Kevad 2016

Arvuteooria 15. praktikumi ülesanded:

Krüptograafia.

1. Teha Fermat' testi abil kindlaks, kas arvud 2813, 2819 ja 2821 on alg- või kordarvud.

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

3. Kasutades loengukonspekti näites 9.8 toodud skeemi ja avalikku võtit $(2773, 13)$, tuvastage digiallkirja õigsus tekstil 210625120846126118251417, mille originaal on PEAMINISTER.

4. Kasutades loengukonspekti näites 9.8 toodud skeemi, dekodeerige RSA sõnum 1992096925731561 saljase võtme $(3293, 667)$ abil.

5. Te olete salakirjade saatmiseks kokku leppinud loengukonspekti näitega 9.8 sarnase, aga sümmeetrilise skeemi, kus arvutused $c = s^d \pmod n$ ja $s = c^e \pmod n$ on asendatud arvutustega $c = s+v \pmod n$ ja $s = c-v \pmod n$. Salajase võtme v leiate te Diffie-Hellmani võtmevahetuse abil, valides rühmaks $\mathbb{Z}_{3329}$ ja algjuureks arvu 3. Mooduliks võtate lihtsalt $n = 3329$. Te olete saanud ühissaladuse leidmiseks sõnumi 710 ja otsustate võtta oma astendajaks arvu 6. Dekodeerige salasõnum 31280201324116952003169532 41.

6. Tõestada, et kõik Carmichaeli arvud on paaritud.

7. Tõestada, et igal Carmichaeli arvul on vähemalt kolm erinevat algtegurit. Tõestuseta võib kasutada fakti, et Carmichaeli arvud on ruuduvabad, st. nende algtegurid on kõik erinevad.

8. Olgu $n = pq$, kus $p > 2$ ja $q > 2$ on erinevad algarvud. Tõestada, et igal arvul $a \equiv b^2 \pmod n$, kus $(a, n) = 1$, on täpselt neli ruutjuurt mooduli n järgi. Näidata, et kui nende ruutjuurte leidmiseks oleks olemas arvutuslikult efektiivne meetod, siis saaks arvu n efektiivselt tegurdada.

9*. Tõestada, et RSA salajane astendaja d ei ole üheselt määratud, st. leidub mitu arvu d, mille korral $c^d \equiv s \pmod n$, kus s on suvaline kodeeritav sõnum, $c = s^e$ kodeeritud sõnum ja e avalik astendaja.

Ajapäevik: 15. nädal

Aeg	Tegevus	Kommentaarid