JULKINEN AVAIN

5.4.2000
Anu Niemi
Jonna Passoja
Annemari Auvinen

Sisällysluettelo

Julkinen avain

Ennen salakirjoitusta käytettiin vain sotilasasioissa, mutta tietoyhteiskunnassa siitä on tullut tärkeä työkalu yksityisyyden, yritysturvallisuuden sekä tietosuojan säilyttämiseksi. Salakirjoitusta käytetään myös erilaisissa pääsykontrolleissa sähköisiin maksuihin ja moniin muihin alueisiin.

Salausmenetelmät voidaan jakaa kahteen eri ryhmään: symmetrisiin ja asymmetrisiin. Symmetrisillä algoritmeilla tarkoitetaan perinteisiä salauksia, jossa on yksi avain, jolla sekä salataan että puretaan sanoma. Tästä kuitenkin seurasi valtavia ongelmia, koska lähettäjän ja vastaanottajan täytyi sopia avaimesta.

Tarkastellaanpa ongelmaa esimerkin avulla:

Oletetaan, että Liisa haluaa lähettää viestin Pekalle tai päinvastoin ja Eeva yrittää salakuunnella. Jos Liisa haluaa lähettää yksityisiä viestejä Pekalle, hän koodaa jokaisen ennen lähettämistä ja käyttää uutta avainta joka kerta. Liisa joutuu aina ratkaisemaan avaintenjako-ongelman, koska hänen täytyy toimittaa avain Pekalle, jotta tämä pystyy avaamaan viestin. Yksi tapa olisi tavata ja vaihtaa samalla useampi avain tai sitten käyttää lähettiä.

Diffie-Hellman

Whitfield Diffie, Martin Hellman ja Ralph Merkle muodostivat kolmikon, joka paneutui avaintenvaihto-ongelmaa. He alkoivat tutkia ongelmaa ja loivat lopulta pohjan erilaisille asymmetrisille algoritmeille. Algoritmeissa on sekä salainen että julkinen avain. Tällaisessa salakirjoituksessa lähettäjän ja vastaanottajan ei tarvitse sopia avaimesta, riittää kun lähettäjä koodaa viestin vastaanottajan julkisella avaimella. Helppoa tämä työ ei ollut, sillä avaintenvaihto tuntui olevan väistämätöntä.

Kuitenkin Diffie ja Hellman tunsivat yhden anekdontin, joka tuntui uhmaavan kyseistä selviötä. Liisa haluaa lähettää hyvin henkilökohtaisen paketin Pekalle ja pakkaa sen laatikkoon ja sulkee sen lukolla pitäen avaimen itsellään. Pekka ei pysty avaamaan laatikkoa. Hän sulkee sen toisella lukolla ja lähettää laatikon takaisin Liisalle pitäen avaimen itsellään. Laatikon saatuaan Liisa aukaisee itse laittamansa lukon ja lähettää laatikon jälleen Pekalle. Nyt Pekka voi aukaista paketin omalla avaimellaan. Tämä osoittaa, että kaksi ihmistä voi vaihtaa viestejä niin, että avaimen vaihtoa ei tarvitse tapahtua.

Salaus ilman avaintenvaihtoa ei kuitenkaan ole ihan näin yksinkertaista, sillä käytännössä on väliä sillä, missä järjestyksessä koodaukset ja avaukset suoritetaan. Yleensä viimeinen koodaus pitää poistaa ensimmäisenä. Äskeisessä esimerkissä poistettiin kuitenkin ensimmäinen koodaus ennen viimeistä.

Otetaanpa esimerkki:

Liisan avain

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Å Ä Ö

H F Ä S U G T A K V D E O Y J B P Ö N X W C Q Å R I M Z L

Pekan avain

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z Å Ä Ö

C Ö P M G A T Å N O J E F W I Q B U Ä R Y H X S D Z K L V

Viesti **T A V A T A A N K E S K I P Ä I V Ä L L Ä**

Koodattu:

Liisan avaimella **X H C H X H H Y D U N D K B Z K C Z E E Z**

Pekan avaimella **S Å P Å S Å Å D M Y W M J Ö Z J P Z G G Z**

Avattu:

Liisan avaimella **D X Q X D X X K Å N U Å O R Ä O Q Ä F F Ä**

Pekan avaimella **Y W P W Y W W Å H I R H J T S J P S M M S**

Kuitenkin jos avaukset suoritettaisiin toisin päin, niin saataisiin alkuperäinen viesti.

Riippulukkoesimerkki innosti Diffietä ja Hellmania jatkamaan ponnisteluita löytääkseen ratkaisun avaintenjako-ongelmaan. He tutkivat erilaisia matemaattisia funktioita. Erityisen kiinnostuneita he olivat yksisuuntaisista funktioista. Yksisuuntainen funktio on erittäin helppo suorittaa, mutta hyvin vaikea purkaa, toisin sanoen kaksisuuntaiset funktiot voidaan muuttaa alkuasetelmaan kun taas yksisuuntaisia ei.

Keltaisen ja sinisen maalin sekoittaminen vihreäksi maaliksi on yksisuuntainen funktio, koska sekoitus on helppo tehdä, mutta sen purkaminen on mahdotonta.

Hellman tutki modulaarista aritmetiikkaa ja lopulta hän keksi menetelmän avaintenjako-ongelman ratkaisemiseen. Hänen ajatus nojaa funktioon $Y^X \pmod P$. Avaimesta sopiminen tapahtuu seuraavasti. Aluksi Liisa ja Pekka ovat sopineet luvuista Y=7 ja P=11.

	Liisa	Pekka
1.vaihe	Liisa valitsee luvun, esim. 3, ja pitää sen salassa. Tätä lukua merkitään A:lla.	Pekka valitsee luvun, esim. 6 ja pitää sen salassa. Pekan lukua merkitään B:llä.
2. vaihe	Liisa laskee funktion $7^A(\text{mod } 11)$ tuloksen $7^3(\text{mod } 11)=2$.	Pekka laskee funktion $7^B(\text{mod } 11)$ tuloksen $7^6(\text{mod } 11)=4$.
3. vaihe	Liisa merkitsee laskemaansa tulosta kirjaimella a ja lähettää sen Pekalle.	Pekka merkitsee laskemaansa tulosta kirjaimella b ja lähettää sen Liisalle.
Vaihto	Normaalisti tämä on se kriittinen paikka, mutta koska funktioista saadut tulokset eivät ole itse avain, niin ei haittaa vaikka salakuuntelija saisikin ne selville.	
4. vaihe	Liisa ottaa Pekan tuloksen ja laskee tuloksen funktiossa $b^A(\text{mod } 11)$: $4^3(\text{mod } 11)=9$.	Pekka ottaa Liisan tuloksen ja laskee tuloksen funktiossa $a^B(\text{mod } 11)$: $2^6(\text{mod } 11)=9$.

Avain on siis luku 9. Todellisuudessa käytetään paljon isompia lukuja, jolloin salakuuntelijan on vaikeampi selvittää avainta.

Tarkastellaanpa avaimen muodostusta hieman salakuuntelijan näkökulmasta. Salakuuntelija tietää vain seuraavat seikat: funktio on muotoa $7^x(\text{mod } 11)$ ja että Liisa lähettää a=2 ja Pekka b=4, mutta koska hän ei tiedä kumpaakaan A:sta tai B:stä ja funktio on yksisuuntainen niin hänen on hyvin vaikea päätellä avainta, varsinkin jos luvut ovat hyvin suuria. Tämä avainten vaihtojärjestelmä tunnetaan nimellä Diffie-Hellman-Merkle-avaintenvaihtojärjestelmänä.

Tämä avainten vaihtojärjestelmä ei kuitenkaan ole kovin käytännöllinen, koska se vaatii sen, että henkilöt ovat linjoilla yhtä aikaa. Seuraava askel olikin keksiä tehokkaampi tapa ratkaista tämä ongelma.

Epäsymmetrinen avain

Sillä aikaa kun Hellman oli kehittänyt menetelmää avainten vaihtamiseksi Whitfield Diffie oli lähestynyt ongelmaa toiselta suunnalta. Lopulta hän keksi uudentyypisen salakirjoituksen, joka sisälsi niin kutsutun epäsymmetrisen avaimen. Tälläisissa salaustavoissa salaus- ja avausavaimet ovat erilaisia. Epäsymmetrisessä salakirjoituksessa lähettäjä voi salata viestin, jos tietää salausavaimen, mutta ei voi avata sitä. Avaajan on tiedettävä avausavain.

Tämän järjestelmän etuna verrattuna Diffie-Helman-Merkle avaintenvaihtoon on, että edestakaista liikennettä ei tarvita. Lisäksi epäsymmetrinen salakirjoitus ratkaisee avaintenjakeluongelman, koska vastaanottajan ei tarvitse kuljettaa avainta turvallisesti lähettäjälle, päinvastoin hän voi julkaista sen niin suurelle yleisölle kuin mahdollista.

Vaikka Diffie olikin keksinyt epäsymmetrisen salakirjoituksen yleisen periaatteen, hänellä ei kuitenkaan ollut toimivaa esimerkkiä. Hän julkaisi pääpiirteet ajatuksestaan kesällä 1975 ja monet muutkin tiedemiehet alkoivat etsiä sopivaa yhdensuuntaista algoritmia.

Mitä tutkijat etsivät:

1. Liisan täytyy luoda julkinen avain, jonka hän voi sitten julkistaa, niin että Pekka (ja kuka tahansa) voi käyttää sitä koodatakseen hänelle lähetettäviä viestejä. Koska julkinen avain on yksisuuntainen funktio, sen täytyy olla käytännöllisesti katsoen peruuttamaton, joten kukaan ei voi avata Liisan viestejä.

2. Liisan täytyy kuitenkin avata hänelle tulevat viestit. Hänellä täytyy siksi olla yksityinen avain, jokin tietty tiedonsiru, jonka avulla hän voi peruuttaa yleisellä avaimella suoritetun koodauksen. Siksi Liisa (ja vain Liisa) kykenee avaamaan hänelle lähetetyt viestit.

RSA

MIT:n (Massachusetts Institute of Technology) tietojenkäsittelylaitoksen kolme työntekijää -Rivest, Shamir ja Adleman- alkoivat etsiä yksisuuntaista funktiota, joka sopisi epäsymmetrisen salakirjoituksen vaatimuksiin. Huhtikuussa 1977, vuosi aloittamisen jälkeen, Rivest teki läpimurron, mutta se oli tulosta vuoden kestäneestä yhteistyöstä Shamirin ja Adlemanin kanssa. Järjestelmä, joka sai nimen RSA (Rivest, Shamir, Adleman) muodostui modernin kryptografian vaikutusvaltaisimmaksi salakirjoitukseksi.

Rivestin epäsymmetrisen salakirjoituksen ytimessä on yksisuuntainen funktio, joka perustuu modulaarisille funktioille. Rivestin yksisuuntaista funktiota voidaan käyttää viestin salaamiseen – viesti, joka on käytännössä luku, pannaan funktioon ja tuloksena on kooditeksti, joka on toinen luku.

N on yksisuuntaisen funktion joustava komponentti, mikä tarkoittaa, että jokainen voi valita N:lle eri arvon ja nimikoida siten yksisuuntaisen funktion. Voidakseen valita oman arvonsa N:lle Liisa valitsee kaksi alkulukua, p:n ja q:n ja kertoo ne keskenään. Esimerkiksi jos valitaan p = 17 159 ja q = 10 247, niin N = 175 828 273. Liisan valinta N:ksi on käytännössä hänen julkinen salausavaimensa. Jos Pekka haluaa salata Liisalle kirjoittamansa viestin, hän etsii käsiinsä Liisan N:n arvon ja panee sen sitten yksisuuntaisen funktion yleiseen muotoon, mistä tulee myös julkista tietoa. Koodatakseen Liisalle kirjoittamansa viestin Pekka ottaa Liisan yksisuuntaisen funktion, asettaa siihen sanoman, kirjaa tuloksen muistiin ja lähettää sen Liisalle.

Tässä vaiheessa viesti on vielä ratkaisematon. Voidakseen lukea hänelle tulleet viestit Liisalla täytyy olla keino peruuttaa yksisuuntainen funktio. Liisalla on edelleen tiedossaan ne kaksi alkulukua, joiden tulo N on. Näiden avulla purku onnistuu. P ja q ovat Liisan yksityisavaimia. Jos N:n arvo on tarpeeksi suuri, on käytännössä mahdotonta päätellä p:n ja q:n arvot.

Jos valitaan esimerkiksi alkulukuja, jotka ovat niinkin isoja kuin 10^{65} , niin N saisi arvon , joka on suurin piirtein 10^{130} . Turvallisuusasiantuntija Simson Garfinkel on arvioinut, että tietokoneelta, jossa on 100 MHz Intel Pentium – prosessori ja 8MB keskusmuistia, tämän tekijöihin jako kestäisi noin 50 vuotta. Jos sata miljoonaa tietokonepäätettä (myytyjen koneiden lukumäärä vuonna 1995) kytkettäisiin yhteen, tekijöihin jako kestäisi 15 sekuntia.

Tärkeissä pankkitapahtumissa N on usein suuruusluokkaa 10^{308}. Sadan miljoonan tietokoneen yhteistyöllä kestäisi yli tuhat vuotta murtaa sellainen salakirjoitus. Kun p:n ja q:n arvot ovat tarpeeksi suuret, RSA on ratkaisematon. Nykyään on jo jokapäiväistä koodata viestejä niin suurilla N:n arvoilla, että maapallon kaikilta tietokoneilta menisi pidempi aika kuin maailmankaikkeuden elinikä salakirjoituksen murtamiseen.

Ainoa vaara on, että tulevaisuudessa voidaan keksiä nopeampi tapa jakaa N tekijöihinsä. Matemaatikot ovat kuitenkin yrittäneet jo yli kaksituhatta vuotta onnistumatta löytää sellaista oikotietä.

Britannian viranomaisten mukaan julkisen avaimen salakirjoitus keksittiinkin alun perin Government Communications Headquartersissa (GCHQ – Valtion viestipäämaja) Cheltenhamissa. Tarina alkoi 1960-luvun loppupuolella, kun brittiarmeija alkoi huolestua avaintenjakeluongelmasta.Vuonna 1975 James Ellis, Clifford Cocks ja Malcolm Williamson olivat löytäneet kaikki julkisen avaimen salakirjoituksen peruspiirteet, mutta eivät saaneet puhua asiasta ennen kuin vasta vuonna 1997.

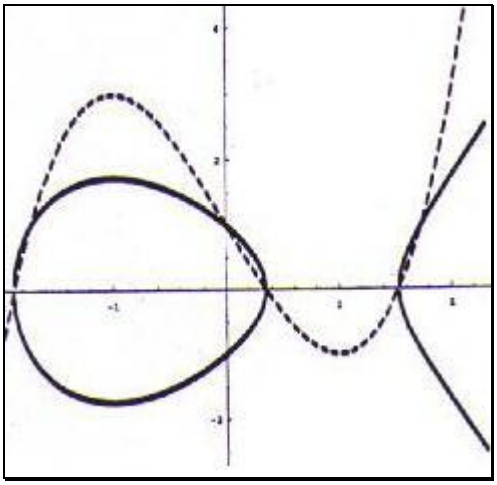
Elliptisen käyrän salausmenetelmä

Eräs salausmenetelmä on Whitfield Diffien ja Martin Hellmanin kehittämä avaimenvaihto, jossa käytetään muunmuassa elliptisiä käyriä.

80-luvulla useat tutkijat havaitsivat elliptisen käyrän olevan mainio ratkaisu kehitettäessä vaikeita ongelmia. Elliptisten käyrien hyödyllisin ominaisuus liittyy juuri julkisten avainten salausmenetelmään. Elliptisen käyrän etu muihin menetelmiin verrattuna on mahdollisuus laskea sen pisteitä käyttäen. Laskutoimitukset ovat turvallisia, koska ne ovat melko monimutkaisia. Laskutoimituksia kutsutaan summaamiseksi, sillä ne noudattavat samoja sääntöjä kuin tavalliset yhteenlaskettavat luvut. Vaikka laskutoimitus tuntuukin keinotekoiselta, niin se on osoittautunut todella hyödylliseksi, kun halutaan luoda vaikea salausmenetelmä. Esimerkiksi sähköpostin salauksessa käytetään avainsalausta, jossa lähettäjä ja vastaanottaja sopivat yhteisestä avaimesta.

Elliptisen käyrän salausmetelmä eli ECC (elliptic curve cryptosystem) on salausalgoritmimenetelmä, joka on johdettu äärellisestä elliptisien käyrien ryhmästä. Tällaisesta ryhmästä johdettavia algoritmeja ovat esimerkiksi ElGamal-analogi ja RSA-analogi. ECC kehitettiin vasta vuonna 1985, kehittäjinä Koblitz ja Miller. Alkuaikoinaan menetelmä oli melko hidas ja hankala, mutta nykyään se on varteenotettava vaihtoehto. Elliptisen käyrien salausmenetelmät ovat yleensä ottaen turvallisempia kuin muut menetelmät. Niitä ei myöskään voida nykykeinoilla purkaa.

Elliptisellä käyrällä laskeminen

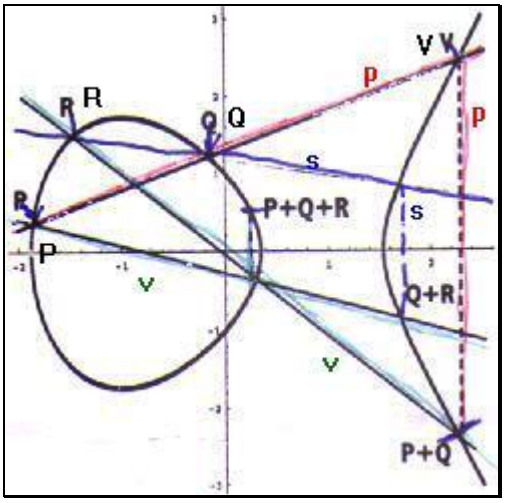


Kuva 1. Elliptinen käyrä (viiva) ja kolmannen asteen kuvaaja (katkoviiva)

Elliptiset käyrät löydettiin jo 1700-luvulla, kun laskettiin ellipsin kaaren pituutta. Salakirjoitukseen ne päätyivät vasta parisataa vuotta myöhemmin. Elliptisten käyrien käyttö salauksessa on kuitenkin hieman heikolla pohjalla, koska ne ovat salakirjoitusmenetelmissä vielä niin tuntemattomia, että niissä voi ilmetä yllättäviä heikkouksia ajan myötä. Menetelmä on kuitenkin tällä hetkellä todella turvallinen. Kuvassa 1 on elliptinen käyrä ja tavallinen kolmannen asteen kuvaaja, jonka yhtälö on muotoa $y^2=x^3+ax+b$, missä a ja b ovat vakioita.

Pisteiden summa

Elliptisen käyrän pisteiden P ja Q summa P+Q löydetään piirtämällä kaksi suoraa. Ensimmäinen vedetään pisteiden P ja Q kautta (punainen viiva=p). Tämä suora leikkaa alkuperäisen käyrän kolmessa pisteessä, P, Q ja V. Toinen suora piirretään pisteen V kautta y-akselin suuntaisesti (punainen katkoviiva). Piste P+Q on edellisen suoran ja alkuperäisen käyrän leikkauspisteessä. Vastaavanlaisesti suoritetaan myös kolmen muuttujan summaus. (Katso kuva; summa Q+R sininen viiva, summa P+Q vihreä viiva)

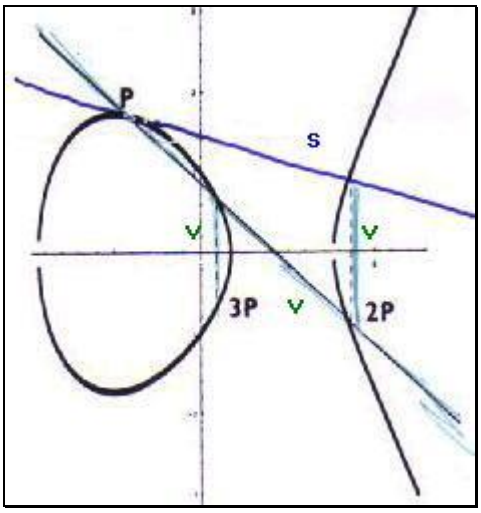


Kuva 2. Piste P+Q+R elliptiseltä käyrältä

Pisteiden monikerrat

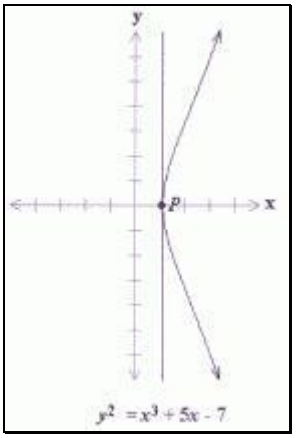
Monikerran laskeminen aloitetaan summaamalla P itsensä kanssa. Tällöin pisteen P kautta piirretään tangentti (kuva 3, sininen suora). Tangentin ja käyrän leikkauspiste peilataan, jolloin saadaan P+P eli 2P. Menetelmää hyväksikäyttäen voidaan laskea 3P, joka on siis 2P+P. Monikerrat, jossa kerroin k on suuri, voidaan laskea tuplaamisperiaatteella muodostamalla ensin 2P, jonka jälkeen voidaan muodostaa 2(2P)=4P, sitten 8P jne.

Pisteestä P ja kertoimesta k on siis helppo johtaa tulos kP, mutta toiseen suuntaan se on ainakin tällä hetkellä mahdotonta. Ratkaisu saadaan ainoastaan kokeilemalla kaikkia k:n arvoja. Jos k on esimerkiksi 50-numeroinen luku, on ratkaisun löytäminen nykyisillä resursseilla mahdotonta.



Kuva 3. Pisteen P monikertoja

Mikäli y-koordinaatti on nolla, pisteeseen P piirretty tangentti ei leikkaa käyrää missään pisteessä. Tästä seuraa, että 2P=0. 3P sen sijaan on 2P+P=0+P=P. Laskemalla muita monikertoja havaitaan seuraavaa: 3P=P, 4P=0, 5P=P, 6P=0... (kuva 4)



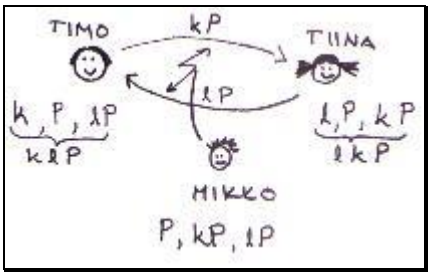
Kuva 4. P=(1,0)

Periaate

Timo ja Tiina haluavat käydä yksityisen keskustelun kanavalla, jota myös Mikko kuuntelee.

1. Timo ja Tiina sopivat yhteisen elliptisen käyrän ja sen pisteen P.
2. Timo valitsee suuren satunnaisluvun k ja muodostaa monikerran kP. Hän laskee pisteen paikan käyrältä ja lähettää sen Tiinalle.
3. Tiina valitsee suuren satunnaisluvun l ja muodostaa monikerran lP. Hän laskee pisteen paikan käyrältä ja lähettää sen Timolle.
    - Timo tietää luvut P, k, lP ja Tiina tietää luvut P, l ,kP. Mikko tietää luvut P, kP, lP. (kuva 1)
    - k ja l ovat niin suuria, ettei niitä voi ratkaista, vaikka tietäisikin P:n.
    - Tiina ei tiedä lukua k, eikä Timo lukua l.

4. Nyt Timo voi laskea yhteisen salaisen avaimen, joka löytyy käyrältä pisteestä k(lP).
5. Myös Tiina voi laskea yhteisen salaisen avaimen, joka löytyy käyrältä pisteestä l(kP).
6. Koska Mikko ei tiedä lukuja k ja l, hän ei voi ratkaista salaista avainta, eikä siten pääse keskusteluun mukaan.



Kuva 5. Timon ja Tiinan keskustelutapaus

Esimerkki

1. *Käyrä on $y^2 = x^3-3x+1$, piste $P = (-1, \sqrt{3})$.*
2. *Valitaan k = 2, muodostetaan monikerta 2P.*
   - *Derivoidaan käyrä implisiittisesti: $y' = (3x^2-3)/2y$, josta saadaan sijoittamalla yhtälöön $(-1, \sqrt{3})$ tangentin kulmakertoimeksi 0, eli tangentin yhtälö on $y = \sqrt{3}$.*
   - *Tangentin ja käyrän leikkauspisteeksi saadaan $(2, \sqrt{3})$. Peilataan x-akselin suhteen, eli monikerta $2P = (2, -\sqrt{3})$, joka lähetetään Tiinalle.*
3. *Valitaan l = 4, muodostetaan monikerta 4P, eli 2(2P).*
   - *Nyt saadaan tangentin kulmakertoimeksi $-3*\sqrt{3}/2$. Tangentin yhtälöksi saadaan $y = -(3*\sqrt{3}/2)x+2*\sqrt{3}$.*
   - *Tangentin ja käyrän leikkauspiste on $(11/4, -1/8*\sqrt{867})$. Peilataan jälleen, jolloin saadaan monikerta $4P = 2(2P) = (11/4, 1/8*\sqrt{867})$, joka lähetetään Timolle.*
4. *Timo laskee yhteisen salaisen avaimen, joka löytyy käyrältä pisteestä k(lP) eli 2(4P) = 8P.*
   - *Tangentin kulmakerroin on nyt $315/(4*\sqrt{867})$. Tästä saadaan tangentin yhtälöksi $y = 315/(4*\sqrt{867})x-1731/(16*\sqrt{867})$.*
   - *Tangentin ja käyrän leikkauspiste on (1.6529, 0.7464). Peilauksen jälkeen saadaan monikerta 8P = (1.6529, -0.7464).*
5. *Tiina laskee yhteisen salaisen avaimen, joka läytyy käyrältä pisteestä l(kP) eli 4(2P) = 8P.*

Lähdeluettelo

1. Tiede 2000, nro 6/98: Elliptinen käyrä pitää sähköpostin yksityisenä

2. J.Lindström, T.Mäkelä: Diffie-Hellman, http://keskus.tct.hut.fi/opetus/s38118/s98/htyo/48/dh.stml

3. Elliptisten käyrien kryptoanalogit, http://www.hut.fi/~zam/sid/SID.html#_Toc408323873

4. Blake, Seroussi, Smart: Elliptic Curves in cryptography, Gambridge Univercity Press 1999

5. Simon Singh: Koodikirja, Gummerus kirjapaino Oy, 1999

6. http://www.cc.jyu.fi/~hmhahto/salaus.htm