07.11.2020

**Term Project CMPE 553 Cryptography and Network Security, Fall 2020**

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

Term project is to be made in **groups of three-four students**.

**Task**

Develop a network application for testing ciphers working over respective alphabets enlisted in Table 1 (18 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 and respective alphabets

|  |  |  |
| --- | --- | --- |
| Variant | Cipher | Alphabet |
|  | Multiplication by a key | English letters |
|  | Multiplication by a key | English letters + digits 0..9 |
|  | Caesar with shifts (26 keys) | English letters |
|  | Caesar with shifts (36 keys) | English letters + digits 0..9 |
|  | Caesar with any permutation (26! keys) | English letters |
|  | Caesar with any permutation (36! keys) | English letters + digits 0..9 |
|  | Playfair  | English letters |
|  | Hill, n=2 | English letters |
|  | Hill, n=2 | English letters + digits 0..9 |
|  | Hill, n=3 | English letters |
|  | Hill, n=3 | English letters + digits 0..9 |

Select one out of 11 variants from Table 1. The variant selected can be repeated at most once for the groups of students. For example, if the variant 3

|  |  |
| --- | --- |
| Caesar with shifts (26 keys) | English letters |

is selected by some group, then this combination can be used by at most one other group. ***Your choices should be conveyed by e-mail to the lecturer (last day is Friday, November 13, 2020). Later choice making will be penalized by 4 points deduction.***

**Grading policy and requirements**

1. Maximum point for the term project is 20.

2. Term project materials should be submitted to the lecturer latest by 11**.01.2020, Monday, before 12.00. Later materials submission will lead to deduction of 2 points per day**.

Your variant choice should be conveyed to the lecturer (**last day is Friday, November 13, 2020)**. **Later choice making will be penalized by 4 points deduction**. Already made choices will be available from the course web-page.

3. Reports will be defended during 12**.01.2021-19.01.2021, date and time will be agreed upon your reports submission. Later defense of reports will lead to deduction of 4 points**.

4. Materials on term project should contain:

- paper 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.

5. 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