18.11-23.12.2020, Wednesday, 18.30-20.20

CMSE491 Lab2 “NTRU for polynomials” task

Implement in Maple NTRU for polynomials providing:

1. Setting NTRU parameters
2. Generation private/public keys
3. Encryption
4. Decryption

The application shall be user-friendly:

* Inputs shall be prompted explaining the user what data is expected from him/her and what constraints it shall meet
* User inputs shall be checked on meeting NTRU constraints
* If data inputs do not meet NTRU constraints, the user shall be notified on the problem with the data, with explanations, and the input shall be repeated

By 23.12.2020, prepare a report (Winrar file with doc or pdf report, and all Lab-related materials: sources, executables, screenstos, etc.), submit it for evaluation, and defend it in Lab hours (demonstrate and answer the questions).

Grading policy: 40% report, 60% defense

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