

Ülesanded

Ülesanne 1 (30 punkti). Šifreerimine toimub valemi $y = E(x) = ax + b \pmod{101}$ järgi. On teada, et $E(2) = 100$ ja $E(50) = 2$. Leia a ja b .

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

$$Y = X^2 \pmod{9} .$$

Leida suuruse Y kombinatoorne entroopia $H_{\text{comb}}[Y]$.

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
REHCPGSEOHTTSLIZMZHSLABEWEECGXIABIMSTHHZTLCPVNOFI
VRYNLVTYYMOHPLXCENSGGINUPNHTZXNUMXDTFNMJNNCTCECMR
JRLHCJTSYVHOYIEGPSUFZTTWWPBDNMOUECSICTJLZRTHACINBE
BIGYRKLLCROEINPZTEYVDSLFAVYDYRJRJXZDTHXJTSYWVMPWM
KHPLXZXEFIOTPLEMEDYGPRPNLZEIJPVNLNMJNQIVOHTMAZAVHI
NSLMCJUNURMELXMITSYXROYIZZLDGIITIRZDTMXCAENLZFCYU
PEYWCYIDNVDBFNMJNDIJGEENIMSTHXCEAFEDNEYBOAYXMITSYG
DPSYVOEINEMETXIITTWEG
```

Lahendused

Ülesanne 1. Ülesande eeldustest saame võrrandisüsteemi:

$$\begin{cases} 2a + b \equiv 100 \pmod{101} \\ 50a + b \equiv 2 \pmod{101} \end{cases}$$

Lahutades ülemisest võrrandist alumise, saame $-48a \equiv 98$ ehk $53a \equiv 98$, mille lahendamiseks on vaja leida $1/53 \pmod{101}$. Eukleidese algoritmi kasutades saame, et

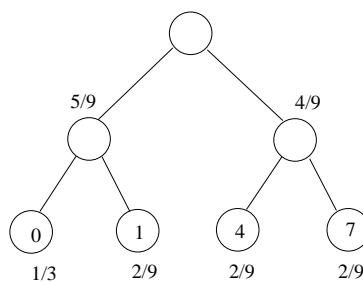
$$-40 \cdot 53 + 21 \cdot 101 = 1,$$

millest tuleneb, et $1/53 \equiv -40 \equiv 61 \pmod{101}$. Seega $a \equiv 61 \cdot 98 \equiv 19 \pmod{101}$. Ja esimesest võrrandist saame seega, et $b \equiv 100 - 2 \cdot 19 = 62$.

Ülesanne 2. Esitades funktsiooni $Y = X^2 \pmod{9}$ tabelina saame:

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

Seega omandab juhuslik suurus Y väärtusi $\{0, 1, 4, 7\}$ tõenäosustega $p(0) = \frac{1}{3}$, $p(1) = p(4) = p(7) = \frac{2}{9}$. Kombinatorse entroopia leidmiseks koostame suuruse Y Huffmani puu:



Et kõikide koodide pikkused tulevad võrdsed 2-ga, siis saame optimaalse koodi keskmiseks pikkuseks $2 \cdot (p(0) + p(1) + p(4) + p(7)) = 2 \cdot 1 = 2$. Seega $H_{\text{comb}}[Y] = 2$.

Ülesanne 3. Õige võtmepikkus on 5. Seda näitab korduvate vähemalt kolmetäheliste sõnade positsioonide vahede suurim ühistegur (vt. *Kasiski test*). Korduvad sõned on näiteks "HPLX", "NMJN", "TSY", "TTW", "EIN", "ZDT", "THX", "EME", "IITT", "XMI" jt.