CS 458 Spring 2024 - Coding assignment II

Due in Blackboard Assignment Saturday, March 23rd, 2024 by 11:59pm

---

Objective

The objective of this assignment is to implement a command-line program in a language of your choice that allows users to perform encryption and decryption using various techniques covered in the lab 2, including substitution ciphers, transposition ciphers, different encryption algorithms, and modes.

Program Features

1. The program should display a list of options for encryption techniques, including:
   - Substitution cipher
     - Shift Cipher
     - Permutation Cipher
   - Transposition ciphers
     - Simple Transposition
     - Double Transposition
   - Vigenére Cipher
   - Different encryption algorithms (e.g., AES-128, DES, 3DES)
   - Different encryption modes (e.g., ECB, CBC, CFB, OFB)
2. Based on the user's selection, prompt the user to enter a message (plaintext) to be encrypted.
3. The size of the message should be greater than the maximum size of the block used by the chosen encryption algorithm.
4. After entering the message, allow the user to choose whether to enter encryption key or use a default key.
5. Perform the encryption using the selected technique and encryption key.
6. Display the encrypted message (ciphertext).
7. Provide an option for decryption, where the user can input the ciphertext and select the appropriate decryption technique based on the encryption method used.
8. If decryption is selected, prompt the user to enter the decryption key or use the same key as encryption by default.
9. Perform decryption using the selected technique and decryption key.
10. Display the decrypted message (plaintext).

Submission

Submit the source code of your program along with a brief report describing the functionality, usage instructions, and any observations or challenges encountered during the implementation. Include screenshots demonstrating the encryption and decryption processes using different techniques. Upload the files to the course Blackboard for evaluation.