04-18.11.2020, Wednesday, 18.30-20.20

CMSE491 Lab 1 “NTRU for integers” task

The lab shall be done by teams of 3-5 people.

Develop an application in Maple that

1. Inputs $q$ 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.

By 18.11.2020, prepare a report (pdf file) and defend it in Lab hours (demonstrate and answer the questions). All lab related materials (report, application source, etc.) shall be uploaded to the place specified by Lab assistants as Winrar archive.

Report shall be arranged as follows:

* 1. Cover page (University, Department, Course, Semester, Year, City, Country, Term Project subject, Team members, Lecturer, Lab assistant)
	2. Outline
	3. Problem definition
	4. Description of NTRU for integers
	5. Keys creation
	6. Encryption
	7. Decryption
1. Description of NTRU for integers implementation
	1. Programming tool used
	2. Overall application structure
	3. Data input
	4. Key creation
	5. Encryption
	6. Decryption
	7. Data output
2. Testing of NTRU for integers
3. Conclusion
4. References
5. Appendices with the code developed and raw results obtained

Grading policy: 40% report, 60% defense