

Kaugõppe koduülesanded aines "Sissejuhatus andmeturbesse".

8.mai,2008

Ülesanne 1 (70 punkti). On teada, et järgmine krüptogramm on saadud afiinse šifriga inglisekeelsest tekstist. Leia võti (a, b) ja avatekst.

WQVHQNXHVNCTSNJTIXWQZXHATPVHNIIVPUNGOPWNWQV
HQNXHVNCTDGXWCNIZVTPDIXGJXGCNIZTWXNG

Ülesanne 2 (30 punkti). On teada, et järgmine krüptogramm on saadud permutatsioonišifri abil (ploki suurusega 6). Leia permutatsioon ja avatekst.

HHCTEOCFOIEAORALGIHCITMBSOCAEREOPRSNSTO
DTHCIOEHCOUAEFNTROIFMARUESIGFNNIOMITRAO

Juhised. Ülesande lahenduse vormistamiseks on vajalik vastus, lahenduskäigu kirjeldus ja kasutatud arvutiprogramm (kui seda vaja oli). Tööd palun vormistada arvutil või paberil ja skaneerida hiljem arvutisse. Lahendused palun saata e-maili aadressile:

ahto.buldas@ut.ee

hiljemalt **5. juunil 2008.**

Hindamiskriteerium. 5(100-91p), 4(90-81), 3(80-71), 2(70-61), 1(60-51).