Difficulty: Tier-0

Learning Outcome: The student will gain experience in using the C programming language to solve a simple cybersecurity problem.

GitHub Classroom Link:

Description:

A substitution cipher is a cipher is an encryption method where one letter is swapped with another in a 1-to-1 mapping. For example, the cipher might indicate the following mapping:

H is replaced be X
E is replaced by N
L is replaced by A
O is replaced by R

If these rules exist in a mapping, the word 'Hello' might be encrypted as 'XNAAO'. Decryption could be achieved by reversing the mappings. If XNAAO were provided as input, the right-hand portion of the rule could be consulted to decrypt the input and produce 'HELLO'.

Your task will be to create a C program that can encrypt and decrypt using a substitution cipher. Your program should ask for a mode (encrypt or decrypt), a text file containing the cipher, and string input (plain text if encrypting, cipher text if decrypting). The output should be the cipher text if encrypting or the plain text if decrypting. Additionally, you should ensure that your program is not case sensitive and validate the cipher file to ensure that it does not have duplicate mappings or incomplete mappings. Each letter must appear on the left-hand side exactly once and the right-hand side exactly once.

The file format for the cipher file should be comma-separated values. There should be one rule per line and each begin with the letter being replaced and end with the letter replacing it. The above rules would be written in this format as:

H,X
E,N
L,A
O,R

Requirements:

- The input to your program must match what is listed in the description (mode, cipher file, string). You may either prompt or use CLI input.

- Your program must not be case sensitive.
    - ‘hello’, ‘Hello’, ‘HELLO’, and ‘HeLlO’ should all produce the same output, for example.
- Your program must validate the structure of the cipher file and output with an appropriate error message if it is not followed.
    - A file with lines *X,A* and *X,R* should be rejected.
    - A file with the lines *x,A* and *X,R* should be rejected
    - A file with the lines *x,A* and *D,a* should be rejected
- You may assume that input will only be single words
- You do not need to consider whitespace, punctuation, or special symbols

Deliverables:

a. By 8:00 PM on 09/08/2022, you must submit a **PDF** containing screenshots of the output of your program executing under the following scenarios:
    a. Encryption, good input
    b. Decryption, good input
    c. Encryption, demonstrating two input strings that only differ in case produce the same output
    d. Decryption, demonstrating two input strings that only differ in case produce the same output
    e. A test case demonstrating an error with letter duplication on the left side of a rule in the cipher file
    f. A test case demonstrating an error with letter duplication on the right side of a rule in the cipher file

b. By 8:00 PM on 09/08/2022**,** you must submit a GitHub classroom link to the drop box on MyCourses
    a. Your GitHub repo must include your source code and the cipher files used in the above examples.