

# Kontrolltöö aines “Sissejuhatus andmeturbesse”

19.mai, 2004

**Ülesanne 1.** Kas on võimalik, et korrektse RSA krüptosüsteemis moodul  $n = 391$  ja avalik astendaja  $e = 7$ ? Kui on võimalik, siis milline on salajane astendaja  $d$ ?

**Ülesanne 2.** Arvuta  $2^{430} \bmod 77$ .

**Ülesanne 3.** Arvuta  $5^{110} \bmod 288$ .

**Lahendus 1.** On küll võimalik. Et  $n = 17 \cdot 23$  ja nii 17 kui 23 on algarvud, siis  $\phi(n) = (17 - 1) \cdot (23 - 1) = 16 \cdot 22 = 352$ . Et  $(7, \phi(n)) = 1$ , siis järelikult on avalikul astendajal  $e$  olemas pöördelement  $d$  mooduli  $\phi(n)$  järgi, mille leidmiseks kasutame Eukleidese algoritmi. Saame, et

$$151 \cdot 7 + (-3) \cdot 352 = 1,$$

mistõttu  $d = 151$ . Praktikas kasutatava RSA krüptosüsteemi jaoks nii väikesed arvud muidugi ei sobi. Seda näitab juba asjaolu, et ülesande läh-teandmetest (kus teada olid vaid avalikud parameetrid) oli üldse võimalik salajast võtit arvutada.

**Lahendus 2.** Kuna  $77 = 7 \cdot 11$ , siis  $\phi(77) = 6 \cdot 10 = 60$  ja et  $(2, 77) = 1$ , siis Euleri teoreemist tulenevalt  $2^{60} \bmod 77 = 1$ , mistõttu

$$2^{430} \bmod 77 = 2^{430 \bmod 60} \bmod 77 = 2^{10} \bmod 77 = 1024 \bmod 77 = 23.$$

**Lahendus 3.** Kuna  $288 = 2^5 \cdot 3^2$ , siis  $\phi(288) = (2^5 - 2^4) \cdot (3^2 - 3^1) = 16 \cdot 6 = 96$  ja et  $(5, 96) = 1$ , siis Euleri teoreemist tulenevalt  $5^{96} \bmod 288 = 1$ , mistõttu

$$5^{110} \bmod 288 = 5^{14} \bmod 288 = 6103515625 \bmod 288 = 169.$$

Võib kasutada väiksemate arvude saamiseks järgmisi lihtsustusi. Et  $5^{14} = 5^8 \cdot 5^4 \cdot 5^2$ ,  $5^4 \equiv (5^2)^2 \equiv 625 \equiv 49 \pmod{288}$  ja  $5^8 \equiv (5^4)^2 \equiv 49^2 \equiv 2041 \equiv 97 \pmod{288}$ , siis  $5^{110} \equiv 97 \cdot 49 \cdot 25 = 118825 \equiv 169 \pmod{288}$ .