27.10.2022

**Term Project CMPE 553 Cryptography and Network Security, Fall 2022**

**Implementation of secure data transmission over network channels**

Term project is to be made in **groups of two-five students**. Each subject can be used by at most **two** teams.

**Task**

Develop a network application for testing ciphers working over respective alphabets enlisted in Table 1 (7 variants). Implemented in the project ciphers should be able both encrypting and decrypting. Communicating parties shall be represented as processes running on **two separate computers** connected via some channel. Each party may send/receive data. Data travels encrypted in the network.

Table 1. Ciphers

|  |  |
| --- | --- |
| Variant | Cipher |
|  | Caesar with any permutation |
|  | Playfair  |
|  | Hill, n=2 |
|  | Vigenere with fixed key |
|  | Vigenere with auto-key |
|  | Transposition using matrices |
|  | Rotor machine |

***Your choices should be conveyed by e-mail to the lecturer (last day is Thursday, November 3, 2022). Later choice making will be penalized by 4 points deduction.***

**Grading policy and requirements**

1. Maximum point for the term project is 100%.
2. 10% bonus if DES encryption/decryption is additionally implemented as a 2nd cipher
3. Term project materials should be submitted to the lecturer latest by 02**.01.2023, Monday, before 16.00. Late materials submission will lead to deduction of 10% a day**. Place and way of the project materials submission will be defined later.
4. Your variant choice should be conveyed to the lecturer (**last day is Thursday, November 3, 2022)**. **Late choice making will be penalized by 10% deduction**. Already made choices will be available from the course web-page.
5. Reports will be defended during **03.01.2023-05.01.2023, date and time will be agreed upon your reports submission. Late defense of reports will lead to deduction of 10% points**.
6. Materials on term project should contain:

- pdf or doc file as a report on the work done

- Winrar archive with all the project related materials: Word document file of report; source codes and executables of developed applications; necessary examples of plaintexts and cipher-texts, test results; necessary for work special libraries if any, user manual and installation guide. It shall be possible installing your application from the archive and running it.

7. Report on term project should have:

- cover page (university, department, course, title of term project, students’ names, instructor’s name, semester, year, city, country);

- task definition;

- brief definition of an algorithm to be implemented;

- description of your network setting;

- description of developed application (including its networking part, describing details of organization of network channel between the peers) and its source codes;

- description of tests conducted to verify correct work of your application (data decrypted/extracted match the data encrypted/embedded), provide screenshots of working program, comment them;

- experiments results and discussion;

- conclusion

- references to used articles, textbooks, web-sites and so on, if any