luvun N, on se erittäin vaikeaa ja hidasta jakaa alkulukutekijöihin p ja q. Menetelmässä olennaista on se, että N on riittävän suuri, jotta tekijöihinjako ei ole tietokoneellakaan riittävän nopeaa. Systeemin murtamiseksi on kehitelty muutamia algoritmeja, kuten Pollardin $p - 1$ -menetelmä, jossa tutkitaan ensin luvun $p - 1$ pieniä tekijöitä ja yritetään niiden avulla selvittää luvun N tekijä p. Tämä ei kuitenkaan useissa tapauksissa ole helppoa, joten RSA-allekirjoitusta voidaan pitää edelleen melko turvallisena.

5 ElGamal-allekirjoitus

ElGamal-allekirjoitus perustuu diskreetin logaritmin ongelmaan ja on sen vuoksi hiukan RSA-allekirjoitusta monimutkaisempi. Menetelmässä joko yksi käyttäjistä tai luotettava ulkopuolinen henkilö valitsee suuren alkuluvun p ja primitiivijuuren g kunnasta $\mathbb{F}_p$. Primitiivijuuren g etsimistä varten lasketaan ensin Eulerin φ-funktion arvo luvulle p. Koska nyt p on alkuluku, Lauseen 3.17 nojalla $\varphi(p) = p - 1$. Luku $p - 1$ voidaan seuraavaksi jakaa alkulukutekijöihin, eli esittää muodossa $p - 1 = p_1^{s_1} \cdot p_2^{s_2} \cdot ... \cdot p_k^{s_k}$, missä $k \in \mathbb{Z}_+$. Tästä nähdään, että $\frac{p-1}{p_i}$ on aina lukua $p - 1$ pienempi kokonaisluku, kun $i = 1, 2, ..., k$. Koska kunnassa $\mathbb{F}_p$ primitiivijuuren g kertaluku on $p - 1$, sille täytyy päteä nyt

$$g^{\frac{p-1}{p_i}} \not\equiv 1 \pmod{p}.$$

Primitiivijuuri g voidaan siis löytää laskemalla kokonaisluvuille a, joille $1 < a < p$, potensseja $a^{\frac{p-1}{p_i}} \pmod{p}$, missä $i = 1, 2, ..., k$. Mikäli jollain arvolla i saadaan tällöin 1, kokeiltu luku a ei voi olla primitiivijuuri. Jos taas jokaisella arvolla i saadaan jotain muuta kuin 1, kokeiltu luku a on primitiivijuuri.

Allekirjoitussysteemin käyttäjä valitsee seuraavaksi itselleen yksityisen allekirjoituseksponentin a niin, että $1 \leq a \leq p - 1$ ja määrittää sen jälkeen oman julkisen varmistusavaimensa A laskemalla

$$A \equiv g^a \pmod{p}.$$

Käyttäjän yksityinen avain ElGamal-allekirjoituksessa on siis a ja julkinen avain on (p, g, A).

Allekirjoitus onnistuu dokumenteille $D \in \mathbb{Z}$, joille pätee $1 < D < p$. Viestin allekirjoittaja valitsee aluksi mielivaltaisen luvun k niin, että $1 < k < p$ ja $syt(k, p-1) = 1$. Ehtojen toteutuminen on tärkeää, sillä alkiolle k täytyy algoritmin seuraavia vaiheita varten olla olemassa käänteisalkio modulo $p - 1$. Turvallisuuden vuoksi jokaiselle allekirjoitettavalle dokumentille valitaan eri luku k, eikä samaa lukua käytetä enää uudelleen. Mikäli samaa lukua k käytettäisiin useaan kertaan eri dokumenteille, dokumentti-allekirjoitusparien avulla olisi mahdollista selvittää käyttäjän yksityinen avain a. Allekirjoituksia voisi siis silloin väärentää.

Menetelmän seuraavassa vaiheessa allekirjoittaja laskee kaksi arvoa

$$S_1 \equiv g^k \pmod{p}$$

ja

$$S_2 \equiv (D - aS_1)k^{-1} \pmod{p - 1}.$$

Dokumentille D saatu allekirjoitus on nyt pari (S_1, S_2). Menetelmässä on tärkeää, että S_2 lasketaan käyttämällä modulona lukua $p-1$ ja S_1 moduloa p.

Allekirjoitus voidaan varmistaa käyttämällä viestin lähettäjän julkista avainta A ja laskemalla sen avulla

$$A^{S_1} S_1^{S_2} \pmod{p}$$

ja

$$g^D \pmod{p}.$$

Jos nämä luvut ovat samat, dokumentin D lähettäjä on oikea henkilö. Jos luvut eivät ole samat, lähettäjä on joku toinen käyttäjä tai dokumentti D on vaihtunut allekirjoittamisen jälkeen.

Varmistus toimii näin, koska allekirjoituksen S_2 laskemisessa on käytetty modulona lukua $p-1$. Koska nyt $k \cdot S_2 \equiv k(D - aS_1)k^{-1} \equiv (D - aS_1) \pmod{p-1}$, Lauseen 3.42 nojalla pätee $g^{k \cdot S_2} \equiv g^{(D-aS_1)} \pmod{p}$. Allekirjoituksen varmistusprosessi toimii siis seuraavasti

$$\begin{aligned} A^{S_1} \cdot S_1^{S_2} &\equiv (g^a)^{S_1} \cdot (g^k)^{S_2} \\ &\equiv g^{aS_1} \cdot g^{kS_2} \\ &\equiv g^{aS_1} \cdot g^{(D-aS_1)} \\ &\equiv g^{aS_1 + (D-aS_1)} \equiv g^D \pmod{p}. \end{aligned}$$

Esimerkki 5.1. Anna valitsee alkuluvun $p = 83$ ja laskee $\varphi(p) = \varphi(83) = 82 = 2 \cdot 41$. Siis luvun 82 alkulukutekijät ovat $p_1 = 2$ ja $p_2 = 41$. Nyt kokeilemalla huomataan, että kunnan $\mathbb{F}_{83}$ eräs primitiivijuuri g on 2, sillä

$$2^{p-1/p_1} \equiv 2^{82/2} \equiv 2^{41} \equiv 82 \not\equiv 1 \pmod{83}$$

ja

$$2^{p-1/p_2} \equiv 2^{82/41} \equiv 2^2 \equiv 4 \not\equiv 1 \pmod{83}.$$

Anna valitsee tämän jälkeen itselleen salaisen allekirjoituseksponentin $a = 27$, sillä tällöin pätee $1 \leq a \leq 82$. Hän laskee nyt julkisen vahvistusavaimen

$$\begin{aligned} A &\equiv g^a \equiv 2^{27} \\ &\equiv 2^{16} \cdot 2^8 \cdot 2^2 \cdot 2 \\ &\equiv 2^{16} \cdot 256 \cdot 4 \cdot 2 \\ &\equiv 2^{16} \cdot 7 \cdot 8 \\ &\equiv 7^2 \cdot 56 \\ &\equiv 49 \cdot 56 \\ &\equiv 2744 \equiv 5 \pmod{83}. \end{aligned}$$

Julkisesti tiedossa ovat nyt siis luvut $(p, g, A) = (83, 2, 5)$ ja Annan salainen avain on eksponentti $a = 27$.

Anna haluaa nyt allekirjoittaa dokumentin $D = 31$. Tämä onnistuu, koska dokumentille D pätee $1 < D < 83$. Anna valitsee ensin itselleen luvun $k = 15$, sillä tällöin $syt(k, 82) = 1$. Käänteisalkio k^{-1} saadaan ratkaisemalla kongruenssiyhtälö

$$\begin{aligned} & 15 \cdot k^{-1} \equiv 1 \pmod{82} \\ \Rightarrow \quad & k^{-1} \equiv 11 \pmod{82}. \end{aligned}$$

Anna voi seuraavaksi laskea dokumentille $D = 31$ allekirjoituksen (S_1, S_2). Nyt

$$\begin{aligned} S_1 &\equiv g^k \equiv 2^{15} \\ &\equiv 2^8 \cdot 2^4 \cdot 2^2 \cdot 2 \\ &\equiv 256 \cdot 16 \cdot 4 \cdot 2 \\ &\equiv 7 \cdot 128 \\ &\equiv 896 \equiv 66 \pmod{83}. \end{aligned}$$

ja

$$\begin{aligned} S_2 &\equiv (D - aS_1)k^{-1} \\ &\equiv (31 - 27 \cdot 66) \cdot 11 \\ &\equiv (31 - 1782) \cdot 11 \\ &\equiv (31 - 60) \cdot 11 \\ &\equiv 53 \cdot 11 \\ &\equiv 583 \equiv 9 \pmod{82}. \end{aligned}$$

Allekirjoitus dokumentille $D = 31$ on siis $(S_1, S_2) = (66, 9)$.

Vastaanottaja varmistaa, että viesti on tullut Annalta laskemalla

$$\begin{aligned} A^{S_1} S_1^{S_2} &\equiv 5^{66} \cdot 66^9 \\ &\equiv 5^{64} \cdot 5^2 \cdot 66^8 \cdot 66 \\ &\equiv 64 \cdot 25 \cdot 31 \cdot 66 \\ &\equiv 1600 \cdot 2046 \\ &\equiv 23 \cdot 54 \\ &\equiv 1242 \equiv 80 \pmod{83} \end{aligned}$$

ja

$$\begin{aligned} g^D &\equiv 2^{31} \equiv 2^{16} \cdot 2^8 \cdot 2^4 \cdot 2^2 \cdot 2 \\ &\equiv 2^{16} \cdot 256 \cdot 16 \cdot 4 \cdot 2 \\ &\equiv 2^{16} \cdot 7 \cdot 128 \\ &\equiv 7^2 \cdot 896 \\ &\equiv 49 \cdot 66 \\ &\equiv 3234 \equiv 80 \pmod{83}. \end{aligned}$$

Siis, koska vastaanottaja saa nyt $g^D \equiv A^{S_1} S_1^{S_2} \pmod{83}$, viestin $D = 31$ lähettäjä on Anna.

Allekirjoituksen väärentäminen on mahdollista, jos ulkopuolinen henkilö saa tietoonsa käyttäjän salaisen allekirjoituseksponentin a. Jos hyökkääjä osaa ratkaista diskreetin logaritmin ongelman, hän voi ratkaista eksponentin a suoraan kongruenssiyhtälöstä $g^a \equiv A \pmod{p}$. Toinen tapa väärentää allekirjoitus on yrittää etsiä kokonaisluvut x ja y siten, että

$$A^x x^y \equiv g^D \pmod{p}.$$

Nyt Lauseen 3.42 nojalla yhtälö saadaan g-kantaista logaritmia käyttäen muotoon

$$x \log_g(A) + y \log_g(x) \equiv D \pmod{p-1}.$$

Jos hyökkääjä osaa ratkaista diskreetin logaritmin ongelman, hän voi valita satunnaisen kokonaisluvun x ja laskea arvot $\log_g(x)$ ja $\log_g(A)$. Sen jälkeen hän voi ratkaista luvun y. Dokumentille D saatu väärennetty allekirjoitus on siten (x, y).

Suurille alkuluvuille p diskreetin logaritmin ongelman ratkaiseminen suoraan on kuitenkin hyvin vaikeaa. Tämän vuoksi on kehitelty muitakin tapoja ja algoritmeja, joilla potenssin a voi ainakin yrittää ratkaista. Seuraavaksi esitellään muutama kehitetty murtamismenetelmä hyvin suurpiirteisesti.

Pollardin ρ-menetelmässä yritetään etsiä eksponentit i, j, k ja l siten, että $g^i \cdot A^j = g^k \cdot A^l$. Tästä saadaan edelleen $g^{i-k} = A^{l-j}$. Eksponenttien i, j, k ja l määrittämiseen käytetään sopivaa funktiota $f : \mathbb{Z}_p \to \mathbb{Z}_p$ ja lopulta g-kantaista logaritmia käyttämällä voidaan ratkaista a. Muita kehitettyjä menetelmiä allekirjoitussysteemin murtamiseksi ovat esimerkiksi Pohlig-Hellman- ja Shanksin Babystep-Giantstep-algoritmi. Pohlig-Hellman-algoritmissa käytetään ratkaisemisen apuna luvun $\varphi(p) = p - 1$ alkulukutekijöitä. Shanksin Babystep-Giantstep-algoritmissa puolestaan muodostetaan kaksi listaa, joista toisessa lasketaan primitiivijuuren g potensseja ja toisessa kerrotaan lukua A primitiivijuuren käänteisalkiolla. Listoista löytyy jokin yhteinen alkio, jonka avulla voidaan ratkaista a.

Diskreetin logaritmin ongelmaan perustuvien kryptosysteemien murtamiseen voidaan käyttää myös indeksimenetelmää. Menetelmässä ei pyritä suoraan ratkaisemaan potenssia a yhtälöstä $g^a \equiv A \pmod{p}$, vaan valitaan jokin kokonaisluku B ja ratkaistaan diskreetin logaritmin ongelma $g^a \equiv l \pmod{p}$ kaikille alkuluvuille l, joille pätee $l \leq B$. Tämän jälkeen lasketaan luvuilla $k = 1, 2, ...$ potensseja $A \cdot g^{-k}$, kunnes saadaan kokonaisluku, jonka tekijöitä ovat aiemmin käytetyt alkuluvut $l \leq B$. Kun näin saadusta yhtälöstä otetaan puolittain g-kantainen logaritmi, saadaan yhtälö, johon voidaan sijoittaa aiemmin saadut diskreetin logaritmin $g^a \equiv l \pmod{p}$ ratkaisut. Näin saadaan siis lopulta ratkaistua käyttäjän yksityinen avain a.

Nyt koska allekirjoituksessa (S_1, S_2) luvuista toinen on laskettu käyttäen moduloa p ja toinen moduloa $p - 1$, allekirjoituksen pituus on suunnilleen $2\log_2(p)$ bittiä. Jos valittu alkuluku p on $1000 - 2000$ bittiä, allekirjoituksen ajatellaan olevan turvallinen edellä mainittua indeksimenetelmähyökkäystä vastaan. Tällöin allekirjoituksen pituudeksi saadaan noin $2000 - 4000$ bittiä, mikä on monesti käytännössä turhan paljon.

6 DSA-allekirjoitus

DSA-allekirjoitus on ElGamal-allekirjoituksen paranneltu versio, joka lyhentää allekirjoitusten pituutta huomattavasti. Tämä tapahtuu siten, että salauksessa käytetään ryhmän $\mathbb{F}_p^*$ aliryhmää, jonka kertaluku on q. Näin voidaan tehdä, sillä diskreetin logaritmin ongelman ratkaiseminen ei ole aliryhmässä lainkaan helpompaa kuin ryhmässä $\mathbb{F}_p^*$.

DSA-allekirjoituksessa käyttäjä tai luotettava ulkopuolinen henkilö valitsee kaksi suurta alkulukua p ja q siten, että

$$p \equiv 1 \pmod{q}.$$

Tällöin luku q on siis luvun $p-1$ alkulukutekijä. Alkuluvut valitaan näin, koska Lagrangen lauseen 3.26 nojalla aliryhmän kertaluvun q täytyy jakaa ryhmän $\mathbb{F}_p^*$ kertaluku $p-1$. Kongruenssin määritelmän nojalla luvut p ja q voidaan esimerkiksi valita siten, että ensin valitaan alkuluku q, jonka jälkeen alkuluku p määritetään laskemalla $p = i \cdot q + 1$, missä $i \geq 2$, kunnes saatu p on alkuluku. Käytetyt alkuluvut p ja q ovat usein niin suuria, että ne toteuttavat ehdot $2^{1000} < p < 2^{2000}$ ja $2^{160} < q < 2^{320}$.

Allekirjoittaja valitsee myös alkion $g \in \mathbb{F}_p^*$, jonka kertaluku on q. Tämä onnistuu helposti esimerkiksi laskemalla

$$g = g_1^{\frac{p-1}{q}},$$

missä g_1 on kunnan $\mathbb{F}_p$ primitiivijuuri. Alkio g voidaan valita näin, koska Fermat'n pienen lauseen 3.41 nojalla $g^q \equiv (g_1^{p-1/q})^q \equiv g_1^{p-1} \equiv 1 \pmod{p}$. Tästä nähdään, että alkion g kertaluvun täytyy olla q, sillä jos kertaluku olisi jokin sitä pienempi kokonaisluku, primitiivijuuren g_1 kertaluvun täytyisi olla lukua $p-1$ pienempi, mikä taas ei ole mahdollista kunnassa $\mathbb{F}_p$.

Käyttäjä valitsee tämän jälkeen itselleen salaisen allekirjoituseksponentin a, joka toteuttaa ehdon $1 \leq a \leq q-1$ ja määrittää julkisen vahvistusavaimensa A laskemalla

$$A \equiv g^a \pmod{p}.$$

Käyttäjän julkinen avain on siis A ja julkisesti tiedossa ovat myös luvut p, q ja g.

DSA-allekirjoitus onnistuu dokumenteille $D \in \mathbb{Z}$, jotka toteuttavat ehdon $1 \leq D < q$. Viestin allekirjoittaja valitsee ensin mielivaltaisen luvun k, jolle $1 < k < q$. Kuten ElGamal-allekirjoituksessa, jokaiselle dokumentille D valitaan eri luku k. Seuraavaksi allekirjoittaja laskee kaksi arvoa

$$S_1 \equiv (g^k \pmod{p}) \pmod{q}$$

ja

$$S_2 \equiv (D + aS_1)k^{-1} \pmod{q}.$$

Allekirjoituksen laskeminen tapahtuu siis hyvin samankaltaisesti, kuin ElGamal-systeemissä, mutta moduloina käytetyt luvut on valittu eri tavalla. On tärkeää huomata, että S_1 lasketaan ensin käyttäen moduloa p ja tämän jälkeen vielä moduloa q.

Saatu digitaalinen allekirjoitus on nyt siis muotoa (S_1, S_2). Allekirjoituksen kumpikin luku on laskettu käyttäen modulona lukua q, joten molemmat luvut ovat noin $\log_2(q)$ bittiä pitkiä. Koko allekirjoituksen pituudeksi tulee siis $2\log_2(q)$ bittiä. Koska nyt $q < p$ ja binäärinen logaritmifunktio on kasvava, allekirjoitus on lyhyempi kuin ElGamal-systeemiä käyttämällä.

Allekirjoituksen varmistamista varten viestin vastaanottaja laskee kaksi arvoa

$$V_1 \equiv DS_2^{-1} \pmod{q}$$

ja

$$V_2 \equiv S_1 S_2^{-1} \pmod{q}.$$

Tämän jälkeen vastaanottaja laskee arvon

$$(g^{V_1} A^{V_2} \pmod{p}) \pmod{q}$$

ja vertaa sitä allekirjoitukseen S_1. Jos luvut ovat samat, lähettäjä on oikea henkilö.

Varmistuksen toimiminen voidaan osoittaa helposti tunnettuja kongruenssiyhtälöitä ja Lausetta 3.43 käyttämällä. Koska nyt $V_1 \equiv DS_2^{-1} \pmod{q}$ ja $V_2 \equiv S_1 S_2^{-1} \pmod{q}$, voidaan Lauseen 3.43 nojalla kirjoittaa $g^{V_1} \equiv g^{DS_2^{-1}} \pmod{p}$ ja $g^{V_2} \equiv g^{S_1 S_2^{-1}} \pmod{p}$. Lisäksi tiedetään, että $S_2 \equiv (D + aS_1)k^{-1} \pmod{q}$ ja $k \cdot k^{-1} \equiv 1 \pmod{q}$, joten saadaan $g^{S_2} \equiv g^{(D+aS_1)k^{-1}} \pmod{p}$ ja $g^{k \cdot k^{-1}} \equiv g \pmod{p}$. Nyt voidaan siis laskea

$$\begin{aligned}
g^{V_1} A^{V_2} &\equiv g^{DS_2^{-1}} \cdot (g^a)^{S_1 S_2^{-1}} \\
&\equiv g^{DS_2^{-1}} \cdot g^{aS_1 S_2^{-1}} \\
&\equiv g^{(D+aS_1)S_2^{-1}} \\
&\equiv g^{(D+aS_1)k^{-1} S_2^{-1} k} \\
&\equiv g^{S_2 S_2^{-1} k} \\
&\equiv g^k \pmod{p}.
\end{aligned}$$

Kun kumpikin puoli lasketaan vielä käyttäen modulona lukua q, saadaan

$$(g^{V_1} A^{V_2} \pmod{p}) \pmod{q} \equiv (g^k \pmod{p}) \pmod{q} \equiv S_1 \pmod{q}.$$

Esimerkki 6.1. Anna valitsee ja julkaisee suuret alkuluvut $p = 59$ ja $q = 29$, joille pätee $59 \equiv 1 \pmod{29}$. Allekirjoittamisessa käytetyn aliryhmän kertaluku on siis 29. Kunnan $\mathbb{F}_{59}$ eräs primitiivijuuri voidaan ratkaista Luvussa 5 esitetyllä tavalla. Nyt $\varphi(p) = \varphi(59) = 58 = 2 \cdot 29$. Siis luvun 58 alkulukutekijät ovat $p_1 = 2$ ja $p_2 = 29$. Kokeilemalla huomataan, että kunnan $\mathbb{F}_{59}$ eräs primitiivijuuri g on 2, sillä

$$2^{p-1/p_1} \equiv 2^{58/2} \equiv 2^{29} \equiv 58 \not\equiv 1 \pmod{59}$$

ja

$$2^{p-1/p_2} \equiv 2^{58/29} \equiv 2^2 \equiv 4 \not\equiv 1 \pmod{59}.$$

Seuraavaksi Anna valitsee luvun g, jonka kertaluku on 29 laskemalla

$$g = g_1^{(p-1)/q} = 2^{58/29} = 2^2 = 4.$$

Anna valitsee itselleen salaisen allekirjoitusavaimen $a = 15$, sillä tällöin pätee $1 \leq a \leq q - 1 = 28$. Nyt hän voi määrittää julkisen avaimensa A laskemalla

$$\begin{aligned} A \equiv g^a &\equiv 4^{15} \equiv 4^8 \cdot 4^4 \cdot 4^3 \\ &\equiv 4^8 \cdot 256 \cdot 64 \\ &\equiv 4^8 \cdot 20 \cdot 5 \\ &\equiv 20^2 \cdot 100 \\ &\equiv 400 \cdot 41 \\ &\equiv 46 \cdot 41 \\ &\equiv 1886 \equiv 57 \pmod{59}. \end{aligned}$$

Annan julkinen vahvistusavain muodostuu nyt siis sekä luvusta $A = 57$, että luvuista $(p, q, g) = (59, 29, 4)$.

Nyt Anna haluaa allekirjoittaa dokumentin $D = 25$. Allekirjoitusta varten hän valitsee satunnaisen luvun $k = 8$, jolle pätee ehto $1 < k < 29$. Nyt luvun $k = 8$ käänteisalkio k^{-1} saadaan ratkaisemalla kongruenssiyhtälö

$$\begin{aligned} 8 \cdot k^{-1} &\equiv 1 \pmod{29} \\ \Rightarrow \qquad k^{-1} &\equiv 11 \pmod{29}. \end{aligned}$$

Allekirjoitusta varten Anna laskee nyt kaksi arvoa

$$\begin{aligned} S_1 &\equiv (g^k \pmod{p}) \pmod{q} \\ &\equiv (4^8 \pmod{59}) \pmod{29} \\ &\equiv (65536 \pmod{59}) \pmod{29} \\ &\equiv (46 \pmod{59}) \pmod{29} \\ &\equiv 17 \pmod{29} \end{aligned}$$

ja

$$\begin{aligned} S_2 &\equiv (D + aS_1)k^{-1} \pmod{q} \\ &\equiv (25 + 15 \cdot 17) \cdot 11 \pmod{29} \\ &\equiv (25 + 255) \cdot 11 \pmod{29} \\ &\equiv 280 \cdot 11 \pmod{29} \\ &\equiv 3080 \pmod{29} \\ &\equiv 6 \pmod{29}. \end{aligned}$$

Allekirjoitus dokumentille $D = 25$ on siis $(S_1, S_2) = (17, 6)$.

Viestin vastaanottaja vahvistaa allekirjoituksen laskemalla ensin käänteisalkion allekirjoitukselle S_2. Kongruenssiyhtälöstä $6 \cdot S_2^{-1} \equiv 1 \pmod{29}$ saadaan $S_2^{-1} \equiv 5 \pmod{29}$, minkä jälkeen vastaanottaja voi laskea kaksi arvoa

$$V_1 \equiv DS_2^{-1} \equiv 25 \cdot 5 \equiv 125 \equiv 9 \pmod{29}$$

ja

$$V_2 \equiv S_1 S_2^{-1} \equiv 17 \cdot 5 \equiv 85 \equiv 27 \pmod{29}.$$

Seuraavaksi vastaanottaja laskee

$$\begin{aligned} g^{V_1} A^{V_2} &\equiv 4^9 \cdot 57^{27} \\ &\equiv 4^9 \cdot 57^{16} \cdot 57^8 \cdot 57^3 \\ &\equiv 7 \cdot 57^{16} \cdot 57^8 \cdot 51 \\ &\equiv 7 \cdot 57^{16} \cdot 20 \cdot 51 \\ &\equiv 7 \cdot 20^2 \cdot 1020 \\ &\equiv 7 \cdot 46 \cdot 17 \\ &\equiv 5474 \equiv 46 \pmod{59}, \end{aligned}$$

mistä edelleen moduloa 29 käyttäen saadaan

$$(g^{V_1} A^{V_2} \pmod{59}) \pmod{29} \equiv 46 \pmod{29} \equiv 17 \pmod{29}.$$

Koska nyt $17 \equiv S_1 \pmod{29}$, viestin lähettäjä on oikea henkilö eli Anna.

DSA perustuu ElGamal-allekirjoituksen tapaan diskreetin logaritmin ongelmaan, joten menetelmän murtamisessa voidaan käyttää Luvussa 5 esiteltyjä algoritmeja. Ryhmien lisäksi DSA-allekirjoitusta voidaan käyttää esimerkiksi elliptisille käyrille, jolloin diskreetin logaritmin ongelma on vieläkin vaikeampi ratkaista ja menetelmä on siten entistäkin turvallisempi. Tällöin puhutaan ECDSA-allekirjoituksesta, jolla on hyvin paljon käyttökohteita. Esimerkiksi Bitcoinin takana toimii ECDSA-algoritmi, joka vahvistaa kaupantekoa ja jonka avulla voidaan varmistaa, että varoja käyttää vain niiden oikea omistaja.

Lähdeluettelo

[1] J. Hoffstein, J. Pipher, J.H. Silverman. *An introduction to mathematical cryptography.* Springer, New York, 2008.

[2] K. Myllylä, M. Niemenmaa, T. Törmä. *Algebralliset rakenteet -kurssin luentorunko.* Oulun yliopisto, 2019.

[3] K. Myllylä, M. Niemenmaa, T. Törmä. *Algebran perusteet -kurssin luentorunko.* Oulun yliopisto, 2019.