TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Pekka Larja

RSA-salaus ja sen lukuteoreettinen pohja

Informaatiotieteiden yksikkö
Matematiikka
Toukokuu 2011

Tampereen yliopisto

Informaatiotieteiden yksikkö

LARJA, PEKKA: RSA-salaus ja sen lukuteoreettinen pohja

Pro gradu -tutkielma, 40 s.

Matematiikka

Toukokuu 2011

Tiivistelmä

Tämä tutkielma käsittelee RSA-salausta ja sen lukuteoreettista perustaa. RSA-salaus on varmasti yksi yleisimmin käytetyistä (ellei yleisin) julkisen avaimen salakirjoitusjärjestelmistä. Nykyisen viestintätekniikan kehityksen mukana salakirjoitusjärjestelmistä on tullut keskeisiä välineitä modernissa yhteiskunnassa.

RSA-salaus perustuu eräisiin lukuteorian keskeisiin tuloksiin ja on perusidealtaan hämmästyttävän yksinkertainen. Tutkielman luvussa 2 tarkastellaan RSA-salauksen käyttämiä lukuteorian osa-alueita, kuten jaollisuutta, alkulukuja ja kongruensseja. Tutkielman luvussa 3 siirrytään tarkastelemaan varsinaista RSA-salausta. Ensin esitellään RSA-salaus yksityiskohtaisesti, ja sen jälkeen käytetään järjestelmää käytännössä muutaman esimerkin muodossa tekstin salaamiseen. Lopuksi käsitellään joitain RSA-salauksen haavoittuvuuksia ja niiltä suojautumista.

Sisältö

1 Johdanto

Tutkielmani käsittelee RSA-salausta ja sen lukuteoreettista perustaa. Olen matematiikan lisäksi opiskellut tietojenkäsittelyoppia pitkänä sivuaineena ja ollut IT-alalla töissä jo pitkään. Suuri osa suorittamistani korkeakoulutason matematiikan opinnoista on ollut niin sanottua analyysiä. Ottamatta mitenkään kantaa analyysin hyödyllisyyteen yleensä, ainakaan omalta kohdaltani käytännön työelämässä IT-alalla analyysin opinnoista ei ole ollut juuri mitään hyötyä.

Lukuteoria sen sijaan on matematiikan osa-alue, jolla on kenties selvimmin yhtymäkohtia tietojenkäsittelyyn. Erityisesti käsittelemäni RSA-salaus on käytännön työkalu, jota tuhannet, elleivät jopa kymmenettuhannet, suomalaiset käyttävät joka päivä työssään. Esimerkiksi yleisesti käytetty **PGP** salausohjelmisto (Pretty Good Privacy) käyttää RSA-salausta keskeisesti salausprosessissaan.

Vuonna 2003 suoritin syventävinä opintoina Lukuteoria-kurssin. Kurssi herätti kiinnostukseni erityisesti salauskirjoitusmenetelmiä kohtaan, ja teinkin harjoitustyön, joka käsitteli niin sanottua **selkäreppuongelmaa** (knapsack problem) ja kuvasi samalla erään julkisen avaimen kryptausmetodin. Tehtyäni tuon harjoitustyön aloin harkita graduni tekemistä jostain salakirjoitukseen liittyvästä aiheesta. Luonnollisesti työni IT-alalla lisäsi motivaatiota tehdä gradu lukuteoriaan ja salakirjoitukseen liittyen. Aivan graduprosessin alkuvaiheessa työni aihe ei vielä ollut täysin tarkentunut RSA-salaukseen, mutta työn edetessä ja keskusteltuani professori Lauri Hellan kanssa päätin rajata graduni käsittelemään RSA-salausta ja sen lukuteoreettista perustaa.

Tutkielmani luvussa 2 käyn läpi joitain lukuteorian peruskäsitteitä, joita tarvitaan erityisesti RSA-salaukseen perehdyttäessä. Näitä käsitteitä ovat esimerkiksi jaollisuus, alkuluvut, kongruenssit ja niiden laskusäännöt. Keskeisistä käsitellyistä lauseista mainittakoon *jakoalgoritmi*, *Eukleideen algoritmi*, kongruenssien laskusäännöt ja niitten yleistykset, *Eulerin lause*, *Wilsonin lause* ja *Fermat'n pieni lause*. Luvussa 2 esitellään myös Eukleideen algoritmin käyttöä suurimman yhteisen tekijän etsimisessä ja sekä modulaarinen potenssiin korotus.

Tutkielmani luvussa 3 käsittelen itse RSA-salausta. Salausalgoritmi käy-

dään ensin läpi huolellisesti ja todistetaan salauksen purkamisen toimiminen. Sen jälkeen tutustutaan RSA-salaussysteemin käytännön suunnitteluun ja käytännön salaukseen esimerkkien avulla. Lopuksi käsitellään RSA-salauksen käyttämistä viestien allekirjoitukseen ja joitain tapoja murtaa RSA-salaus sekä keinoja välttää murtaminen.

Tutkielmani lukijan on hyvä olla perehtynyt matemaattiseen esitystapaan ja todistustekniikkaan. Korkeakoulutason matematiikan opinnot antavat varmasti riittävät valmiudet tutkielmani ymmärtämiseen. Myös hyvin suoritettu lukion laaja matematiikka on hyvä pohja ymmärtää tämä esitys. Erityisesti näin on, jos laajan matematiikan opintoihin on kuulunut lukuteoriaa käsittelevä kurssi.

Tutkielmassani olen käyttänyt kahta päälähdettä: Kenneth H. Rosenin teosta *Elementary Number Theory - Fourth Edition* [3] ja Arto Salomaan *Public Key Cryptography - Second Enlarged Edition* [1]. Rosenin teos on ollut pääosin käytössä lukuteoriaosuudessa ja Salomaan teos puolestaan RSA-salausta käsittelevässä osuudessa tutkielmassani. Rosenin ja Salomaan teosten lisäksi olen käyttänyt joitain WWW-lähteitä. Näitä lähteitä on käytetty lähinnä tuoreimman mahdollisen tiedon löytämiseksi.

2 Lukuteorian peruskäsitteitä

Tässä luvussa käsitellään joitain lukuteorian peruskäsitteitä, jotka ovat keskeisessä asemassa erityisesti RSA-salauksessa.

2.1 Jaollisuus

Määritelmä 2.1. [3, s. 31] Jos a ja b ovat kokonaislukuja ja $a \neq 0$, voidaan sanoa, että a jakaa luvun b, jos on olemassa kokonaisluku c siten että $b = ac$. Jos luku a jakaa luvun b, voidaan myös sanoa, että luku a on luvun b jakaja tai tekijä. Lisäksi voidaan sanoa, että luku b on jaollinen luvulla a.

Jos luku a jakaa luvun b, merkitään $a \mid b$, ja jos luku a ei jaa lukua b, merkitään $a \nmid b$.

Esimerkki 2.1. $2 \mid 4$, $3 \nmid 5$.

Lause 2.1. *[3, s. 31] Jos luvut a, b ja c ovat kokonaislukuja siten, että $a \mid b$ ja $b \mid c$, niin tällöin $a \mid c$.*

Todistus. Koska $a \mid b$ ja $b \mid c$, on olemassa kokonaisluvut e ja f siten, että $ae = b$ ja $bf = c$. Joten $c = bf = (ae)f = a(ef)$ ja nähdään, että $a \mid c$. □

Esimerkki 2.2. Koska $5 \mid 10$ ja $10 \mid 20$, niin lauseen 2.1 mukaan $5 \mid 20$.

Lause 2.2. *[3, s. 32] Oletetaan, että luvut a, b, c, m ja n ovat kokonaislukuja ja $c \mid a$ ja $c \mid b$. Tällöin $c \mid (ma + nb)$.*

Todistus. Koska $c \mid a$ ja $c \mid b$, on olemassa kokonaisluvut e ja f siten, että $a = ce$ ja $b = cf$. Joten $ma + nb = mce + ncf = c(me + nf)$ ja nähdään, että $c \mid (ma + nb)$. □

Esimerkki 2.3. Koska $7 \mid 14$ ja $7 \mid 21$ niin lauseen 2.2 mukaan luku 7 jakaa luvun

$$2 * 14 + 3 * 21 = 91.$$

Esitetään ja todistetaan seuraavaksi niin sanottu *jakoalgoritmi*. Jakoalgoritmin todistusta varten esitetään ensin positiivisten kokonaislukujen *hyvinjärjestysominaisuus*.

Hyvinjärjestysominaisuus: Jokaisessa epätyhjässä positiivisten kokonaislukujen joukossa on olemassa pienin alkio. [3, s. 6]

Lause 2.3. *[3, s. 32]* ***Jakoalgoritmi.*** *Oletetaan, että luvut a ja b ovat kokonaislukuja ja $b > 0$. Tällöin on olemassa yksikäsitteiset kokonaisluvut q ja r siten, että $a = bq + r$ ja $0 \leq r < b$.*

Todistus. Olkoon joukko S kaikkien muotoa $a - bk$ olevien kokonaislukujen joukko, missä k on kokonaisluku. Merkitään $S = \{a - bk \mid k \in \mathbf{Z}\}$. Olkoon T kaikkien positiivisten kokonaislukujen joukko joukossa S. Joukko T on epätyhjä, koska $a - bk$ on positiivinen aina, kun $k < a/b$.

Hyvinjärjestysominaisuuden mukaan joukolla T on pienin alkio $k = q$. Asetetaan $r = a - bq$. (Arvot r ja q ovat jakoalgoritmissä esitetyt luvut.) Joukon T määritelmän mukaan $r \geq 0$ ja on helppoa nähdä, että $r < b$. Jos $r \geq b$, niin $r > r - b = a - bq - b = a - b(q + 1)$, joka on ristiriidassa sen kanssa, että luku $r = a - bq$ on pienin positiivinen kokonaisluku muotoa $a - bk$. Näin ollen $0 \leq r < b$.

Osoitetaan seuraavaksi, että luvut q ja r ovat yksikäsitteisiä. Muodostetaan kaksi yhtälöä $a = bq_1 + r_1$ ja $a = bq_2 + r_2$, joissa $0 \leq r_1 < b$ ja $0 \leq r_2 < b$. Vähentämällä toinen yhtälö ensimmäisestä saadaan

$$0 = b(q_1 - q_2) + (r_1 - r_2).$$

Nyt näemme, että

$$r_2 - r_1 = b(q_1 - q_2).$$

Viimeisimmästä yhtälöstä näemme, että b jakaa luvun $r_2 - r_1$. Koska $0 \leq r_1 < b$ ja $0 \leq r_2 < b$, saadaan $-b < r_1 - r_2 < b$. Näin ollen luku b voi jakaa luvun $r_2 - r_1$ vain, jos $r_2 - r_1 = 0$. Toisin sanoen $r_2 = r_1$. Koska $bq_1 + r_1 = bq_2 + r_2$ ja $r_2 = r_1$, nähdään helposti, että $q_2 = q_1$. Nyt siis nähdään, että luvut q ja r ovat yksikäsitteisiä. □

Esimerkki 2.4. Jos $a = 143$ ja $b = 17$, niin tällöin $q = 8$ ja $r = 7$, koska $143 = 17 * 8 + 7$.

2.2 Alkuluvut

Alkuluvut ovat keskeisessä osassa RSA-salauksen toteuttamisessa. RSA-salaus perustuu kahden hyvin suuren alkuluvun tuloon, jonka tekijöihin jakaminen

on äärimmäisen hankalaa.

Määritelmä 2.2. [3, s. 66] *Alkuluku* on positiivinen kokonaisluku, joka on suurempi kuin luku 1 ja ei ole jaollinen muilla positiivisilla kokonaisluvuilla kuin luvulla 1 ja itsellään.

Esimerkki 2.5. Kymmenen ensimmäistä alkulukua ovat seuraavat: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29. Lisäksi esimerkiksi luvut 149, 283 ja 419 ovat alkulukuja.

Määritelmä 2.3. [3, s. 66] Positiivinen kokonaisluku, joka ei ole alkuluku ja on suurempi kuin luku 1, on *yhdistetty luku*.

Esimerkki 2.6. Yhdistettyjä lukuja ovat esimerkiksi $4 = 2 * 2$, $6 = 3 * 2$ ja $35 = 7 * 5$.

Määritelmä 2.4. [3, s. 80] *Suurin yhteinen tekijä* kahdelle kokonaisluvulle a ja b, jotka molemmat ovat erisuuria kuin 0, on suurin kokonaisluku, joka jakaa luvun a ja luvun b. Lukujen a ja b suurinta yhteistä tekijää merkitään tässä esityksessä (a, b).

Esimerkki 2.7. Lukujen 10 ja 15 suurin yhteinen tekijä on $(10, 15) = 5$. $(12, 36) = 12$ ja $(7, 11) = 1$.

Määritelmä 2.5. [3, s. 80] Luvut a ja b ovat *suhteellisia alkulukuja*, jos niiden suurin yhteinen tekijä $(a, b) = 1$.

Esimerkki 2.8. Koska $(15, 22) = 1$, ovat luvut 15 ja 22 suhteellisia alkuluja.

Suurin tunnettu alkuluku tällä hetkellä on vuonna 2008 elokuussa löytynyt Mersennen alkuluku $2^{43112609} - 1$. Alkuluvun löysi University of Californian matematiikan osaston tietokone. Se on 45. tunnettu Mersennen alkuluku ja siinä on 12 978 189 numeroa. Tilan puutteen vuoksi lukua ei esitetä auki kirjoitettuna tässä [4].

2.3 Eukleideen algoritmi

Aiemmassa esimerkissä 2.7 käytetyt luvat ovat niin pieniä, että suurin yhteinen tekijä on nähtävissä varsin helposti. Suurien lukujen ollessa kyseessä

käytetään suurimman yhteisen tekijän määrittämiseen Eukleideen algoritmia. Eukleideen algoritmi todistetaan tässä esityksessä myöhemmin, mutta ennen sitä todistetaan kaksi lausetta, joita käytetään Eukleideen algoritmin todistuksessa.

Lause 2.4. *[3, s. 81] Olkoot a, b ja c kokonaislukuja. Tällöin $(a + cb, b) = (a, b)$.*

Todistus. Olkoot a, b ja c kokonaislukuja. Osoitetaan, että yhteiset jakajat luvuille a ja b ovat täsmälleen samat kuin yhteiset jakajat luvuille $a + cb$ ja b. Tämä osoittaa, että $(a + cb, b) = (a, b)$. Olkoon luku e lukujen a ja b yhteinen jakaja. Lauseen 2.1 mukaan nähdään, että $e \mid (a + cb)$, joten luku e on lukujen $a + cb$ ja b yhteinen jakaja. Jos luku f on yhteinen jakaja luvuille $a + cb$ ja b, niin lauseen 2.1 mukaan luku f jakaa luvun $(a + cb) - cb = a$. Näin ollen luku f on yhteinen jakaja luvuille a ja b. Joten $(a + cb, b) = (a, b)$. □

Apulause 2.1. *[3, s. 87] Olkoot e ja d kokonaislukuja ja $e = dq + r$, jossa luvut q ja r ovat kokonaislukuja. Tällöin $(e, d) = (d, r)$.*

Todistus. Apulause seuraa suoraan lauseesta 2.4. Valitaan $a = r$, $b = d$ ja $c = q$. Nyt siis lauseen 2.4 mukaan $(r + qd, d) = (r, d)$, eli $(e, d) = (r, d)$. □

Määritelmä 2.6. Olkoot a ja b kokonaislukuja siten, että $a \geq b > 0$. Merkitään nyt $r_0 = a$ ja $r_1 = b$. Nyt jakoalgoritmin mukaan $r_0 = r_1 q_1 + r_2$ ja $r_1 = r_2 q_2 + r_3$. Määritellään kokonaisluvut r_j ja q_j jakoalgoritmin avulla siten, että $r_j = r_{j+1} q_{j+1} + r_{j+2}$. Jakoalgoritmin mukaan $0 < r_{j+2} < r_{j+1}$.

Lause 2.5. *[3, s. 86]* ***Eukleideen algoritmi.*** *Olkoot a ja b kokonaislukuja siten, että $a \geq b > 0$. Merkitään nyt $r_0 = a$ ja $r_1 = b$. Soveltamalla toistuvasti jakoalgoritmia saadaan $r_j = r_{j+1} q_{j+1} + r_{j+2}$, missä r_j ja q_j ovat määritelmässä 2.6 määriteltyjä kokonaislukuja. Kun $j = 0, 1, 2, \ldots, n - 2$ ja $r_{n+1} = 0$, niin $(a, b) = r_n$, joka on viimeinen nollasta poikkeava jäännös.*

Todistus. Olkoot $r_0 = a$ ja $r_1 = b$ positiivisia kokonaislukuja siten, että $a \geq b$. Soveltamalla toistuvasti jakoalgoritmia saadaan

$$r_0 = r_1 q_1 + r_2 \qquad 0 \leq r_2 < r_1,$$

$$r_1 = r_2 q_2 + r_3 \qquad 0 \leq r_3 < r_2,$$

$$\vdots$$

$$r_{j-2} = r_{j-1}q_{j-1} + r_j \quad 0 \leq r_j < r_{j-1},$$

$$\vdots$$

$$r_{n-4} = r_{n-3}q_{n-3} + r_{n-2} \quad 0 \leq r_{n-2} < r_{n-3},$$

$$r_{n-3} = r_{n-2}q_{n-2} + r_{n-1} \quad 0 \leq r_{n-1} < r_{n-2},$$

$$r_{n-2} = r_{n-1}q_{n-1} + r_n \quad 0 \leq r_n < r_{n-1},$$

$$r_{n-1} = r_n q_n.$$

Voidaan olettaa, että lopulta yhtälöketjusta saadaan jäännökseksi luku nolla, sillä jäännösten jono $a = r_0 \geq r_1 > r_2 > \ldots \geq 0$ voi sisältää korkeintaan a termiä, koska jokainen jäännös on kokonaisluku. Apulauseen 2.1 mukaan $(a, b) = (r_0, r_1) = (r_1, r_2) = (r_2, r_3) = \ldots = (r_{n-3}, r_{n-2}) = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = (r_n, 0) = r_n$. Joten $(a, b) = r_n$, joka on viimeinen nollasta eroava jäännös. □

Esimerkki 2.9. Olkoon nyt $a = 72$ ja $b = 29$. Etsitään lukujen a ja b suurin yhteinen tekijä käyttämällä Eukleideen algoritmia.

$$72 = 29 * 2 + 14$$

$$29 = 14 * 2 + \mathbf{1}$$

$$14 = 1 * 14$$

Nyt siis Eukleideen algoritmin avulla näytettiin, että $(72, 29) = 1$. Toisin sanoen luvuilla 72 ja 29 ei ole yhteisiä tekijöitä.

Esimerkki 2.10. Olkoon nyt $a = 124$ ja $b = 44$. Etsitään lukujen a ja b suurin yhteinen tekijä käyttämällä Eukleideen algoritmia.

$$124 = 44 * 2 + 36$$

$$44 = 36 * 1 + 8$$

$$36 = 8 * 4 + \mathbf{4}$$

$$8 = 4 * 2 + 0$$

Nyt Eukleideen algoritmin avulla näytettiin, että $(142, 44) = 4$.

2.4 Kongruenssit

Määritelmä 2.7. [3, s. 128] Olkoon luku m positiivinen kokonaisluku ja luvut a ja b kokonaislukuja. Tällöin luku a on kongruentti luvun b kanssa modulo m, jos $m \mid (a - b)$.

Jos luku a on kongruentti luvun b kanssa modulo m, merkitään $a \equiv b \pmod{m}$. Jos $m \nmid (a - b)$, merkitään $a \not\equiv b \pmod{m}$.

Esimerkki 2.11. $13 \equiv 3 \pmod{5}$, koska $5 \mid (13 - 3) = 10$. Toisaalta $10 \not\equiv 2 \pmod{7}$, koska $7 \nmid (10 - 2) = 8$.

Lause 2.6. *[3, s. 128] Oletetaan, että luvut a ja b ovat kokonaislukuja. Nyt $a \equiv b \pmod{m}$, jos ja vain jos on olemassa kokonaisluku k siten, että $a = b + km$.*

Todistus. Olkoon $a \equiv b \pmod{m}$, tällöin $m \mid (a - b)$. Nyt täytyy olla olemassa kokonaisluku k siten, että $km = a - b$ Nyt siis $a = b + km$. □

Esimerkki 2.12. $13 \equiv 3 \pmod{5}$. Nyt $13 = 3 + 2 * 5$.

Seuraavaksi esitetään ja todistetaan kongruenssirelaation refleksisyys, symmetrisyys ja transitiivisuus.

Lause 2.7. *[3, s. 129] Olkoon m positiivinen kokonaisluku. Tällöin seuraavat kohdat ovat voimassa:*

(i) Refleksisyys. Olkoon a kokonaisluku. Tällöin $a \equiv a \pmod{m}$.

(ii) Symmetrisyys. Olkoot a ja b kokonaislukuja siten, että $a \equiv b \pmod{m}$. Tällöin $b \equiv a \pmod{m}$.

(iii) Transitiivisuus. Olkoot a, b ja c kokonaislukuja siten, että $a \equiv b \pmod{m}$ ja $b \equiv c \pmod{m}$. Tällöin $a \equiv c \pmod{m}$.

Todistus.

(i) Koska $m \mid (a - a) = 0$, niin $a \equiv a \pmod{m}$.

(ii) Olkoon $a \equiv b \pmod{m}$. Nyt $m \mid (a - b)$. Tällöin on olemassa kokonaisluku k siten, että $km = a - b$. Kerrotaan yhtälö puolittain luvulla -1 ja saadaan $(-k)m = b - a$. Siis $m \mid (b - a)$. Joten $b \equiv a \pmod{m}$.

(iii) Olkoon $a \equiv b \pmod{m}$ ja $b \equiv c \pmod{m}$. Siis $m \mid (a-b)$ ja $m \mid (b-c)$. Joten on olemassa kokonaisluvut k ja l siten, että $km = a - b$ ja $lm = b - c$. Nyt $a - c = (a - b) + (b - c) = km + lm = (k + l)m$. Selvästi nähdään, että $m \mid (a - c)$ ja $a \equiv c \pmod{m}$.

□

Lauseen 2.7 perusteella nähdään, että kokonaisluvut on jaettu luvun m osoittamaan määrään joukkoja, joita kutsutaan *jäännösluokiksi modulo* m. Jokaisen jäännösluokan luvut ovat keskenään kongruentteja modulo m. [3, s. 129]

Esimerkki 2.13. Kolme jäännösluokkaa modulo 3 ovat

$$\ldots \equiv -6 \equiv -3 \equiv 0 \equiv 3 \equiv 6 \ldots \pmod{3}$$

$$\ldots \equiv -5 \equiv -2 \equiv 1 \equiv 4 \equiv 7 \ldots \pmod{3}$$

$$\ldots \equiv -4 \equiv -1 \equiv 2 \equiv 5 \equiv 8 \ldots \pmod{3}.$$

Määritelmä 2.8. [3, s. 130] *Täydellinen jäännössysteemi modulo* m on joukko kokonaislukuja siten, että jokainen kokonaisluku on kongruentti modulo m täsmälleen yhden joukkoon kuuluvan kokonaisluvun kanssa.

Esimerkki 2.14. Esimerkiksi joukot $\{0, 1, 2\}$ ja $\{4, 8, 12\}$ ovat täydellisiä jäännössysteemejä modulo 3.

Seuraavaksi esitetään ja todistetaan kongruenssin yhteen-, vähennys- ja kertolaskusäännöt.

Lause 2.8. *[3, s. 130] Olkoot a, b ja c kokonaislukuja ja m positiivinen kokonaisluku siten, että $a \equiv b \pmod{m}$. Tällöin*

(i) $a + c \equiv b + c \pmod{m}$,

(ii) $a - c \equiv b - c \pmod{m}$,

(iii) $ac \equiv bc \pmod{m}$.

Todistus.

(i) Koska $a \equiv b \pmod{m}$, niin $m \mid (a-b)$. Nyt $(a+c)-(b+c) = a-b$, siis $m \mid ((a+c)-(b+c))$, joten $a+c \equiv b+c \pmod{m}$.

(ii) Koska $(a-c)-(b-c) = (a-b)$, niin edellisen kohdan perusteella nähdään, että $a-c \equiv b-c \pmod{m}$.

(iii) Koska $ac-bc = c(a-b)$ ja $m \mid (a-b)$, niin $m \mid c(a-b)$. Siis $ac \equiv bc \pmod{m}$.

□

Esimerkki 2.15. $13 \equiv 3 \pmod{5}$. Nyt lauseen 2.8 mukaan $13+7 \equiv 3+7 \pmod{5}$, $13-2 \equiv 3-2 \pmod{5}$ ja $13*4 \equiv 3*4 \pmod{5}$.

Kongruenssiyhtälöiden jakaminen ei onnistu yhtä suoraviivaisesti kuin edellä esitetyt yhteen-, vähennys- ja kertolaskut.

Lause 2.9. *[3, s. 131] Olkoot luvut a, b, c ja m kokonaislukuja siten, että* $m > 0$, $d = (c, m)$ *ja* $ac \equiv bc \pmod{m}$. *Tällöin* $a \equiv b \pmod{m/d}$.

Todistus. Koska $ac = bc \pmod{m}$, niin $m \mid (ac-bc) = c(a-b)$. Tällöin on olemassa kokonaisluku k niin, että $c(a-b) = km$. Jaetaan molemmat puolet luvulla d ja saadaan $(c/d)(a-b) = k(m/d)$. Koska $(c, m) = d$, niin $(m/d, c/d) = 1$. Nyt $m/d \mid (a-b)$, koska $m/d \nmid c/d$. Joten $a \equiv b \pmod{m/d}$.

□

Esimerkki 2.16. Tarkastellaan kongruenssia $100 \equiv 40 \pmod{15}$. Nyt $(10, 15) = 5$, joten kun kongruenssi jaetaan puolittain luvulla 10 ja moduli luvulla 5, saadaan $10 \equiv 4 \pmod{3}$. Jaetaan kongruenssi $111 \equiv 15 \pmod{12}$ luvulla 3 ja saadaan $37 \equiv 5 \pmod{4}$, sillä $(3, 12) = 3$.

Seuraus 2.1. [3, s. 131] *Olkoot a, b, c ja m kokonaislukuja siten, että* $m > 0$, $(c, m) = 1$ *ja* $ac \equiv bc \pmod{m}$. *Nyt* $a \equiv b \pmod{m}$.

Esimerkki 2.17. Tarkastellaan kongruenssia $135 \equiv 18 \pmod{13}$. Nyt $135 = 15*9 \equiv 2*9 = 18 \pmod{13}$. Koska $(9, 13) = 1$, voidaan seurauksen 2.1 mukaan jakaa kongruenssi puolittain luvulla 9 ja saadaan $15 \equiv 2 \pmod{13}$.

Esitellään seuraavaksi lauseen 2.8 hieman yleisempi muoto. Todistus on samankaltainen kuin lauseessa 2.8.

Lause 2.10. *[3, s. 131] Olkoot a, b, c ja d kokonaislukuja ja m positiivinen kokonaisluku siten, että $a \equiv b \pmod{m}$ ja $c \equiv d \pmod{m}$. Tällöin*

(i) $a + c \equiv b + d \pmod{m}$,

(ii) $a - c \equiv b - d \pmod{m}$,

(iii) $ac \equiv bd \pmod{m}$.

Todistus. Koska $a \equiv b \pmod{m}$ ja $c \equiv d \pmod{m}$, niin tällöin $m \mid (a - b)$ ja $m \mid (c - d)$. On siis olemassa kokonaisluvut k ja l siten, että $km = a - b$ ja $lm = c - d$.

(i) $(a + c) - (b + d) = (a - b) + (c - d) = km + lm = (k + l)m$, joten $m \mid [(a + c) - (b + d)]$. Tällöin $a + c \equiv b + d \pmod{m}$.

(ii) $(a - c) - (b - d) = (a - b) - (c - d) = km - lm = (k - l)m$, joten $m \mid [(a - c) - (b - d)]$. Tällöin $a - c \equiv b - d \pmod{m}$.

(iii) $ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d) = ckm + blm = m(ck + bl)$, joten $m \mid (ac - bd)$. Tällöin $ac \equiv bd \pmod{m}$.

□

Esimerkki 2.18. Koska $11 \equiv 3 \pmod{4}$ ja $6 \equiv 2 \pmod{4}$, niin lauseen 2.10 mukaan saadaan $17 = 11 + 6 \equiv 3 + 2 = 5 \pmod{4}$, $5 = 11 - 6 \equiv 3 - 2 = 1 \pmod{4}$ ja $66 = 11 * 6 \equiv 3 * 2 = 6 \pmod{4}$.

Lause 2.11. *[3, s. 133] Olkoot luvut a, b, k ja m kokonaislukuja siten, että $k > 0$, $m > 0$ ja $a \equiv b \pmod{m}$. Tällöin $a^k \equiv b^k \pmod{m}$.*

Todistus. Koska $a \equiv b \pmod{m}$, niin $m \mid (a - b)$. Kirjoitetaan nyt lauseke $(a^k - b^k)$ hieman eri muodossa:

$$(a^k - b^k) = (a - b)(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1}).$$

Nyt nähdään, että $(a - b) \mid (a^k - b^k)$. Koska $m \mid (a - b)$, niin lauseen 2.1 mukaan $m \mid (a^k - b^k)$, joten $a^k \equiv b^k \pmod{m}$. □

Esimerkki 2.19. Tarkastellaan kongruenssia $13 \equiv 6 \pmod{7}$. Nyt lauseen 2.11 perusteella $28561 = 13^4 \equiv 6^4 = 1296 \pmod{7}$.

Apulause 2.2. [3, s. 133] *Olkoot a, b ja c kokonaislukuja. Tällöin $[a,b] \mid c$ jos ja vain jos $a \mid c$ ja $b \mid c$. Missä $[a,b]$ on pienin yhteinen jaettava kokonaisluvuille a ja b.*

Todistus. Oletetaan ensin, että $[a,b] \mid c$. Koska $a \mid [a,b]$, niin $a \mid c$. Samalla tavalla $b \mid c$. Oletetaan nyt, että $a \mid c$ ja $b \mid c$. Merkitään $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$, $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$ ja $c = p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n}$. Koska $a \mid c$ ja $b \mid c$, niin $\max(a_i, b_i) \leq c_i$, kun $i = 1, 2, \ldots, n$. Joten $[a,b] \mid c$. □

Lause 2.12. *[3, s. 133] Jos $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$, missä a, b ovat kokonaislukuja ja $m_1, m2, \ldots, m_k$ ovat positiivisia kokonaislukuja, niin tällöin*

$$a \equiv b \pmod{[m_1, m_2, \ldots, m_k]},$$

missä $[m_1, m_2, \ldots, m_k]$ on pienin yhteinen jaettava luvuille $m_1, m_2, \ldots, m_k$.

Todistus. Koska $a \equiv b \pmod{m_1}, a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$ tiedetään, että $m_1 \mid (a-b)$, $m_2 \mid (a-b), \ldots, m_k \mid (a-b)$. Apulauseen 2.2 mukaan

$$[m_1, m_2, \ldots, m_k] \mid (a-b).$$

Joten

$$a \equiv b \pmod{[m_1, m_2, \ldots, m_k]}.$$

□

Esimerkki 2.20. Tarkastellaan kongruensseja $15 \equiv 3 \pmod 2$, $15 \equiv 3 \pmod 4$ ja $15 \equiv 3 \pmod 6$. Nyt lukujen 2, 4 ja 6 pienin yhteinen jaettava $[2,4,6] = 12$. Lauseen 2.12 perusteella $15 \equiv 3 \pmod{12}$.

2.5 Modulaarinen potenssiin korotus

Esitellään ensin merkintä, jota käytetään jakolaskun a/b jakojäännöksestä.

Määritelmä 2.9. Jakolaskun a/b jakojäännöstä kuvaava merkintä on tässä esityksessä $(a, \bmod b)$.

Esimerkki 2.21. Olkoon $a = 10$ ja $b = 4$. Nyt

$$(a, \bmod b) = (10, \bmod 4) = 2.$$

Eräs operaatio, jota tarvitaan RSA-salauksessa ja salauksen purkamisessa, on *modulaarinen potenssiin korotus*. Salauksessa ja salauksen purkamisessa joudutaan etsimään jakojäännöksiä luvuista, jotka korotetaan ennen jakojäännöksen laskemista erittäin korkeisiin kokonaislukupotensseihin. Modulaarisella potenssiin korotuksella pystytään välttämään potenssiin korottaminen niin, että käytössä ovat erittäin suuret eksponentit. Tutustutaan asiaan esimerkin avulla.

Esimerkki 2.22. Lasketaan nyt jakojäännös $(35^{34}, \text{mod } 23)$. Jos luku 35^{34} lasketaan raa'alla voimalla auki, saadaan 53 numeroa pitkä luku. Parempi tapa etsiä jakojäännös on ensin muodostaa eksponentin 34 binääriesitys, joka on $(34)_{10} = (100010)_2$. Sen jälkeen lasketaan jakojäännökset

$$35, 35^2, 35^4, 35^8, 35^{16}, 35^{32}$$

modulo 23 siten, että korotetaan aina edellinen jakojäännös potenssiin 2 ja lasketaan seuraava jakojäännös näin saadusta luvusta. Saadaan siis kongruenssit

$$35 \equiv 12 \pmod{23}$$

$$35^2 \equiv 6 \pmod{23}$$

$$35^4 \equiv 13 \pmod{23}$$

$$35^8 \equiv 8 \pmod{23}$$

$$35^{16} \equiv 10 \pmod{23}$$

$$35^{32} \equiv 2 \pmod{23}.$$

Voimme nyt laskea jakojäännöksen $(35^{34}, \text{mod } 23)$ kertomalla keskenään sopivat jakojäännökset. Siis

$$35^{34} = 35^{32+2} = 35^{32} * 35^2 \equiv 2 * 6 = 12 \pmod{23}.$$

Esimerkissä 2.22 on käyty läpi modulaarinen potenssiin korotus. Modulaarinen potenssiin korotus tarkoittaa siis jakojäännöksen $(b^N, \text{mod } m)$ laskemista, jossa b, m ja N ovat positiivisia kokonaislukuja. Muunnetaan ensin eksponentti N binäärimuotoon $N = (a_k a_{k-1} \dots a_1 a_0)_2$. Etsitään pienimmät positiiviset jakojäännökset luvuille $b, b^2, b^4, \dots, b^{2^k}$, kun jakajana on luku m.

Etsintä tapahtuu esimerkin mukaisesti toistuvasti neliöön korottamalla ja supistamalla modulo m. Lopuksi kerrotaan ne jakojäännökset j, joille $a_j = 1$. Tämän jälkeen lasketaan vielä saadusta luvusta jakojäännös modulo m. [3, s. 134].

2.6 Lineaarinen Diofantoksen yhtälö

Yhtälöä $ax + by = c$ kutsutaan *kahden muuttujan lineaariseksi Diofantoksen yhtälöksi.*

Lause 2.13. *[3, s. 120] Olkoot luvut a ja b kokonaislukuja ja $d = (a, b)$. Yhtälöllä $ax + by = c$ ei ole ratkaisuja, jos $d \nmid c$. Jos $d \mid c$, ratkaisuja on ääretön määrä. Lisäksi jos $x = x_0$ ja $y = y_0$ on yhtälön eräs ratkaisu, kaikki ratkaisut saadaan seuraavista yhtälöistä:*

$$x = x_0 + (b/d)n, \ y = y_0 - (a/d)n,$$

jossa luku n on kokonaisluku.

Todistus. Sivuutetaan. □

Esimerkki 2.23. Ratkaistaan yhtälö $20x+15y = 12$. Koska $(20, 15) = 5 \nmid 12$ yhtälö ei ole ratkeava.

Esimerkki 2.24. Ratkaistaan yhtälö $64x + 54y = 8$. Etsitään ensin lukujen 54 ja 64 suurin yhteinen tekijä Eukleideen algoritmilla.

$$64 = 54 * 1 + 10$$

$$54 = 10 * 5 + 4$$

$$10 = 4 * 2 + \mathbf{2}$$

$$4 = 2 * 2 + 0$$

Siis $(54, 64) = 2$ ja koska $2 \mid 8$ on yhtälö ratkeava. Etsitään yksittäinen ratkaisu Eukleideen algoritmilla

$$2 = 10 - 4 * 2 = 10 - (54 - 10 * 5) * 2 = 10 - 2 * 54 + 10 * 10$$

$$= 64 - 54 - 2 * 54 + 10(64 - 54) = 11 * 64 - 13 * 54$$

Kerrotaan puolittain luvulla 4 (eli luvulla $c/(a,b)$) ja saadaan

$$44 * 64 - 52 * 54 = 8.$$

Siis yksittäinen ratkaisu on $x_0 = 44$ ja $y_0 = -52$. Yhtälön kaikki ratkaisut ovat

$$x = x_0 + (b/d)n = 44 + 27n,\ y = y_0 - (a/d)n = -52 - 32n,$$

kun n on kokonaisluku.

2.7 Lineaarikongruenssi ja sen erikoistapaus käänteisluku modulo m

Kongruenssia, joka on muotoa $ax \equiv b \pmod{m}$ ja jossa luku x on tuntematon kokonaisluku, kutsutaan *yhden muuttujan lineaarikongruenssiksi.*

Lause 2.14. *[3, s. 139] Olkoot a, b ja m kokonaislukuja siten, että $m > 0$ ja $(a,b) = d$. Jos $d \nmid b$, ei kongruenssilla $ax \equiv b \pmod{m}$ ole ratkaisuja. Jos $d \mid b$, on kongruenssilla $ax \equiv b \pmod{m}$ täsmälleen d ei-kongruenttia ratkaisua modulo m.*

Todistus. Sivuutetaan. □

Esimerkki 2.25. Ratkaistaan kongruenssi $18x \equiv 5 \pmod{8}$. Nyt $d = (a,m) = (18,8) = 2$ ja $b = 5$. Kongruenssi ei ole ratkeava, sillä $2 \nmid 5$.

Esimerkki 2.26. Ratkaistaan kongruenssi $17x \equiv 12 \pmod{167}$. Muunnetaan kongruenssi Diofantoksen yhtälöksi $17x - 167y = 12$. Etsitään ensin lukujen 17 ja 167 suurin yhteinen tekijä Eukleideen algoritmin avulla ja käytetään sitten algoritmia määrittämään Diofantoksen yhtälön ratkaisut:

$$167 = 17 * 9 + 14$$

$$17 = 14 * 1 + 3$$

$$14 = 3 * 4 + 2$$

$$3 = 2 * 1 + \mathbf{1}$$

$$2 = 1 * 2.$$

Nyt

$$1 = 3 - 2 * 1 = 3 - (14 - 3 * 4) = 3 * 5 - 14$$

$$(17 - 14) * 5 - 14 = 17 * 5 - 14 * 6$$

$$17 * 5 - (167 - 17 * 9) * 6 = 17 * 59 - 167 * 6 = 1.$$

Kerrotaan saatu yhtälö nyt puolittain luvulla 12 ja saadaan

$$17 * 708 - 167 * 72 = 12.$$

Eräs ratkaisu Diofantoksen yhtälölle $17x - 167y = 12$ on $x_0 = 708$ ja $y_0 = 72$. Yleinen ratkaisu kongruenssille on

$$x \equiv 708 \equiv 40 \pmod{167}.$$

Tarkastellaan nyt kongruensseja, jotka ovat muodossa $ax \equiv 1 \pmod{m}$. Lauseen 2.14 mukaan tällaiselle kongruenssille on ratkaisu, jos ja vain jos $(a, m) = 1$, ja silloin kaikki ratkaisut ovat kongruentteja modulo m.

Määritelmä 2.10. [3, s. 140] Olkoon a kokonaisluku ja $(a, m) = 1$. Tällöin kongruenssin $ax \equiv 1 \pmod{m}$ ratkaisua kutsutaan luvan a käänteisluvuksi modulo m.

Esimerkki 2.27. Kongruenssiyhtälön $6x \equiv 1 \pmod{11}$ ratkaisu on $x \equiv 2 \pmod{11}$. Nyt voidaan sanoa, että luvun 6 käänteisluku modulo 11 on 2. Samalla tavoin luvun 2 käänteisluku modulo 11 on 6.

Määritelmä 2.11. Olkoot luvut a ja n kokonaislukuja. Tässä esityksessä merkintä $(a^{-1}, \bmod n)$ tarkoittaa luvun a käänteislukua modulo n.

Esimerkki 2.28. Olkoon nyt $a = 9$ ja $n = 13$. Nyt $(a^{-1}, \bmod n) = (9^{-1}, \bmod 13) = 3$, sillä $9 * 3 \equiv 1 \pmod{13}$.

Lause 2.15. *[3, s. 141] Olkoon luku p alkuluku. Positiivinen kokonaisluku a on itsensä käänteisluku modulo p, jos ja vain jos $a \equiv 1 \pmod{p}$ tai $a \equiv -1 \pmod{p}$.*

Todistus. Oletetaan ensin, että $a \equiv 1 \pmod{p}$ tai $a \equiv -1 \pmod{p}$, tällöin lauseen 2.11 mukaan $a^2 \equiv 1 \pmod{p}$. Joten luku a on oma käänteislukunsa modulo p.

Oletetaan nyt, että a on itsensä käänteisluku modulo p. Tällöin $a^2 = a * a \equiv 1 \pmod{p}$. Nyt $p \mid (a^2 - 1) = (a + 1)(a - 1)$, joten $p \mid (a + 1)$ tai $p \mid (a - 1)$. Eli $a \equiv 1 \pmod{p}$ tai $a \equiv -1 \pmod{p}$. □

2.8 Eulerin phi-funktio ja Eulerin lause

Eulerin phi-funktio $\phi(n)$ on keskeisessä asemassa RSA-salauksessa.

Määritelmä 2.12. [3, s. 215] Olkoon n positiivinen kokonaisluku. Tällöin $\phi(n)$ on niiden kokonaislukujen määrä, jotka ovat pienempiä tai yhtä suuria kuin luku n ja suhteellisia alkulukuja luvun n kanssa. Funktiota $\phi(n)$ kutsutaan *Eulerin phi-funktioksi*.

Esimerkki 2.29. $\phi(1) = 1$, koska $(1, 1) = 1$. $\phi(6) = 2$, sillä vain $(1, 6) = 1$ ja $(5, 6) = 1$. $\phi(5) = 4$, koska $(1, 5) = (2, 5) = (3, 5) = (4, 5) = 1$.

Määritelmä 2.13. [3, s. 215] *Supistettu jäännössysteemi modulo n* on funktion $\phi(n)$ suuruinen joukko kokonaislukuja siten, että jokainen joukon alkio on suhteellinen alkuluku luvulle n ja mitkään joukon kaksi alkiota eivät ole kongruentteja modulo n.

Esimerkki 2.30. Joukko $A = \{1, 2, 4, 5, 7, 8\}$ on supistettu jäännössysteemi modulo 9, sillä $\phi(9) = 6$ ja kaikki joukon A alkiot ovat suhteellisia alkulukuja luvun 9 kanssa. Toisaalta mitkään kaksi joukon A alkiota eivät ole kongruentteja keskenään modulo 9.

Seuraavaa lausetta supistetun jäännössysteemin ominaisuuksista tarvitaan myöhemmin *Eulerin lauseen* todistuksessa.

Lause 2.16. *[3, s. 216] Olkoon joukko $\{r_1, r_2, \ldots, r_{\phi(n)}\}$ supistettu jäännössysteemi modulo n. Olkoon nyt a positiivinen kokonaisluku ja $(a, n) = 1$. Tällöin joukko $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ on myös supistettu jäännössysteemi modulo n.*

Todistus. Sivuutetaan. □

Esimerkki 2.31. Joukko $A = \{1, 2, 4, 5, 7, 8\}$ on supistettu jäännössysteemi modulo 9, sillä $\phi(9) = 6$. Lauseen 2.16 mukaan myös esimerkiksi joukko $B = \{5*1, 5*2, 5*4, 5*5, 5*7, 5*8\}$ on supistettu jäännössysteemi modulo 9, sillä $(5, 9) = 1$.

Määritelmä 2.14. [3, s. 222] Aritmeettista funktiota f kutsutaan *multiplikatiiviseksi funktioksi*, jos $f(mn) = f(m)f(n)$, missä m ja n ovat positiivisia kokonaislukuja ja samalla suhteellisia alkulukuja. Funktiota kutsutaan

totaalisesti multiplikatiiviseksi, jos $f(mn) = f(m)f(n)$ kaikilla positiivisilla kokonaisluvuilla m ja n.

Lause 2.17. *[3, s. 224] Olkoot m ja n positiivisia kokonaislukuja ja suhteellisia alkulukuja. Tällöin $\phi(mn) = \phi(m)\phi(n)$.*

Todistus. Sivuutetaan. □

Esimerkki 2.32. $\phi(30) = \phi(5)\phi(6) = 4 * 2 = 8$.

Seuraavaksi esitetään ja todistetaan alkulukutesti, jossa Eulerin phi-funktiota käytetään apuna.

Lause 2.18. *[3, s. 223] Olkoon luku p alkuluku. Tällöin $\phi(p) = p - 1$. Käänteisesti jos p on positiivinen kokonaisluku ja $\phi(p) = p - 1$, niin luku p on alkuluku.*

Todistus. Olkoon luku p alkuluku. Nyt jokainen positiivinen kokonaisluku, joka on pienempi kuin luku p, on suhteellinen alkuluku luvun p kanssa. Koska tällaisia lukuja on $p - 1$ kappaletta, saadaan $\phi(p) = p - 1$.

Olkoon nyt $\phi(p) = p - 1$. Tehdään vastaoletus, jonka mukaan luku p on yhdistetty luku. Näin ollen luvulla p on tekijä d, joka on kokonaisluku väliltä $1 < d < p$. Tällöin p ja d eivät ole suhteellisia alkulukuja. Nyt tiedetään, että ainakin yksi (luku d) luvuista $1, 2, \ldots, p - 1$ ei ole suhteellinen alkuluku luvun p kanssa, joten $\phi(p) \leq p - 2$. Tämä on ristiriita oletuksen kanssa, joten luvun p täytyy olla alkuluku. □

Esimerkki 2.33. Luvut 5, 7 ja 11 ovat alkulukuja, joten $\phi(5) = 4$, $\phi(7) = 6$ ja $\phi(11) = 10$.

Lause 2.19. *Olkoot p ja q alkulukuja. Tällöin $\phi(pq) = (p - 1)(q - 1)$.*

Todistus. Lauseen 2.17 mukaan $\phi(pq) = \phi(p)\phi(q)$. Koska luvut p ja q ovat alkulukuja, niin lauseen 2.18 mukaan $\phi(p) = p - 1$ ja $\phi(q) = q - 1$. Siis $\phi(pq) = (p - 1)(q - 1)$. □

Lause 2.20. *[3, s. 223] Olkoon p alkuluku. Tällöin $\phi(p^a) = p^a - p^{a-1}$.*

Todistus. Tarkastellaan niitä positiivisia kokonaislukuja, jotka ovat pienempiä kuin luku p^a eivätkä ole suhteellisia alkulukuja luvun p kanssa. Siis kokonaislukuja, jotka ovat pienempiä kuin luku p^a ja jaollisia luvulla p. Merkitään näitä lukuja kahden kokonaisluvun tulona kp, missä $1 \leq k \leq p^{a-1}$. Koska tällaisia lukuja on täsmälleen p^{a-1} kappaletta, on olemassa $p^a - p^{a-1}$ kokonaislukua, jotka ovat pienempiä kuin p^a ja suhteellisia alkulukuja luvulle p^a. Joten $\phi(p^a) = p^a - p^{a-1}$. □

Esimerkki 2.34. Käyttäen lausetta 2.20 saadaan $\phi(2^9) = 2^9 - 2^8 = 256$ ja $\phi(13^2) = 13^2 - 13 = 156$.

Lause 2.21. *[3, s. 217]* ***Eulerin lause.*** *Olkoon m positiivinen kokonaisluku ja a kokonaisluku niin, että $(a, m) = 1$. Tällöin $a^{\phi(m)} \equiv 1 \pmod{m}$.*

Ennen Eulerin lauseen todistusta tarkastellaan todistuksen ideaa seuraavan esimerkin avulla.

Esimerkki 2.35. Tiedetään, että joukot $A = \{1, 2, 4, 5, 7, 8\}$ ja $B = \{5 * 1, 5 * 2, 5 * 4, 5 * 5, 5 * 7, 5 * 8\}$ ovat supistettuja jäännössysteemeitä modulo 9. Näin niillä molemmilla on samat pienimmät positiiviset jakojäännökset modulo 9. Nyt siis kaikki joukon A alkiot ovat kongruentteja jonkin joukon B alkion kanssa modulo 9. Esimerkiksi $1 \equiv 5*2 \pmod{9}$ ja $7 \equiv 5*5 \pmod{9}$. Lauseen 2.10 perusteella saadaan kongruenssi

$$(5*1)*(5*2)*(5*4)*(5*5)*(5*7)*(5*8) \equiv 1*2*4*5*7*8 \pmod{9}$$

ja

$$5^6 * 1 * 2 * 4 * 5 * 7 * 8 \equiv 1 * 2 * 4 * 5 * 7 * 8 \pmod{9}.$$

Koska $(1*2*4*5*7*8, 9) = 1$, voidaan seurauksen 2.1 mukaan kongruenssi jakaa puolittain luvulla $1 * 2 * 4 * 5 * 7 * 8$ ja saadaan

$$5^6 = 5^{\phi(9)} \equiv 1 \pmod{9}.$$

Käytetään nyt yllä olevan esimerkin ideoita apuna Eulerin lauseen todistamisessa.

Todistus. Olkoon nyt joukko $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ supistettu jäännössysteemi modulo m, joka sisältää positiivisia kokonaislukuja, jotka ovat pienempiä

kuin luku m ja suhteellisia alkulukuja luvun m kanssa. Lauseen 2.16 mukaan joukko $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ on myös supistettu jäännössysteemi modulo m, kun $(a, m) = 1$. Siten positiivisten kokonaislukujen joukon $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ kaikki alkiot ovat kongruentteja jonkin joukon $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ alkion kanssa modulo m. Nyt lauseen 2.10 perusteella saadaan kongruenssi

$$ar_1 ar_2 \cdots ar_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m}.$$

Näin ollen

$$a^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m}.$$

Koska $(r_1 r_2 \cdots r_{\phi(m)}, m) = 1$, niin seurauksen 2.1 mukaan voidaan yllä oleva kongruenssi jakaa puolittain tulolla $r_1 r_2 \cdots r_{\phi(m)}$ ja saadaan $a^{\phi(m)} \equiv 1 \pmod{m}$. □

Seuraavassa esimerkissä hyödynnetään Eulerin lausetta ja modulaarista potenssiin korotusta suuren eksponentin supistamisessa.

Esimerkki 2.36. Lasketaan $(11^{89}, \text{ mod } 67)$. Eulerin lauseen mukaan $11^{66} \equiv 1 \pmod{67}$. Merkitään nyt

$$(*) \qquad 11^{89} \equiv x \pmod{67}.$$

Nyt $(*)$ voidaan kirjoittaa muodossa

$$(**) \qquad 11^{23} * 11^{66} \equiv 1 * x \pmod{67}.$$

Kohdasta $(**)$ saadaan lauseen 2.10 mukaan

$$(***) \qquad 11^{23} \equiv x \pmod{67}.$$

Joten kohtien $(*)$, $(**)$ ja $(***)$ perusteella nähdään selvästi, että

$$(11^{89}, \text{mod } 67) = (11^{23}, \text{mod } 67).$$

Lasketaan nyt jakojäännös $(11^{23}, \text{mod } 67)$ modulaarisen potenssiin korotuksen avulla. Eksponentin 23 binääriesitys on 10111. Etsitään nyt pienimmät positiiviset jakojäännökset luvuille

$$11, 11^2, 11^4, 11^8, 11^{16}$$

modulo 67 siten, että korotetaan aina edellinen jakojäännös potenssiin 2 ja lasketaan seuraava jakojäännös näin saadusta luvusta. Saadaan siis kongruenssit

$$11 \equiv 11 \pmod{67}$$

$$11^2 \equiv 54 \pmod{67}$$

$$11^4 \equiv 35 \pmod{67}$$

$$11^8 \equiv 19 \pmod{67}$$

$$11^{16} \equiv 26 \pmod{67}.$$

Koska luvun 23 binääriesitys on 10111, saamme halutun tuloksen laskemalla

$$(11^{23}, \text{mod } 67) = (26 * 35 * 54 * 11), \text{mod } 67) = (540540, \text{mod } 67) = 51.$$

2.9 Wilsonin lause

Wilsonin lausetta pystytään hyödyntämään alkulukutesteissä.

Lause 2.22. *[3, s. 198]* ***Wilsonin lause.*** *Olkoon p alkuluku. Tällöin* $(p-1)! \equiv -1 \pmod{p}$.

Ennen Wilsonin lauseen todistusta käytetään esimerkkiä havainnollistamaan todistuksen ideaa.

Esimerkki 2.37. Olkoon luku $p = 13$. Saadaan $(13-1)! = 12! = 1*2*3*4*5*6*7*8*9*10*11*12$. Järjestetään tulon kertoimet uudelleen pareittain niin, että ne muodostavat käänteislukupareja modulo 13. Saadaan siis parit $2*7 \equiv 1 \pmod{13}$, $3*9 \equiv 1 \pmod{13}$, $4*10 \equiv 1 \pmod{13}$, $5*8 \equiv 1 \pmod{13}$, $6*11 \equiv 1 \pmod{13}$. Täten $12! \equiv 1*(2*7)*(3*9)*(4*10)*(5*8)*(6*11)*12 \equiv 1*12 \equiv -1 \pmod{13}$. Nyt on osoitettu todeksi erikoistapaus Wilsonin lauseesta.

Todistus. Kun $p = 2$, saadaan $(p-1)! \equiv 1 \equiv -1 \pmod{2}$. Wilsonin lause on siis tosi, kun $p = 2$. Oletetaan nyt, että luku p on alkuluku ja suurempi kuin 2. Lauseen 2.14 mukaan jokaisella kokonaisluvulla a, välillä $1 \leq a \leq p-1$, on käänteisluku $\bar{a}$ modulo p samalla välillä. Siis $a\bar{a} \equiv 1 \pmod{p}$. Lauseen 2.15 mukaan ainoat positiiviset kokonaisluvut, jotka ovat oma käänteislukunsa

modulo p ja pienempiä kuin p, ovat luvut 1 ja $p-1$. Voidaan siis ryhmitellä välin $[2, p-2]$ kokonaisluvut $(p-3)/2$ pariin siten, että jokaisen parin tulo on kongruentti luvun 1 kanssa modulo p. Nyt saadaan

$$2 * 3 \cdots (p-3) * (p-2) \equiv 1 \pmod{p}.$$

Kerrotaan molemmat puolet ensin luvulla 1 ja sitten luvulla $p-1$ ja saadaan

$$(p-1)! = 1 * 2 * 3 \cdot (p-3) * (p-2) * (p-1) \equiv 1 * (p-1) \equiv -1 \pmod{p}.$$

□

2.10 Fermat'n pieni lause

Lause 2.23. *[3, s. 199]* ***Fermat'n pieni lause.*** *Olkoon p alkuluku ja a positiivinen kokonaisluku niin, että $p \nmid a$. Tällöin $a^{p-1} \equiv 1 \pmod{p}$.*

Todistus. Koska $p \nmid a$, niin $(a, p) = 1$. Tällöin lauseen 2.21 (Eulerin lause) mukaan $a^{\phi(p)} \equiv 1 \pmod{p}$. Luku p on alkuluku, joten $\phi(p) = p - 1$ eli $a^{p-1} \equiv 1 \pmod{p}$. □

Esimerkki 2.38. Valitaan $a = 5$ ja $p = 3$. Nyt $3 \nmid 5$, joten $5^2 \equiv 1 \pmod{3}$.

Lause 2.24. *[3, s. 200] Olkoon p alkuluku ja a positiivinen kokonaisluku. Tällöin $a^p \equiv a \pmod{p}$.*

Todistus. Oletetaan ensin, että $p \nmid a$. Tällöin Fermat'n pienen lauseen mukaan $a^{p-1} \equiv 1 \pmod{p}$. Kertomalla kongruenssi puolittain luvulla a saadaan $a^p \equiv a \pmod{p}$. Oletetaan nyt, että $p \mid a$. Siis $p \mid a^p$ myös, joten $a^p \equiv a \equiv 0 \pmod{p}$. Todistus on valmis, sillä $a^p \equiv a \pmod{p}$, aina kun $a \nmid p$ tai $a \mid p$. □

Esimerkki 2.39. Valitaan $a = 4$ ja $p = 5$. Nyt $4^5 = 1024 \equiv 4 \pmod{5}$.

Lukuteoriassa on usein tarve etsiä jakojäännös kokonaisluvulle, jolla on hyvin suuri eksponentti. Erityisesti kryptologiassa tämä tarve korostuu. Seuraavassa esimerkissä käytetään Fermat'n pientä lausetta jakojäännöksen etsimiseen.

Esimerkki 2.40. Lasketaan $(7^{121}, \mathrm{mod}\ 13)$. Fermat'n pienen lauseen mukaan $7^{12} \equiv 1 \pmod{13}$. Korotetaan kongruenssi ensin puolittain potenssiin 10 ja saadaan $7^{120} \equiv 1 \pmod{13}$. Kerrotaan vielä kongruenssi puolittain luvulla 7. Nyt $7^{121} \equiv 7 \pmod{13}$. Siis $(7^{121}, \mathrm{mod}\ 13) = 7$.

3 RSA

3.1 Yleistä RSA-salauksesta

Maailman käytetyimmän ja testatuimman julkisen avaimen kryptosysteemin ovat kehittäneet MIT-yliopistossa työskennelleet Ron Rivest, Adi Shamir ja Leonard Adleman. Nykyisin sitä kutsutaan RSA-systeemiksi. RSA on julkaistu vuonna 1978. Nimi tulee kehittäjien sukunimien alkukirjaimista. RSA perustuu äärimmäisen yksinkertaiseen lukuteoreettiseen ideaan ja on toistaiseksi pitänyt pintansa kryptoanalyyttisiä hyökkäyksiä vastaan.

Brittiläinen matemaatikko Clifford Cocks kuvasi vastaavanlaisen systeemin jo vuonna 1973 työskennellessään Britannian tiedustelupalvelussa. Tällöin tietokoneiden laskentateho ei kuitenkaan vielä ollut riittävä systeemin käyttöön, joten sitä ei ilmeisesti käytännössä hyödynnetty. Cocksin löydöt tulivat kuitenkin julkisuuteen vasta vuonna 1998 tiukkojen salassapitomääräysten johdosta. Rivest, Shamir ja Adleman kehittivätkin RSA-systeemin itsenäisesti tietämättä Cocksin aikaansaannoksista.

RSA-salaus perustuu kahden erittäin suuren alkuluvun kertomiseen keskenään. On varsin helppoa kertoa kaksi alkulukua keskenään, mutta on erittäin hankalaa jakaa tekijöihin kahden suuren alkuluvun tulo. Tämän vuoksi kahden suuren alkuluvun tuloa voidaankin käyttää julkisena avaimena. Toisaalta alkulukuja voidaan käyttää salauksen purkamisessa. Näin saadaan erittäin hyvät puitteet julkisen avaimen kryptosysteemille.

RSA-salauksesta puhuttaessa täytyy muistaa, ettei ole olemassa todistusta siitä, että

- kahden suuren alkuluvun tulon tekijöihin jakaminen olisi vaikeaa ja hidasta
- RSA-salauksen käyttämä tulo pitää jakaa tekijöihin salauksen murtamiseksi.

On kuitenkin olemassa runsaasti empiirisiä todisteita sen puolesta, että molemmat mainitut väitteet pitävät paikkansa [1, s. 125] [2].

3.2 RSA-salaus laillisen käyttäjän näkökulmasta

Käydään nyt RSA-salaus yksityiskohtaisesti läpi. RSA-salauksessa keskeisessä asemassa on Eulerin phi-funktio (määritelmä 2.12) ja sen ominaisuudet.

Olkoot p ja q erisuuria satunnaisia isoja alkulukuja. (Tyypillisesti aidossa salaustilanteessa molempien lukujen desimaaliesitys on noin 100 numeroa pitkä.) Merkitään

$$n = pq.$$

Tällöin lauseen 2.19 mukaan $\phi(n) = (p-1)(q-1)$. Valitaan suuri satunnainen luku d siten, että $(d, \phi(n)) = 1$. Suurin yhteinen tekijä voidaan määrittää käyttämällä Eukleideen algoritmia. Eukleideen algoritmin yhtälöketjuista saadaan myös luku $e, 1 < e < \phi(n)$, joka toteuttaa kongruenssin

$$ed \equiv 1 \pmod{\phi(n)}.$$

Lukuja n, e ja d kutsutaan *kertoimeksi, salaus-* ja *salauksen purku eksponenteiksi*. Luvut n ja e muodostavat *julkisen salausavaimen*, kun taas loput luvut p, q, $\phi(n)$ ja d muodostavat *salaisen takaoven*. Salauksen purkuun tarvittava takaovi-informaatio ei välttämättä vaadi tietoa kaikista neljästä luvusta [1, s. 125-126].

Oletetaan, että kryptoanalyytikolla on tieto luvusta p. Koska luku n on julkista tietoa, saadaan $q = n/p$. Nyt selvillä ovat luvut p ja q, joten $\phi(n) = (p-1)(q-1)$. Luku e on julkista tietoa ja $ed \equiv 1 \pmod{\phi(n)}$, joten luku d saadaan laskemalla luvun e käänteisluku modulo $\phi(n)$.

Määritellään nyt niin sanottu *selväteksti*. Selvätekstillä tarkoitetaan tässä esityksessä normaalista tekstistä kymmenjärjestelmään koodattua desimaalilukua. (Luonnollisesti voitaisiin käyttää myös binääriesitystä.) Luku jaetaan sopivan kokoisiin blokkeihin, jotka salataan erikseen. Sopiva koko blokeille on yksikäsitteinen kokonaisluku i, joka toteuttaa epäyhtälön $10^{i-1} < n < 10^i$. Joskus voidaan valita $i-1$ blokin kooksi tai varmistaa, että jokainen blokki on pienempi kuin n. Näin salauksen purkaminen on varmasti yksikäsitteistä. Muutoin näin ei aina välttämättä ole.

Salaus tapahtuu korottamalla selväteksti potenssiin e ja laskemalla saadusta luvusta jakojäännös luvun n suhteen. Toisin sanoen kryptotekstiksi tulee potenssiin e korotetun selvätekstin ja luvun n jakojäännös [1, s. 126].

Jos w on selvätekstiblokki ja c on vastaava kryptotekstiblokki, voidaan salaus esittää seuraavalla yhtälöllä

$$c = (w^e, \text{mod } n)$$

[1, s. 126]. Nyt siis voidaan merkitä myös $c \equiv w^e \pmod{n}$.

Todistetaan seuraavaksi, että salauksen purku toimii. Todistuksessa käytetään apuna Eulerin lausetta (Lause 2.21).

Apulause 3.1. *[1, s. 126] Oletetaan, että w ja c on määritelty kuten yllä. Tällöin*

$$(*) \qquad w \equiv c^d \pmod{n}.$$

Näin ollen jos salauksen purku on yksikäsitteinen, niin $w = (c^d, \text{mod } n)$.

Todistus. On olemassa kokonaisluku j siten, että $ed = j\phi(n) + 1$. Oletetaan ensin, että kumpikaan luvuista p tai q ei ole luvun w tekijä. Tällöin myöskään luku n ei ole luvun w tekijä, koska $n = pq$. Nyt siis $(w, n) = 1$, joten Eulerin lauseen mukaan saadaan $w^{\phi(n)} \equiv 1 \pmod{n}$. Koska $\phi(n)|(ed-1)$, saadaan kongruenssin laskusääntöjen mukaan $w^{ed-1} \equiv 1 \pmod{n}$. Kerrotaan kongruenssi puolittain luvulla w ja saadaan $w^{ed} \equiv w \pmod{n}$. Nyt nähdään

$$c^d \equiv (w^e)^d \equiv w \pmod{n}.$$

Oletetaan, että luvuista p ja q vain luku p on luvun w tekijä. Tällöin $w^{q-1} \equiv 1 \pmod{q}$. Tämä seuraa Eulerin lauseesta, sillä $\phi(q) = q - 1$. Edelleen

$$w^{\phi(n)} \equiv 1 \pmod{q},\ w^{j\phi(n)} \equiv 1 \pmod{q},\ w^{ed} \equiv w \pmod{q}.$$

Koska luku p oli luvun w tekijä, on viimeinen kongruenssi voimassa myös modulo p. Nyt siis on $w^{ed} \equiv w \pmod{q}$ ja $w^{ed} \equiv w \pmod{p}$. Lauseen 2.12 perusteella saadaan $w^{ed} \equiv w \pmod{n}$.

Vastaavasti saadaan tapaus, jossa vain luku q on luvun w tekijä. Näin ollen $(*)$ pitää paikkansa molemmissa tapauksissa.

Jos molemmat luvut p ja q ovat luvun w tekijöitä, niin tällöin $n|w$, sillä $n = pq$. Edelleen $n|w^{ed}$, joten $n|(w^{ed} - w)$. Nyt saadaan selvästi $w^{ed} \equiv w \pmod{n}$. □

3.3 Kryptosysteemin suunnittelu

Tutustutaan nyt itse kryptosysteemin suunnitteluun. Kuinka salauksessa tarvittavat luvut generoidaan? Satunnaisluvun valinnassa tai valittaessa jotain satunnaisesti käytetään satunnaislukugeneraattoria. Käytännössä siis tietokoneohjelmaa, joka generoi joukon niin satunnaisia lukuja kuin mahdollista. [1, s. 127] Tässä esityksessä emme puutu satunnaislukujen generointiin yksityiskohtaisesti.

Valittaessa kaksi suurta satunnaista alkulukua p ja q valitaan ensin satunnaisesti pariton kokonaisluku r, joka on samaa suuruusluokkaa (RSA-salauksessa suuruusluokka on noin 100 numeroa) kuin satunnaisen alkuluvun halutaan olevan, ja testataan, onko se alkuluku. Jos satunnaisesti valittu luku ei ole alkuluku, valitaan seuraavaksi testattavaksi luku $r + 2$ ja jatketaan näin, kunnes alkuluku löytyy [1, s. 127].

Alkulukuteoreeman mukaan lukua x pienempien alkulukujen summittainen määrä saadaan kaavasta

$$\frac{x}{ln\ x}.$$

Tämän pohjalta voidaan laskea summittaisesti sadan numeron pituisten alkulukujen määrä

$$\frac{10^{100}}{ln\ 10^{100}} - \frac{10^{99}}{ln\ 10^{99}}.$$

Kun tätä lukua verrataan sadan numeron pituisten parittomien kokonaislukujen määrään $(10^{100} - 10^{99})/2$, saadaan todennäköisyys yhden alkulukutestin onnistumiselle, joka on noin $0,00868$ [1, s. 127].

Alkulukujen p ja q valinnan jälkeen luku d etsitään Eukleideen algoritmin avulla. Kun d täyttää ehdon $(d, \phi(n)) = 1$, saadaan luku e Eukleideen algoritmin yhtälöketjuista [1, s. 127]. Seuraava esimerkki valottaa Eukleideen algoritmin käyttöä ja ja lukujen d ja e valintaa.

Esimerkki 3.1. Olkoon nyt $\phi(n) = 99$ ja $d = 46$. Testataan ensin Eukleideen algoritmilla, ovatko $\phi(n)$ ja d suhteellisia alkulukuja.

$$99 = 46 * 2 + 7$$

$$46 = 7 * 6 + 4$$

$$7 = 4 * 1 + 3$$

$$4 = 3 * 1 + \mathbf{1}$$

$$3 = 1 * 3.$$

Nyt siis Eukleideen algoritmin avulla näytettiin, että $(99, 46) = 1$. Etsitään luku e soveltamalla Eukleideen algoritmia takaperin.

$$1 = 4 - 3 * 1 = 4 - (7 - 4) = 4 * 2 - 7$$

$$= 2 * (46 - 7 * 6) - 7 = 46 * 2 - 7 * 13$$

$$= 46 * 2 - (99 - 46 * 2) * 13 = 46 * \mathbf{28} - 99 * 13.$$

Luku $e = 28$ on esitetty yllä tummennettuna. Nyt siis on $ed \equiv 1 \pmod{\phi(n)}$ eli tässä tapauksessa $28 * 46 \equiv 1 \pmod{99}$.

3.4 RSA-salaus käytännössä

Tarkastellaan seuraavassa esimerkissä RSA-salausta käytännössä. Käytetyt luvut ovat esimerkin luettavuuden vuoksi hyvin pieniä eivätkä sovellu käytännön salaukseen.

Esimerkki 3.2. Valitaan $p = 7$, $q = 13$, $n = pq = 91$, $\phi(n) = (p-1)(q-1) = 72$, $d = 29$ ja $e = 5$. Luvulle d on voimassa $syt(d, \phi(n)) = 1$ ja luvulle e pätee $ed \equiv 1 \pmod{\phi(n)}$.

Nyt selvätekstit ovat kokonaislukuja suljetulta väliltä $[1, 90]$. Lisäksi pitää poistaa sellaiset luvut, joiden suurin yhteinen tekijä luvun 91 kanssa on suurempi kuin 1. Sellaisia ovat luvut, jotka ovat jaollisia luvuilla 7 tai 13. Siis esimerkiksi luvut $7, 14, 21, \ldots$ tai $13, 26, 39, \ldots$ Jos $(w, n) > 1$ jollekin selvätekstille w, voidaan n jakaa tekijöihin laskemalla suurin yhteinen tekijä luvulle n ja luvun w kryptatulle versiolle. Luonnollisesti tässä esimerkissä n on niin pieni, että se voidaan jakaa tekijöihin joka tapauksessa. Yleisesti todennäköisyys sille, että selvätekstissä on luvun n tekijä, on vähemmän kuin $1/p + 1/q$. Joten todennäköisyys on merkityksetön lukujen p ja q ollessa hyvin suuria.

Taulukossa 1 on esitetty suomenkieliselle aakkostolle täydellinen salaustaulukko käyttäen äsken määriteltyjä lukuja salauksessa. Taulukon perusteella esimerkiksi sana *PEKKA* kryptautuu lukusarjaksi 80 31 38 38 1. Esimerkistä nähdään selvästi, että julkisen avaimen kryptosysteemi ei toimi pienillä selvätekstin paloilla. Salauksen murtaja voi tehdä täydellisen dekryptaustaulukon yksinkertaisesti vain salaamalla kaikki mahdolliset selvätekstit ja järjestämällä tulos sopivaan aakkosjärjestykseen.

Taulukko 1:

Selväteksti	Lukukoodaus	Kryptoteksti
A	1	1
B	2	32
C	3	61
D	4	23
E	5	31
F	6	41
G	8	11
H	9	81
I	10	82
J	11	72
K	12	38
L	15	71
M	16	74
N	17	75
O	18	44
P	19	80
Q	20	76
R	22	29
S	23	4
T	24	33
U	25	64
V	27	27
W	29	22
X	30	88
Y	31	5
Z	32	2
Å	33	24
Ä	34	34
Ö	36	43

Esimerkki 3.3. Tarkastellaan tässä esimerkissä RSA-salausta käyttäen hieman suurempia lukuja lähtöarvoina. Valitaan $p = 53$ ja $q = 61$. Nyt saadaan $n = pq = 3233$ ja $\phi(n) = (p-1)(q-1) = 3120$. Valitaan $d = 253$. Nyt $(d, \phi(n)) = 1$ ja Eukleideen algoritmin yhtälöketjun avulla saadaan $e = 37$. Nyt siis $ed \equiv 1 \pmod{\phi(n)}$ eli $9361 \equiv 1 \pmod{3120}$.

Koodataan selväteksti neljän numeron mittaisiin blokkeihin, käyttäen suomalaista 29 kirjaimen aakkostoa siten, että A-kirjan koodautuu luvuksi 01, B-luvuksi 02 ja niin edelleen. Tällöin Ä-kirjain koodautuu siis luvuksi 28 ja Ö-kirjain luvuksi 29. Nyt siis suurin mahdollinen nelinumeroinen blokki on 2929.

Kryptataan teksti *TEEN GRADUA* käyttäen esimerkissä laskettuja arvoja kryptaukseen. Koodataan teksti ensin luvuiksi siten, että välilyönti saa arvon 00.

Taulukko 2:

Selvätekstiblokki	TE	EN	-G	RA	DU	A-
Koodaus	2005	0514	0007	1801	0421	0100

Modulaariset potenssiin korotukset, jotka tarvitaan kryptausta varten, on tehty neliöimällä. Nämä on esitetty taulukossa 3.

Taulukko 3:

Selväteksti w	2005	0514	0007	1801	0421	0100
w^2	1416	2323	49	902	2659	301
w^4	1473	452	2401	2121	2943	77
w^8	386	625	362	1538	42	2696
w^{16}	278	2665	1724	2121	1764	632
w^{32}	2925	2557	1049	1538	1550	1765
w^{36}	2169	1583	142	1	3120	119
Kryptoteksti w^{37}	460	2179	994	1801	922	2201

Kryptaustulokset voidaan tarkistaa dekryptaamalla eli korottamalla kryptoteksti c potenssiin d ja laskemalla jakojäännös modulo n. Dekryptataan $c = 2179$ käyttäen modulaarista potenssiin korotusta.

$$c^2 = 1997,\ c^4 = 1720,\ c^8 = 205,\ c^{16} = 3229,$$

$$c^{32} = 16,\ c^{64} = 256,\ c^{128} = 876,\ c^{192} = 1179,$$

$$c^{224} = 2699,\ c^{240} = 2136,\ c^{248} = 1425,$$

$$c^{252} = 386,\ c^{253} = 514.$$

Nyt siis tulokseksi saatiin $0514 = (2179^{253}, \text{mod } 3233)$, joka tarkoittaa siis selvätekstiblokkia "EN".

Seuraavat kaksi asiaa aiheuttavat usein hämmennystä [1, s. 131 ja 133]:

(i) Luvun n tekijöihin jaettavuus voidaan selvittää suhteellisen helposti, mutta luvun n tekijöitten löytäminen voi olla äärimmäisen vaikeaa. Useiden eri menetelmien avulla voidaan selvittää, onko luku n alkuluku. Jollei n ole alkuluku, se voidaan jakaa tekijöihin, mutta tekijöihin jako on kuitenkin käytännössä mahdotonta, jos luku n on muodostettu kertomalla kaksi hyvin suurta alkulukua keskenään.

(ii) Reaaliluvuilla potenssiin korotus ja logaritmien laskeminen on yhtä kompleksista. Sen sijaan modulaarinen potenssiin korotus on hyvin helppoa, mutta logaritmit muodostavat tässä suhteessa hankalan ongelman.

3.5 RSA-allekirjoitus silloin, kun viestin salaus ei ole tarpeellista

RSA-salausta voidaan käyttää myös autentikointiin ja digitaaliseen allekirjoitukseen. Seuraavassa esityksessä alaindeksit kuvaavat kulloistakin salauksen käyttäjää. Joten merkinnät e_A, d_A ja n_A tarkoittavat kryptaus- ja dekryptauseksponentteja sekä modulia, jotka ovat viestin lähettäjän A käytössä.

Oletetaan ensin, että viestin salaus on tarpeetonta, mutta se pitää allekirjoittaa turvallisesti. Tällöin käyttäjä A lähettää parin $(w, D_A(w))$ vastaanottajalle, jossa

$$D_A(w) = (w^{d_A}, \text{mod } n_A).$$

Vastaanottaja voi varmentaa allekirjoituksen aitouden käyttämällä lähettäjän A julkista kryptauseksponenttia e_A. Koska lähettäjä A on ainoa henkilö, joka tietää dekryptauseksponentin d_A, kukaan muu ei ole voinut allekirjoittaa viestiä w.

Käytetään esimerkin 3.3 lukuja allekirjoitettaessa viesti $w = 19$. Nyt siis $d_A = 253$, $e_A = 37$ ja $n_A = 3233$. Lasketaan $D_A(w) = (19^{253} \bmod 3233) = 903$, ja viestin vastaanottaja saa siis parin $(19, 903)$. Vastaanottaja voi todeta allekirjoituksen aitouden käyttämällä lähettäjän julkista kryptauseksponenttia $e_A = 37$. Nyt $(903^{37} \bmod 3233) = 19$, eli alkuperäinen viesti ja allekirjoitus voidaan todeta aidoksi [1, s. 133].

Huijari voi kuitenkin valita luvun c ja laskea

$$E_A(c) = (c^{e_A}, \bmod n_A).$$

Tämän jälkeen huijari voi onnistuneesti väittää, että luku c on lähettäjän A allekirjoitus viestiin $E_A(c)$ ja lähettää vastaanottajalle parin $(E_A(c), c)$. Huijari voi siis esimerkiksi valita $c = 10$ ja laskea $E_A(c) = (10^{37}, \bmod 3233) = 1316$, jolloin vastaanottajalle lähetetään pari $(1316, 10)$. Nyt vastaanottaja laskee tästä parista täsmälleen saman jakojäännöksen kuin huijari ja saa sen vaikutelman, että allekirjoitus on aito [1, s. 133].

Huijaus onnistuu vain silloin, kun lähettäjän A allekirjoittama viesti ei ole vastaanottajan tiedossa etukäteen. Jos viestin lähettäjä A ja vastaanottaja ovat keskenään etukäteen sopineet jonkin viestin, jonka A allekirjoittaa käyttäen omaa salaista avaintaan d_A, ei huijari pysty tällöin allekirjoittamaan etukäteen sovittua viestiä, sillä hänen tiedossaan ei ole salaista avainta d_A. Tässä viestillä tarkoitetaan tietenkin sellaista selvätekstiä, jonka lähettäjä ja vastaanottaja ovat keskenään sopineet käytettäväksi allekirjoitukseen, sillä ei liene tiedonvälitysmielessä järkevää lähetellä etukäteen sovittuja viestejä.

Oletetaan nyt, että on valittu viesti $w = 10$. Lähettäjä A laskee $D_A(w) = (10^{253}, \bmod 3233) = 2593$ ja lähettää vastaanottajalle parin $(10, 2593)$. Vastaanottaja voi varmentaa lähettäjän allekirjoituksen aitouden laskemalla $(2593^{37} \bmod 3233) = 10$. Koska vastaanottajalla oli jo etukäteen tiedossa viestin sisältö, hän tiesi, että lähetetyn parin toisen luvun jakojäännös modulo 3233 täytyi olla viesti eli 10 [1, s. 133].

Selvätekstin vaihtelevuus on tärkeää. Erityisesti merkityksellisen viestin

käänteisviestin tai kahden merkityksellisen viestin tulon ei tulisi olla merkityksellisiä. Muutoin huijari, joka tietää lähettäjän A allekirjoitukset s_1 ja s_2 viesteihin w_1 ja w_2, voi allekirjoittaa viestit $(w_1 w_2, \mathrm{mod}\ n)$ ja $(w_1^{-1}, \mathrm{mod}\ n)$ käyttäen allekirjoituksia $(s_1 s_2, \mathrm{mod}\ n)$ ja $(s_1^{-1}, \mathrm{mod}\ n)$ [1, s. 133]. *(Merkinnät $(w_1^{-1}, \mathrm{mod}\ n)$ ja $(s_1^{-1}, \mathrm{mod}\ n)$ tulkitaan määritelmän 2.11 mukaan.)*

Käytetään taas esimerkin 3.3 lukuja. Valitaan nyt $w_1 = 100$ ja $w_2 = 50$ ja $n = 3233$. Allekirjoitukset viesteille 100 ja 50 ovat $s_1 = (100^{253}, \mathrm{mod}\ 3233) = 2242$ ja $s_2 = (50^{253}, \mathrm{mod}\ 3233) = 3161$. Nyt nähdään, että

$$(*) \qquad (w_1 w_2, \mathrm{mod}\ n) = (100 * 50, \mathrm{mod}\ 3233) = 1767 \text{ ja}$$

$$(**) \qquad (w_2^{-1}, \mathrm{mod}\ n) = (50^{-1}, \mathrm{mod}\ 3233) = 194.$$

Saadut viestit $(*)$ ja $(**)$ voidaan allekirjoittaa käyttämällä seuraavia lukuja:

$$(s_1 s_2, \mathrm{mod}\ n) = (2242 * 3161, \mathrm{mod}\ 3233) = 226 \text{ ja}$$

$$(s_2^{-1}, \mathrm{mod}\ n) = (3161^{-1}, \mathrm{mod}\ 3233) = 1841.$$

Käytännössä viestin vastaanottaja käyttää kryptauseksponenttia $e_A = 253$ allekirjoituksen varmentamiseen. Hän siis laskee $(1767^{253}, \mathrm{mod}\ 3233) = 226$ viestille $(*)$ ja $(194^{253}, \mathrm{mod}\ 3233) = 1841$ viestille $(**)$ todeten molempien viestien allekirjoituksen olevan kunnossa.

3.6 RSA-allekirjoitus silloin, kun viestin salaus on tarpeellista

Oletetaan nyt molempien, viestin salauksen ja allekirjoituksen, olevan tarpeellisia. Lähettäessään allekirjoitetun viestin vastaanottajalle B lähettäjä A ensin allekirjoittaa viestin käyttäen omaa pariaan (d_A, n_A) ja sen jälkeen kryptaa viestin käyttäen vastaanottajan paria (e_B, n_B). Vastaanotettuaan viestin B ensin dekryptaa sen käyttämällä dekryptauseksponenttia d_B. Sen jälkeen alkuperäinen viesti saadaan esiin käyttämällä lähettäjän A kryptauseksponenttia e_A. Dekryptauseksponentin d_A käyttö viestissä takaa sen, että viestin lähettäjä oli A. Kuten aiemminkin, pitää vastaanottajan olla varovainen allekirjoitusten väärentämisen varalta ennakoimattomiin viesteihin [1, s. 133, 134].

Ongelmia voi aiheutua, kun A ja B käyttävät eri modulia. Oletetaan ensin, että $n_A > n_B$. Tällöin $D_A(w)$ ei välttämättä ole välillä $[1, n_B - 1]$ ja supistaminen modulo n_B tekisi laillisen dekryptauksen paljon vaikeammaksi. On kaksi tapaa välttää tämä ongelma. (i) Kaikki käyttäjät sopivat yhteisestä kynnysluvusta t. Jokainen käyttäjä A valitsee kaksi RSA-avainta: toisen allekirjoituksia varten ja toisen salausta varten. Merkitään nyt kaikkia allekirjoituksessa tarvittavia symboleita yläindeksillä s ja salauksessa tarvittavia symboleita yläindeksillä e. Jokainen käyttäjä A huolehtii, että $n_A^s < t < n_A^e$. Nyt ongelmia ei tule, jos A lähettää viestin käyttäjälle B muodossa

$$E_B^e(D_A^s(w)).$$

(ii) Myös kynnysluvun käyttö voidaan välttää, jos viestit lähettäjältä A vastaanottajalle B lähetetään muodossa $E_B(D_A(w))$ tai $D_A(E_B(w))$ riippuen siitä, onko $n_A < n_B$ tai $n_B < n_A$ [1, s. 134].

3.7 RSA-salauksen murtaminen ja siltä puolustautuminen

Monia kryptoanalyyttisiä hyökkäyksiä on kohdistettu RSA-kryptosysteemejä vastaan. Mikään näistä hyökkäyksistä ei ole osoittautunut vakavaksi. Käydään läpi joitakin tyypillisiä hyökkäyksiä ja niiltä puolustautumista.

Pohditaan lukujen p ja q valintaa. Lukujen pitäisi olla satunnaisia alkulukuja, ei esimerkiksi jostain tunnetusta alkulukutaulukosta poimittuja. Mikäli luvut p ja q poimitaan taulukosta, hyökkääjä voi käydä koko taulukon läpi ja näin onnistuneesti jakaa luvun n tekijöihin.

Alkulukuja p ja q ei pitäisi myöskään valita hyvin läheltä toinen toistaan. Oletetaan ensin, että $p > q$ ja alkuluvut on valittu hyvin läheltä toisiaan. Nyt $(p-q)/2$ on hyvin pieni ja $(p+q)/2$ on vain hieman suurempi kuin luku $\sqrt{n}$. Muodostetaan yhtälö

$$\begin{gathered} pq = n \Leftrightarrow \\ \frac{p^2 + 2pq + q^2}{4} - n = \frac{p^2 - 2pq + q^2}{4} \Leftrightarrow \\ \frac{(p+q)^2}{4} - n = \frac{(p-q)^2}{4}. \end{gathered}$$

Viimeisestä lausekkeesta nähdään selvästi, että yhtälön vasen puoli on neliö. Jotta luku n saadaan jaettua tekijöihin, testataan kokonaislukuja $x > \sqrt{n}$, kunnes löydetään sellainen luku, että $x^2 - n$ on neliö. Voidaan merkitä siis $x^2 - n = y^2$. Nyt $n = x^2 - y^2 = (x + y)(x - y)$, joten $p = x + y$ ja $q = x - y$ [1, s. 134].

Esimerkki 3.4. Valitaan $n = 176399$. Nyt $\sqrt{n} = 419,9988095$, joten kokonaisluvun x tulee olla suurempi kuin 419. Saadaan $420^2 - n = 1$, joten nyt $x = 420$ ja $y = 1$. Siis $p = x + y = 421$, $q = x - y = 419$ ja luku n on jaettu tekijöihin, sillä $419 * 421 = 176399$.

Myös valittaessa alkulukuja p ja q, täytyy pitää silmällä luvun $\phi(n)$ tekijärakennetta. Selvästi molemmat luvut $p-1$ ja $q-1$ ovat parillisia, joten $\phi(n)$ on jaollinen luvulla 4. Oletetaan, että $(p - 1, q - 1)$ on suuri ja vastaavasti lukujen $p - 1$ ja $q - 1$ **pienin yhteinen jaettava** u on pieni verrattaessa sitä lukuun $\phi(n)$. Tällöin mikä tahansa luvun e käänteisluku modulo u toimii dekryptauseksponenttina. Modulona voidaan käyttää lukua u, koska $u \mid \phi(n)$. Nyt on huomattavasti helpompi löytää käänteisluku d kokeilemalla kuin normaalissa tapauksessa. Luvuilla $p-1$ ja $q-1$ ei saisikaan olla suuria yhteisiä tekijöitä [1, s. 134].

Kryptosysteemiä suunniteltaessa pitää myös välttää tilannetta, jossa luku $\phi(n)$ koostuu pienistä alkulukutekijöistä. Tällöin saattaisi nimittäin olla mahdollista käydä läpi kaikki $\phi(n)$ ehdokkaat a, joille $(a, e) = 1$, ja laskea luvun e käänteisluku modulo a ja sen jälkeen dekryptata jokin kryptoteksti ja näin kokeilemalla löytää luku $\phi(n)$. Kun tunnetaan luvut $\phi(n)$ ja n, luvut p ja q saadaan ratkaisemalla yhtälöpari

$$\begin{cases} n = pq \\ \phi(n) = (p-1)(q-1) \end{cases}$$

[5, s. 67].

Molemmat lukuun $\phi(n)$ liittyvät ongelmat voidaan välttää, jos käytetään niin sanottuja *turvallisia alkulukuja* lukuina p ja q. Alkuluvun p sanotaan olevan turvallinen, jos ja vain jos $(p-1)/2$ on myös alkuluku. Tällaisia alkulukuja ovat esimerkiksi luvut 7, 11 ja 47. On selvää, että turvallisen alkuluvun löytäminen on huomattavasti vaikeampaa kuin normaalin alkuluvun löytä-

minen. Tällä hetkellä ei tiedetä, onko turvallisia alkulukuja ääretön määrä. Lisäksi jotkut ovat sitä mieltä, että turvallisia alkulukuja on niin vähän, että niiden käyttö saattaa itse asiassa vähentää turvallisuutta [1, s. 135][5, s. 68].

Viitteet

[1] Salomaa, Arto. *Public-Key Cryptography.*, Second, Enlarged Edition: Springer 1996. ISBN 3-540-61356-0.

[2] Wikipedia, RSA. *http://en.wikipedia.org/wiki/RSA*

[3] Rosen, Kenneth H. *Elementary Number Theory.*, Fourth Edition: Addison Wesley Longman, Inc 2000. ISBN 0-201-87073-8.

[4] Wikipedia, RSA. *http://fi.wikipedia.org/wiki/Alkuluku*

[5] Ruohonen, Keijo *Matemaattinen kryptologia*, `http://math.tut.fi/~ruohonen/MK.pdf`