

Kaugõppe koduülesanded aines "Sissejuhatus andmeturbesse".

24.aprill,2009

Ülesanne 1 (60 punkti). RSA krüptosüsteemis valitud algarvud on $p = 1777$ ja $q = 1171$. Kas teie matriklinumber m või (juhul kui m on paaris) $m + 1$ sobib avalikuks astendajaks e ? Kui jah, siis leia salajane astendaja d .

Ülesanne 2 (40 punkti). Nagu teada, kasutatakse RSA algoritmis kahte (juhuslikult valitud) suurt algarvu p ja q . Miks ei tohi aga valitud algarvud olla teineteisele liiga lähedal. Illustreeri seda näite varal, kus avalik moodul $n = 12659363$.

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 **1. juunil 2009**.

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