6-13.12.2019, Friday, 8.30-10.20

CMSE491 Lab3 “NTRU for polynomials” task

1. Implement in Maple three batches of code:
   1. NTRU for polynomial parameters setting,
   2. encryption,
   3. decryption.

Check correctness of NTRU work on the inputs used in Seminar 3 “NTRU for polynomials”

1. Implement Extended Euclid algorithm as a batch. Compare its outputs versus those from Maple Gcdex()

Hint: you may use the code provided in [Lecture notes example](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMSE491/Fall2019/NTRU%20example%2028112019.mw).

By 13.12.2019, prepare a paper report and defend it in Lab hours (demonstrate and answer the questions). Provide also a CD with all Lab related materials (report, application source, etc.)

Grading policy: 40% report, 60% defense