

EESNIMI: ÖPPERÜHM:
PEREKONNANIMI:
MATRIKLI NUMBER:

Ülesanne 1 (30 punkti). Leia järgmise märgijada Y kokkulangevuse indeks $I_c(Y)$ ja püüa selle arvutuse põhjal vastata küsimusele, kas tegemist on asendusšifri abil loodud krüptogrammiga inglisekeelsest avatekstist):

WOOEGMFTIFUDSTNSNVTNDPASNHESBGSEGEMRDRSHEAIEO

Ülesanne 2 (30 punkti). Juhuslik suurus X on valitud ühtlase jaotusega hulgast $\{0, 1, \dots, 7\}$. Suurus Y arvutatakse suurisest X valemiga

$$Y = X^2 \pmod{8} .$$

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

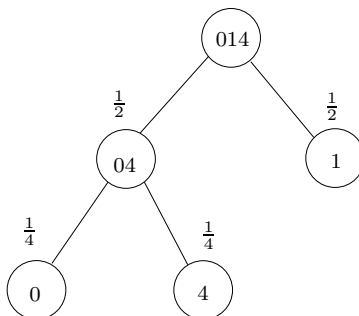
Ülesanne 3 (40 punkti). Šifreerimine toimub valemi $y = E(x) = ax + b \pmod{101}$ järgi. On teada, et $E(2) = 90$ ja $E(42) = 9$. Leia a ja b .

VASTUSED:

Ü1.1.
Ü1.2.
Ü1.3.

Lahendus 1. Et $I_c(Y) = 0.054545$, siis võib oletada, et see on tõepoolest loomulikus keeles kirjutatud sõnumi krüptogramm (lähmal väärtusele 0.065 kui väärtusele 0.038).

Lahendus 2. Saame, et $\Pr[1] = \frac{4}{8}$, $\Pr[0] = \Pr[4] = \frac{2}{8} = \frac{1}{4}$. Seega tuleb Huffmani puu järgmine:



ja koodi keskmine pikkus $2 \cdot \frac{1}{4} + 2 \cdot \frac{1}{4} + 1 \cdot \frac{1}{2} = 1.5$, mis ongi kombinatoorne entroopia.

Lahendus 3. Tavalisel viisil lineaarvõrrandisüsteemi lahendades saaksime $a = -\frac{81}{40}$ ja $b = \frac{1881}{20}$, mis *modulo* 101 annab $a = 51$ ja $b = 89$.