07.11.2020

**CMSE-491 Term Project “Implementation of a secure chat system with NTRU encryption” Fall 2020**

**Task**:

1. Implement a chat system allowing user communications via Internet channels using NTRU-encrypted messages.
2. Report on the Term project shall be submitted to the place to be specified later by Lab Coordinator Nada Ibrahim Saadeldin latest on **Monday, January 11, 2021, before 16.00. Later submission will be penalized by 10% off per day.**
3. Date of the defense will be agreed with Lab Coordinator after the report submission during January 12-19, 2021.
4. Report is prepared by a team. Teams are the same as in Laboratory works.
5. 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 (see Item 1 above extended as necessary)
	4. Description of chat system (CS)
		1. Structure of the CS
		2. Implementation of CS without encryption
		3. Testing of CS without encryption
	5. Description of NTRU encryption in CS

5.5.1 Description of NTRU

5.5.2. Implementation of NTRU as standalone application

5.5.3. Testing of NTRU as standalone application

* 1. Integration of CS and NTRU
		1. Design of interface CS-NTRU
		2. Implementation of CS-NTRU system
		3. Testing of CS-NTRU system
	2. Conclusion
	3. References
	4. Appendices with the code developed and raw results obtained

Winrar archive with all Term Project related materials (report, images used, test results, sources, executables, user guide) shall be submitted. It shall be have runnable codes (it is possible to install your program from the archive, run it on your examples, and view results you got).

1. **Grading policy: 40% report and 60% explanations out of totally 20 points**