1-29.11.2019, Friday, 8.30-10.20

CMSE491 Lab2 “GLR attack on NTRU for integers” task

The lab is based on Lab 1 results where an application in Maple was to be developed such that

1. Inputs and defines private and public keys according to NTRU for integers requirements (see [NTRU for integers description](https://staff.emu.edu.tr/alexanderchefranov/Documents/CMSE491/Fall2019/Hoffstein2015%20Introduction%20to%20Mathematical%20Cryptography373-376.pdf))
2. Inputs message to be encrypted and generates a random number also according to the requirements.
3. Encrypts your message and outputs a ciphertext.
4. Decrypts the ciphertext getting back your original message.

For Lab 2, develop an application that

1. Takes a public key, h and q, secret key, , ciphertext, e, and plaintext, m, from NTRU for integers
2. Generates vectors,
3. Applies GLR to
4. Checks whether reduced vectors contain secret vector ), or can be used the ciphertext decryption, restoring m

By 29.11.2019, 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