Kevad 2020

Vihjeid 15. praktikumiks

1. Näide 9.3.

2. Näide 9.7.

3. Näide 9.8.

4. Tegurdada moodul n ehk leida $\varphi(n)$. Näide 9.8.

5. Näited 9.8 ja 9.9.

6. Välistada $q = 2p - 3$ abil muud jäägid mooduli 5 järgi. Selle abil näidata, et salajase võtme kandidaat on tõesti arvu 5 kordne ja rahuldab RSA salajase võtme definitsiooni.

7. Astendada kongruentsi $2^{2^n} \equiv -1 \pmod{F_n}$ sobiva kahe astmega.

8. Sõeluda Korselti kriteeriumi (viimast tuleb põhjendada!) abil läbi kõik võimalikud kolme piisavalt väikese algteguriga variandid.