Kevad 2018

# Arvuteooria 15. praktikumi ülesanded:

# Krüptograafia ja teisi rakendusi.

1. Teha Fermat' testi abil kindlaks, kas arvud 6601, 6641 ja 6661 on alg- või kordarvud.

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

3. Kasutades loengukonspekti näites 9.8 toodud skeemi ja avalikku võtit $(7169, 5)$, tuvastada digiallkirja õigsus tekstil 22154378100160481316, mille originaal on PRESIDENT.

4. Kasutades loengukonspekti näites 9.8 toodud skeemi neljatäheliste (st. kaheksanumbriliste) blokkide jaoks ja mooduli väiksust, dekodeerida RSA sõnum 92676572442562033471623149769736 avaliku võtmega $(99944311, 667)$.

5. Te olete salakirjade saatmiseks kokku leppinud loengukonspekti näitega 9.8 sarnase, aga sümmeetrilise 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 $\mathbb{Z}_{3323}$ ja algjuureks arvu 5. Mooduliks võtate $n = 3323$. Te olete saanud ühissaladuse leidmiseks sõnumi 2510 ja otsustate võtta oma astendajaks arvu 32. Dekodeerida salasõnum 3259042100170428181812261122324508171938112 2.

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

7. Tõestada, et ükski Fermat' arv ei ole Carmichaeli arv. Tõestuseta võib kasutada Korselti kriteeriumit, mille põhjal iga Carmichaeli arvu $n$ jaoks kehtib

$$[(p \mid n) \wedge (p \in \mathbb{P})] \Rightarrow [(p-1) \mid (n-1)].$$

8. Olgu antud sõnum $s$, *sama mooduliga* RSA avalikud võtmed $(n, e)$ ja $(n, e')$, kusjuures $(e, e') = 1$, ning vastavad salasõnumid $c = s^e$ ja $c' = s^{e'} \pmod n$. Leida avaliku info $n, e, e', c, c'$ abil "kiiresti" esialgne sõnum $s$.

9*. Tõestada, et RSA avaliku võtme $(n, e)$ jaoks leidub selline $k \in \mathbb{N}$, et $x^{e^k} \equiv x \pmod n$ iga $x \in \mathbb{Z}$ korral. Kas arvu $k$ teades saab antud konkreetset RSA skeemi murda ja kui nii, siis kui efektiivselt?

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).