

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):

$Y_1$ : EMTXBHMRXXXBMGXLLKMGXAGLLPHTGTHFLBKRGX

$Y_2$ : MGXAGLLPHTGTHFLBKRGXHBTLMXGWHVBEAAXHKZLWWGF

**Ülesanne 2 (30 punkti).** Olgu meil krüptosüsteem kõikvõimalike avatek-  
stide hulgaga  $\{1, \dots, 10\}$  (mis on ühtlasi ka kõigi krüptogrammide ja võtmete  
hulk) ja krüpteerimisteisendusega:

$$y = E(x) = a \cdot x \pmod{11},$$

kus  $x$  on avatekst ja  $a$  on võti. Kas see krüptosüsteem on täielikult salas-  
tav, arvestades et võti  $a$  on ühtlase jaotusega valitud hulgast  $\{1, \dots, 10\}$  ja  
krüptosüsteemi kasutatakse vaid ühe sõnumi  $x \in \{1, \dots, 10\}$  krüpteerimiseks?

**Ülesanne 3 (40 punkti).** Šifreerimine toimub valemi  $y = E(x) = ax + b$   
mod 103 järgi. On teada, et  $E(2) = 80$  ja  $E(35) = 10$ . Leia  $a$  ja  $b$ .

VASTUSED:

Ül.1. ....  
Ül.2. ....  
Ül.3. ....

**Lahendus 1.** Et  $I_c(Y_1, Y_2) = 0.082168$ , siis võib oletada, et krüpteeritud on sama asendusšifriga.

**Lahendus 2.** Et 11 on algarv, siis kõik mittenuollised jäägid mod 11 on pööratavad ja seega on korrutamine  $a$ -ga hulga  $\{1, \dots, 10\}$  üksühene teisendus. Suvalisele arvude paarile  $x$  ja  $y$  hulgast  $\{1, \dots, 10\}$  leidub üks ja ainult üks võti  $a$ , nii et  $a \cdot x \pmod{11} = y$ , nimelt  $a = y \cdot \frac{1}{x} \pmod{11}$ . Seega

$$p(x | y) = \frac{1}{10} = p(x) ,$$

mistõttu šiffer on täielikult salastav.

**Lahendus 3.** Tavalisel viisil lineaarvõrrandisüsteemi lahendades saaksime  $a = -\frac{70}{33}$  ja  $b = \frac{2780}{33}$ , mis *modulo* 103 annab  $a = 1$  ja  $b = 78$ .