**13.03.2024**

**Term Project Task**

**CMSE-512 “Database and File Security”**

**Spring-2024**

1. The project concerns development of an on-line “Secure Teams-Like Chat System” with Sysadmin and User actors. Access to the system is by user name and password. Sysadmin is responsible for introducing users to the system. User chooses a user from the list of registered users for chatting and texts a message to him/her. The messages are sent digitally signed and encrypted by DES. DES secret key is created/updated periodically by User. Server has public/private RSA key pair. RSA key pair are created/updated by Sysadmin and User. Transactions issued by users are digitally signed by RSA with 48-bit hash obtained by XOR of plaintext blocks. Database records are kept DES-encrypted.
2. The project is expected to be done by a team of at most four students. Notify me, please about your teams latest by March, 20, 2024. Later notification will be penalized by 2 points off per day
3. Implement solution using any appropriate tools
4. Conduct tests with your application to validate its correctness
5. Prepare (in Word) on your assignment having:

* outline,
* task formulation,
* database schema (E-R diagram), constraints on the DB content
* description of algorithm for solving your task,
* description of tools you used for implementation of your task and the way of their installation and preparation for usage
* description of developed program (parts of the program, ways of interaction, synchronization, etc.)
* user guide (how to use your program – what and where should be installed, launched, how it should be interpreted)
* description of conducted tests and their results with screenshots of the runs
* conclusion
* references on used sources (books, articles, web-sites, etc.)

1. Report and all the Term Project-related materials (doc-file with your report, sources and executables of your application, database structure and content, results of your tests, and an instruction how to use your program) shall be printed as a hard copy and respective WinRAR file will be submitted via Teams.
2. Submit the report printed to the lecturer and be ready to show your application working and to give necessary explanations about it. Reports shall be uploaded in Teams **27.05.2024, Monday, 16.00. Later submission will be penalized (2 points/day).**
3. Presentation of your working application will be held in the period 28-30.05.2024. Presentation time will be specified on the report submission. The report will be assessed out of 8 points, and 12 points – for presentation of the working application and its explanation