

I Kontrolltöö aines "Sissejuhatus andmeturbesse"

Variant B

5.aprill, 2005

Ülesanded

Ülesanne 1 (15 punkti). Arvuta:

$$(1) \text{ s\"ut}(161, 56) \quad (2) \frac{1}{4} \pmod{23} \quad (3) x^4 + x + 1 \pmod{x^2 + x} .$$

Ülesanne 2 (25 punkti). Šifreerimine toimub valemi

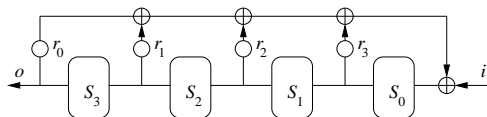
$$y = E(x) = 7x + 18 \pmod{48}$$

järgi. Leia vastav dešifreerimisteisendus $x = D(y)$ ja tõesta, et leitud teisendus on korrektne, s.t. $D(E(x)) = x$ iga $x \in \{0, \dots, 47\}$ korral.

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

0001010001 ?

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



Ülesanne 4 (30 punkti). Juhuslik suurus X valitakse ühtlase jaotusega hulgast $\{0, 1, \dots, 8\}$. Juhuslik suurus Y arvutatakse juhuslikust suurusest X valemi $Y = X^3 \pmod{9}$ järgi. Leia juhusliku suuruse Y entroopia $H[Y]$.

Lahendused

Ülesanne 1. Esimeses alamülesandes kasutame Eukleidese algoritmi:

$$\begin{aligned}(1) \text{ s\"ut}(161, 56) &= \text{ s\"ut}(161 - 2 \cdot 56, 56) = \text{ s\"ut}(49, 56) = \text{ s\"ut}(49, 56 - 49) \\ &= \text{ s\"ut}(49, 7) = \text{ s\"ut}(49 - 6 \cdot 7, 7) = \text{ s\"ut}(7, 7) \\ &= \mathbf{7} .\end{aligned}$$

(2) Teises alamülesandes tähistame esmalt $A = 4$, $B = 23$ ja arvutame suurima ühisteguri, säilitades samal ajal vastust lineaaravaldisena muutujaist A ja B :

$$\begin{aligned}\text{ s\"ut}(A, B) &= \text{ s\"ut}(4, 23) \\ \text{ s\"ut}(A, B - 5A) &= \text{ s\"ut}(4, 3) \\ \text{ s\"ut}(A - (B - 5A), B - 5A) &= \text{ s\"ut}(6A - B, B - 5A) = \text{ s\"ut}(1, 3) .\end{aligned}$$

Järelikult $6A - B = 1$, millest tuleneb, et $6 \cdot 4 \equiv 1 \pmod{23}$, ja seega $\frac{1}{4} \pmod{23} = \mathbf{6}$.

(3) Kasutame polünoomide jagamist:

$$\begin{array}{r}x^4 + x + 1 \quad \div \quad x^2 + x = x^2 + x + 1 \\ \underline{x^4 + x^3} \\ x^3 + x + 1 \\ \underline{x^3 + x^2} \\ x^2 + x + 1 \\ \underline{x^2 + x} \\ 1 .\end{array}$$

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

Ülesanne 2. Dešifreerimisfunktsioon on kujul $D(y) = \frac{1}{7}(y - 18) \pmod{48}$, mille ilmutatud kujul kirjapanekuks tuleb leida $\frac{1}{7} \pmod{48}$. Selleks kasutame Eukleidese algoritmi, tähistades $A = 7$ ja $B = 48$:

$$\begin{aligned}\text{ s\"ut}(A, B) &= \text{ s\"ut}(7, 48) \\ \text{ s\"ut}(A, B - 6A) &= \text{ s\"ut}(7, 6) \\ \text{ s\"ut}(A - (B - 6A), B - 6A) &= \text{ s\"ut}(7A - B, B - 6A) = \text{ s\"ut}(1, 6) .\end{aligned}$$

Seega, $7A - B = 1$ ja $7 \cdot 7 \equiv 1 \pmod{48}$, millest järeldub $\frac{1}{7} \pmod{48} = \mathbf{7}$ ja

$$x = D(y) = 7(y - 18) \pmod{48} = 7y + 18 \pmod{48}.$$

Näitame, et D on korrektne dešifreerimisteisendus. Võtame suvalise $x \in \{0, \dots, 47\}$ ja arvutame:

$$\begin{aligned} D(E(x)) &= D(7x + 18 \pmod{48}) = D(7x + 18 + 48m) \\ &= 7(7x + 18 + 48m - 18) \pmod{48} \\ &= 49x + 7 \cdot 48m \pmod{48} = x + 48 \cdot (x + 7m) \pmod{48} \\ &= x . \end{aligned}$$

Ülesanne 3. Tähistame väljundjada $Z = z_0 z_1 \dots z_9 = 0001010001$. 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 :

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

mille lahendamisel saame $r_3 = r_1 = 0$, $r_0 = r_2 = 1$. Jääb üle kontrollida, kas leitud lahend on kooskõlas väljundjada kahe viimase bitiga $z_8 z_9 = 01$. Kontrolliks arvutame z_8 ja z_9 seose (1) abil (võttes $k = 7, 8$):

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

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 $f(x) = x^3 \pmod{9}$ määramispiirkond $\{0, \dots, 8\}$ on suhteliselt väike, siis arvutame funktsiooni $f(x)$ tabeli kujul, arvutades esmalt $z = x^2 \pmod{9}$ ja seejärel $f(x) = z \cdot x \pmod{9}$.

x	$x^2 \pmod{9}$	$y = f(x)$
0	0	0
1	1	1
2	4	8
3	0	0
4	7	1
5	7	8
6	0	0
7	4	1
8	1	8

Tabelist on näha, et suurusel Y on kolm erinevat võimalikku väärtust: $\{0, 1, 8\}$, kusjuures igal väärtusel on täpselt kolm originaali hulgas $X = \{0, 1, \dots, 8\}$. Et X on ühtlase jaotusega (s.t. kõik tõenäosused võrdsed $\frac{1}{9}$), siis iga $y \in \{0, 1, 8\}$ tõenäosus on $\frac{3}{9} = \frac{1}{3}$. Seega, entroopia tuleb:

$$H[Y] = 3 \cdot \frac{1}{3} \log_2 \frac{1}{\frac{1}{3}} = \log_2 3 \approx \mathbf{1.585} .$$