

I Kontrolltöö aines "Sissejuhatus andmeturbesse"

Variant A

5.aprill, 2005

Ülesanded

Ülesanne 1 (15 punkti). Arvuta:

$$(1) \text{ s\"ut}(204, 68) \quad (2) \frac{1}{5} \pmod{17} \quad (3) x^4 + 1 \pmod{x^2 + 1} .$$

Ülesanne 2 (25 punkti). Šifreerimine toimub valemi

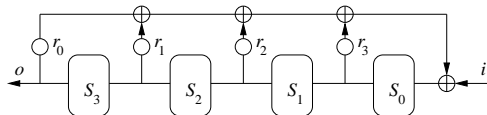
$$y = E(x) = 6x + 15 \pmod{49}$$

järgi. Leia vastav dešifreerimisteisendus $x = D(y)$ ja tõesta, et leitud teisendus on korrektne, s.t. $D(E(x)) = x$ iga $x \in \{0, \dots, 48\}$ korral.

Ülesanne 3 (30 punkti). Kas leidub esimest liiki 4 trigeriga lineaarne nihkeregister (nullise sisendjadaga i), mille väljundjada sisaldab lõiku:

0001111010 ?

Kas leidub ka 3 trigeriga lin. nihkeregister sama väljundjadaga? Põhjenda.



Ülesanne 4 (30 punkti). Juhuslik suurus X valitakse ühtlase jaotusega hulgast $\{1, 2, \dots, 16\}$. Juhuslik suurus Y arvutatakse juhuslikust suurusel X valemi $Y = X^2 \pmod{17}$ järgi. Leia juhusliku suuruse Y entroopia $H[Y]$.

Lahendused

Ülesanne 1. Esimeses alamülesandes kasutame Eukleidese algoritmi:

$$\begin{aligned}(1) \text{ s\"ut}(204, 68) &= \text{ s\"ut}(204 - 2 \cdot 68, 68) = \text{ s\"ut}(68, 68) \\ &= \mathbf{68} .\end{aligned}$$

(2) Teises alamülesandes tähistame esmalt $A = 5$, $B = 17$ ja arvutame suurima ühisteguri, säilitades samal ajal vastust lineaaravaldisena muutujaist A ja B :

$$\begin{aligned}\text{ s\"ut}(A, B) &= \text{ s\"ut}(5, 17) \\ \text{ s\"ut}(A, B - 3A) &= \text{ s\"ut}(5, 2) \\ \text{ s\"ut}(A - 2(B - 3A), B - 3A) &= \text{ s\"ut}(7A - 2B, B - 3A) = \text{ s\"ut}(1, 2) .\end{aligned}$$

Järelikult $7A - 2B = 1$, millest tuleneb, et $7 \cdot 5 \equiv 1 \pmod{17}$, ja seega $\frac{1}{5} \pmod{17} = \mathbf{7}$.

(3) Kasutame polünoomide jagamist:

$$\begin{array}{r}x^4 + 1 \quad \div \quad x^2 + 1 = x^2 + 1 \\ \underline{x^4 + x^2} \\ x^2 + 1 \\ \underline{x^2 + 1} \\ 0 .\end{array}$$

Et jagamisel tekki jääk tuleb 0, siis järelikult $x^4 + 1 \pmod{x^2 + 1} = \mathbf{0}$.

Ülesanne 2. Dešifreerimisfunktsioon on kujul $D(y) = \frac{1}{6}(y - 15) \pmod{49}$, mille ilmutatud kujul kirjapanekuks tuleb leida $\frac{1}{6} \pmod{49}$. Selleks kasutame Eukleidese algoritmi, tähistades $A = 6$ ja $B = 49$:

$$\begin{aligned}\text{ s\"ut}(A, B) &= \text{ s\"ut}(6, 49) \\ \text{ s\"ut}(A, B - 8A) &= \text{ s\"ut}(6, 1) .\end{aligned}$$

Seega, $B - 8A = 1$ ja $(-8) \cdot 6 \equiv 1 \pmod{49}$, millest järeldub $\frac{1}{6} \pmod{49} \equiv -8 \equiv 41 \pmod{49}$ ja

$$x = D(y) = 41(y - 15) \pmod{49} = 41y + 22 \pmod{49}.$$

Näitame, et D on korrektne dešifreerimisteisendus. Võtame suvalise $x \in \{0, \dots, 48\}$ ja arvutame:

$$\begin{aligned} D(E(x)) &= D(6x + 15 \pmod{49}) = D(6x + 15 + 49m) \\ &= 41(6x + 15 + 49m - 15) \pmod{49} \\ &= 246x + 41 \cdot 49m \pmod{49} = x + 49 \cdot (5x + 41m) \pmod{49} \\ &= x . \end{aligned}$$

Ülesanne 3. Tähistame väljundjada $Z = z_0 z_1 \dots z_9 = 00011111010$. Vastavalt esimest liiki lineaarse nihkeregistri ehitusele (Joonis), rahuldab väljundjada iga $k \geq 3$ korral seost:

$$r_0 z_{k-3} \oplus r_1 z_{k-2} \oplus r_2 z_{k-1} \oplus r_3 z_k = z_{k+1} . \quad (1)$$

Kirjutades üles võrrandid $k = 3, 4, 5, 6$ korral, saame järgmine võrrandisüsteemi üle \mathbb{Z}_2 :

$$\begin{cases} 0 \cdot r_0 + 0 \cdot r_1 + 0 \cdot r_2 + 1 \cdot r_3 = 1 \\ 0 \cdot r_0 + 0 \cdot r_1 + 1 \cdot r_2 + 1 \cdot r_3 = 1 \\ 0 \cdot r_0 + 1 \cdot r_1 + 1 \cdot r_2 + 1 \cdot r_3 = 1 \\ 1 \cdot r_0 + 1 \cdot r_1 + 1 \cdot r_2 + 1 \cdot r_3 = 0 \end{cases} ,$$

mille lahendamisel saame $r_3 = r_0 = 1$, $r_1 = r_2 = 0$. Jääb üle kontrollida, kas leitud lahend on kooskõlas väljundjada kahe viimase bitiga $z_8 z_9 = 10$. Kontrolliks arvutame z_8 ja z_9 seose (1) abil (võttes $k = 7, 8$):

$$\begin{aligned} z_8 &= 1 \cdot z_4 + 0 \cdot z_5 + 0 \cdot z_6 + 1 \cdot z_7 = 1 \\ z_9 &= 1 \cdot z_5 + 0 \cdot z_6 + 0 \cdot z_7 + 1 \cdot z_8 = 0 . \end{aligned}$$

Et bittide z_8 ja z_9 arvutatud langesid kokku jadas Z olevate väärtustega, siis järelikult leidub neljandat järku esimest liiki lineaarne nihkeregister väljundjadaga Z .

Kolmandat järku nihkeregistrit väljundjadaga Z aga ei leidu, sest $z_0 z_1 z_2 = 000$ ja registri algolek peaks olema nullolek. See on aga vastuolus jada Z järgmise bitiga $z_3 = 1$.

Ülesanne 4. Et funktsiooni $f(x) = x^2 \pmod{17}$ määramispiirkond $\{1, \dots, 16\}$ on suhteliselt väike, siis arvutame funktsiooni $f(x)$ tabeli:

x	$f(x)$
1	1
2	4
3	9
4	16
5	8
6	2
7	15
8	13
9	13
10	15
11	2
12	8
13	16
14	9
15	4
16	1

Tabelist on näha, et suurusel Y on kaheksa erinevat võimalikku väärtust: $Y = \{1, 2, 4, 8, 9, 13, 15, 16\}$, kusjuures igal väärtusel on täpselt kaks originaali hulgas $X = \{1, \dots, 16\}$. Et X on ühtlase jaotusega (s.t. kõik tõenäosused võrdsed $\frac{1}{16}$), siis iga $y \in Y$ tõenäosus on $\frac{2}{16} = \frac{1}{8}$. Seega, entroopia tuleb:

$$H[Y] = 8 \cdot \frac{1}{8} \log_2 \frac{1}{\frac{1}{8}} = \log_2 8 = \mathbf{3} .$$