

Kaugõppe koduülesanded aines "Sissejuhatus andmeturbesse".

10.mai,2010

Ülesanne 1 (40 punkti). RSA krüptosüsteemis valitud algarvud on $p = 1759$ ja $q = 1777$. 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 (60 punkti). On põhjust arvata, et järgmine krüptogramm on moodustatud Vigenere'i šifrit kasutades. Leidke avatekst ja võti.

KSSCVCAVNNXDEVPNLTPWWYZTJIPPRTBXWYXPQMAJYHRVPRISZCBYRNFMRSGGGP
JIMYQEJIHULTPIRPCERSVPEEFCXQDGLGTPRTBMIGWEPIUCVPZPTRSTPVDLXWCWX
BIDDGPSXXMRXLHTCHIFIHREICSURLTYVIMJPRXPAOHYKGRHREVGTZLGGWTIMKG
YTWGGHALTKIRYRDLPNKSKCJDPAPPHNGIABMCEFTRXTPECBFTRXTPEIRERIWDDXT
LAWCRUYGTBAXRLPLMCASBNPTRIPRXPAOLFMRFGDSPSCEHGPNZISGWBGWHCHPQTG
YGIGGPJPNGVGCPTTECRGGWTIMKGYTWCVHNVTDIGRSRMRHGHTPMIGWPLESTECAS
UEGLMCEWXPJXWYXXLHXAEICWIFEIDYGRLTPEIRERIWBYCQCJDPXWASBGRVYWP
ASCQIFSICAIDDXWGWRYIGSJQRTQWPTIGWWIPSCEHTDMCGXXMRDDGDLJXBICRMP
JMIWMHSWTBMCAVNNXDEVPNLNULTLERPCERSVPEEFMRQWCQTDDEXJWIMERFMTTII
FMHBIUGRXRMDLMIAEAJWUMVPPIPAXXMRXLXWCIPPPNQXPEIHRLTZIHRVTYGIGSC
GWIMTPRGWMVSSQERLTQCHRIBBIECRSGRVMRIFITVERRRPRYGCSURLTYXIYGZYJI
CVIFIHWWICQWYWQCICUMSCPMBIEJSNCHJLPTQWXRMSXICVAWFGMOTLECBGPJPH
DSGGQBCHXYXTPIEJERCQTLXIFIQCWIPIPAXXMRXQXDQXPPXEP I EYVXLKPPIEJER
CQTLXPLHPNLPQIDSXHRVPRIVW

Juhised. Ülesande lahenduse vormistamiseks on vajalik vastus, lahendus-
käigu kirjeldus ja kasutatud arvutiprogramm (kui seda vaja oli). Tööd palun
vormistada arvutil või paberil ja skaneerida hiljem arvutisse. Lahendused
palun saata hiljemalt **10. juunil 2010**. e-maili aadressile:

ahto.buldas@ut.ee