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

1. Tee ketjumurtolukukehitelmä:
(a) $\frac{129}{47}$
(b) $\frac{63}{8}$

Ratkaisu. Suoralla laskulla saadaan:

(a)

$$\frac{129}{47} = 2 + \frac{35}{47} = 2 + \frac{1}{1 + \frac{12}{35}} = 2 + \frac{1}{1 + \frac{1}{2 + \frac{11}{12}}} = 2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{11}}}} = [2; 1, 2, 1, 11]$$

ja

(b)

$$\frac{63}{8} = 7 + \frac{7}{8} = 7 + \frac{1}{1 + \frac{1}{7}} = [7; 1, 7].$$

2. Olkoon RSA:n julkinen eksponentti $(n, e) = (8051, 5)$, missä $8051 = 83 \cdot 97$. Määritä d.

Ratkaisu. Koska 83 ja 97 ovat alkulukuja, niin Eulerin φ-funktion multiplikatiivisuutta käyttäen saadaan $\varphi(8051) = \varphi(83)\varphi(97) = 82 \cdot 96 = 7872$. Tiedetään, että d toteuttaa kongruenssiyhtälön $ed \equiv 1 \pmod{\varphi(n)}$. Tehtävän tilanteessa tämä on yhtäpitävää Diofantoksen yhtälön $5d - 7872k = 1$ kanssa. Etsitään tälle yhtälölle sellainen ratkaisupari (d, k), jossa $d > 0$. Huomataan, että pätee $7872 = 1574 \cdot 5 + 2$ ja $5 = 2 \cdot 2 + 1$. Siten saadaan

$$1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (7872 - 1574 \cdot 5) = 5 \cdot 3149 - 2 \cdot 7872.$$

Näin ollen pari $(d, k) = (3149, 2)$ kelpaa ratkaisuksi. Siis $d = 3149$.

3. Käytetään edellisen tehtävän RSA:ta. Salaa $w = 1023$.

Ratkaisu. Haluttu salaus on $1023^e = 1023^5 \pmod{8051}$. Suoraan laskemalla saadaan

$$1023^5 = 1023^2 \cdot 1023^2 \cdot 1023 \equiv 7950 \cdot 7950 \cdot 1023 \equiv 1340 \cdot 7950 \equiv 1527 \pmod{8051}.$$

Siten kysytty salaus on 1527.

4. Käytetään tehtävän 2 RSA:ta. Vastaanotettu viesti on 1000. Pura kryptaus, eli selvitä kryptattu viesti.

Ratkaisu. Nyt halutaan selvittää $1000^d \pmod{8051}$ eli $1000^{3149} \pmod{8051}$. Tämä saadaan jälleen suoralla laskulla. Ensin havaitaan, että $3149 = 2048 + 1024 + 64 + 8 + 4 + 1$. Siten

$$1000^{3149} = (10^3)^{2^{11}} \cdot (10^3)^{2^{10}} \cdot (10^3)^{2^6} \cdot (10^3)^{2^3} \cdot (10^3)^{2^2} \cdot (10^3)^{2^0}.$$

Nyt

$$\begin{aligned}
(10^3)^{2^0} &\equiv 1000 \pmod{8051} \\
(10^3)^{2^2} = (10^3)^4 &\equiv 7228 \pmod{8051} \\
(10^3)^{2^3} = ((10^3)^{2^2})^2 &\equiv 7228^2 \equiv 1045 \pmod{8051} \\
(10^3)^{2^6} = ((10^3)^{2^3})^8 &\equiv 1045^8 \equiv 4948 \pmod{8051} \\
(10^3)^{2^{10}} = ((10^3)^{2^6})^{16} &\equiv 4948^{16} \equiv 3590 \pmod{8051} \\
(10^3)^{2^{11}} = ((10^3)^{2^{10}})^2 &\equiv 3590^2 \equiv 6500 \pmod{8051}
\end{aligned}$$

Siten

$$1000^{3149} \equiv 1000 \cdot 7228 \cdot 1045 \cdot 4948 \cdot 3590 \cdot 6500 \equiv 6867 \pmod{8051}.$$

Näin ollen kryptattu viesti oli 6867.

5. Jaa luku 159062543 alkutekijöihin (vihje: tämä on kahden alkuluvun tulo ja menetelmä, jolla RSA murtuu, kun luvun n tekijät ovat liian lähellä toisiaan voisi hyvinkin soveltua myös tähän).

Ratkaisu. Merkitään $n := 159062543$. Tällöin $t := \lceil \sqrt{n} \rceil = 12612$ ja $r := \sqrt{t^2 - n} = \sqrt{159062544 - 159062543} = 1$. Nyt

$$n = t^2 - r^2 = (t - r)(t + r) = (12612 - 1)(12612 + 1) = 12611 \cdot 12613.$$

6. Käytä Wienerin hyökkäystä murtaaksesi RSA, kun $n = 43327327$ ja $e = 38501369$.

Ratkaisu. Suoralla laskulla saadaan, että luvulla $\frac{e}{n}$ on ketjumurtolukukehitelmä $[0; 1, 7, 1, 44, 2, 2, 25, 2, 1, 2, 2, 43]$. Tällöin konvergentit $\frac{k}{d}$ ovat $0, 1, \frac{7}{8}, \frac{8}{9}, \ldots$ Tiedetään, että Diofantoksen yhtälö $ed - \varphi(n)k = 1$ on voimassa. Tästä ratkaistaan

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

Ensimmäinen pari (d, k) jolla tämä on kokonaisluku on $(d, k) = (9, 8)$. Tässä tapauksessa $\varphi(n) = 43314040$. Seuraavaksi havaitaan, että jos $n = pq$, missä p ja q ovat alkulukuja, niin $p + q = pq - (p - 1)(q - 1) + 1 = n - \varphi(n) + 1$. Nyt p ja q ovat yhtälön $(x - p)(x - q) = 0$ juuret. Siispä kertomalla sulut auki näemme, että p ja q toteuttavat yhtälön

$$x^2 - (p + q)x + pq = 0$$

eli

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

Sijoittamalla $n = 43327327$ ja yllä ratkaistu $\varphi(n)$ tähän yhtälöön sekä ratkaisemalla saatu toisen asteen yhtälö päädytään juuriin $x = 5741$ ja 7547, mitkä ovat kysytyt n:n alkutekijät.

7. Wienerin hyökkäyksessä oletettiin, että $p < q < 2p$. Miten tilanne muuttuisi (ja erityisesti, mikä raja riittäisi laittaa luvulle d), jos tiedettäisiinkin vain, että $p < q < 8p$?

Ratkaisu. Koska $p < q < 8p$, niin $n - \varphi(n) = p + q - 1 < 9p < 9\sqrt{n}$. Nyt

$$\left| \frac{e}{n} - \frac{k}{d} \right| = \left| \frac{ed - k\varphi(n) + k\varphi(n) - kn}{nd} \right| \leq \frac{1 + k(n - \varphi(n))}{nd} \leq \frac{9\sqrt{n}k}{nd} = \frac{9k}{d\sqrt{n}} < \frac{9}{\sqrt{n}}.$$

Viimeinen epäyhtälö seuraa siitä, että koska $ed - k\varphi(n) = 1$ ja $e < \varphi(n)$, niin $d > k$. Ernvall-Hytösen monisteen "RSA ja Diffie-Hellmannin avaimenvaihtoprotokolla" lauseen 4 nojalla RSA murtuu (koska konvergentit on nopea laskea) kun

$$\frac{9}{\sqrt{n}} \leq \frac{1}{2d^2}.$$

Tästä ratkaistaan $d \leq n^{\frac{1}{4}} \sqrt{\frac{1}{18}}$.