Kryptografian alkeet
4. harjoitukset, ratkaisuja
Jesse Jääsaari (jesse.jaasaari@helsinki.fi)

1. Alice ja Bob käyttävät Diffie-Hellmannin avaimenvaihtoprotokollaa alkuluvulla 13 ja primitiivisellä juurella 2. Alice valitsee salaisen eksponentin 4 ja Bob valitsee salaisen eksponentin 5. Määritä yhteinen salasana.

Ratkaisu. Alice laskee luvun $2^4 \pmod{13}$, jolloin hän saa tulokseksi 3. Bob puolestaan laskee $2^5 \pmod{13}$, jolloin hän saa tulokseksi luvun 6. Alice kertoo lukunsa Bobille, ja Bob kertoo omansa Alicelle. Tällöin Alice saa yhteisen salasanan selville kun hän laskee $6^4 \pmod{13}$ ja Bob saa yhteisen salasanan selville kun hän laskee $3^5 \pmod{13}$. Siten saadaan, että yhteinen salasana on 9.

2. Alice ja Bob päättävät seuraavaksi käyttää RSA:n salaisena eksponenttina lukua d=edellisen tehtävän ratkaisu+2. Luvuksi n on valikoitunut $1061 \cdot 1163 = 1233943$. Määritä jokin sopiva julkinen eksponentti e.

Ratkaisu. Nyt $d = 9 + 2 = 11$. Koska 1061 ja 1163 ovat alkulukuja, niin Eulerin φ-funktion multiplikatiivisuudella saadaan $\varphi(n) = 1060 \cdot 1162 = 1231720$. Tiedetään, että e toteuttaa kongruenssiyhtälön $de \equiv 1 \pmod{\varphi(n)}$, eli $11e \equiv 1 \pmod{1231720}$. Ratkaistaan siis Diofantoksen yhtälö $11e - 1231720k = 1$. Huomataan, että

$$\begin{aligned} 1231720 &= 111974 \cdot 11 + 6 \\ 11 &= 6 \cdot 1 + 5 \\ 6 &= 5 \cdot 1 + 1 \end{aligned}$$

Siten saadaan

$$1 = 6 - 5 \cdot 1 = 6 - 1 \cdot (11 - 6 \cdot 1) = 2 \cdot 6 - 1 \cdot 11 = 2 \cdot (1231720 - 111974 \cdot 11) - 1 \cdot 11 = -223949 \cdot 11 + 2 \cdot 1231720.$$

Siten $(e, k) = (-223949, -2)$ on ratkaisu. Halutaan positiivinen e, mikä saadaan lisäämällä $\varphi(n)$ lukuun e ts. luvuksi e kelpaa $-223949 + 1231720 = 1007771$ (huom. tällöin myös k muuttuu, mutta ei samalla tavalla. Uuden k:n arvo saataisiin helposti, mutta tässä sitä ei tarvitse määrittää).

3. Käytä Wienerin hyökkäystä murtaaksesi edellisen tehtävän RSA.

Ratkaisu. Muodostetaan luvun $\frac{e}{n}$ ketjumurtolukukehitelmä:

$$\frac{e}{n} = [0; 1, 4, 2, 5, 6, 1, 1, 4, 4, 2, 2, 1, 4, 2].$$

Ensimmäiset konvergentit $\frac{k}{d}$ ovat 0, 1, $\frac{9}{11}, \ldots$. Ensimmäinen konvergentti, jolla

$$\varphi(n) = \frac{de - 1}{k}$$

on kokonaisluku on $(d, k) = (11, 9)$. Tässä tapauksessa $\varphi(n) = 1231720$. Jos nyt $n = pq$, missä p ja q ovat alkulukuja, niin samoin kuin harjoitusten 3 ratkaisuissa täytyy päteä

$$x^2 - (n - \varphi(n) + 1)x + n = 0,$$

eli

$$x^2 - 2224x + 1233943 = 0.$$

Tästä toisen asteen yhtälöstä saadaan ratkaisukaavalla luvun n alkutekijät 1061 ja 1163.

4. Wienerin hyökkäyksessä oletettiin, että $0 < e < \varphi(n)$. Tarkastele, miten tilanne muuttuu, jos lukuun e lisätään luvun $\varphi(n)$ monikertoja. Kuinka monta monikertaa on riittävästi, jotta Alicen ja Bobin RSA ei murru Wieneriä käyttäen?

Ratkaisu. Lisätään lukuun e $\varphi(n)$:n monikertoja, jolloin e on muotoa $e = \varphi(n) \cdot \ell + t$, missä $\ell \in \mathbb{Z}_+$ ja $0 < t < \varphi(n)$. Ernvall-Hytösen monisteen lauseen 4 alun argumentti menee läpi sellaisenaan:

$$\left| \frac{e}{n} - \frac{k}{d} \right| < \frac{3k}{d\sqrt{n}}.$$

Nyt, koska $ed - k\varphi(n) = 1$, saadaan

$$d = \frac{1 + k\varphi(n)}{e} = \frac{1 + k\varphi(n)}{\varphi(n) \cdot \ell + t} > \frac{k\varphi(n)}{\varphi(n) \cdot \ell + \varphi(n)} = \frac{k}{\ell + 1}.$$

Siten

$$\left| \frac{e}{n} - \frac{k}{d} \right| < \frac{3k}{\sqrt{n}} \cdot \frac{\ell + 1}{k} = \frac{3(\ell + 1)}{\sqrt{n}}.$$

Tiedetään, että RSA murtuu varmasti kun

$$\frac{3(\ell + 1)}{\sqrt{n}} \leq \frac{1}{2d^2}$$

eli

$$\ell \leq \frac{\sqrt{n}}{6d^2} - 1.$$

Alicen ja Bobin RSA:n tapauksessa ($n = 1233943$ ja $d = 11$) RSA murtuu varmasti Wieneriä käyttäen kun $\ell \leq 1,54$ ts. $\ell \leq 1$. Tarkastellaan mitä tapahtuu kun $\ell = 2$. Tällöin $e = 2 \cdot 1231720 + 1007771 = 3471211$. Lasketaan sitten luvun $\frac{e}{n}$ ketjumurtolukukehitelmä:

$$\frac{3471211}{1233943} = [2; 1, 4, 2, 1, 5, 1, 3, 2, 1, 2, 1, 1, 2, 1, 3, 3, 3].$$

Ensimmäiset konvergentit $\frac{k}{d}$ ovat $2, 3, \frac{14}{5}, \frac{31}{11}, \ldots$. Samoin kuin tehtävässä 3 huomataan, että parilla $(d, k) = (11, 31)$ RSA murtuu Wieneriä käyttäen. Katsotaan sitten mitä tapahtuu kun $\ell = 3$. Tällöin $e = 3 \cdot 1231720 + 1007771 = 4702931$. Lasketaan luvun $\frac{e}{n}$ ketjumurtolukukehitelmä

$$\frac{4702931}{1233943} = [3; 1, 4, 3, 2, 1, 19, 1, 2, 25, 15].$$

Laskemalla konvergentteja $\frac{k}{d}$ nähdään, että yhdessäkään konvergentissa ei ole nimittäjänä lukua 11. Siten Alicen ja Bobin RSA ei murru Wienerin hyökkäystä käyttäen. Siis kolmen $\varphi(n)$:n lisääminen riittää siihen, että Alicen ja Bobin RSA ei murru Wienerin hyökkäyksellä.

Huomautus. Tietenkin tapauksen $\ell = 1$ olisi voinut laskea samalla tavalla kuin tapaukset $\ell = 2, 3$, mutta tässä tarkasteltiin yleistä tapausta, jotta nähtäisiin millainen raja lisäysten määrälle ℓ saataisiin.

5. Mitä ovat neliönjäännökset ja mitä ovat epäneliönjäännökset? Kuinka monta kumpaakin on modulo p (p alkuluku)? Millä luvun a arvoilla yhtälöllä $x^2 \equiv a \pmod 5$ on ratkaisu? Kuinka monta ratkaisua on kussakin tilanteessa?

Ratkaisu. Luku q on neliönjäännös modulo n, jos on olemassa kokonaisluku x, jolle $x^2 \equiv q \pmod n$. Jos tällaista lukua x ei ole olemassa, niin q on epäneliönjäännös modulo n. Sekä neliönjäännöksiä, että epäneliönjäännöksiä on $\frac{p-1}{2}$, kun p on pariton alkuluku[1]. Tämän

[1] Yleensä määritelmässä 0 ei ole neliönjäännös, eikä epäneliönjäännös.

todistus löytyy täältä:

http://www.proofwiki.org/wiki/Number_of_Quadratic_Residues_of_a_Prime

Kun taas $p = 2$, niin jokainen kokonaisluku on neliönjäännös. Selvitetään sitten millä a:n arvoilla yhtälöllä $x^2 \equiv a \pmod 5$ on ratkaisu. Lasketaan luvun x^2 mahdolliset arvot modulo 5:

$x \pmod 5$	$x^2 \pmod 5$
0	0
1	1
2	4
3	4
4	1

Siten a voi olla vain $\equiv 0, 1$ tai $4 \pmod 5$. Toisaalta jokainen näistä käy selvästi. Kun $a \equiv 0 \pmod 5$ ratkaisuja on yksi: $x \equiv 0 \pmod 5$. Kun taas $a \equiv 1 \pmod 5$ ratkaisuja on 2 kappaletta: $x \equiv 1, 4 \pmod 5$. Lopuksi, kun $a \equiv 4 \pmod 5$ ratkaisuja on jälleen 2 kappaletta: $x \equiv 2, 3 \pmod 5$.

6. Millä luvun x arvolla yhtälöllä

$$y^2 \equiv x^3 + 1 \pmod 5$$

on ratkaisu y?

Ratkaisu. Lasketaan lausekkeen $x^3 + 1$ mahdolliset arvot modulo 5:

$x \pmod 5$	$x^3 + 1 \pmod 5$
0	1
1	2
2	4
3	3
4	0

Koska edellisen tehtävän nojalla neliönjäännökset modulo 5 ovat 2 ja 4 (ja lisäksi kongruenssilla $x^2 \equiv 0 \pmod n$ on aina ratkaisu), nähdään, että kongruenssiyhtälö $y^2 \equiv x^3 + 1 \pmod 5$ voisi toteutua, täytyy siis olla $x \equiv 0, 2$ tai $4 \pmod 5$. Toisaalta, jokainen näistä ratkaisee tehtävän kongruenssiyhtälön:

- Kun $x \equiv 0 \pmod 5$, voidaan valita $y \equiv 1 \pmod 5$.
- Kun $x \equiv 2 \pmod 5$, voidaan valita $y \equiv 2 \pmod 5$.
- Kun $x \equiv 4 \pmod 5$, voidaan valita $y \equiv 0 \pmod 5$.