Kevad 2015

Vihjeid 15. praktikumiks

1. Näide 9.3.

2. Näide 9.7.

3. Näide 9.8.

4. Näide 9.8.

5. Näide 9.9.

6. Kuuenda praktikumi 4. ülesanne ja 561 algteguriteks lahutus.

7. Tõestada abitulemusena, et juhul, kui $n = p^l \cdot m$, kus $p \in \mathbb{P}$, $m, l \in \mathbb{N}$, $l \geq 2$, siis $(1 + pm)^{n+1} \not\equiv 1 \pmod{p^2}$.

8. Alapeatükk 9.2.1. Saab lahendada otse RSA üldise skeemi abil, aga on võimalik ka moodul n algteguriteks lahutada.