Kevad 2015

Arvuteooria 15. praktikumi ülesanded:

Krüptoloogia.

1. Teha Fermat' testi abil kindlaks, kas arvud 1729, 1731 ja 1733 on alg- või kordarvud.

2. Kontrollida eelmise ülesande tulemust Miller-Rabini testi abil.

3. Kasutades loengukonspekti näites 9.8 toodud skeemi ja avalikku võtit $(3053, 19)$, tuvastage digiallkirja õigsus tekstil 2693155901380855, mille originaal on AUTENTNE.

4. Kasutades loengukonspekti näites 9.8 toodud skeemi, dekodeerige RSA sõnum 523121600122800 saljase võtme $(2867, 373)$ abil.

5. Diffie-Hellmani võtmevahetuseks on valitud rühm $\mathbb{Z}_{23}$ ja algjuur 5. Te olete saanud ühissaladuse leidmiseks sõnumi 21 ja otsustate võtta oma astendajaks samuti 21. Mis on ühine saladus?

6. Tõestada, et 561 on Carmichaeli arv.

7. Tõestada, et Carmichaeli arvud on ruuduvabad, st. nende algtegurid on kõik erinevad.

8. Kuidas murda RSA kodeeringut, kui mooduli $n = pq$ jaoks on teada Euleri φ-funktsiooni väärtus $\varphi(n)$, aga algtegurid p ja q on jäänud salajasteks?

9*. Öeldakse, et sõnum s on RSA süsteemi *püsipunkt*, kui $m^e \equiv m \pmod{n}$, kus (n, e) on avalik võti. Leida RSA süsteemi püsipunktide arv.

Ajapäevik: 15. nädal

Aeg	Tegevus	Kommentaarid