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

Muutama huomautus näistä ratkaisuista:

• Viittaus Ernvallin monisteeseen tarkoittaa kurssisivulta löytyvää Reijo Ernvallin "Koodausteoria"-luentomonistetta.
• Merkintä (a, b) tarkoittaa positiivisten kokonaislukujen a ja b suurinta yhteistä tekijää.

1. Olkoon

$$w = 0000000100100011010001010110011111000100110101011110011011110111 1.$$

Tämä tahdotaan salata DES-järjestelmällä. Suorita ensimmäinen permutaatio, ja jako blokkeihin L_0 ja R_0.

Ratkaisu. Permutoidaan Ernvallin monisteen taulukon mukaisesti:

1	1	0	0	1	1	0	0
0	0	0	0	0	0	0	0
1	1	0	0	1	1	0	0
1	0	1	1	1	1	1	1
1	1	1	1	0	0	0	0
1	0	1	0	1	0	1	0
1	1	1	1	0	0	0	0
1	0	1	0	1	0	1	0

Vasemmanpuoleinen blokki on L_0 ja oikeanpuoleinen on R_0.

Huomautus. Luennolla jako blokkeihin L_0 ja R_0 suoritettiin jakamalla taulukko keskeltä kahtia vaakasuuntaisella suoralla niin, että ylempi blokki on L_0 ja alempi blokki on R_0. Jako on suoritettava niin kuin se on ylläolevassa ratkaisussa tehty, sillä tehtävässä 2 blokkiin L_0 lisätään biteittäin blokki B', jossa on 4 saraketta.

2. Olkoon DES-järjestelmän salainen avain

$$K = 0001001000110100010101100111100010011010101111001101111 0.$$

Laske tarkistusbitit. Määritä lisäksi blokit C_0, D_0, C_1, D_1, muodosta näiden avulla avain K_1 ja käytä sitä laskeaksesi blokit L_1 ja R_1.

Ratkaisu. Lisätään tarkistusbitit paikoille $8, 16, 24, ...$ niin, että jokainen kahdeksan pituinen blokki on pariton:

$$0001001\underline{1}\ 0001101\underline{0}\ 0001010\underline{1}\ 1100111\underline{0}\ 1000100\underline{1}\ 1101010\underline{1}\ 1111001\underline{0}\ 1011110\underline{0}\ .$$

Yllä tarkistusbitit on alleviivattu. Muodostetaan sitten blokit C_0 ja D_0 käyttäen Ernvallin monisteen permutaatioita:

C_0	1	1	1	1	1	0	0
	0	0	1	1	0	1	0
	0	0	1	1	0	0	0
	0	0	0	1	1	1	0

D_0	0	1	0	0	1	0	1
	1	1	0	1	0	1	1
	0	0	1	0	0	1	1
	0	1	0	0	1	1	1

Blokki C_1 saadaan C_0:sta siirtämällä bittejä syklisesti yhden askeleen vasemmalle, ja samoin D_1 muodostetaan D_0:sta:

C_1	1	1	1	1	0	0	0
	0	1	1	0	1	0	0
	0	1	1	0	0	0	0
	0	0	1	1	1	0	1

D_1	1	0	0	1	0	1	1
	1	0	1	0	1	1	0
	0	1	0	0	1	1	0
	1	0	0	1	1	1	0

Nyt K_1 saadaan permutoimalla Ernvallin monisteen sivun 26 mukaisesti:

K_1	0	1	0	1	1	0
	1	1	0	0	0	1
	0	0	1	1	1	0
	1	0	0	0	0	1
	1	0	0	0	1	1
	0	1	0	0	0	1
	1	0	0	0	1	1
	0	0	1	1	1	1

Nyt L_1 ja R_1 saadaan seuraavilla kaavoilla:

$$\begin{cases} L_1 = R_0 \\ R_1 = L_0 + f(R_0, K_1) \end{cases}$$

Siten L_1 on vain edellisen tehtävän R_0. Määritetään seuraavaksi $f(R_0, K_1)$. Muodostetaan tehtävässä 1. lasketusta R_0:sta 48-bittinen Ernvallin monisteen sivun 27 esittämällä tavalla:

0	1	1	0	0	0
0	0	0	0	0	1
0	1	1	0	0	1
0	1	1	1	1	0
1	0	0	0	0	1
0	1	0	1	0	0
0	0	0	0	0	1
0	1	0	1	0	1

Laskemalla tämä yhteen K_1:n kanssa biteittäin modulo 2 saadaan

0	0	1	1	1	0
1	1	0	0	0	0
0	1	0	1	1	1
1	1	1	1	1	1
0	0	0	0	1	0
0	0	0	1	1	1
1	0	0	0	1	0
0	1	1	0	1	0

Tämä on siis $B = B_1B_2 \cdots B_8$, missä

$B_1 = 001110$

$B_2 = 110000$

$B_3 = 010111$

$B_4 = 111111$

$B_5 = 000010$

$B_6 = 000111$

$B_7 = 100010$

$B_8 = 011010$

Seuraavaksi muodostetaan B' käyttämällä S-bokseja. B_1:n ensimmäinen ja viimeinen numero muodostavat luvun 00, mikä binäärijärjestelmän lukuna vastaa kymmenjärjestelmän lukua 0. Neljä keskimmäistä numeroa 0111 binäärijärjestelmässä tulkittuna vastaavat kymmenjärjestelmän lukua 7. Katsotaan sitten Ernvallin monisteen sivun 27 taulukosta S_1 nollannen rivin ja seitsemännen sarakkeen (numerointi alkaa nollasta) yhteinen alkio, joka on 8. Tämän binääriesitys on $B'_1 = 1000$. Määritetään esimerkin vuoksi vielä B'_2. B_2:n ensimmäinen ja viimeinen numero muodostavat binäärissä luvun 10, mikä on kymmenjärjestelmässä 2. Keskimmäiset luvut muodostavat binäärijärjestelmässä luvun 1000, mikä on kymmenjärjestelmässä 8. Katsotaan sitten taulukosta S_2 toisen rivin ja kahdeksannen sarakkeen yhteinen alkio, joka on 5. Binäärissä se on $B'_2 = 0101$. Samalla periaatteella lasketaan:

$B'_3 = 1110$

$B'_4 = 1110$

$B'_5 = 1100$

$B'_6 = 0010$

$B'_7 = 0100$

$B'_8 = 0000$

Siten $B' = B'_1 \cdots B'_8 = 10000101111101110110000010010000000$. Sovelletaan tähän vielä Ernvallin monisteen sivun 28 permutaatiota saadaksemme, että $f(R_0, K_1)$ on

0	0	0	0
0	0	0	1
1	1	1	1
0	1	0	1
0	1	0	1
0	0	0	1
0	1	0	1
0	1	0	0

Nyt, lopultakin, voidaan määrittää $R_1 = L_0 + f(R_0, K_1) \pmod 2 =$

1	1	0	0
0	0	0	1
0	0	1	1
1	1	1	0
1	0	1	0
1	0	1	1
1	0	1	0
1	1	1	0

3. Milloin kahden muuttujan ensimmäisen asteen Diofantoksen yhtälöllä on ratkaisu? Ratkaise Diofantoksen yhtälö

$$8x + 5y = 3.$$

Ratkaisu. Todistetaan ensin, että kahden muuttujan Diofantoksen yhtälöllä $ax + by = c$ on ratkaisu täsmälleen silloin kun $(a, b)|c$.

Todistus. "Vain jos"-suunta on triviaali: jos yhtälö ratkeaa, niin varmasti

$$\frac{a}{(a,b)}x + \frac{b}{(a,b)}y = \frac{c}{(a,b)} \in \mathbb{Z},$$

sillä aina pätee $(a, b)|a$ ja $(a, b)|b$.

Todistetaan sitten "jos"-suunta. Koska $(a, b)|c$, niin on olemassa $m \in \mathbb{Z}$, jolla $c = (a, b) \cdot m$. Bezoutin lemman nojalla luku (a, b) voidaan esittää lukujen a ja b lineaarikombinaationa ts. on olemassa kokonaisluvut k ja ℓ siten, että $ak + b\ell = (a, b)$. Kertomalla yhtälö puolittain luvulla m saadaan $amkx + b\ell my = (a, b) \cdot m = c$. Siten yhtälölle löydettiin ratkaisu $(x, y) = (mk, m\ell)$. □

Ratkaistaan sitten tehtävän yhtälö. Helposti nähdään, että pari $(x, y) = (1, -1)$ toteuttaa tehtävän yhtälön. Olkoon $(x, y) \neq (1, -1)$ jokin yhtälön ratkaisu[1]. Merkitään $t = 1 - x$ ja $h = -1 - y$. Tällöin $8t + 5h = -8x - 5y + 3 = 0$ eli $8t = -5h$. Koska $(8, 5) = 1$, niin tästä seuraa, että $t = 5\ell$, $h = -8\ell$ jollakin $\ell \in \mathbb{Z}$. Siten yleiseksi ratkaisuksi saadaan $(x, y) = (1-t, -1-h) = (1-5\ell, -1+8\ell)$, jollakin $\ell \in \mathbb{Z}$ (myös erikoisratkaisu $(x, y) = (1, -1)$ on mukana tässä ratkaisuperheessä).

4. Muistele, mikä on Fermat'n pieni lause. Laske $3^{58} \pmod{59}$.

Ratkaisu. Fermat'n pienen lauseen mukaan $a^{p-1} \equiv 1 \pmod{p}$, kun p on alkuluku ja $(a, p) = 1$ (yhtäpitävästi $a^p \equiv a \pmod{p}$, kaikilla alkuluvuilla p ja kokonaisluvuilla a). Koska 59 on alkuluku ja $(3, 59) = 1$, niin Fermat'n pieni lause antaa suoraan $3^{58} \equiv 1 \pmod{59}$.

5. Mikä onkaan primitiivinen juuri? Entä kertaluku? Määritä primitiiviset juuret modulo 7 sekä redusoidun jäännössysteemin kaikkien jäsenten kertaluvut.

Ratkaisu. Luku g on primitiivinen juuri modulo n, jos jokainen n:n kanssa yhteistekijätön luku on kongruentti jonkin g:n potenssin kanssa modulo[2] n. Luvun a kertaluku modulo n, merkitään $\mathrm{ord}_n a$, on pienin postiivinen kokanaisluku ℓ, jolle pätee $a^\ell \equiv 1 \pmod{n}$. Kerrataan vielä redusoidun jäännössysteemin määritelmä: Joukko $\mathcal{R} \subset \mathbb{Z}$ on redusoitu jäännössysteemi modulo m, jos seuraavat kolme ehtoa pätevät:

- $|\mathcal{R}| = \varphi(m)$
- $(a, m) = 1$ kaikilla $a \in \mathcal{R}$
- $a \not\equiv b \pmod{m}$ kaikilla $a \neq b$, $a, b \in \mathcal{R}$.

Koska 7 on alkuluku, niin sen redusoitu jäännössysteemi on selvästi $\{1, 2, 3, 4, 5, 6\}$. Lasketaan alkioiden kertaluvut:

- $1^1 \equiv 1 \pmod{7}$, joten $\mathrm{ord}_7(1) = 1$.
- $2^1 \equiv 2 \pmod{7}$, $2^2 \equiv 4 \pmod{7}$, $2^3 \equiv 1 \pmod{7}$, joten $\mathrm{ord}_7(2) = 3$.
- $3^1 \equiv 3 \pmod{7}$, $3^2 \equiv 2 \pmod{7}$, $3^3 \equiv 6 \pmod{7}$, $3^4 \equiv 4 \pmod{7}$, $3^5 \equiv 5 \pmod{7}$, $3^6 \equiv 1 \pmod{7}$, joten $\mathrm{ord}_7(3) = 6$ ja 3 on primitiivinen juuri modulo 7.
- $4^1 \equiv 4 \pmod{7}$, $4^2 \equiv 2 \pmod{7}$, $4^3 \equiv 1 \pmod{7}$, joten $\mathrm{ord}_7(4) = 3$.
- $5^1 \equiv 5 \pmod{7}$, $5^2 \equiv 4 \pmod{7}$, $5^3 \equiv 6 \pmod{7}$, $5^4 \equiv 2 \pmod{7}$, $5^5 \equiv 3 \pmod{7}$, $5^6 \equiv 1 \pmod{7}$, joten $\mathrm{ord}_7(5) = 6$ ja 5 on primitiivinen juuri modulo 7.

[1] Tällainen ratkaisu on olemassa, esim. $(x, y) = (6, -9)$

[2] Voidaan osoittaa, että primitiivinen juuri on olemassa vain kun $n = 1, 2, 4, p^k, 2p^k$, missä p on pariton alkuluku ja k on positiivinen kokonaisluku.

• $6^1 \equiv 6 \pmod 7$, $6^2 \equiv 1 \pmod 7$, joten $\mathrm{ord}_7(6) = 2$.

6. Mikä on Eulerin φ-funktio? Laske

$$\varphi(29), \varphi(30), \varphi(16).$$

Ratkaisu. Eulerin φ-funktio määritellään seuraavasti: Luku $\varphi(n)$ on niiden positiivisten lukujen k lukumäärä, joilla $k \leq n$ ja $(n,k) = 1$. Voidaan osoittaa (katso esim. s. 27 T.M. Apostolin kirjasta Introduction to Analytic Number Theory), että jos n:llä on alkutekijähajotelma $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, niin

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Tämän kaavan avulla voidaan helposti laskea kysytyt φ-funktion arvot:

$$\varphi(29) = 29 \left(1 - \frac{1}{29}\right) = 28,$$

$$\varphi(30) = \varphi(2 \cdot 3 \cdot 5) = 30 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 8,$$

$$\varphi(16) = \varphi(2^4) = 16 \left(1 - \frac{1}{2}\right) = 8.$$

7. Mitä kertookaan Eulerin lause? Laske $7^{25} \pmod{30}$.

Ratkaisu. Eulerin lauseen mukaan $a^{\varphi(n)} \equiv 1 \pmod n$, kun $(a,n) = 1$. Tehtässä 6. on laskettu, että $\varphi(30) = 8$. Koska $(7, 30) = 1$, niin Eulerin lauseen mukaan $7^8 \equiv 1 \pmod{30}$. Nyt saadaan

$$7^{25} = 7 \cdot (7^8)^3 \equiv 7 \cdot 1^3 \equiv 7 \pmod{30}.$$