

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):

WEBQBUAWWQRWWXANTBDPXXRDWBFAXCWMNJJFAIACN

Ülesanne 2 (30 punkti). Olgu meil krüptosüsteem kõikvõimalike avatekstide hulgaga $\{1, \dots, 6\}$ (mis on ühtlasi ka kõigi krüptogrammide ja võtmete hulk) ja krüpteerimisteisendusega:

$$y = E(x) = a \cdot x \pmod{7},$$

kus x on avatekst ja a on võti. Kas see krüptosüsteem on täielikult salastav, arvestades et võti a on ühtlase jaotusega valitud hulgast $\{1, \dots, 6\}$ ja krüptosüsteemi kasutatakse vaid ühe sõnumi $x \in \{1, \dots, 6\}$ krüpteerimiseks?

Ülesanne 3 (40 punkti). Leia $\frac{1}{8} \pmod{101}$ ja $\frac{1}{18} \pmod{34}$.

VASTUSED:

Ü1.1.
Ü1.2.
Ü1.3.

Lahendus 1. Et $I_c(Y) = 0.063415$, siis võib oletada, et see on tõepoolest loomulikus keeles kirjutatud sõnumi krüptogramm.

Lahendus 2. Et 7 on algarv, siis kõik mittenullised jäägid $\pmod{7}$ on pööratavad ja seega on korrutamine a -ga hulga $\{1, \dots, 6\}$ üksühene teisendus. Suvalisele arvude paarile x ja y hulgast $\{1, \dots, 7$ leidub üks ja ainult üks võti a , nii et $a \cdot x \pmod{7} = y$, nimelt $a = y \cdot \frac{1}{x} \pmod{7}$. Seega

$$p(x | y) = \frac{1}{6} = p(x) \text{ ,}$$

mistõttu šiffer on täielikult salastav.

Lahendus 3. $\frac{1}{8} \pmod{101} = 38$ ja $\frac{1}{18} \pmod{34}$ ei leidu, sest $(18, 34) = 2 \neq 1$.