DAT 510: Assignment 1

Submission Deadline: 23:59, Friday, Sept. 26, 2025

Encryption Analysis and Enhancing Security

Objective

This assignment is designed to provide students with hands-on experience in classical cryptographic techniques, specifically focusing on transposition and substitution ciphers. Students will begin by encrypting a plain text, composed of their name and course name, using a personalized numeric key derived from their phone number. They will implement both encryption methods, assess the strength of the ecryption, and improve the strength of the encryption.

Input

Plain text:

Your name and course name. For example, if your name is "Jane Smith" and the course is "Security and Vulnerability in Networks", your input text should be "Jane Smith Security and Vulnerability in Networks ".

Numeric Key:

Use the last five digits of your phone number as a key for transposition. For example, phone number 51811, key 41523, phone number 52811, and key 43512. Replace the smallest number with one and the second smallest with 2, and so on. In the given example, 1 is repeated, so replace the first one with 1, the second with 2, and so on. Use the last two or one digit of your phone number (should be less than 25) as a key for Caeser cipher substitution.

Task 1 Apply Encryption and Decryption: (10%)

Implement substitution and Transposition encryption and decryption separately. Develop an interactive system, where Alice and Bob send messages to each other using different encryption schemes.

Task 2. Analysis: (30%)

Analyze the computation time and strength of each encryption with different method(s), different plaintext inputs, and key sizes. Plot your analysis through different graphs. Explain your choice of analysis method(s) and why you selected that specific method. Explain the graphs. Discuss the weakness of these encryptions.

Task 3. Optimize/improve the encryptions: (40%)

Improve encryption methods to overcome the weaknesses and enhance the strength of encryption. Implement the new encryptions and explain how the improvement enhances the encryption.

Task 4. Analysis and comparison: (20%) Analyze the computation time and strength of the new encryption with the same methods in Task 2. Visualize the analysis and compare it with the old encryption. Summarize your findings and mention the improvement. Describe the applications of these encryptions. Suggest future recommendations.

Note:

Be sure to review and cite materials (Books, research articles) related to topics used in your assignments.

Assignment Approval (by TA and SA)

Approval Deadline: 16:00 Tuesday, Sept. 23, 2025.

If you are not going to get the approval before the deadline, your assignment will not be evaluated and you will fail the assignment.

What needs to be done to get the approval for the assignment:

1. demonstrates all parts of the assignment are working, i.e., show the code with proper comments and results.
2. You **CAN** use basic libraries for implementing the core functionality of the assignment. If you are unsure about the libraries, ask the TA.
3. Do not change the code or add more functionalities after approval. The code presented during approval is counted as final.
4. Approval is only possible during lab time.

You need to implement this assignment using Python.

Assignment Submission

Deadline: 23:59, Friday, Sept. 26, 2025 (submit your assignment through canvas)

Final submission:

1. Source Code (50%)
   - The Source code submitted for the assignment should be your own code. If you have used sources from the internet, everything should be added to the references. If you used someone's code without reference, that will also be treated as plagiarism.
   - Source code should be a single, compressed directory in .zip format.
   - Directory should contain a file called README that describes the contents of the directory and any special instructions needed to run your programs (i.e., if it requires packages, commands to install the package. Describe any command line arguments with the required parameters).
2. **Final** report with PDF format (50%)
   - Texts in the report should be readable by humans, and recognizable by machines;
   - Other formats will **NOT** be opened, read, and will be considered missing;
   - Report **should** follow the **template** report style uploaded with Assignment 1 as a zip file of Overleaf format.
   - Each student should write an individual report. Each report will be checked for plagiarism. If it is copied from somewhere else, you will fail the assignment.

NOTE: Please upload the archive file in *.zip only and final report in *.pdf format only to the website https://stavanger.instructure.com/.

Note: The assignment is individual and can **NOT** be solved in groups.