DAT 510: Assignment 1

Submission Deadline: 23:59, Friday, Sept. 13, 2024

Encryption Analysis and Optimization: Understanding Avalanche Effect and Enhancing Security with Block Ciphers

Objective

This assignment is designed to provide students with hands-on experience in classical cryptographic techniques, specifically focusing on the combination of 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 one of two encryption sequences, either transposition followed by substitution or the reverse and justify their choice.

The core of the assignment involves evaluating the Avalanche Effect and optimizing the encryption process by balancing the Avalanche Effect against computational efficiency and identifying the optimal number of encryption rounds. Further, students will optimize the encryption process by balancing the Avalanche Effect against computational efficiency, identifying the optimal number of encryption rounds. Finally, to enhance the security of their chosen encryption combination, students will implement a block cipher mode of operation, such as ECB or CBC, and analyze its effectiveness in mitigating the weaknesses of transposition and substitution ciphers.

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: (20%)

- Select and implement one of the following encryption combinations:
  - Option A: First, apply a transposition cipher to the input text. Then, use a substitution cipher to the transposed text.
  - Option B: First, apply a substitution cipher to the input text. Then, use a transposition cipher to the substituted text.
- Describe the combination you chose and justify your selection. Implement the encryption process using your chosen combination.

Task 2. Evaluate the Avalanche Effect: (30%)

- **Step 1: Initial Avalanche Effect Analysis** Modify the input by changing or flipping a single bit or character. Re-encrypt the modified input using the same combination. Compare the original and modified cipher texts by calculating the percentage of differing bits. Document your findings on how the small change in input affected the cipher text.
- **Step 2: Repeated Avalanche Effect Analysis** Repeat the encryption multiple times (at least sixteen) and evaluate how the avalanche effect changes with each additional round of encryption. For example, Apply the selected encryption combination twice in succession to the input text (i.e., encrypt the text once, then encrypt the resulting cipher text again) and evaluate the avalanche effect. Repeat the same procedure at least up to sixteen times. Write a function that returns the avalanche effect after each increment in the round, along with computation time.

Task 3. Analyze the Avalanche effect: (15%)

Provide a detailed analysis of how the avalanche effect changes or is unchanged with additional rounds of encryption. Discuss the reasons behind the observed behavior and provide insights into how transposition and substitution ciphers interact in terms of avalanche effect.

Task 4. Optimize Avalanche Effect with Reasonable Computation: (15%)

- **Objective:** Determine the optimal balance between achieving a high avalanche effect and maintaining reasonable computational efficiency. Identify the point where the avalanche effect reaches a satisfactory level without significantly increasing computational cost. Find the best trade-off between a strong avalanche effect and efficient computation.
- **Deliverable:** Provide a detailed analysis that includes graphs or charts showing the relationship between the number of encryption combinations, the avalanche effect, and

the computation time. Conclude with the optimal number of combinations that provide a good balance between security (avalanche effect) and performance (computation time).

Task 5. Enhance Security with Block Ciphers: (20%)

- **Identify Weaknesses:** Briefly describe the inherent weaknesses of transposition and substitution ciphers (e.g., susceptibility to pattern recognition, lack of diffusion, etc.).
- **Enhance with Block Cipher:** Implement the chosen combination with any mode of operation (Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), Counter (CTR)) to enhance the security of your chosen encryption combination.
- **Analysis:** Evaluate the impact of using a block cipher on the avalanche effect and overall security. Discuss how the block cipher mode mitigates the weaknesses of the transposition and substitution ciphers.

Note:

The following topics covered in this assignment correspond to the respective sections in your course materials:

- Substitution and Transposition Ciphers: Refer to Lecture 03 ("03_Classical") for detailed explanations and examples.
- Avalanche Effect: This concept is explained in Lecture 04 ("04_Block_Des").
- Block Cipher Modes of Operation: Consult Lecture 07 ("07_Block_Ops") for insights into different block cipher modes.

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

Assignment Approval (by TA and SA)

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. Code should have a proper README file 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).
3. 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.
4. Provide the references in Code and Report, and show these parts to TAs and Student Assistants.
5. You **CAN** use available libraries/packages/classes for implementing the core functionality of the assignment.
6. Do not change the code or add more functionalities after approval. The code presented during approval is counted as final.

You need to implement this assignment using Python.

Assignment Submission

Deadline: 23:59, Friday, Sept. 13, 2024 (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).
   - You **CAN** use available libraries/packages/classes for implementing the core functionality of the assignment.
2. A **separate** 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 formal report style guide on the next page.
   - Compile your findings, implementation, and analysis into a comprehensive report (3000-5000 words).
   - 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 report in *.pdf format only to the website https://stavanger.instructure.com/.

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

Project Title

Abstract

A one-paragraph summary of the entire assignment - your procedure, results, and analysis.

1. Introduction

Briefly explain the overall goal of the project. Describe the background topics for the project. If you are building on top of any existing resources, highlight them in this section and cite them in your references.

2. Design and Implementation

A detailed description of the design, procedure, and implementation of your project.

2.1. Apply Encryption

2.2. Evaluate the Avalanche Effect

2.3. Analyze the Avalanche effect

2.4. Optimize Avalanche Effect with Reasonable Computation

2.5. Enhance Security with Block Ciphers

3. Discussion

Discuss analysis of your results.

4. Conclusion

A short paragraph that restates the objective from your introduction and relates it to your results and discussion and describes any future improvements on your techniques that you would recommend.

References

A bibliography of all of the sources you got information from in your report.