

EESNIMI: ÖPPERÜHM:
PEREKONNANIMI:
MATRIKLI NUMBER:

Ülesanne 1 (30 punkti). Leia järgmiste märgijadade Y_1 ja Y_2 omavahe-
lise kokkulangevuse indeks $I_c(Y_1, Y_2)$ ja püüa selle arvutuse põhjal vastata
küsimusele, kas tegemist võib olla ühe ja sama asendusšifri ja sama võtme
abil loodud krüptogrammidega (inglisekeelsetest avatekstidest):

Y_1 : ARANOBQRASAJNVRAPT CXUGRJRUQTHLVGRLJHNGYNQRRG
 Y_2 : RUQTHLVGRLJHNGYNQRRGINRYQPVEEBRVRHIRIE

Ülesanne 2 (30 punkti). Juhuslik suurus X on valitud ühtlase jaotusega
hulgast $\{0, 1, \dots, 11\}$. Suurus Y arvutatakse suurisest X valemiga

$$Y = X^2 + 3 \pmod{12} .$$

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

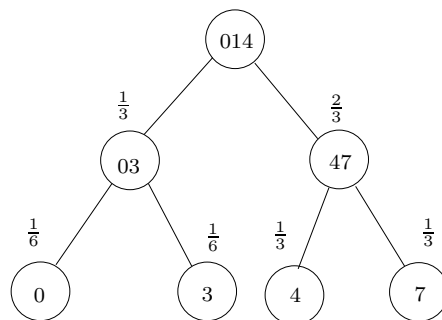
Ülesanne 3 (40 punkti). Leia $\frac{1}{10} \pmod{103}$ ja $\frac{1}{17} \pmod{51}$.

VASTUSED:

Ü1.1.
Ü1.2.
Ü1.3.

Lahendus 1. Et $I_c(Y_1, Y_2) = 0.074163$, siis võib oletada, et krüpteeritud on sama asendusšifriga.

Lahendus 2. Saame, et $\Pr[0] = \Pr[3] = \frac{2}{12} = \frac{1}{6}$, $\Pr[4] = \Pr[7] = \frac{4}{12} = \frac{1}{3}$. Seega tuleb Huffmani puu järgmine:



ja koodi keskmine pikkus $2 \cdot 2 \cdot \frac{1}{6} + 2 \cdot 2 \cdot \frac{1}{3} = 2$, mis ongi kombinatoorne entroopia.

Lahendus 3. $\frac{1}{10} \pmod{103} = 31$ ja $\frac{1}{17} \pmod{51}$ ei leidu sest $(17, 51) = 17 \neq 1$.