

I Kontrolltöö aines "Sissejuhatus andmeturbesse"

Variant D

5.aprill, 2005

Ülesanded

Ülesanne 1 (15 punkti). Arvuta:

$$(1) \text{ s\"ut}(162, 63) \quad (2) \frac{1}{8} \pmod{61} \quad (3) x^4 + x + 1 \pmod{x^2} .$$

Ülesanne 2 (25 punkti). Šifreerimine toimub valemi

$$y = E(x) = ax + b \pmod{56}$$

järgi. On teada, et $E(2) = 19$ ja $E(7) = 25$. 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:

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

Krüpteerimine toimub eeskirja $y_i = x_i \oplus z_i$ järgi, kus \oplus tähistab liitmist mooduliga 2. On teada, et $Y = y_3 y_4 \dots y_8 = 010111$ ja $X = x_3 x_4 \dots x_8 = 110011$. Leia algvõti $K = K_0 K_1 \dots K_5$.

Ülesanne 4 (30 punkti). Juhuslik suurus X valitakse ühtlase jaotusega hulgast $\{0, 1, \dots, 23\}$. Juhuslik suurus Y arvutatakse juhuslikust suurusest X valemi $Y = 3X \pmod{24}$ järgi. Leia juhusliku suuruse Y entroopia $H[Y]$.

Lahendused

Ülesanne 1. Esimeses alamülesandes kasutame Eukleidese algoritmi:

$$\begin{aligned}(1) \text{ s\"ut}(162, 63) &= \text{ s\"ut}(162 - 2 \cdot 63, 63) = \text{ s\"ut}(36, 63) = \text{ s\"ut}(36, 63 - 36) \\ &= \text{ s\"ut}(36, 27) = \text{ s\"ut}(36 - 27, 27) = \text{ s\"ut}(9, 27) \\ &= \text{ s\"ut}(9, 27 - 2 \cdot 9) = \text{ s\"ut}(9, 9) \\ &= 9 .\end{aligned}$$

(2) Teises alamülesandes tähistame esmalt $A = 8$, $B = 61$ ja arvutame suurima ühisteguri, säilitades samal ajal vastust lineaaravaldisena muutujaist A ja B :

$$\begin{aligned}\text{ s\"ut}(A, B) &= \text{ s\"ut}(8, 61) \\ \text{ s\"ut}(A, B - 7A) &= \text{ s\"ut}(8, 5) \\ \text{ s\"ut}(A - (B - 7A), B - 7A) &= \text{ s\"ut}(8A - B, B - 7A) = \text{ s\"ut}(3, 5) \\ \text{ s\"ut}(8A - B, (B - 7A) - (8A - B)) &= \text{ s\"ut}(8A - B, 2B - 15A) = \text{ s\"ut}(3, 2) \\ \text{ s\"ut}(8A - B - (2B - 15A), 2B - 15A) &= \text{ s\"ut}(23A - 3B, 2B - 15A) = \text{ s\"ut}(1, 2) .\end{aligned}$$

Järelikult $23A - 3B = 1$, millest tuleneb, et $23 \cdot 8 \equiv 1 \pmod{61}$, ja seega $\frac{1}{8} \pmod{61} = 23$.

(3) Kasutame polünoomide jagamist:

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

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

Ülesanne 2. Seostest $E(2) = 19$ ja $E(7) = 25$ saame võrrandisüsteemi:

$$\begin{cases} 2a + b \equiv 19 \pmod{56} \\ 7a + b \equiv 25 \pmod{56} \end{cases}$$

Lahutades alumisest võrrandist ülemise, saame $5a \equiv 6 \pmod{56}$, mille lahendamiseks tuleb esmalt arvutada $\frac{1}{5} \pmod{56}$. Tähistades $A = 5$, $B = 56$ ja rakendades Eukleidese algoritmi, saame:

$$\begin{aligned}\text{ s\"ut}(A, B) &= \text{ s\"ut}(5, 56) \\ \text{ s\"ut}(A, B - 11A) &= \text{ s\"ut}(5, 1) .\end{aligned}$$

Seega, $B - 11A = 1$ ja $(-11) \cdot 5 \equiv 1 \pmod{56}$, mistõttu $\frac{1}{5} \pmod{56} \equiv -11 \equiv 56 - 11 = 45$. Nüüd avaldame a ja saame $a \equiv 6 \cdot 45 = 270 \equiv \mathbf{46} \pmod{56}$ ja $b = 19 - 2 \cdot 46 \equiv \mathbf{39} \pmod{56}$.

Ülesanne 3. Esmalt leiame vastava võtmejada lõigu $Z = z_3 z_4 \dots z_8 = X \oplus Y = 110011 \oplus 010111 = 100100$, st $z_4 = z_5 = z_7 = z_8 = 0$ ja $z_3 = z_6 = 1$. See teadmine võimaldab välja kirjutada võrrandisüsteemi võtmete K_3, K_4 ja K_5 leidmiseks:

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

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

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

mille ainus lahend on $K_0 = 1, K_1 = 0$ ja $K_2 = 0$. Seega $K = K_0 \dots K_5 = 100100$.

Ülesanne 4. Vahetu arvutuse teel võib veenduda, et funktsiooni

$$f(x) = 3x \pmod{24}$$

väärtuste hulk Y on 8-elementiline: $Y = \{0, 3, 6, 9, 12, 15, 18, 21\}$, kusjuures igal väärtusel $y \in Y$ on täpselt kolm originaali, mis avalduvad kujul:

$$x, \quad x + 8 \pmod{24}, \quad x + 16 \pmod{24} ,$$

kus x on üks originaalidest. See tuleneb tähelepanekust, et $f(x_1) = f(x_2)$ parajasti siis, kui $x_1 \equiv x_2 \pmod{8}$. Tõepoolest, kui $x_1 \equiv x_2 \pmod{8}$, siis leidub $m \in \mathbb{Z}$, nii et $x_1 = x_2 + 8m$, mistõttu

$$\begin{aligned} f(x_1) &= f(x_2 + 8m) = 3(x_2 + 8m) \pmod{24} \\ &= (3x_2 + 24m) \pmod{24} = 3x_2 \pmod{24} \\ &= f(x_2) . \end{aligned}$$

Teiselt poolt, kui $f(x_1) = f(x_2)$, siis järelikult $3x_1 \equiv 3x_2 \pmod{24}$, s.t. leidub $m \in \mathbb{Z}$, nii et $3x_1 = 3x_2 + 24m$. Seega, jagades võrrandi mõlemad pooli kolmega, saame $x_1 = x_2 + 8m$, ehk $x_1 \equiv x_2 \pmod{8}$.

Et X on ühtlase jaotusega, siis iga originaali x tõenäosus on $\frac{1}{24}$, millest järgneb, et hulga Y (juhusliku suuruse) iga elemendi tõenäosus on $\frac{3}{24} = \frac{1}{8}$. Seega, entroopia tuleb

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