

Ülesanded

Ülesanne 1 (30 punkti). Šifreerimine toimub valemi $y = E(x) = ax + b \pmod{101}$ järgi. On teada, et $E(3) = 80$ ja $E(51) = 7$. Leia a ja b .

Ülesanne 2 (30 punkti). Juhuslik suurus X on valitud ühtlase jaotusega hulgast $\{0, 1, \dots, 8\}$. Suurus Y arvutatakse suurisest X valemiga

$$Y = (X^4 - 1) \pmod{9} .$$

Leida suuruse Y Shannoni entroopia $H[Y]$.

Ülesanne 3 (40 punkti). On teada, et järgmine krüptogramm on moodustatud inglisekeelsest avatekstist kasutades Vigenere'i šifrit. Leida võtme märkide arv ja põhjendada vastust! Avateksti ennast ei ole vaja leida. Krüptogrammi esimene arvudest koosnev rida on mõeldud analüüsi kergendamiseks.

```
12345678901234567890123456789012345678901234567890
HSWVDWGTHVJHHEWPAOAGLZPUSMSTVUNWPUWCGIAVPHAVDLBDYW
LFNGZLHNRAEVEELSSCLUWWCNDDEVISLDIBFLTHUGAZBCVHSSRFF
ZFAAQZHHRJXCNBSWDHNTPHIPKFPSPGAEITVGYQICZPFIAOSWCUS
RWVRFZAVFESXGDPHTRJTGAYOLMSRFNFYCLPRIALZHHRKLAEPA
AVEELPLTYWEHEESSRUFFEGZPSXCDBAGAZBFBJEVIFOPOKAW
DGAFAQZICNFCSAQAYHHRHLHCNBNPZSZWYHIBFPRIFLSOTGZPTRRI
FSNPQOWSGJTPUGAZBSBXWSTGWCGIALSSPYSTBTRPEONQAYHHRU
TDHRJESXGS
```

Lahendused

Ülesanne 1. Ülesande eeldustest saame võrrandisüsteemi:

$$\begin{cases} 3a + b \equiv 80 \pmod{101} \\ 51a + b \equiv 7 \pmod{101} \end{cases}$$

Lahutades ülemisest võrrandist alumise, saame $-48a \equiv 73$ ehk $53a \equiv 73$, mille lahendamiseks on vaja leida $1/53 \pmod{101}$. Eukleidese algoritmi kasutades saame, et

$$-40 \cdot 53 + 21 \cdot 101 = 1 \text{ ,}$$

millest tuleneb, et $1/53 \equiv -40 \equiv 61 \pmod{101}$. Seega $a \equiv 61 \cdot 73 \equiv 9 \pmod{101}$. Ja esimesest võrrandist saame seega, et $b \equiv 80 - 3 \cdot 9 = 53$.

Ülesanne 2. Esitades funktsiooni $Y = (X^4 - 1) \pmod{9}$ väärtused tabelina:

X	Y
0	8
1	0
2	6
3	8
4	3
5	3
6	8
7	6
8	0

näeme, et juhuslik suurus Y omandab väärtusi $\{0, 3, 6, 8\}$ tõenäosustega $p(0) = p(3) = p(6) = \frac{2}{9}$ ja $p(8) = \frac{3}{9} = \frac{1}{3}$. Seega on suuruse Y Shannoni entroopia:

$$H[Y] = 3 \cdot \frac{2}{9} \cdot \log_2 \frac{9}{2} + \frac{1}{3} \cdot \log_2 3 = \frac{2}{3} \cdot \log_2 \frac{9}{2} + \frac{1}{3} \cdot \log_2 3 \approx 1.975 \text{ .}$$

Ülesanne 3. Õige võtmepikkus on 5. Seda näitab korduvate vähemalt kolmetäheliste sõnade positsioonide vahede suurim ühistegur (vt. *Kasiski test*). Korduvad sõned on näiteks "VEEL", "HHR", "SXG", "GAZB" jt.