Kevad 2020

Arvuteooria 15. praktikumi ülesanded:

Krüptograafia.

1. Uurida Fermat' testi abil, kas 15841, 15871 ja 15881 on alg- või kordarvud.

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

3. Kasutades loengukonspekti näites 9.8 toodud skeemi ja avalikku võtit $(9523, 13)$, tuvastada digiallkirja õigsus tekstil 1400524754868259, mille originaal on SALATÕBI.

4. Kasutades loengukonspekti näites 9.8 toodud skeemi neljatäheliste (st. kaheksanumbriliste) blokkide jaoks ja mooduli väiksust, dekodeerida avaliku võtmega $(93122201, 91)$ kodeeritud RSA sõnum

$$61234207848790290138316043954689900164124272475789574723.$$

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 $\mathbb{Z}_{31111123}$ ja algjuureks arvu 2. Mooduliks võtate $n = 31111123$. Te olete saanud ühissaladuse leidmiseks sõnumi 19874654 ja otsustate võtta oma astendajaks arvu 666. Dekodeerida salasõnum 216830150855229225694015257029300155249 7.

6. Olgu $(n, 5)$ RSA avalik võti, kus $p, q \in \mathbb{P}$, $p > 5$ ja $q = 2p - 3$. Tõestada, et $p \equiv 3 \pmod 5$ ja $(n, \frac{(p-1)(q-1)+1}{5})$ sobib vastavaks salajaseks võtmeks.

7. Tõestada, et arv 2 ei ole ühegi Fermat' arvu (st arvu kujul $F_n = 2^{2^n} + 1$) jaoks Fermat' tunnistaja.

8. Tõestada, et 561 on vähim Carmichaeli arv. Tõestuseta võib kasutada fakte, et Carmichaeli arvud on paaritud, ruuduvabad (st nende algtegurid on kõik erinevad) ja et neil on vähemalt kolm algtegurit.

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

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).