

I Kontrolltöö aines "Sissejuhatus andmeturbesse"

Variant C

5.aprill, 2005

Ülesanded

Ülesanne 1 (15 punkti). Arvuta:

$$(1) \text{ s\"ut}(204, 84) \quad (2) \frac{1}{6} \pmod{59} \quad (3) x^5 + 1 \pmod{x^2 + x + 1} .$$

Ülesanne 2 (25 punkti). Šifreerimine toimub valemi

$$y = E(x) = ax + b \pmod{55}$$

järgi. On teada, et $E(2) = 18$ ja $E(6) = 24$. Leia a ja b .

Ülesanne 3 (30 punkti). Jadašiffer genereerib algvõtmest $K = K_0 \dots K_5 \in \{0, 1\}^6$ võtmejada $z_0 z_1 z_2 \dots z_n \dots$ järgmiselt:

$$\begin{aligned} z_0 &= K_0 \\ z_1 &= K_1 \\ z_2 &= K_2 \\ z_{k+1} &= K_5 \cdot z_k + K_4 \cdot z_{k-1} + K_3 \cdot z_{k-2} \pmod{2} \quad (\text{kui } k > 2) . \end{aligned}$$

Krüpteerimine toimub eeskirja $y_i = x_i \oplus z_i$ järgi, kus \oplus tähistab liitmist mooduliga 2. On teada, et $Y = y_3 y_4 \dots y_8 = 101110$ ja $X = x_3 x_4 \dots x_8 = 001001$. Leia algvõti $K = K_0 K_1 \dots K_5$.

Ülesanne 4 (30 punkti). Juhuslik suurus X valitakse ühtlase jaotusega hulgast $\{0, 1, \dots, 19\}$. Juhuslik suurus Y arvutatakse juhuslikust suurusel X valemi $Y = 5X \pmod{20}$ järgi. Leia juhusliku suuruse Y entroopia $H[Y]$.

Lahendused

Ülesanne 1. Esimeses alamülesandes kasutame Eukleidese algoritmi:

$$\begin{aligned}(1) \text{ s\"ut}(204, 84) &= \text{ s\"ut}(204 - 2 \cdot 84, 84) = \text{ s\"ut}(36, 84) = \text{ s\"ut}(36, 84 - 2 \cdot 36) \\ &= \text{ s\"ut}(36, 12) = \text{ s\"ut}(36 - 2 \cdot 12, 12) = \text{ s\"ut}(12, 12) \\ &= \mathbf{12} .\end{aligned}$$

(2) Teises alamülesandes tähistame esmalt $A = 6$, $B = 59$ ja arvutame suurima ühisteguri, säilitades samal ajal vastust lineaaravaldisena muutujaist A ja B :

$$\begin{aligned}\text{ s\"ut}(A, B) &= \text{ s\"ut}(6, 59) \\ \text{ s\"ut}(A, B - 9A) &= \text{ s\"ut}(6, 5) \\ \text{ s\"ut}(A - (B - 9A), B - 9A) &= \text{ s\"ut}(10A - B, B - 9A) = \text{ s\"ut}(1, 5) .\end{aligned}$$

Järelikult $10A - B = 1$, millest tuleneb, et $10 \cdot 6 \equiv 1 \pmod{59}$, ja seega $\frac{1}{6} \pmod{59} = \mathbf{10}$.

(3) Kasutame polünoomide jagamist:

$$\begin{array}{r}x^5 + 1 \quad \div \quad x^2 + x + 1 = x^3 + x^2 + 1 \\ \underline{x^5 + x^4 + x^3} \\ x^4 + x^3 + 1 \\ \underline{x^4 + x^3 + x^2} \\ x^2 + 1 \\ \underline{x^2 + x + 1} \\ x .\end{array}$$

Et jagamisel tekkinud jääk tuleb x , siis järelikult $x^5 + 1 \pmod{x^2 + x + 1} = x$.

Ülesanne 2. Seostest $E(2) = 18$ ja $E(6) = 24$ saame võrrandisüsteemi:

$$\begin{cases} 2a + b \equiv 18 \pmod{55} \\ 6a + b \equiv 24 \pmod{55} \end{cases}$$

Lahutades alumisest võrrandist ülemise, saame $4a \equiv 6 \pmod{55}$, mille lahendamiseks tuleb esmalt arvutada $\frac{1}{4} \pmod{55}$. Tähistades $A = 4$, $B = 55$ ja rakendades Eukleidese algoritmi, saame:

$$\begin{aligned}\text{ s\"ut}(A, B) &= \text{ s\"ut}(4, 55) \\ \text{ s\"ut}(A, B - 13A) &= \text{ s\"ut}(4, 3) \\ \text{ s\"ut}(A - (B - 13A), B - 13A) &= \text{ s\"ut}(14A - B, B - 13A) = \text{ s\"ut}(1, 3) .\end{aligned}$$

Seega, $14A - B = 1$ ja $14 \cdot 4 \equiv 1 \pmod{55}$, mistõttu $\frac{1}{4} \pmod{55} \equiv 14$. Nüüd avaldame a ja saame $a \equiv 6 \cdot 14 \equiv \mathbf{29} \pmod{55}$ ja $b = 18 - 2 \cdot 29 \equiv \mathbf{15} \pmod{55}$.

Ülesanne 3. Esmalt leiame vastava võtmejada lõigu $Z = z_3 z_4 \dots z_8 = X \oplus Y = 001001 \oplus 101110 = 100111$, st $z_3 = z_6 = z_7 = z_8 = 1$ ja $z_4 = z_5 = 0$. See teadmine võimaldab välja kirjutada võrrandisüsteemi võtmete K_3, K_4 ja K_5 leidmiseks:

$$\begin{cases} z_7 \cdot K_5 + z_6 \cdot K_4 + z_5 \cdot K_3 = z_8 \\ z_6 \cdot K_5 + z_5 \cdot K_4 + z_4 \cdot K_3 = z_7 \\ z_5 \cdot K_5 + z_4 \cdot K_4 + z_3 \cdot K_3 = z_6 \end{cases} \sim \begin{cases} 1 \cdot K_5 + 1 \cdot K_4 + 0 \cdot K_3 = 1 \\ 1 \cdot K_5 + 0 \cdot K_4 + 0 \cdot K_3 = 1 \\ 0 \cdot K_5 + 0 \cdot K_4 + 1 \cdot K_3 = 1 \end{cases} ,$$

mida lahendades saame $K_3 = 1, K_4 = 0$ ja $K_5 = 1$. Edasi saab aga tuletada võrrandisüsteemi K_0, K_1 ja K_2 leidmiseks:

$$\begin{cases} z_4 \cdot K_5 + z_3 \cdot K_4 + z_2 \cdot K_3 = z_5 \\ z_3 \cdot K_5 + z_2 \cdot K_4 + z_1 \cdot K_3 = z_4 \\ z_2 \cdot K_5 + z_1 \cdot K_4 + z_0 \cdot K_3 = z_3 \end{cases} \sim \begin{cases} 0 \cdot 1 + 1 \cdot 0 + K_2 \cdot 1 = 0 \\ 1 \cdot 1 + K_2 \cdot 0 + K_1 \cdot 1 = 0 \\ K_2 \cdot 1 + K_1 \cdot 0 + K_0 \cdot 1 = 1 \end{cases} ,$$

mille ainus lahend on $K_0 = 1, K_1 = 1$ ja $K_2 = 0$. Seega $K = K_0 \dots K_5 = 110101$.

Ülesanne 4. Vahetu arvutuse teel võib veenduda, et funktsiooni

$$f(x) = 5x \pmod{20}$$

väärtuste hulk Y on 4-elementiline: $Y = \{0, 5, 10, 15\}$, kusjuures igal väärtusel $y \in Y$ on täpselt viis originaali, mis avalduvad kujul:

$$x, \quad x+4 \pmod{20}, \quad x+8 \pmod{20}, \quad x+12 \pmod{20}, \quad x+16 \pmod{20} ,$$

kus x on üks originaalidest. See tuleneb tähelepanekust, et $f(x_1) = f(x_2)$ parajasti siis, kui $x_1 \equiv x_2 \pmod{4}$. Tõepoolest, kui $x_1 \equiv x_2 \pmod{4}$, siis leidub $m \in \mathbb{Z}$, nii et $x_1 = x_2 + 4m$, mistõttu

$$\begin{aligned} f(x_1) &= f(x_2 + 4m) = 5(x_2 + 4m) \pmod{20} \\ &= (5x_2 + 20m) \pmod{20} = 5x_2 \pmod{20} \\ &= f(x_2) . \end{aligned}$$

Teiselt poolt, kui $f(x_1) = f(x_2)$, siis järelikult $5x_1 \equiv 5x_2 \pmod{20}$, s.t. leidub $m \in \mathbb{Z}$, nii et $5x_1 = 5x_2 + 20m$. Seega, jagades võrrandi mõlemad pooli viiega, saame $x_1 = x_2 + 4m$, ehk $x_1 \equiv x_2 \pmod{4}$.

Et X on ühtlase jaotusega, siis iga originaali x tõenäosus on $\frac{1}{20}$, millest järgeldub, et hulga Y (juhusliku suuruse) iga elemendi tõenäosus on $\frac{5}{20} = \frac{1}{4}$. Seega, entroopia tuleb

$$H[Y] = 4 \cdot \frac{1}{4} \cdot \log_2 \frac{1}{\frac{1}{4}} = \log_2 4 = 2 \text{ .}$$