Kevad 2019

Arvuteooria 15. praktikumi ülesanded: Krüptograafia

1. Uurida Fermat' testi abil, kas 8911, 8933 ja 8977 on alg- või kordarvud.

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

3. Kasutades loengukonspekti näites 9.8 toodud skeemi ja avalikku võtit $(8633, 13)$, tuvastada digiallkirja õigsus tekstil 3565022003414432308268 64, mille originaal on INGLISE NALI.

4. Kasutades loengukonspekti näites 9.8 toodud skeemi neljatäheliste (st. kaheksanumbriliste) blokkide jaoks ja mooduli väiksust, dekodeerida avaliku võtmega $(88867241, 421)$ kodeeritud RSA sõnum

$$5081405085821557541220420267429242900438.$$

5. Te olete salakirjade saatmiseks kokku leppinud loengukonspekti näitega 9.8 sarnase, aga sümmeetrilise ning neljatäheliste blokkidega 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 Diffie-Hellmani võtmevahetuse abil, valides rühmaks $\mathbb{Z}_{31111121}$ ja algjuureks arvu 3. Mooduliks võtate $n = 31111121$. Te olete saanud ühissaladuse leidmiseks sõnumi 24102187 ja otsustate võtta oma astendajaks arvu 673. Dekodeerida salasõnum 266720472367323014663738017508112478382 9.

6. Näidata, miks Mersenne'i arvude $2^p - 1$ ja Fermat' arvude $2^{2^k} + 1$ jaoks ei ole mõtet kasutada Fermat' testi alusel $a = 2$.

7. Leida kõik Carmichaeli arvud kujul $3pq$, kus $p, q \in \mathbb{P}$.

8. Näidata, et kui $n = pq$, ning p ja $q \in \mathbb{P}$ on üksteisele väga lähedal, siis arvu n saab "kiirelt" (tunduvalt alla $|p-q|$ sammuga) tegurdada. Rakendada seda tegurdamisalgoritmi arvule 23360947609.

9*. Tõestada, et RSA mooduli n efektiivne (st polünomiaalses ajas $\log n$ suhtes) tegurdamine on samaväärne salajase astendaja d teadasaamisega.

10**. Olgu $p \in \mathbb{P}$ ja $k > 1$. Tõestada, et kui leidub polünomiaalne (suuruse $\log p$ suhtes) algoritm diskreetse logaritmi leidmiseks korpuses $\mathbb{Z}_p$, siis leidub ka polünomiaalne (suuruse $\log(p^k)$ suhtes) algoritm diskreetse logaritmi leidmiseks korpuses $\mathbb{Z}_{p^k}$. (Niisugust algoritmi õnneks küll teada ei ole).