23-06.01.2020, Wednesday, 18.30-20.20

CMSE491 Lab3 “GLR attack on NTRU for integers” task

Develop an application that

1. Takes public q, secret keys, $f,g$, defines the public key, h and q, encrypts a plaintext, m, and gets the ciphertext, c, by NTRU for integers (as in Lab 1).
2. Generates vectors, $v\_{1}=\left(1,h\right), v\_{2}=(0,q)$
3. Applies GLR to $v\_{1}=\left(1,h\right), v\_{2}=(0,q)$
4. Checks whether reduced vectors contain secret vector $(f,g$), or can be used for the ciphertext decryption, restoring m

By 06.01.2021, prepare a paper report and defend it in Lab hours (demonstrate and answer the questions). Provide also an archived file (rar, zip, etc.) with all Lab related materials (report, application source, etc.)

Grading policy: 40% report, 60% defense