RSA ja Diffie-Hellmannin avaimenvaihtoprotokolla

29. tammikuuta 2014

1 RSA

RSA perustuu siihen, että tekijöihinjako on hankalaa isoilla luvuilla. (Voidaan itse asiassa todistaa, että jos RSA murtuu yleisessä tilanteessa, niin myös tekijöihinjako-ongelma on ratkeava polynomiaalisessa ajassa.)

RSA:ssa on julkinen avain (julkinen avain on siis sellainen, joka voidaan levittää kaiken kansan tietoisuuteen), (n, e), missä $n = pq$ sekä p ja q ovat parittomia alkulukuja, keskenään erisuuria. Kriittistä on kuitenkin se, että käytetään vain lukua n, eikä anneta sen alkutekijähajotelmaa. Pointti on se, että isoa lukua on hankala jakaa tekijöihin, jolloin jos alkuluvut p ja q ovat molemmat isoja, voidaan olettaa, että alkutekijöhajotelmaa ei tunneta.

Salainen avain puolestaan on $(p, q, \varphi(n), d)$, missä $ed \equiv 1 \pmod{\varphi(n)}$. Huomaa, että luku e pitää valita niin, että käänteisluku on olemassa, eli että $\text{syt}(e, \varphi(n)) = 1$. Luku d on siis helppo määrittää (käänteislukuja erilaisissa moduloissa on aiemminkin laskettu), jos tunnetaan e ja $\varphi(n)$ (ja tämän funktion arvon laskemiseksi tarvitaan tieto luvuista p ja q).

Tiivistettynä siis: Julkinen avain (n, e), salainen avain $(p, q, \varphi(n), d)$, ja näistä oletetaan $pq = n$, $p \neq q$, p ja q parittomia alkulukuja, $ed \equiv 1 \pmod{\varphi(n)}$, ja $\varphi(n)$ on Eulerin funktio. Sisäänrakennettu oletus on siis, että $\text{syt}(e, \varphi(n)) = \text{syt}(d, \varphi(n)) = 1$.

Nyt luvun $1 \leq w \leq n$ salaaminen tapahtuu seuraavasti:

$$w' \equiv w^e \pmod{n}$$

ja purkaminen seuraavasti:

$$w'' \equiv w'^d \pmod{n}.$$

Nyt $w \equiv w'' \pmod{n}$, sillä

$$w'' \equiv w'^d \equiv w^{ed} \pmod{n},$$

ja Eulerin lauseen nojalla

$$w^{\varphi(n)} \equiv 1 \pmod{n},$$

jolloin $w^{ed} = w^{1+k\varphi(n)} \pmod{n}$, kunhan $\text{syt}(w, n) = 1$.

Valotetaan RSA:n toimintaa esimerkillä:

Esimerkki 1. Olkoon $n = 83 \cdot 103 = 8549$. Nyt $\varphi(n) = (83 - 1)(103 - 1) = 82 \cdot 102 = 8364$. Valitaan $e = 13$. Tämä on täysin laillista, sillä $\text{syt}(13, 8364) = 1$. Ratkaistaan nyt d yhtälöstä

$$de - +k\varphi(n) = 1,$$

eli

$$13d + k8364 = 1.$$

Ensinnäkin

$$8364 = 643 \cdot 13 + 5,$$

ja

$$13 = 2 \cdot 5 + 3,$$

josta

$$5 = 1 \cdot 3 + 2,$$

nyt

$$3 = 1 \cdot 2 + 1,$$

ja vihdoinkin jako menee tasan: $2 = 2 \cdot 1 + 0$. Siispä

$$1 = 3 - 1 \cdot 2,$$

johon sijoittaen saadaan

$$1 = 3-1(5-3) = 2\cdot 3-5 = 2(13-2\cdot 5)-5 = 2\cdot 13-5\cdot 5 = 2\cdot 13-5(8364-643\cdot 13) = 3217\cdot 13-5\cdot 8364.$$

Voidaan siis valita $d = 3217$. Salataan nyt luku 87. Tämä tapahtuu yksinkertaisesti seuraavasti: Lasketaan $87^{13} \pmod{8549}$. Nyt

$$87^{13} \equiv 7929 \pmod{8549}.$$

Purkaminen tulee olemaan selvästi työläämpi operaatio. On siis laskettava

$$7929^{3217} \pmod{8549}.$$

Tämä on todennäköisesti kivuttominta tehdä toistuvalla neliöinnillä, jota varten kirjoitetaan

$$3217_{10} = 110010010001_2$$

binääriesitys. (Binääriesityksestä näkee helposti, miten luku on laskettava.) Nyt

$$7929^{3217} = 7929^{2048} \cdot 7929^{1024} \cdot 7929^{128} \cdot 7929^{16} \cdot 7929.$$

Tämän laskutavan nerokkuus on nopeus: korotetaan neliöön, ja saadaan aina hoidettua monta laskutoimitusta kerralla. Siispä:

$$7929^{16} \equiv \left(7929^2\right)^8 \equiv 8244^8 \equiv 305^8 \equiv 7535^4 \equiv 2316^2 \equiv 3633 \pmod{8549}.$$

Koska $128 = 16 \cdot 8$, niin

$$7929^{128} \equiv 3633^8 \pmod{8549}.$$

Nyt voidaan laskea

$$3633^8 \equiv 7582^4 \equiv 3248^2 \equiv 38 \pmod{8549}.$$

Koska taas $1024 = 8 \cdot 128$, voidaan laskea

$$7929^{1024} \equiv 38^8 \pmod{8549},$$

joten lasketaan

$$38^8 = 1444^4 \equiv 7729^2 \equiv 5578 \pmod{8549}.$$

Lopulta vielä $2048 = 1024$, joten riittää laskea

$$7929^{2048} \equiv 5578^2 \equiv 4273 \pmod{8549}.$$

Ja nyt

$$7929^3217 \equiv 4273 \cdot 5578 \cdot 38 \cdot 3633 \cdot 7929 \equiv 87 \pmod{8549}.$$

2 RSA:n murtaminen

Osoitetaan nyt, että $p - q$ ei saa olla liian pieni:

Lause 2. *Mikäli* $\left|\frac{p-q}{2}\right|^2 < 2\sqrt{n}+1$*, niin luku* $n = pq$ *saadaan välittömästi jaettua tekijöihin (ts. RSA murtuu).*

Todistus. Jos $p = q$, on tekijöihinjako helppo tehdä. Olkoon siis $p > q$, ja kirjoitetaan $p = t + r$ ja $q = t - r$, missä t ja r ovat positiivisia kokonaislukuja. Nyt $p - q = 2r$, eli $r^2 < 2\sqrt{n} + 1$ ja

$$n = pq = (t + r)(t - r) = t^2 - r^2.$$

Toisaalta

$$(\lceil\sqrt{n}\rceil + 1)^2 = \lceil\sqrt{n}\rceil^2 + 2\lceil\sqrt{n}\rceil + 1 > n + 2\sqrt{n} + 1 > n + r^2.$$

Nyt $t^2 = n + r^2$, joten $t^2 > n$. Kuitenkin $t^2 < (\lceil\sqrt{n}\rceil + 1)^2$, joten $t = \lceil\sqrt{n}\rceil$. Tämän avulla puolestaan saadaan ratkaistua r:

$$r^2 = \lceil\sqrt{n}\rceil^2 - n,$$

ja nyt

$$p = \lceil\sqrt{n}\rceil + r$$

ja

$$q = \lceil\sqrt{n}\rceil - r.$$

□

2.1 Wienerin hyökkäys

Ketjumurtoluvuksi kutsutaan luvun esitystä muodossa

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{\cdots}}}}}$$

Ylläolevaa esitystä merkitään lyhyesti $x = [a_0; a_1, a_2, a_3, a_4, \dots]$. Luvun esitys ketjumurtolukuna voi olla äärellinen tai ääretön. On helppo nähdä, että rationaalilukujen esitys ketjumurtolukuna on äärellinen, irrationaalilukujen ääretön.

Lukuja $[a_0] = a_0$, $[a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1}$, $[a_0; a_1, a, a_2] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}}$, jne kutsutaan ketjumurtoluvun *konvergenteiksi.*

Esimerkki 3. Esitetään $\frac{53}{15}$ ketjumurtolukuna. Ensinnäkin

$$\frac{53}{15} = 3 + \frac{8}{15} = 3 + \frac{1}{\frac{15}{8}} = 3 + \frac{1}{1 + \frac{7}{8}} = 3 + \frac{1}{1 + \frac{1}{\frac{8}{7}}} = 3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{7}}} = [3; 1, 1, 7]$$

Seuraava lause kertoo yhden ketjumurtolukujen oleellisen ominaisuuden:

Lause 4. *Olkoon α reaaliluku,*

1. *Olkoon $\frac{r}{s}$ luvun α konvergentti supistetussa muodossa. Tällöin*
$$\left|\alpha - \frac{r}{s}\right| \leq \frac{1}{s^2}.$$
2. *Olkoon $\frac{u}{v}$ sellainen murtoluku, joka toteuttaa ehdon*
$$\left|\alpha - \frac{u}{v}\right| \leq \frac{1}{2v^2}.$$
Tällöin $\frac{u}{v}$ on luvun α konvergentti.

Todistus. Todistus sivuutetaan. Se löytyy esimerkiksi Hardyn ja Wrightin lukuteorian eepoksesta An Introduction to the Theory of Numbers. □

Edellisen lauseen pointti on siinä, että ketjumurtoluvut tarjoavat valtavan hyviä approksimaatioita reaaliluvuilla.

Lause 5. *Olkoon $n = pq$ ja $p < q < 2p$. Oletetaan, että $e < \varphi(n)$. RSA murtuu, kun $d < \frac{1}{3}n^{1/4}$.*

Todistus. Todistuksen idea on se, että n on about yhtä suuri kuin $\varphi(n)$.

Arvioidaan siis ensin erotusta $n - \varphi(n)$:

$$n - \varphi(n) = n - (p-1)(q-1) = n - pq + p + q - 1 = p + q - 1 < p + q < 3p < 3\sqrt{n}.$$

Tiedetään, että $ed - k\varphi(n) = 1$. Nyt

$$\left|\frac{e}{n} - \frac{k}{d}\right| = \frac{|ed - kn|}{nd} = \frac{|ed - kn + k\varphi(n) - k\varphi(n)|}{nd} = \frac{|1 + k(\varphi(n) - n)|}{nd}$$
$$< \frac{k(n - \varphi(n))}{nd} < \frac{3\sqrt{n}k}{nd} = \frac{3k}{d\sqrt{n}}.$$

Koska $ed - k\varphi(n) = 1$ ja $e < \varphi(n)$, niin $d > k$. Siispä

$$\frac{3k}{d\sqrt{n}} < \frac{3}{\sqrt{n}} < \frac{3}{9d^2} = \frac{1}{3d^2}.$$

Täten luku $\frac{k}{d}$ on luvun $\frac{e}{n}$ konvergentti, ja konvergentit on nopea laskea. Siispä RSA murtuu. □

Boneh ja Durfee paransivat tulosta ja osoittivat, että RSA murtuu, kun $d < n^{0{,}292}$. (Menetelmä on tuhottoman paljon hankalampi ja sotkuisempi kuin Wienerin menetelmä.) Uskotaan yleisesti, että RSA murtuu, kun $d < \sqrt{n}$.

3 Diffie-Hellmannin avaimenvaihtoprotokolla

Diffie-Hellmannin avaimenvaihtoprotokolla sopii tilanteeseen, jossa on sovittava jokin satunnaisehko luku yhteisesti, mutta käytössä on vain julkinen kanava kommunikointiin. (Julkiseksi kanavaksi voi ajatella esimerkiksi Hesarin etusivun, puhelinpylvään, ilmoitustaulun tai muun vastaavaan esineen, jonka yksityisyyttä ei voi valvoa.)

1. Ensin tahot (olkoot Bonnie ja Clyde) sopivat alkuluvusta p ja primitiivisestä juuresta g modulo p. Nämä voidaan julkistaa, eli sopiminen voi käytännössä tarkoittaa sitä, että Bonnie postaa Hesariin ilmoituksen: "Valitaan alkuluvuksi p ja primitiiviseksi juureksi g."

2. Seuraavaksi Bonnie ja Clyde valitsevat omat eksponenttinsa b ja c, ja näitä he eivät kerro kellekään, edes toisilleen (koska turvallista kanavaa ei ole käytettävissä).

3. Nyt Bonnie laskee luvun g^b ja redusoi sen modulossa p ja Clyde puolestaan laskee luvun luvun g^c ja redusoi sen modulossa p. Merkitään näitä uusia lukuja b' ja c'. Nyt Bonnie postaa luvun b' ja Clyde postaa luvun c'.

4. Nyt Bonnie laskee luvun c'^b modulossa p ja Clyde laskee luvun b'^c modulossa p, ja molemmat ovatkin saaneet saman luvun, sillä

$$c'^b \equiv (g^c)^b = g^{cb} \equiv (g^b)^c \equiv b'^c \pmod{p}.$$

Kriittistä on reduktio modulossa p: Se ei muuta tuloksia mitenkään, mutta se toimii salauksena. Jos Bonnie ja Clyde vain laskisivat luvut g^b ja g^c, eivätkä redusoisi, olisi lukujen b ja c selvittäminen ihan liian helppoa (g-kantainen logaritmi).