Luentorunko

SALAUSMENETELMÄT
801346A, 4 op

Pohjautuu Leena Leinosen, Marko Rinta-ahon, Tapani Matala-ahon ja
Keijo Väänäsen luentoihin

Sisältö

HUOM: Ilmoittautukaa Web-oodiissa kurssille, jotta saisitta tietoja mahdollisista muutoksista ja peruutuksista.

Luennot: Aloitetaan 14:10
Ke 14–16 IT133
To 14–16 IT138

LUENNOT LOPPUU VIIKOLLA 41.

Loppukoe: 29.10.2012, 26.11.2012

Linkkejä:
Johdatus matemaattiseen päättelyyn
Kirjallisuus:

1 Johdanto

Tällä kurssilla tarkastellaan menetelmiä, jotka mahdollistavat tiedon siirtämisen tai tallentamisen niin, että ainoastaan tarkoitettu vastaanottaja saa viestin selville. Lähettäjän tehtävänä on salakirjoittaa (encrypt) selväkielinen teksti (plaintext) salakirjoitukseksi (cryptotext) ja vastaanottajan tehtävänä puolestaan avata (decrypt) salakirjoitus selväkieliseksi tekstiksi. Menettelyn tulee olla sellainen, että mahdollinen salakirjoituksen sieppaaja ei kykene murtamaan sitä eli selvittämään selväkielistä tekstiä, ainakaan nopeasti.

Aikaisemmin salakirjoituksia tarvittiin lähinnä sotilaallisiin ja diplomaattisiin tarkoituksiin. Kuluneiden noin 30 vuoden aikana tietokoneisiin perustuvan tiedonvälityksen yleistyminen on merkinnyt sitä, että salausmenetelmiä tarvitaan päivittäin hyvin monilla muillakin yhteiskunnan alueilla kuten pankeissa ja yrityksissä.

Selväkielinen teksti ja salakirjoitettu teksti kirjoitetaan käyttämällä jotakin aakkostoa (kirjaimet, numerot, muut merkit). Suomen- ja englanninkielisellä aakkostolla tarkoitetaan tällä kurssilla seuraavia aakkostoja:

S) Suomenkielinen aakkosto , 29 kirjanta.

E) Englanninkielinen aakkosto, 26 kirjainta.

```
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
0 1 2 3 4 5 6 7 8 9 10111213141516171819202122232425
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
```

Jotta matemaattisia menetelmiä voitaisiin käyttää, kirjaimet korvataan usein luvuilla. Selväkielinen teksti ja salakirjoitus jaetaan viestiyksiköihin ja salaaminen tehdään yksikkö kerrallaan. Viestiyksikkö voi olla kirjain (kuten yllä olevassa esimerkissä), kirjainpari tai tietyn pituinen kirjainjono. Salakirjoittamiseen käytetään yleensä bijektiivistä funktiota $E\colon P \to C$, missä

$$P = \{\text{selväkieliset viestiyksiköt}\} = \{m\},$$
$$C = \{\text{salakirjoitetut viestiyksiköt}\} = \{c\}.$$

Avaaminen tapahtuu tällöin käänteisfunktion $D = E^{-1}$ avulla. Salakirjoitusjärjestelmään kuuluvat siis: (i) P, (ii) C, (iii) avainjoukko $K = \{k\}$, missä kukin avain k määrää salausfunktion E_k ja avausfunktion D_k, joille $D_k(E_k(m)) = m$. Lähettäjä tuntee ennakolta funktion E_k ja vastaanottaja funktion D_k, jolloin järjestelmä toimii seuraavan kaavion mukaisesti.

$$\begin{array}{ccc} A & \longrightarrow & B \\ \boxed{m \mapsto E_k(m) = c} & \xrightarrow{c} & \boxed{D_k(c) = m} \\ & \updownarrow & \\ & E & \end{array}$$

(E =salakuuntelija, eavesdropper, murtaja, breaker)

Hyvältä salakirjoitusjärjestelmältä edellytetään:

1) $E_k(m)$ ja $D_k(c)$ voidaan laskea helposti.

2) Jollei tunneta funktiota D_k, niin selväkielinen viesti m ei selviä salakirjoituksesta c, eli sieppaajalla on vaikea tehtävä.

Kaikissa perinteisissä salakirjoitusjärjestelmissä D_k saadaan välittömästi funktiosta E_k, ei tosin aina niin helposti kuin äskeisessä esimerkissä. Näin ollen lähettäjän ja vastaanottajan tulee sopia jollakin tavalla avaimesta ja pitää tämä sopimuksensa salassa muilta. Tästä syystä näitä järjestelmiä kutsutaan yksityisen avaimen salakirjoituksiksi. Vuosina 1976–1978 kehitettiin ensimmäiset julkisen avaimen järjestelmät, joille on ominaista se, että E_k ei paljasta funktiota D_k, ainakaan helposti. Nämä perustuvat ns. yksisuuntaisiin funktioihin (one-way function), joiden käänteisfunktiota on käytännössä mahdotonta tai ainakin hyvin vaikeaa määrittää. Useimmat käytössä olevat salakirjoitusmenetelmät perustuvat lukuteorian tuloksiin. Tästä syystä kurssi aloitetaan kertaamalla eräitä lukuteorian alkeiden tuloksia.

Esimerkki 1.1. Esimerkkinä käy Caesarin yhteenlaskumenetelmä, jossa salakirjoitus tehdään siirtämällä kirjaimia k askelta eteenpäin. Esimerkiksi $k = 17$ antaa seuraavaa:

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

Selväteksti: prime
Salattu: GIZDV

2 Perinteisiä salakirjoitusmenetelmiä

2.1 Caesar ja sen yleistyksiä

2.1.1 Caesarin yhteenlaskumenetelmä

On yksinkertaista asettaa joukon $\mathbb{Z}_n$ alkiot vastaamaan n-kirjaimisen aakkoston symboleja. Esimerkiksi englanninkielistä aakkostoa vastaa $\mathbb{Z}_{26}$ eli

```
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
0 1 2 3 4 5 6 7 8 9 10111213141516171819202122232425
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
```

missä jäännösluokkien modulo $n = 26$ yläviivat on jätetty pois. Voidaan sopia, että selkoviesti kirjoitetaan pienillä kirjaimilla ja SALATTU VIESTI ISOILLA KIRJAIMILLA.

Aikaisemmin tarkastellun Caesarin menetelmän salausfunktio E_k ja avausfunktio D_k ovat yllä olevin merkinnöin yksinkertaisesti

$$E_k(x) = x + k \quad \text{ja} \quad D_k(x) = x - k,$$

missä laskutoimitukset tehdään joukossa $\mathbb{Z}_N$.

2.1.2 Affiinikuvaus

Tarkastellaan nyt yleisempää järjestelmää, missä yhteenlasku korvataan *affiinilla* kuvauksella. Valitaan tätä varten $a \in \mathbb{Z}_n^*$ ja $b \in \mathbb{Z}_n$. Avaimena on nyt pari (a, b) ja salausfunktio on

$$E(x) = E_{a,b}(x) = ax + b, \quad E : \mathbb{Z}_n \to \mathbb{Z}_n.$$

Avainten lukumäärä on tällöin $\varphi(n) \cdot n$. Erikoistapauksina

- $a = 1$ antaa Caesarin yhteenlaskumenetelmän, $E(x) = x + b$
- $b = 0$ antaa ns. kertolasku-Caesarin, $E(x) = ax$.

Lause 2.1. *Kuvaus* $E\colon \mathbb{Z}_n \to \mathbb{Z}_n$ *on bijektio ja ja avausfunktioksi saadaan*

$$D(y) = D_{a,b}(y) = a^{-1}y - a^{-1}b. \tag{1}$$

Todistus: Edellä $a \in \mathbb{Z}_n^*$, joten $a^{-1} \in \mathbb{Z}_n^*$ on olemassa.
Asetetaan nyt

$$E(x_1) = E(x_2) \quad \Rightarrow \quad ax_1 + b = ax_2 + b \quad \Rightarrow \quad ax_1 = ax_2 \tag{2}$$

$$\Rightarrow \quad a^{-1}ax_1 = a^{-1}ax_2 \quad \Rightarrow \quad x_1 = x_2. \tag{3}$$

Siten $E\colon \mathbb{Z}_n \to \mathbb{Z}_n$ on injektio ja edelleen bijektio Lauseen 11.1 nojalla.
Asetetaan seuraavaksi

$$E(x) = y \quad \Rightarrow \quad ax + b = y \quad \Rightarrow \quad x = a^{-1}(y - b) = D(y). \quad \square \tag{4}$$

Yhteenveto affiinista järjestelmästä:

- $P = C = \mathbb{Z}_n$
- $K = \{(a, b)\}$, missä $a \in \mathbb{Z}_n^*$ ja $b \in \mathbb{Z}_n$
- salausfunktio $E(x) = ax + b$
- avausfunktio $D(y) = a^{-1}y - a^{-1}b$.

Affiini järjestelmä voidaan murtaa seuraavilla tavoilla:

- Brute de force. Kokeillaan kaikki avaimet.
- Frekvenssianalyysi. Käytetään hyväksi kirjainten esiintymistiheyksiä.

Alla olevassa taulukossa on esitetty suomen ja englannin kielen kymmenen yleisintä kirjainta esiintymistiheyksineen.

suomi				englanti			
kirjain	%	kirjain	%	kirjain	%	kirjain	%
A	11,5	S	6,6	e	13,11	r	6,83
I	10,5	L	5,9	t	10,47	i	6,35
T	9,7	O	5,5	a	8,15	s	6,10
N	9,1	Ä	5,2	o	8,00	h	5,26
E	8,4	K	4,9	n	7,10	d	3,79

Saksan kielen kymmenen yleisintä kirjainta ovat E, N, I, S, R, A, T, D, H, U ja ranskan kielen E, S, A, I, T, N, R, U, L, O. Tiheydet ovat suuntaa-antavia ja vaihtelevat hieman tekstistä riippuen. Yleisyysjärjestyskin voi poiketa hieman lähteestä riippuen.

Esimerkki 2.2. Avaa Caesarin yhteenlaskumenetelmällä laadittu englanninkielinen salakirjoitus

`ALYUNYMNWIGGIHXCPCMIL`.

Mikä on ollut avain?
1. Ylläolevan nojalla englanninkielen Top-6 kirjainjoukko on

$$E_M := \{\texttt{e,t,a,o,n,r}\} = \{4, 19, 0, 14, 13, 17\}. \tag{5}$$

2. Salatun tekstin Top-6 joukoksi saadaan

$$C_M := \{\texttt{I,Y,G,M,C,L}\} = \{8, 24, 6, 12, 2, 11\}. \tag{6}$$

3. Tutkitaan miten joukko E_M kuvautuu joukolle C_M Caesar-salauksessa.
On todennäköistä, että:
3a. Kirjain e kuvautuu kirjaimelle I;
tai
3b. Kirjain e kuvautuu kirjaimelle Y;
tai ...
3a. Tässä salausfunktio on

$$E_4(\texttt{e}) = \texttt{I}, \quad \Rightarrow \quad E_4(E_M) = \{8, 23, 4, 18, 17, 21\}, \tag{7}$$

joten

$$E_4(E_M) \cap C_M = \{8\}. \tag{8}$$

Tämä on epätodennäköistä!
3b. Tässä salausfunktio on

$$E_{20}(\mathtt{e}) = \mathtt{Y}, \quad \Rightarrow \quad E_{20}(E_M) = \{24, 13, 20, 8, 7, 11\}, \tag{9}$$

joten

$$E_{20}(E_M) \cap C_M = \{24, 8, 11\}. \tag{10}$$

Nyt jo puolet Top-joukoista täsmää, joten yritetään avausta dekryptausfunktiolla

$$D_{20}(y) = y - 20 = y + 6, \tag{11}$$

jolloin aluksi saadaan

$$D_{20}(\mathtt{A}) = \mathtt{g}, \quad D_{20}(\mathtt{L}) = \mathtt{r}, \quad D_{20}(\mathtt{Y}) = \mathtt{e}, \quad D_{20}(\mathtt{U}) = \mathtt{a}, \quad D_{20}(\mathtt{N}) = \mathtt{t}. \tag{12}$$

Tämä on selkokieltä, joten jatketaan avausta. Siten selkoviesti on ollut

$$\mathtt{greatestcommondivisor} \tag{13}$$

ja kryptausavain $k = 20$.

Esimerkki 2.3. Seuraava englanninkielestä salattu viesti

VCLMPCAVESVFYDVOVIZHPCYXAXGBDATYZ

on muodostettu affiinilla järjestelmällä.
Mikä on selkokielinen teksti ja kryptausfunktio?
1. Ylläolevan nojalla englanninkielen Top-6 kirjainjoukko on

$$E_M := \{\mathtt{e,t,a,o,n,r}\} = \{4, 19, 0, 14, 13, 17\}. \tag{14}$$

2. Salatun tekstin Top-6 joukoksi saadaan

$$C_M := \{\mathtt{V,C,A,Y,D,Z}\} = \{21, 2, 0, 24, 3, 25\}. \tag{15}$$

3. Tutkitaan miten joukko E_M kuvautuu joukolle C_M affiinilla kuvauksella. On todennäköistä, että:
3a. Kirjain e kuvautuu kirjaimelle V;
ja
4a. Kirjain t kuvautuu kirjaimelle C;
tai
4b. Kirjain a kuvautuu kirjaimelle C;
tai
4c. Kirjain o kuvautuu kirjaimelle C;
tai
4d. Kirjain n kuvautuu kirjaimelle C;
tai ...
5. Olkoon salausfunktio

$$E(x) = ax + b, \quad a \in \mathbb{Z}_{26}^*, \ b \in \mathbb{Z}_{26}. \tag{16}$$

Tarvitaan siis yhtälöpari lukujen a ja b ratkaisemiseen.
3a+4a...

2.2 Sijoitusjärjestelmät

Edellä mainitut järjestelmät ovat erikoistapauksia yksinkertaisesta sijoitusjärjestelmästä. Siinä on avainjoukkona joukon $\mathbb{Z}_n$ permutaatioiden muodostama joukko S_n, jonka alkiot σ kirjoitetaan usein muotoon

$$\sigma = \begin{pmatrix} 0 & 1 & \dots & n-1 \\ \sigma(0) & \sigma(1) & \dots & \sigma(n-1) \end{pmatrix}.$$

Nämä ovat bijektioita, joten niillä on käänteiskuvaus σ^{-1}.

Yksinkertainen sijoitusjärjestelmä:

- $P = C = \mathbb{Z}_n$
- $K = S_n$
- salausfunktio $E_\sigma(x) = \sigma(x)$

- avausfunktio $D_\sigma(y) = \sigma^{-1}(y)$.

Joukon S_n alkioiden lukumäärä on $n!$, joten avaimia on runsaasti.

Yksinkertainen sijoitusjärjestelmä on murrettavissa kirjainten esiintymistiheyksiä tutkimalla, koska kirjaimen x kuva $E(x)$ on sama koko ajan. Tästä johtuen on kehitetty myös *moniaakkosjärjestelmiä*, joista esimerkkinä tarkastellaan Vigenéren järjestelmää.

2.3 Vigenéren järjestelmä

Vigenéren järjestelmän avain koostuu useasta Caesarin menetelmän avaimesta, joita sovelletaan jaksollisesti. Oletetaan, että $k_1, k_2, \ldots, k_r \in \mathbb{Z}_n$. Jaetaan selväkielinen teksti r:n pituisiin osiin $x_1 x_2 \ldots x_r$. Kunkin osan i:s kirjain x_i salakirjoitetaan Caesarin salausfunktion E_{k_i} avulla:

$$\text{selvä} \qquad x_i \mapsto E_{k_i}(x_i) = x_i + k_i = y_i \qquad \text{sala.}$$

Vastaava avausfunktio on $D_{k_i}(y_i) = y_i - k_i$. Avaimet k_i annetaan usein avainsanan avulla.

Vigenéren järjestelmässä sama kirjain kuvautuu eri kirjaimiksi paikasta riippuen, joten yksinkertainen kirjainten esiintymistiheyteen perustuva analyysi ei toimi. Kuitenkin, jos avaimen pituus r selviää, voidaan kukin k_i murtaa erikseen kuten Caesarissa. Myös avaimen pituuden määrittämiseksi on olemassa menetelmiä.

2.4 Salakirjoitus matriiseilla

Jos viestiyksikön pituus on $r > 1$ kirjainta, on luontevaa tarkastella viestiyksikköjä joukon $\mathbb{Z}_n^r$ vektoreina ja käyttää salauksessa $r \times r$-matriiseja. Rajoitutaan seuraavassa tapaukseen $r = 2$. Kerrataan lyhyesti matriisien laskusääntöjä:

- Joukon $\mathbb{Z}_n^2$ alkiot ovat $\begin{bmatrix} x \\ y \end{bmatrix}$.

- 2×2-matriisit ovat $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{Z}_n)$.
- Kaksi matriisia ovat identtiset, jos ja vain jos niissä samoilla paikoilla olevat alkiot ovat identtiset, ts.

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \iff a_{ij} = b_{ij} \text{ kaikilla } i, j \in \{1, 2\}.$$

- Yhteenlasku on määritelty seuraavasti:

$$\begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} x+u \\ y+v \end{bmatrix}, \qquad \begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} x & u \\ y & v \end{bmatrix} = \begin{bmatrix} a+x & b+u \\ c+y & d+v \end{bmatrix}.$$

- Skalaarilla kertominen on määritelty seuraavasti:

$$a \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax \\ ay \end{bmatrix}, \qquad u \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} ua & ub \\ uc & ud \end{bmatrix}.$$

- Kertolasku on määritelty seuraavasti:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax+by \\ cx+dy \end{bmatrix}, \qquad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x & u \\ y & v \end{bmatrix} = \begin{bmatrix} ax+by & au+bv \\ cx+dy & cu+dv \end{bmatrix}.$$

  Kertolasku ei ole vaihdannainen.
- Yksikkömatriisi $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ on kertolaskun neutraalialkio.
- Matriisin $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ käänteismatriisi on matriisi A^{-1}, jolle $AA^{-1} = A^{-1}A = I$, mikäli tällainen matriisi on olemassa. Voidaan osoittaa, että A^{-1} on olemassa, jos ja vain jos

$$D = \det A = |A| = ad - bc \in \mathbb{Z}_n^*. \tag{17}$$

  Tällöin

$$A^{-1} = D^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Lause 2.4. *Olkoon*

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{Z}_n), \quad a, b, c, d \in \mathbb{Z}_n, \quad \det A = ad - bc \in \mathbb{Z}_n^* \tag{18}$$

ja

$$B = \begin{bmatrix} e \\ f \end{bmatrix} \in \mathbb{Z}_n^2.$$

Tällöin affiini kuvaus

$$E\colon \mathbb{Z}_n^2 \to \mathbb{Z}_n^2,\ E(X) = AX + B, \tag{19}$$

on bijektio, jonka käänteiskuvaus on

$$D\colon \mathbb{Z}_n^2 \to \mathbb{Z}_n^2,\ D(Y) = A^{-1}(Y - B). \tag{20}$$

Todistus: Edellä $\det A \in \mathbb{Z}_n^*$, joten $A^{-1} \in M_2(\mathbb{Z}_n)$ on olemassa.
Asetetaan nyt

$$E(X_1) = E(X_2) \quad \Rightarrow \quad AX_1 + B = AX_2 + B \quad \Rightarrow \quad AX_1 = AX_2 \tag{21}$$

$$\Rightarrow \quad A^{-1}AX_1 = A^{-1}AX_2 \quad \Rightarrow \quad IX_1 = IX_2 \quad \Rightarrow \quad X_1 = X_2. \tag{22}$$

Siten $E\colon \mathbb{Z}_n^2 \to \mathbb{Z}_n^2$ on injektio. Koska

$$\#\mathbb{Z}_n^2 = n^2 < \infty, \tag{23}$$

niin Lauseen 11.1 nojalla $E\colon \mathbb{Z}_n^2 \to \mathbb{Z}_n^2$ on bijektio.
Asetetaan seuraavaksi

$$E(X) = Y \quad \Rightarrow \quad AX + B = Y \quad \Rightarrow \quad X = A^{-1}(Y - B) = D(Y). \quad \square \tag{24}$$

Matriisisalakirjoitus:

- $P = C = \mathbb{Z}_n^2 = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} \;\middle|\; x, y \in \mathbb{Z}_n \right\}$

- avain $\{A, B\}$, $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $ad - bc \in \mathbb{Z}_n^*$, $B = \begin{bmatrix} e \\ f \end{bmatrix} \in \mathbb{Z}_n^2$
- salausfunktio $E(X) = AX + B$
- avausfunktio $D(Y) = A^{-1}Y - A^{-1}B$.

Esimerkki 2.5. Olkoon

$$A = \begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix} \in M_2(\mathbb{Z}_{26}).$$

Lasketaan determinantti

$$\det A = -5 \in \mathbb{Z}_{26}^*,$$

joten käänteismatriisi on olemassa ja

$$A^{-1} = \begin{bmatrix} 14 & 11 \\ 17 & 10 \end{bmatrix} \in M_2(\mathbb{Z}_{26}).$$

Kryptaus- ja dekryptausfuntiot

$$E(X) = AX, \quad D(Y) = A^{-1}Y.$$

Salataan selkoteksti

$$P = \begin{bmatrix} 13 \\ 14 \end{bmatrix}$$

seuraavasti

$$E(P) = AP = \begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix} \begin{bmatrix} 13 \\ 14 \end{bmatrix} = \begin{bmatrix} 16 \\ 21 \end{bmatrix} := C.$$

Avataan kryptoteksti C seuraavasti

$$D(C) = A^{-1}C = \begin{bmatrix} -12 & 11 \\ -9 & 10 \end{bmatrix} \begin{bmatrix} -10 \\ -5 \end{bmatrix} = \begin{bmatrix} 13 \\ 14 \end{bmatrix} = P.$$

Huomautus 2.6. Jos valitaan $A = I = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$, niin $E(X) = X + B$, joten kyseessä on Vigenéren järjestelmä, missä $r = 2$. Vastaavasti matriisisalakirjoituksen erikoistapauksena saadaan yleinen Vigenéren järjestelmä, jos tarkastellaan $r \times r$-matriiseja.

Tarkastellaan nyt matriisisalakirjoituksen murtamista. Oletetaan ensin, että $B = \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right]$ ja tunnetaan kaksi paria selväkielistä tekstiä ja vastaavat salakirjoitukset. Tämä on mahdollista esimerkiksi niin, että sieppaaja onnistuu jotenkin lähettämään tekstiä tarkasteltavan kanavan kautta. Olkoot tunnetut selväkieliset tekstit

$$P_1 = \begin{bmatrix} p_{11} \\ p_{21} \end{bmatrix} \quad \text{ja} \quad P_2 = \begin{bmatrix} p_{12} \\ p_{22} \end{bmatrix}$$

sekä vastaavat salakirjoitukset

$$C_1 = \begin{bmatrix} c_{11} \\ c_{21} \end{bmatrix} \quad \text{ja} \quad C_2 = \begin{bmatrix} c_{12} \\ c_{22} \end{bmatrix}.$$

Tällöin $C_1 = AP_1$ ja $C_2 = AP_2$ eli

$$C = AP, \quad \text{missä } P = \begin{bmatrix} P_1 & P_2 \end{bmatrix} = \begin{bmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{bmatrix} \quad \text{ja}$$

$$C = \begin{bmatrix} C_1 & C_2 \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix}.$$

Jos nyt P_1 ja P_2 on valittu niin, että $\det P \in \mathbb{Z}_n^*$, niin P^{-1} on olemassa. Tällöin saadaan

$$A = CP^{-1}, \quad A^{-1} = PC^{-1}$$

ja järjestelmä on murrettu.

Tapauksessa $B \neq \left[\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right]$ murtamiseen tarvitaan vielä kolmas pari P_3 ja C_3:

$$C_1 = AP_1 + B,\ C_2 = AP_2 + B,\ C_3 = AP_3 + B.$$

Tällöin päästään yllä olevan kaltaiseen tilanteeseen vähentämällä kolmas yhtälö kahdesta ensimmäisestä:

$$C_1 - C_3 = A(P_1 - P_3),\ C_2 - C_3 = A(P_2 - P_3).$$

Jos tästä saadaan A, niin sen jälkeen $B = C_1 - AP_1$.

Esimerkki 2.7. Olkoot tunnetut selväkieliset tekstit

$$P_1 = \begin{bmatrix} 3 \\ 4 \end{bmatrix} \quad \text{ja} \quad P_2 = \begin{bmatrix} 4 \\ 7 \end{bmatrix}$$

sekä vastaavat salakirjoitukset

$$C_1 = \begin{bmatrix} 2 \\ 1 \end{bmatrix} \quad \text{ja} \quad C_2 = \begin{bmatrix} 1 \\ 2 \end{bmatrix}.$$

a) Murra järjestelmä eli määrää käytetty salausmatriisi ja sitä vastaava avausmatriisi.
b) Dekryptaa salattu viesti

$$C_3 = \begin{bmatrix} 3 \\ 2 \end{bmatrix}.$$

3 Julkisen avaimen salakirjoitus (public key cryptography)

3.1 Yleinen periaate/General principle

Nykyaikaisissa tiedonvälitysjärjestelmissä perinteisillä salakirjoitusmenetelmillä on esimerkiksi seuraavat ongelmat:

- Avaimista sopiminen ja niiden välittäminen. Jos verkossa on n käyttäjää, tarvitaan $\binom{n}{2} = n(n-1)/2$ avainta. Jos joku käyttäjä haluaa vaihtaa avaimensa (tai uusi käyttäjä liittyy verkkoon), tarvitaan $n-1$ (tai n) sopimusta uusista avaimista.

- Allekirjoitusongelma, koska normaali allekirjoitus on korvattava jotenkin.

Aikaisemmin, kun salausta käytettiin lähinnä sotilaallisissa tai diplomaattisissa tarkoituksissa, nämä seikat eivät tuottaneet suurta ongelmaa. Vuonna 1976 Diffie ja Hellman esittivät ajatuksen julkisen avaimen järjestelmistä, joissa yllä mainitut ongelmat on selvitetty. Tällaisessa järjestelmässä kukin

käyttäjä U muodostaa oman salausmenettelynsä E_U ja avausmenettelynsä D_U, jotka toteuttavat ehdon

$$D_U(E_U(m)) = m \quad \text{kaikilla selväkielisillä viestiyksiköillä } m. \tag{25}$$

Kukin käyttäjä U julkaisee salausmenettelynsä E_U avainkirjassa, joka on kaikkien käytettävissä. Avausmenettelyn D_U käyttäjä U pitää vain omana tietonaan. Jos A haluaa lähettää selväkielisen viestiyksikön m käyttäjälle B, hän etsii avainkirjasta käyttäjän B salakirjoitusmenettelyn E_B ja salakirjoittaa viestinsä sen avulla, ts. $c = E_B(m)$. Kun B saa salakirjoitetun viestin c, hän saa ehdon (25) avulla viestin m selville käyttämällä (salaista) avausmenettelyään D_B:

$$D_B(c) = D_B(E_B(m)) = m.$$

Jotta menettely olisi toimiva ja salaisuus säilyisi, tarvitaan seuraavat ehdot, joiden tulee olla voimassa kaikille käyttäjille U:

$$\text{Menettelyt } E_U \text{ ja } D_U \text{ ovat nopeita eivätkä tarvitse liian paljon muistia.} \tag{26}$$

$$\text{Menettelyn } E_U \text{ avulla on käytännössä mahdotonta määrittää menettelyä } D_U^*, \text{ jolle } D_U^*(E_U(m)) = m \text{ kaikilla } m \in P. \tag{27}$$

Ominaisuus (27) säilyttää järjestelmän salaisena ja mahdollistaa salausmenettelyn julkaisemisen avainkirjassa. Jos joku käyttäjistä vaihtaa avaimensa, riittää vaihtaa uusi E_U avainkirjaan. Uuden käyttäjän mukaantulo on yhtä yksinkertaista. Edellä mainittu menettely muodostetaan usein käyttämällä yksisuuntaista funktiota tai salaovifunktiota.

Määritelmä 3.1. Funktiota f sanotaan *yksisuuntaiseksi, one-way*, jos sen arvot ovat helposti laskettavissa ja käänteisfunktion f^{-1} (joka on olemassa) määrääminen on hyvin vaikeaa. Yksisuuntaista funktiota sanotaan *salaovifunktioksi*, jos sen käänteisfunktio on helppoa määrätä jonkin lisätiedon (salaovi, trapdoor) avulla.

Funktiota ei yleensä onnistuta todistamaan yksisuuntaiseksi, joten joudutaan käyttämään funktioita, joiden uskotaan olevan yksisuuntaisia. Tällaisten funktioiden muodostaminen perustuu usein vaikeisiin ja paljon tutkittuihin lukuteorian ongelmiin, esimerkiksi RSA-järjestelmässä suurten lukujen tekijöihin jakamisen vaikeuteen. Jos käytössä on salaovifunktioita f_U, niin voidaan muodostaa ehdot (25)–(27) toteuttava järjestelmä valitsemalla

$$E_U = f_U \quad \text{ja} \quad D_U = f_U^{-1}.$$

Koska julkisen avaimen salakirjoitus vaatii yleensä paljon enemmän aikaa kuin perinteiset menetelmät, sitä käytetään usein perinteisen menetelmän ohella avainten vaihdossa eli käytettävän perinteisen menetelmän avaimet vaihdetaan julkisen avaimen menetelmällä.

3.2 Allekirjoitussopimus/Signature protocol

Tarkastellaan nyt allekirjoitusongelmaa, jonka ratkaisemiseksi asetetaan kaksi uutta vaatimusta, joiden tulee olla voimassa kaikille käyttäjille U:

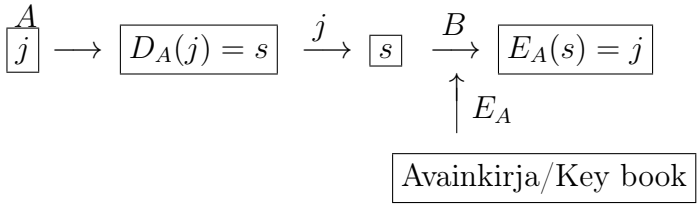
$$E_U(D_U(j)) = j \quad \text{kaikilla viesteillä } j. \tag{28}$$

$$\text{Menettelyn } E_U \text{ avulla on käytännössä mahdotonta määrittää menettelyä } D_U^*, \text{ jolle } E_U(D_U^*(j)) = j \text{ kaikilla } j \in C. \tag{29}$$

Julkisen avaimen järjestelmässä on usein $P = C$ sama kaikilla käyttäjillä. Jos A lähettää käyttäjälle B selväkielisen viestin, hän lähettää viestin j allekirjoituksen muodossa $S = D_A(J)$, jolloin B etsii avainkirjasta menettelyn E_A ja laskee ehdon (28) avulla

$$E_A(s) = E_A(D_A(j)) = j.$$

Allekirjoituksen (signature) muodostaa pari (j, s). Menettely edellyttää ehtoja (26), (28) ja (29), erityisesti ehto (29) varmistaa, että vain A voi toimia lähettäjänä. Käyttäjä A ei voi myöskään jälkikäteen kieltää viestiä.



SIGNATURE PROTOCOL:

A	Public channel	B
Message $j \in P$	E_A	
Secret data		
A signs message j:		
$D_A(j) = s$	Message with a signature to B	
	$(j, s) \to$ B	B verifies the signature:
		$E_A(s) = j$

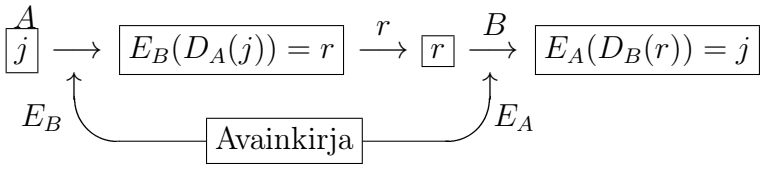
Edellä oleva menettely voidaan toteuttaa salaovifunktiolla f valitsemalla $E_A = f$, $D_A = f^{-1}$.

3.2.1 Salattu allekirjoitus/Encrypted signature

Jos halutaan suorittaa salakirjoitus ja allekirjoitus, tarvitaan ominaisuudet (25)–(29). Tällöin A muodostaa salatun viestin $c = E_B(j)$ ja allekirjoitusosasta s tekstin $r = E_B(s) = E_B(D_A(j))$. Käyttäjä B soveltaa tähän funktiota $E_A \circ D_B$:

$$E_A(D_B(r)) = E_A(D_B(E_B(D_A(j)))) = E_A(D_A(j)) = j.$$

Menettely E_A löytyy avainkirjasta, mutta vain B tuntee menettelyn D_B ja voi varmistaa salatun allekirjoituksen (c, r).



SIGNATURE PROTOCOL WITH ENCRYPTING:

A	Public channel	B
Secret data		Secret data
Message $j \in P$	E_A, E_B	
A encrypts message j:		
$E_B(j) = c$	$(c, r) \rightarrow$ B	B decrypts c:
		$D_B(c) = j$
A signs message j:		
$D_A(j) = s$		
A encrypts signature s:		
$E_B(s) = r$		B verifies the signature:
		$E_A(D_B(r)) = j$

Huomaa, että jos allekirjoitusta s ei salata, niin se voidaan avata seuraavasti. Koska E_A on julkisesti tiedossa, niin

$$E_A(s) = E_A(D_A(j)) = j, \tag{30}$$

jolloin alkuperäinen viesti j paljastuu.

4 RSA

4.1 RSA-salaus/RSA-encrypting

RSA-menetelmässä (Rivest, Shamir, Adleman 1978) salaovifunktion muodostus perustuu vuosisatoja tutkittuun lukuteorian ongelmaan: kuinka annettu (suuri) luku n jaetaan alkutekijöihin? Yksisuuntaisen funktion perusta on nyt se, että annettujen lukujen tulo on nopeasti laskettavissa, mutta tekijöiden löytäminen tulosta vaatii nopeiltakin koneilta liikaa aikaa. Olkoot p ja q kaksi eri alkulukua ja $n = pq$. Tällöin $\varphi(n) = (p-1)(q-1)$. Valitaan sellainen luku e, $1 < e < \varphi(n)$, että $\text{syt}(e, \varphi(n)) = 1$ (mikä tahansa alkuluku

e väliltä $\max\{p,q\} < e < \varphi(n)$ käy). Eukleideen algoritmin avulla löydetään ehdon $1 < d < \varphi(n)$ toteuttava luku d, jolle

$$ed \equiv 1 \pmod{\varphi(n)} \tag{31}$$

eli

$$ed = 1 + \ell\varphi(n), \quad l \in \mathbb{N}. \tag{32}$$

Lause 4.1. *Olkoon $n = pq$, missä $p, q \in \mathbb{P}$, $p \neq q$. Tällöin*

$$a^{l\varphi(n)+1} \equiv a \pmod{n}, \quad \forall\, a \in \mathbb{Z}, \quad l \in \mathbb{N}. \tag{33}$$

Todistus:

1) Jos $\text{syt}(a,n) = 1$, niin Euler-Fermat'n (160) nojalla

$$a^{\varphi(n)} \equiv 1 \pmod{n} \quad \Rightarrow \quad a^{l\varphi(n)} \equiv 1 \pmod{n} \tag{34}$$

$$\Rightarrow \quad a^{l\varphi(n)+1} \equiv a \pmod{n}. \tag{35}$$

2) Jos $\text{syt}(a,n) \neq 1$, niin meillä on kolme tapausta:

$$a \equiv 0 \pmod{n}; \tag{36}$$

$$a \equiv 0 \pmod{p}, \quad a \not\equiv 0 \pmod{q}; \tag{37}$$

$$a \not\equiv 0 \pmod{p}, \quad a \equiv 0 \pmod{q}. \tag{38}$$

Tapaus (36):

$$a \equiv 0 \pmod{n} \quad \Rightarrow \quad a^{l\varphi(n)+1} \equiv 0 \pmod{n}. \quad \square \tag{39}$$

Tapaus (37): Nyt

$$a \equiv 0 \pmod{p} \quad \Rightarrow \quad a^{l\varphi(n)+1} \equiv 0 \pmod{p} \tag{40}$$

$$\Rightarrow \quad a^{l\varphi(n)+1} \equiv a \pmod{p}. \tag{41}$$

Toisaalta Pikku Fermat'n (163) nojalla

$$a^{q-1} \equiv 1 \pmod{q} \quad \Rightarrow \quad a^{(q-1)(p-1)} \equiv 1 \pmod{q}. \tag{42}$$

Koska

$$\varphi(n) = \varphi(pq) = (q-1)(p-1), \tag{43}$$

niin

$$\Rightarrow \quad a^{l\varphi(n)+1} \equiv a \pmod{q}. \tag{44}$$

Soveltamalla Lausetta 9.1 tuloksiin (41) ja (44) saadaan

$$a^{l\varphi(n)+1} \equiv a \pmod{pq}. \quad \square \tag{45}$$

Tapaus (38) kuten (37). $\square$

Lause 4.2.

$$a^{ed} = a \quad \forall a \in \mathbb{Z}_n. \tag{46}$$

Todistus: Tuloksien (32) ja (33) mukaan

$$a^{ed} \equiv a \pmod{n}, \quad \forall\, a \in \mathbb{Z}. \quad \square \tag{47}$$

Lause 4.3. *Funktiot*

$$E(x) = x^e, \qquad D(y) = y^d \tag{48}$$

ovat bijektioita : $\mathbb{Z}_n \to \mathbb{Z}_n$ *ja*

$$D = E^{-1}. \tag{49}$$

Todistus: Asetetaan

$$E(x_1) = E(x_2) \quad \Rightarrow \quad D(E(x_1)) = D(E(x_2)) \quad \Rightarrow \tag{50}$$

$$x_1^{ed} = x_2^{ed} \quad \Rightarrow \quad x_1 = x_2 \tag{51}$$

joten $E\colon \mathbb{Z}_n \to \mathbb{Z}_n$ on injektio ja siten bijektio. Siten myös $D\colon \mathbb{Z}_n \to \mathbb{Z}_n$ on bijektio. Edelleen

$$D(E(x)) = x \quad \forall x \in \mathbb{Z}_n, \tag{52}$$

joten $D = E^{-1}$. $\square$

Määritelmä 4.4. Funktio

$$E(x) = x^e, \qquad E\colon \mathbb{Z}_n \to \mathbb{Z}_n \tag{53}$$

on RSA-kryptausfunktio, missä e on kryptauseksponentti (julkinen avain) ja

$$D(y) = y^d, \qquad D\colon \mathbb{Z}_n \to \mathbb{Z}_n \tag{54}$$

on RSA-dekryptausfunktio, missä d on dekryptauseksponentti (salainen avain).∎

Esimerkki 4.5.

$$p = 7,\ q = 13, n = pq = 91, \quad \varphi(n) = 72, \quad e = 5, \quad d = 29 \tag{55}$$

Selkoteksti

$$ok = 1410 = m_1 m_2, \tag{56}$$

$$m_1 = 14, \quad m_2 = 10 \tag{57}$$

Kryptoteksti

$$c_1 c_2, \quad c_1 = m_1^e = 14^5 = 14, \quad c_2 = m_2^e = 10^5 = 82 \tag{58}$$

Dekryptataan

$$c_1^d = 14^{29} = 14 = o, \quad c_2^d = 82^{29} = 10 = k. \tag{59}$$

Esimerkki 4.6.

$$p = 101,\ q = 107, \quad n = pq, \quad \varphi(n) = 10600, \quad e = 3, \quad d = 7067. \tag{60}$$

Funktioiden arvot ovat nopeasti laskettavissa potenssiinkorotuksella modulo n, kun e ja d tunnetaan. Jos n ja e tunnetaan, niin $E(m)$ on laskettavissa, mutta luvun d laskeminen ei onnistu ilman lukua $\varphi(n)$, jonka löytäminen edellyttää alkulukujen p ja q tuntemista eli luvun n tekijöihinjakoa. Luku d on siis salaovi (trapdoor), jota ilman $D = E^{-1}$ ei löydy, ja E on salaovifunktio.

RSA-järjestelmässä kukin käyttäjä U valitsee yllä olevaan tapaan alkuluvut p_U ja q_U, laskee luvun $n_U = p_U q_U$, valitsee sitten luvun e_U, $1 < e_U < \varphi(n_U)$, ja laskee luvun d_U, jolle $e_U d_U \equiv 1 \pmod{\varphi(n_U)}$. Avainkirjassa kukin käyttäjä julkaisee avaimensa $K_U = (n_U, e_U)$, mutta pitää omana tietonaan luvun d_U (ja luvut p_U, q_U), joka muodostaa salaoven.

Kun käyttäjä A haluaa lähettää viestin käyttäjälle B, hän muuntaa viestinsä joukon $\mathbb{Z}_{n_B}$ alkioiksi esimerkiksi seuraavassa kappaleessa esitettävällä tavalla ja toimii edellä kuvatun yleisen periaatteen mukaisesti.

Viestin $m \in \mathbb{Z}_{n_B}$ salakirjoitus on

$$E_B(m) = m^{e_B} = c \in \mathbb{Z}_{n_B}.$$

Vain B tietää luvun d_B, joten hänen avausfunktionsa on

$$D_B(c) = c^{d_B} = m^{e_B d_B} = m.$$

A	Public channel	B
<u>Secret data</u>		<u>Secret data</u>
		$p, q \in \mathbb{P}_{\geq 3}, p \neq q$
$m \in P$		$n = n_B = pq$
Encrypting	$n = n_B, e = e_B$	$\leftarrow n_B$ to be published
$c = m^e \in \mathbb{Z}_n$		$\varphi(n) = (p-1)(q-1)$
		$e = e_B \in \mathbb{Z}^*_{\varphi(n)}$
Cryptotext sent to B		$\leftarrow e = e_B$ to be published
$c \rightarrow$ B		$d = e^{-1} \in \mathbb{Z}^*_{\varphi(n)}$
		Decrypting
	$c \rightarrow$ B	$c^d = m$

Esimerkki 4.7.

A Secret data	Public channel	B Secret data
		$p = 1223, q = 1987$
$1070777 \in P$		$n = n_B = 2430101$
Encrypting	$n = n_B, e = e_B$	$\leftarrow n_B$ to be published
$c = m^e =$		$\varphi(n) = 2426892$
$1070777^{948047} =$		$e_B = 948047 \in \mathbb{Z}^*_{\varphi(n)}$
$1473513 \in \mathbb{Z}_n$		$\leftarrow e = e_B$ to be published
Cryptotext sent to B		$d = e^{-1} = 1051235 \in \mathbb{Z}^*_{\varphi(n)}$
$c = 1473513 \rightarrow$ B		Decrypting
	$c = 1473513 \rightarrow$ B	$c^d = 1473513^{1051235} = 1070777$

4.2 RSA-allekirjoitus/RSA-signature

Esimerkki 4.8.

$$p = 7,\ q = 13, n = pq = 91,\ \varphi(n) = 72,\ e_A = 5,\ d_A = 29. \tag{61}$$

A	Public channel	B
Message $j = 82 \in \mathbb{Z}_{91}$	$E_A(x) = x^{e_A} = x^5$	
Secret data		
$D_A(x) = x^{d_A} = x^{29}$		
A signs message $j = 82$:		
$D_A(82) = 82^{29} = 10 = s$	Message with a signature to B	
	$(j, s) = (82, 10) \rightarrow$ B	B verifies the signature:
		$E_A(s) = 10^5 = 82 = j$

Esimerkki 4.9.

$$n_A = p_A q_A = 119,\ \varphi(n_A) = 96,\ e_A = 5,\ d_A = 77. \tag{62}$$

$$n_B = p_B q_B = 143,\ \varphi(n_B) = 120,\ e_B = 7,\ d_B = 103. \tag{63}$$

SIGNATURE PROTOCOL WITH ENCRYPTING: Note that we need to have $n_A < n_B$!!

A	Public channel	B
Secret data		Secret data
Message $j = 2 \in \mathbb{Z}_{119}$	$E_A(x) = x^5, E_B(x) = x^7$	
A encrypts message $j = 2$:		
$E_B(j) = j^{e_B} = 2^7 =$	$(c, r) = (128, 98) \to$ B	B decrypts $c = 128$:
$128 = c \in \mathbb{Z}_{143}$		$D_B(c) = c^{d_B} =$
A signs message $j \in \mathbb{Z}_{119}$:		$128^{103} = 2 = j$
$D_A(j) = j^{d_A} = 2^{77} = 32 = s$		
A encrypts signature $s \in \mathbb{Z}_{143}$:		
$E_B(s) = s^{e_B} = 32^7 =$		B verifies the signature:
$98 = r \in \mathbb{Z}_{143}$		$E_A(D_B(r)) = E_A(r^{d_B}) =$
		$E_A(98^{103}) = E_A(32) =$
		$32^5 = 2 = j$. :)

4.3 Tekstin esittäminen joukon $\mathbb{Z}_n$ alkioina

Esimerkki 4.10. Olkoot

$$p = 1223,\ q = 1987, n = pq = 2430101, \quad e = 948047, \quad d = 1051235. \tag{64}$$

Selkoteksti

$$\text{plaintext} = 151100081319042319 = m_1 m_2 m_3, \tag{65}$$

kannattaa jakaa paloihin

$$m_1 = 151100, \quad m_2 = 081319, \quad m_3 = 042319, \tag{66}$$

joiden pituus (tässä 6 bittiä) on pienempi kuin luvun $n = 2430101$ (tässä 7 bittiä). Siten varmuudella

$$0 \leq m_1, m_2, ... \leq n - 1, \tag{67}$$

joten luvut (66) voidaan tulkita yksikäsitteisiksi joukon $\mathbb{Z}_n$ alkioiksi eli

$$m_1, m_2, ... \in \mathbb{Z}_n. \tag{68}$$

Kryptaaminen tapahtuu joukossa $\mathbb{Z}_n$ seuraavasti

$$c_1 c_2 c_3, \quad c_1 = m_1^e, \quad c_2 = m_2^e, ..., \tag{69}$$

missä

$$c_1, c_2, ... \in \mathbb{Z}_n. \tag{70}$$

4.4 RSA-turvallisuus/security

Turvallisuus perustuu dekryptauseksponentin d piilottamiseen.
Vaikka kryptauseksponentti e tunnetaan, niin tarvittaisiin $\varphi(n)$ luvun d laskemiseen

$$ed \equiv 1 \pmod{\varphi(n)}. \tag{71}$$

Jos murretaan:
1) tekijöihinjako

$$n = pq, \tag{72}$$

niin saataisiin $\varphi(n)$.
Tämä on vaikeaa isoille luvuille.

4.4.1 Neliöseula-hyökkäys/Quadratic sieve attack

Neliöseula-hyökkäys=Quadratic sieve attack.

Olkoon

$$n = pq, \quad p < q, \quad p, q \in \mathbb{P}_{\geq 3}. \tag{73}$$

Asetetaan

$$p = a - b, \quad q = a + b \quad \Rightarrow \quad a, b \in \mathbb{Z}^+, \tag{74}$$

ja

$$n = pq = a^2 - b^2 < a^2 \quad \Rightarrow \quad A := \lceil \sqrt{n} \rceil \leq a. \tag{75}$$

ALGORITMI I:

Lasketaan lukuja

$$a^2 - n, \quad a = A + k, \quad k = 0, 1, ..., \left\lceil (\sqrt{2} - 1)A \right\rceil, \tag{76}$$

ja tutkitaan tuleeko neliö:

$$a^2 - n = \begin{cases} \square & \Leftrightarrow \quad = b^2, \quad b \in \mathbb{Z}^+; \\ \boxtimes & \Leftrightarrow \quad \neq b^2, \quad b \in \mathbb{Z}^+. \end{cases} \tag{77}$$

ALGORITMI II:

Lasketaan lukuja

$$n + b^2, \quad b = 1, ..., A - 1, \tag{78}$$

ja tutkitaan tuleeko neliö.

Huomautus 4.11. Käytännössä ylärajat ovat kokoluokkaa $\log A$.

Esimerkki 4.12. Olkoon $n = 1147$, $A = 34$.

ALGORITMI I:

Lasketaan lukuja

$$(34 + k)^2 - 1147, \quad k = 0, 1, ... \tag{79}$$

Koska

$$(34 + 0)^2 - 1147 = 3^2, \tag{80}$$

niin saadaan hajotelma

$$1147 = 34^2 - 3^2 = 31 \cdot 37. \tag{81}$$

ALGORITMI II:

Lasketaan lukuja

$$1147 + b^2, \quad b = 1, 2, ... \tag{82}$$

$$1147 + 1^2 = 1148 = \boxtimes; \tag{83}$$

$$1147 + 2^2 = 1151 = \boxtimes; \tag{84}$$

$$1147 + 3^2 = 1156 = 34^2 \quad \Rightarrow \quad 1147 = 34^2 - 3^2 = 31 \cdot 37. \tag{85}$$

Esimerkki 4.13. Olkoon $n = 1891$, $A = 44$.
ALGORITMI I:

$$44^2 - 1891 = \boxtimes; \tag{86}$$

$$45^2 - 1891 = \boxtimes; \tag{87}$$

$$46^2 - 1891 = 225 = 15^2 \quad \Rightarrow \quad 1891 = ... \tag{88}$$

Esimerkki 4.14. Olkoon $n = 403$.
ALGORITMI II:

$$403 + 1^2 = \boxtimes; \tag{89}$$

...

$$403 + 8^2 = \boxtimes; \tag{90}$$

$$403 + 9^2 = 484 = 22^2; \quad \Rightarrow \quad 403 = 13 \cdot 31. \tag{91}$$

Siten, jos alkutekijät ovat kaukana toisistaan, niin algoritmista tulee pitkä. Voidaan kokeilla seuraavaa algoritmia.

ALGORITMI III:
Valitaan luvun $k \in \mathbb{Z}^+$ arvoja $k = 3, 4, ...$ ja lasketaan lukuja

$$kn + c^2, \quad c = 0, 1, ..., \tag{92}$$

ja tutkitaan tuleeko neliö.

$$kn + c^2 = \begin{cases} \square? \\ \boxtimes? \end{cases} \tag{93}$$

Huomautus 4.15. Tapauksessa $k = 2$, saataisiin

$$kn + c^2 = 2n + c^2 = \boxtimes \quad \forall c = 0, 1, ... \tag{94}$$

Todistus: Vastaoletus

$$2n + c^2 = \square. \tag{95}$$

Aluksi huomataan

$$2n = 4k + 2 \equiv 2 \pmod 4 \tag{96}$$

ja

$$\square \equiv \begin{cases} 0 \\ 1 \end{cases} \pmod 4. \tag{97}$$

Siten

$$2n + c^2 = 2 + \begin{cases} 0 \\ 1 \end{cases} = \begin{cases} 0 \\ 1 \end{cases} \pmod 4. \tag{98}$$

Ristiriita.

Esimerkki 4.16. Olkoon $n = 403$ ja $k = 3$, jolloin $kn = 1209$.
ALGORITMI III:

$$1209 + 0^2 = \boxtimes; \tag{99}$$

...

$$1209 + 4^2 = 1225 = 35^2; \quad \Rightarrow \quad 3n = 3 \cdot 13 \cdot 31. \tag{100}$$

Ehto

$$kn + c^2 = \square \tag{101}$$

tarkoittaa, että

$$kn = d^2 - c^2 \quad \Leftrightarrow \tag{102}$$

$$d^2 \equiv c^2 \pmod{n}. \tag{103}$$

Kongruenssit (103) muodostavatkin neliöseula-menetelmien perustan.

ALGORITMI IV:

Lasketaan kongruensseja

$$(A \pm k)^2 \equiv \begin{cases} \square? \\ \boxtimes? \end{cases} \pmod{n}. \tag{104}$$

Esimerkki 4.17. Olkoon $n = 403$, $A = 21$.

ALGORITMI IV:

$$20^2 \equiv -3 \pmod{n} \quad -3 = \boxtimes; \tag{105}$$

$$21^2 \equiv 38 \pmod{n} \quad 38 = \boxtimes; \tag{106}$$

$$22^2 \equiv 9^2 \pmod{n} \quad ... \tag{107}$$

ALGORITMI V:

Kongruenssi

$$d^2 \equiv c^2 \pmod{n} \tag{108}$$

on yhtäpitävää yhtälön

$$(d - c)(d + c) = ln, \quad l \in \mathbb{Z} \tag{109}$$

kanssa. Kun luvut $c \neq d$ ovat isoja, niin lasketaan

$$syt(d \pm c, n) = d_{\pm}. \tag{110}$$

Jos pätee

$$d_{\pm} \neq \begin{cases} 1; \\ n, \end{cases} \tag{111}$$

niin

$$d_{\pm} \in \{p, q\}. \tag{112}$$

Esimerkki 4.18. Olkoon $n = 799$, $A = 29$.
ALGORITMI V:

$$27^2 \equiv -2 \cdot 5 \cdot 7 \pmod{n}; \tag{113}$$

$$28^2 \equiv -3 \cdot 5 \pmod{n}; \tag{114}$$

$$29^2 \equiv 2 \cdot 3 \cdot 7 \pmod{n}; \tag{115}$$

$$30^2 \equiv 101 \pmod{n}. \tag{116}$$

Oikealle puolelle ei tullut neliöita mutta kertomalla kongruenssit (113–115) puolittain saadaan

$$(27 \cdot 28 \cdot 29)^2 \equiv (2 \cdot 3 \cdot 5 \cdot 7)^2 \pmod{799} \tag{117}$$

$$\Leftrightarrow \quad 351^2 \equiv 210^2 \pmod{799} \tag{118}$$

$$\Leftrightarrow \quad (351 - 210)(351 + 210) = l \cdot 799. \tag{119}$$

Nyt Eukleideen algoritmilla

$$\text{syt}(799, 141) = 47 \in \{p, q\} \quad \Rightarrow \quad p = 17, q = 47. \tag{120}$$

ALGORITMI VI:
Edellisiä kongruensseja $\pmod{n}$ kannattaa laskea myös lukujen

$$A_j := \left\lceil \sqrt{jn} \right\rceil, \quad j = 1, 2, 3, ... \tag{121}$$

ympäristöissä.

Esimerkki 4.19. Olkoon $n = 4841$, $A_1 = 70, A_2 = 99, A_3 = 121$.
ALGORITMI VI:

$$70^2 \equiv 59 \pmod{n}; ... \tag{122}$$

$$99^2 \equiv 119 \pmod{n}; ... \tag{123}$$

$$121^2 \equiv 118 \pmod{n}; ... \tag{124}$$

4.4.2 Kryptausfunktio-iteraatiot

Osa kryptotekstiä voidaan mahdollisesti murtaa kohdistamaalla siihen kryptausfunktion iteraatioita.

Lause 4.20. *Jos*

$$E^{h+1}(c) = c, \quad h = 0, 1, ..., \tag{125}$$

niin

$$m = E^h(c). \tag{126}$$

Todistus.

Esimerkki 4.21. Olkoot

$$n = 65, \quad e = 5. \tag{127}$$

Murretaan kryptotekstit

$$c_1 = 32, c_2 = 49. \tag{128}$$

Laskemalla

$$E(c_1) = E(32) = 2, \quad E^2(c_1) = E(2) = 32 = c_1, \quad \Rightarrow \quad m = E(c_1) = 2. \tag{129}$$

5 Diskreetti logaritmi

5.1 Diskreetti logaritmi kertolaskuryhmässä

Olkoon H äärellinen syklinen kertalukua $h = \#H$ oleva ryhmä eli

$$H = \langle \beta \rangle = \{\beta^j |\ j = 0, 1, ..., h-1\} =$$

$$\{1, \beta, \beta^2, ..., \beta^{h-1}\}. \tag{130}$$

Huomaa, että

$$\beta^0 = \beta^h = \beta^{2h} = ... = 1. \tag{131}$$

Määritelmä 5.1. Alkion $y \in H$ diskreetti logaritmi kannan β suhteen on eksponentti $k \in \{0, 1, \ldots, h-1\}$, jolle pätee $y = \beta^k$. Tällöin käytetään merkintää

$$k = \log_\beta y. \tag{132}$$

Lause 5.2.

$$\log_\beta 1 = 0; \tag{133}$$

$$\log_\beta xy \equiv \log_\beta x + \log_\beta y \pmod{h}; \tag{134}$$

$$\log_\beta x^k \equiv k \log_\beta x \pmod{h}. \tag{135}$$

Esimerkki 5.3. $H = \mathbb{Z}_{71}^* = \langle 7 \rangle$ on syklinen ja $h = \varphi(71) = 70$. Lasketaan siis $\pmod{71}$ ja eksponentit $\pmod{70}$.

$$\begin{array}{cc}
7^2 = 49 & \log_7 49 = 2 \\
7^3 = 59 & \log_7 59 = 3 \\
7^6 = 2 & \log_7 2 = 6 \\
\vdots & \\
7^? = 33 & \log_7 33 = ? \\
7^{35} = 70 = -1 & \log_7 70 = \log_7 -1 = 35 \\
\vdots & \\
7^{69} = 61 & \log_7 61 = 69 \\
7^{70} = 1 = 7^0 & \log_7 1 = 0
\end{array}$$

5.2 Ryhmät $\mathbb{Z}_n^*$

5.2.1 Primitiivijuuret

Määritelmä 5.4. Olkoon $n \in \mathbb{Z}_{\geqslant 2}$. Luku $b \in \{1, 2, \ldots, n-1\}$ on primitiivijuuri (mod n), jos $\mathbb{Z}_n^* = \langle \overline{b} \rangle$ eli $\overline{b}$ generoi ryhmän $\mathbb{Z}_n^*$.

Käytetään myös merkintää $\text{ind}_b y = \log_{\overline{b}} \overline{y}$.

Lause 5.5. *$\mathbb{Z}_n^*$ on syklinen* $\Leftrightarrow$

$$n = 2, 4, p^l, 2p^l, \quad l \in \mathbb{Z}^+,\ p \in \mathbb{P}_{\geq 3}. \tag{136}$$

Todistus: Lukuteoria A

Siten

Primitiivijuuri (mod n) $\exists$ $\Leftrightarrow$ $n \in \{2, 4\} \cup \mathbb{P}_{\geq 3}^{\mathbb{Z}^+} \cup 2\mathbb{P}_{\geq 3}^{\mathbb{Z}^+}$.

Huomaa, että

Lause 5.6.

$$\mathbb{Z}_n^* = \langle \overline{b} \rangle \quad \Leftrightarrow \quad ord\ \overline{b} = \varphi(n). \tag{137}$$

5.3 Diskreetin logaritmin ongelma

D.L=Diskreetin logaritmin ongelma.
Olkoon $H = \langle \beta \rangle,\ \#H = h$, missä β ja h tunnetaan. Valitaan $y \in H$ vapaasti. Määritä tällöin $\log_\beta y$, kun h=ISO.

ESIM: Valitaan $h \sim 2^{1000},\ 1 \leqslant r \leqslant h-1$. Tällöin

$$r = e_{t-1}2^{t-1} + \ldots + e_0,\ t \leqslant 1000.$$

Potenssin a^r laskemiseen tarvitaan ainoastaan$\leqslant 2000$ laskutoimitusta (Lemma 10.1), kun taas diskreetin logaritmin $\log_\beta y$ määrääminen vaatii jopa 2^{1000} laskua H:ssa. Eli **D.L** sanoo sen, että käytännössä potenssiinkorotus on nopeaa ja logaritmin määrittäminen ∞:n hidasta.

Huomautus 5.7.

$$2^{10} = 1024 \cong 10^3 \Rightarrow \underbrace{\frac{\log 2}{\log 10}}_{=0.30103} \cong \frac{3}{10} = 0.300$$

$$\Rightarrow 2^{1000} = 10^{1000 \cdot \frac{\log 2}{\log 10}} \cong 10^{300}.$$

Huomautus 5.8. **D.L** ongelman vaikeus riippuu valitusta ryhmästä:

(a) $(H, \cdot) = (\mathbb{Z}_n, +)$, missä $\mathbb{Z}_n = \langle \overline{\beta} \rangle = \{k\overline{1} \mid k \in \mathbb{Z}\} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$. Tässä **D.L** on HELPPO.

(b) $(H, \cdot) = (\mathbb{Z}_n^*, \cdot)$, $n = p^l,\ 2p^l,\ p \in \mathbb{P}_{\geqslant 3}$. Tässä **D.L** on yleensä VAIKEA.

(c) $(H, \cdot) = (\mathbb{F}_q^*, \cdot)$ eli äärellisen kunnan kertolaskuryhmä, missä **D.L** on yleensä VAIKEA.

(d) $(H, \cdot) = (E, +)$ eli elliptisen käyrän yhteenlaskuryhmä, missä **D.L** on yleensä **VAIKEA**.

6 Diffie-Hellman avaimenvaihto

Tarkastellaan järjestelmää yleisessä syklisessä ryhmässä $H = \langle \beta \rangle,\ h = \#H$. Siis ryhmä H sen generaattori β ja kertaluku h ovat kaikkien käyttäjien $\mathcal{U} = A, B, C, \ldots$ tiedossa.
Jokainen käyttäjä $\mathcal{U} = A, B, C, \ldots$ valitsee *salaisen avaimen* $m_{\mathcal{U}}$=eksponentin, jonka avulla $\mathcal{U}$ laskee luvun $k_{\mathcal{U}} = \beta^{m_{\mathcal{U}}}$, joka *julkaistaan*. Olkoot

$$a = m_A,\ b = m_B, \ldots \tag{138}$$

salaisia avaimia (secret keys) ja

$$k_A(= \beta^a),\ k_B(= \beta^b), \ldots \tag{139}$$

julkisia avaimia (public keys).
Tällöin käyttäjä A laskee luvun

$$k_{A,B} = (k_B)^a \tag{140}$$

ja vastaavasti käyttäjä B laskee luvun

$$k_{B,A} = (k_A)^b. \tag{141}$$

Nyt

$$k_{A,B} = (k_B)^a = (\beta^b)^a = (\beta^a)^b = (k_A)^b = k_{B,A} \tag{142}$$

eli saadaan yhteinen avain.

A	Public channel	B
Secret data		Secret data
	$H = \langle\beta\rangle,\ h = \#H$	
$a = m_A$		$b = m_B$
$k_A = \beta^a$		$k_B = \beta^b$
$k_A \to$ B	$k_A \to$ B	
	A $\leftarrow k_B$	A $\leftarrow k_B$
$k_{A,B} = (k_B)^a$		$k_{B,A} = (k_A)^b$

Esimerkki 6.1. Olkoon ryhmänä

$$\mathbb{Z}_{71}^* = \langle 7 \rangle, \tag{143}$$

ja julkisina avaimina

$$k_A = 59, \quad k_B = 62. \tag{144}$$

A: Salainen eksponentti $a = 3$.

Laskee

$$k_{A,B} = (k_B)^a = 62^3 = 52. \tag{145}$$

Toisaalta

B: Salainen eksponentti $b = 17$.

Laskee

$$k_{B,A} = (k_A)^{17} = 59^{17} = 52. \tag{146}$$

Siten saadaan yhteinen avain 52.

A	Public channel	B
Secret data		Secret data
	$H = \mathbb{Z}_{71}^* = \langle 7 \rangle,\ h = 70$	
$a = 3$		$b = 17$
$k_A = 7^3 = 59$		$k_B = 7^{17} = 62$
$k_A = 59 \rightarrow$ B	$k_A = 59 \rightarrow$ B	
	A $\leftarrow k_B = 62$	A $\leftarrow k_B = 62$
$k_{A,B} = 62^3 = 52$		$k_{B,A} = 59^{17} = 52$

Useampi käyttäjä:

$\mathcal{U}$	salainen avain$= x$	julkinen $k_{\mathcal{U}} (= \beta^x)$
A	a	k_A
B	b	k_B
C	c	k_C
$\vdots$	$\vdots$	

$\mathcal{U}$	Yhteinen avain $k_{\mathcal{U},Y} = (k_Y)^x$	
A	$k_{A,B}$	$k_{A,C}$
B	$k_{B,A}$	$k_{B,C}$
C	$k_{C,A}$	$k_{C,B}$
$\vdots$		

missä $k_{X,Y} = k_{Y,X} \quad \forall X, Y \in \{A, B, C, \ldots\}$ ja käyttäjien X ja Y yhteinen avain on vain X:n ja Y:n tiedossa.
Järjestelmän turvallisuus perustuu Diffie-Hellman ongelmaan.

6.1 Diffie-Hellman ongelma

D.H=Diffie-Hellman ongelma.
Määrää β^{ab} luvuista $\beta, \beta^a, \beta^b, h$ (a, b salaisia).

Yleisesti oletetaan, että

$$\mathbf{D.H} \Leftrightarrow \mathbf{D.L}.$$

Perustelua: Olkoot $y = \beta^a,\ z = \beta^b$. Tehdään yritelmiä:
1) $a = \log_\beta y,\ b = \log_\beta z \Rightarrow ab \Rightarrow \beta^{ab}$, mutta pitäisi laskea logaritmit.
2) $\begin{cases} yz = \beta^{a+b} \\ \frac{y}{z} = \beta^{a-b} \end{cases} \Rightarrow \begin{cases} a+b = \log_\beta(yz) \\ a-b = \log_\beta(\frac{y}{z}) \end{cases} \Rightarrow a, b \Rightarrow ab$, mutta jälleen tarvitaan logaritmit.
3) Jotain muuta ... ?
Siten, vaikka käyttäjä C tietää luvut k_A ja k_B, niin $C \neq A, B$ ei voi päätellä ilman logaritmeja A:n ja B:n yhteistä avainta $k_{A,B}$.

7 ElGamal kryptausjärjestelmä

Nyt $R = H,\ S = H \times H$ ja

$$E:\ H \to H \times H.$$

Tässäkin jokainen käyttäjä $\mathcal{U} = A, B, C, \ldots$ valitsee *salaisen avaimen* $m_\mathcal{U}$=eksponentin, jonka avulla $\mathcal{U}$ laskee luvun $k_\mathcal{U} = \beta^{m_\mathcal{U}}$, joka *julkaistaan*.

Seurataan miten käyttäjä A kryptaa viestin m ja lähettää sen käyttäjälle B.
Julkiset avaimet

$$k_A = \beta^a, \quad k_B = \beta^b. \tag{147}$$

A: Määrittää yhteisen avaimen

$$k_{A,B} = {k_B}^a \tag{148}$$

ja laskee luvun

$$v_A = m{k_B}^a = mk_{A,B}. \tag{149}$$

	salaisia		julkisia		
A	a	m	k_A	$E_A(m) = (k_A, v_A)$	$v_A = mk_{A,B}$
B	b		k_B	$\Downarrow$	

Nyt käyttäjä B dekryptaa saadun sanoman:
B: Laskee aluksi yhteisen avaimen eli

$$k_{B,A} = {k_A}^b = k_{A,B} \tag{150}$$

ja jakaa

$$\frac{v_A}{k_{B,A}} = \frac{mk_{A,B}}{k_{A,B}} = m. \tag{151}$$

TURVALLISUUDESTA: 1. Avain a on vaihdettava jokaisen käyttökerran jälkeen, sillä jos C on saanut tiedon aikaisemmasta viestistä m_1, niin

$$\begin{cases} v_1 = m_1 k_{B,A} \\ v_2 = m_2 k_{B,A} \end{cases} \Rightarrow m_2 = \frac{v_2}{v_1} m_1. \tag{152}$$

2. Muutoin järjestelmän turvallisuus perustuu D.H. ongelmaan.

Esimerkki 7.1. Jatketaan Esimerkin 6.1 parametreilla. Olkoon lähetettävä viesti $m = 41$.
Nyt A kryptaa:

$$v_A = mk_{A,B} = 41 \cdot 52 = 2. \tag{153}$$

B dekryptaa

$$\frac{v_A}{k_{A,B}} = \frac{2}{52} = 41. \tag{154}$$

Esimerkki 7.2. Jatketaan Esimerkkien 6.1 ja 7.1 parametreilla.
Merkitään $m_1 = 41$ ja $v_1 = 2$ ja olkoon uusi viesti $m_2 = 3$, jolloin $v_2 = 14$.
Jos C tietää aikaisemman viestin $m_1 = 41$, niin laskemalla

$$m_1 \frac{v_2}{v_1} = 41 \frac{14}{2} = 3 \tag{155}$$

käyttäjä C saa selville uuden viestin $m_2 = 3$.

8 Huomautuksia

Edellä ei ole käsitelty esiteltyjen julkisen avaimen järjestelmien heikkouksia, kuten murtamismahdollisuuksia. RSA:ta pidetään varsin turvallisena, kun p ja q ovat riittävän suuria sekä niiden valinnassa otetaan huomioon eräitä rajoituksia. Vuonna 2010 turvallisena avainpituutena pidetään 1024 bittiä (reilut 300 numeroa 10-kanteisena). Myös 512-bittiset avaimet antavat melko hyvän suojan, vaikkeivat ne järeitä hyökkäyksiä kestäkään. On arvioitu, että parin vuosikymmenen kuluttua RSA-avaimen olisi oltava 3072-bittinen ($3072 = 2^{11} + 2^{10}$, $2^{3072} \approx 10^{925}$) ollakseen turvallinen. Myös diskreetti logaritmi lienee luotettava, kun kunta $\mathbb{Z}_p$ (tai yleisempi äärellinen kunta) on riittävän suuri. Voidaan myös kysyä täsmällisempää tietoa eri menetelmien vaatimien laskutoimitusten määristä eli tarvittavasta laskenta-ajasta. Luonnollisesti tulee esille myös kysymys siitä, miten esimerkiksi RSA:n tarvitsemia suuria alkulukuja on löydettävissä. Syventävien opintojen kurssilla Kryptografia tarkastellaan lähemmin näitä kysymyksiä sekä esitellään menetelmiä, jotka vaativat syvällisempiä matematiikan tietoja.

9 Lukuteoriaa

9.1 Eräs kongruenssiryhmä

Lause 9.1. *A) Olkoot $p, q \in \mathbb{P}$ ja $p \neq q$. Näytä, että yhtälöistä*

$$\begin{cases} a \equiv b \pmod{p} \\ a \equiv b \pmod{q} \end{cases} \tag{156}$$

seuraa

$$a \equiv b \pmod{pq}. \tag{157}$$

B) Olkoot $m_i \in \mathbb{Z}$ ja $m_i \perp m_j$ kaikilla $i \neq j$. Näytä, että yhtälöistä

$$a \equiv b \pmod{m_i} \quad \forall \quad i = 1, ..., r \tag{158}$$

seuraa

$$a \equiv b \pmod{m_1 \cdots m_r}. \tag{159}$$

9.2 Euler-Fermat

Lause 9.2. *EULER-FERMAT: Olkoot $a \in \mathbb{Z}$, $n \in \mathbb{Z}_{\geq 2}$ annettu ja $a \perp n$. Tällöin*

$$a^{\varphi(n)} \equiv 1 \pmod{n}. \tag{160}$$

Lause 9.2 voidaan lausua myös muodossa:

$$\overline{a}^{\varphi(n)} = \overline{1}, \quad \forall\ \overline{a} \in \mathbb{Z}_n^*. \tag{161}$$

Tästä käy ilmi, että

$$\overline{a}^{-1} = \overline{a}^{\varphi(n)-1}, \tag{162}$$

joten käänteisalkio $\overline{a}^{-1}$ saadaan potenssiinkorotuksella laskemalla $\overline{a}^{\varphi(n)-1}$.

Lause 9.3. *FERMAT'N PIKKULAUSE: Olkoon $p \in \mathbb{P}$ annettu. Tällöin*

$$a^{p-1} \equiv 1 \pmod{p}, \quad \textit{jos} \quad p \nmid a \in \mathbb{Z}; \tag{163}$$

$$a^p \equiv a \pmod{p}, \quad \forall\ a \in \mathbb{Z}. \tag{164}$$

Olettaen (163) todistetaan (164):
Jos $\text{syt}(a, p) = 1$, niin Pikku Fermat'n (163) nojalla

$$a^p \equiv a \pmod{p}. \tag{165}$$

Jos $p|a$, niin

$$a \equiv 0 \pmod{p} \quad \Rightarrow \quad a^p \equiv 0 \pmod{p} \tag{166}$$

$$\Rightarrow \quad a^p \equiv a \pmod{p}. \quad \square \tag{167}$$

10 Nopeaa potenssilaskentaa

10.1 Nopeaa potenssilaskentaa/kertolaskuryhmässä

Lasketaan ryhmässä H alkion $a \in H$ potenssi:

$$a^r,\ r \in \mathbb{Z}^+, \quad r \leq h = \#H,$$

$$r = e_{t-1}2^{t-1} + \ldots + e_0,\ e_i \in \{0,1\},\ e_{t-1} = 1. \tag{168}$$

Aluksi:

$$\begin{aligned} a_1 &= a \\ a_2 &= a_1^2 = a^{2^1} \\ a_3 &= a_2^2 = a^{2^2} \\ &\vdots \\ a_t &= a_{t-1}^2 = a^{2^{t-1}}. \end{aligned} \tag{169}$$

Yhteensä $t-1$ kertolaskua.
Seuraavaksi:

$$a^r = a_t^{e_{t-1}} \cdot a_{t-1}^{e_{t-2}} \cdot \ldots \cdot a_1^{e_0}, \tag{170}$$

missä korkeintaan $t-1$ kertolaskua. Siten

Lause 10.1. *Olkoon $1 \leq r \leq h = \#H$. Tällöin potenssin a^r laskemiseen tarvitaan*

$$\leqslant 2t - 2 \leq 2\log_2 r \leq 2\log_2 h \tag{171}$$

ryhmän H laskutoimitusta.

Esimerkki 10.2.

$$a \in \mathbb{Z}_p^*, \quad \#\mathbb{Z}_p^* = p - 1 = h. \tag{172}$$

$$r \leq p - 1 \leq 2^{500} \quad \Rightarrow \quad 2t - 2 \leq 1000. \tag{173}$$

11 Funktioista

Kurssilta Johdatus matemaattiseen päättelyyn löytyy peruskäsitteet, kuten injektio, surjektio ja bijektio.

Lause 11.1. *Olkoon*

$$\#A = \#B \tag{174}$$

ja

$$f : A \to B \tag{175}$$

injektio. Tällöin $f : A \to B$ on bijektio.