

Arvuteooria 15. praktikumi ülesanded

1. Teha Fermat' testi abil kindlaks, kas arvud 2257, 2423, 3127, 6601 on alg- või kordarvud.
2. Kontrollida eelmise ülesande tulemust Miller-Rabini testi abil.
3. Kasutades loengukonspekti näites 9.8 toodud skeemi ja avalikku võtit (3149, 5), tuvastage digiallkirja õigsus tekstil 20051920, mille originaal on TEST.
4. Kasutades loengukonspekti näites 9.8 toodud skeemi, dekodeerige RSA saljase võtmega kodeeritud sõnum 005827741186095213691244 avaliku võtme (3053, 11) abil.
5. Kuna moodul 3053 on väike, siis avalikku võtit (3053, 11) on võimalik suhteliselt lihtsalt murda ja saada saljast võtit. Tehke seda, dekodeerige avaliku võtmega kodeeritud sõnum 10760041 ja kodeerige sõnum PWND saljase võtme abil.
6. Diffie-Hellmani võtmevahetuseks on valitud rühm $\mathbb{Z}_{19}$ ja algjuur 13. Te olete saanud ühissaladuse leidmiseks sõnumi 6 ja otsustate võtta oma astendajaks arvu 7. Mis on ühine saladus?
7. Tõestada, 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* Öeldakse, et sõnum s on RSA süsteemi püsipunkt, kui $me \equiv m \pmod{n}$, kus (n, e) on avalik võti. Leida RSA süsteemi püsipunktide arv.

Selle nädala ülesannete lahendamisel pikade arvutuste jaoks ON SOOVITATAV kasutada arvutit, kuid saab ka ilma.

1. Näide 9.3.
2. Näide 9.7.
3. Näide 9.8.
4. Näide 9.8.
5. Tegurdage moodul n kahe algarvu korrutiseks. Leidke $\varphi(n)$ ja avaliku astendaja pöördlemendi vastavas rühmas. Näide 9.8.
6. Näide 9.9.
7. Tõestada abitulemusena, et juhul, kui $n = p^l \cdot m$, kus $p \in P$, $m, l \in N$, $l \geq 2$, siis $(1 + pm)^{n+1} \equiv 1 \pmod{p^2}$.
8. Vaadelda ruutjuurt arvust 1, mis ei ole 1 ega -1 . Eukleidese algoritmi võib lugeda arvutuslikult efektiivseks.