DAT 510: Assignment 1

Submission Deadline: 23:59, Friday, Sept. 15, 2023

Encryption and Decryption

In this assignment, you will try your skills to encrypt, attach and decrypt plain text.
Warning: Although the encryption techniques used in this assignment are extremely primitive compared to practical encryption schemes used in the real world, they are not necessarily easy to solve (even with computer assistance). Start early and deadline for submission is soon!

Apply a Vigenère cipher followed by a row-column transposition for encryption, and then decrypt the cipher text using row-column transposition followed by the Vigenère cipher. This would create a combination of encryption methods that may improve the security level. Then apply the reverse combination to find out which one is better. Assess the security after each encryption to find out the vulnerability of encryption.
The process would work as follow:
Key: First three letters of your first name. Replace the special character in your name with a reasonable nearby character.
Plain text: wearediscoveredusingchapgptsaveyourself
Cipher text: ?

Part I. Encryption

In this part of the assignment, you are supposed to write generic code for encryption, assessment method, and decryption. Generic code means your code should also work on other different inputs. For example, if we provide different key lengths or plain text, your code needs to work properly.

Task 1 Implement your own Vigenère cipher to encrypt the plain text using the first three letters of your first name as a keyword as an encryption key. Show the Vigenère cipher text produced by encryption.
Task 2. Assessing the security of the Vigenère cipher involves evaluating its vulnerabilities and understanding its resistance to various cryptographic attacks. Assess the security of the Vigenère cipher in task 1 using any method. Suggest a mechanism to improve the security of the Vigenère cipher.
Task 3. Implement and apply row-column transposition to the ciphertext produced in task 1, trying to strengthen the encryption. This would create a combination of encryption methods that may provide an additional layer of security. You should use the last five digits

of your cell phone number as a key.

for example 51811

Key: 41523

and

for example 52811

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.

Task 4. Again assess the security of cipher text in task 3 using the same method and compare it with the previous one. Comment on your findings from the comparison.

Part II. Decryption

Reverse the row-column transposition on the ciphertext by arranging the cipher text. Apply the Vigenère decryption process using the same keyword that is used for decryption. This would recover the original text.

Part III. Reverse the Combination

The security of combining the two encryptions depends on various factors. Apart from other factors, it also depends on the sequence of combinations. Apply the row-column transposition first and then Vigenère.

Task 1. First, Apply row-column transposition on the given plain text to retrieve cipher text. Use the same key from part 1.

Task 2. Assess the security of the row-column transition in task 1 using the same method. Suggest a mechanism to improve the security of the row-column transposition.

Task 3. Second, implement and apply the Vigenère cipher to the ciphertext, trying to strengthen the encryption. Use the same key as part 1.

Task 4. Again assess the security of the Vigenère cipher in task 3 using the same method and compare it with the previous one. comment on your findings from the comparison based on the assessment method.

Task 5. Decrypt the original text by applying the Vigenère decryption process and then reversing the row-column transposition.

Part IV. Combination Analysis

Task 1. Could you find out which combination (Vigenère then row-column transposition, row-column transposition then Vigenère) is the better option through assessment methods?
Task 2. Apart from the combinations discussed above, suggest some other mechanisms to improve the security of encryption.

Assignment Approval (by TA and SA)

Assignment approval will have a weight on your grade for the assignment. 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. Show 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. 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 for TAs and Student Assistants.
5. You should **NOT** use available libraries/packages/classes for implementing the core functionality of the assignment.

You need to implement this assignment using Python.

Assignment Submission

Deadline: 23:59, Friday, Sept. 15, 2023 (submit your assignment through canvas)

Final submission:

1. Source Code
   - 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 .tar.gz or .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 and packages, commands to install the package. describe any command line arguments with the required parameters).
   - You should **NOT** use available libraries/packages/classes for implementing the core functionality of the assignment.
2. A **separate** report with PDF format
   - 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.
   - 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, *.tar 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

Describe the background 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

Detail description of the design, procedure, and implementation of your project along with the following details from Part I to Part IV.

2.1 Part I

- Describe your implementation of the Vigenère encryption. Include the cipher text.
- Discuss the security strengths and weaknesses of the Vigenère cipher. What kind of attacks is it susceptible to, and how can they be mitigated?
- Explain which method you applied to assess the security of the Vigenère cipher.
- Suggest mechanisms to improve the security of the Vigenère cipher

2.2 Part II

- Describe your implementation of the Vigenère decryption.
- Does the order in which row-column transposition and Vigenère cipher are applied first matter when decrypting the ciphertext?
- What are the potential benefits of using multiple encryption techniques in sequence? How does this enhance the overall security of the message?

2.3 Part III

- Discuss the results of reversing the Vigenère and row-column transposition combination.
- Analyze the security aspects of the row-column transposition. How does it contribute to the overall security of the combined encryption?

2.4 Part IV

Discuss the questions stated in the problem description.

3. Test Results

Results of testing the software, as you observed/recorded them. Note that this section is only for observations you make during testing. Your analysis belongs in the Discussion section.

4. Discussion

Your analysis of what your testing results mean, and your error analysis.

5. Conclusion

A short paragraph that restates the objective from your introduction and relates it to your results, 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.