Intro to Cyber Security

(Assignment 4: Break the Cipher)

Deadline: April 07, 2023, 11:59 PM

Objective:

The objective of this assignment is to introduce students to the concept of frequency analysis as a method to break simple substitution ciphers. Students will write a program in python to break a simple substitution cipher using frequency analysis attack.

Instructions:

Note: This is a group assignment, and you can work in a group of 3-4 people maximum. If a student wants to work alone, he/she should provide a valid reason for not working in a group.

You are required to decide the group members by 03/21/2023. The group members names should be sent by email to my TA.

Step 1: Ciphertext

Your program will take ciphertext (a text message that has been encrypted using a Random substitution cipher) as input. The ciphertext will consist of **uppercase letters**, spaces, and punctuation marks. Your task is to decipher this message using frequency analysis.

Step 2: Frequency Analysis

Frequency analysis is a technique that involves analyzing the frequency of letters or symbols in a given text to make educated guesses about the substitutions used in the cipher. In the English language, certain letters occur more frequently than others. You can find English letters frequency chart on internet.

Your program should perform the following steps:

- On execution, the program should prompt the user to input cipher text.
- It should Calculate the frequency of each letter (A-Z) in the ciphertext.
- Create a frequency distribution table or dictionary or a graph, mapping each letter to its frequency.

Step 3: Decipher the Text

- Using the mapping obtained from the frequency analysis, decipher the entire ciphertext. Replace the ciphered letters with their corresponding guesses. Spaces and punctuation marks should remain unchanged.
- Frequency analysis doesn't work 100% . After the automated partial/full decryption , your program should give the user an option to manually replace the ciphered letters with

user's suggested plaintext letters. This will allow you to completely decipher the ciphertext.

Step 4: Output the Deciphered Text

Print the deciphered on the text as the final output.

Step 5: Testing and Validation

Test your program with various ciphertexts to ensure that it works correctly and consistently.

You can use various online resources to generate simple substitution ciphertexts. For example

https://cryptii.com/pipes/alphabetical-substitution

Step 6: Submission and Demonstration

1. Submit your code along with comments explaining the logic and any assumptions you made during the process to Canvas **(April 07, 2023, 11:59 PM)**
2. Demonstration of the program (Date and Venue will be announced on Canvas)

Grading:

Your assignment will be graded based on the following criteria:

1. Correctness of the frequency analysis and decryption process.
2. Clarity and organization of your code.
3. Explanation of your code and assumptions in comments.
4. Demonstration

Note:

- You may assume that the input ciphertext will be in **uppercase** and will not contain digits or special characters other than spaces and punctuation marks.
- You can refer to English letter frequency charts available online to aid your analysis.
- Keep in mind that this assignment is focused on simple substitution ciphers and frequency analysis. More complex ciphers are not within the scope of this assignment.
- *Similarities in code among groups or from online resources like Stack Overflow , ChatGPT etc or failing to explain the code will be considered plagiarism and will be reported to NJIT . Plagiarism is a serious offense . Please refer to NJIT academic code of integrity policy for more information.*