Kevad 2022

Arvuteooria 15. praktikumi ülesanded:

Krüptograafia.

1. Uurida Fermat' testi abil, kas 115901, 115911, 115921 ja 115931 on alg- või kordarvud.

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

3. Kasutades loengukonspekti näites 9.8 toodud skeemi ja avalikku võtit $(6887, 3439)$, tuvastada digiallkirja õigsus tekstil 53811838590463330754, mille originaal on PRESIDENT.

4. Kasutades loengukonspekti näites 9.8 toodud skeemi 16-täheliste (st. 32-numbriliste) blokkide jaoks ja mooduli väiksust, dekodeerida avaliku võtmega $(476806851099979911288326509231 97, 666666667)$ kodeeritud RSA sõnum

$$3301933543035988102580817649676020005271809859513240431765160932005004765274608596573387822609 96.$$

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 $s = c + v \pmod n$, seejuures $n = 96312883$. Salajase võtme v leiate Diffie-Hellmani võtmevahetuse abil, valides rühmaks $\mathbb{Z}_{97165291}$ ja algjuureks arvu 2. Te olete saanud ühissaladuse leidmiseks sõnumi 42655264 ja otsustate võtta oma astendajaks arvu 3003. Dekodeerida salasõnum

$$7744765264437359605477507064705078436846775062417058716177586953795872567458725 3.$$

6. Olgu n kordarv, mis **ei** läbi Milleri-Rabini testi alusel $1 < a < n$. Leida vähemalt üks arvu n tegur, mis ei ole 1 ega n ise.

7. Tõestada *Korselti kriteerium*: **kord**arv n on Carmichaeli arv parajasti siis, kui ta on ruuduvaba ja iga $p \in \mathbb{P}$, $p \mid n$, korral kehtib $(p-1) \mid (n-1)$. Carmichaeli arvude ruuduvabadust võib eeldada ilma seda tõestamata. Ruuduvabaduse tõestamisel tahvlile vabatahtlikkuse alusel: +1 punkt.

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 $p \in \mathbb{P}$ 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).