Kevad 2024

Arvuteooria 15. praktikumi ülesanded:

Krüptograafia.

1. Uurida Fermat' testi abil, kas 46637, 46657, 46667 ja 46687 on alg- või kordarvud.

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

3. Kasutades loengukonspekti näites 9.8 toodud skeemi ja avalikku võtit $(7081, 2423)$, tuvastada digiallkirja õigsus tekstil 688202412614187717 92, mille originaal on PROFESSOR.

4. Kasutades loengukonspekti näites 9.8 toodud skeemi 32-täheliste (st. 64-numbriliste) blokkide jaoks ja mooduli väiksust, dekodeerida avaliku võtmega $(71106412503920777013851106255631919241912341265175703699652435 31, 65537)$ kodeeritud RSA sõnum

$$2032579136919773158215117368529439893520160991814640904365307062163939638475252532585280094396032078587303396440304437620603936 4.$$

5. Te olete salakirjade saatmiseks kokku leppinud loengukonspekti näitega 9.8 sarnase, aga sümmeetrilise ning neljatäheliste blokkidega skeemi, kus arvutused $c = s^e \pmod n$ ja $s = c^d \pmod n$ on asendatud arvutustega $c = s - v \pmod n$ ja $s = c + v \pmod n$, seejuures $n = 99022109$. Salajase võtme v leiate Diffie-Hellmani võtmevahetuse abil, valides rühmaks $\mathbb{Z}_{93720163}$ ja algjuureks arvu 2. Te olete saanud ühissaladuse leidmiseks sõnumi 12013873 ja otsustate võtta enda astendajaks arvu 2024. Dekodeerida salasõnum

$$28027918390782082313919945038311231799204103910026987917451981 99.$$

6. Tõestada, et kui n on Carmichaeli arv, siis mooduli n järgi ei leidu algjuuri.

7. Tõestada, et kui $n = 3p$ ja $3 < p \in \mathbb{P}$, siis ükski arvudest 2,7,17 ei saa olla Fermat' valetaja arvu n jaoks. Kas nad võivad olla Milleri-Rabini valetajad?

8. Arvutuslikel põhjustel on RSA avaliku võtmena e populaarsed Fermat' algarvud. Miks ei ole hea mõte võtta e väärtuseks alla $F_4 = 65537$?

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

10**. Olgu $2 < p \in \mathbb{P}$ 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 teada ei ole).