Network Security Project - Option 2

Symmetric Encryption/Decryption

Total 20 points

(Due on Apr 22 11:59 pm, 2025)

Part 1 (10 points) – Encryption/Decryption using Polyalphabetic Ciphers

- Input
  - A given text file for plaintext (assume only 26 letters, no special characters, numbers nor punctuations)
  - 3 substitution ciphers, M1,M2,M3
    - M1 – right shift 8 letters
    - M2 – Plain: a b c d e f g h i j k l m n o p q r s t u v w x y z
Cipher: D K V Q F G B X W P E S C J H T M Y A U O L R I Z N
    - M3 – left shift 12 letters
  - cycling pattern
    - n=4: M2,M3,M1,M3; M2,M3,M1,M3; M2,M3,M1,M3;
- Output
  - Encrypted ciphertext and decrypted plaintext
- See the requirements for submission

Part 2 (10 points) – Encryption/Decryption using Rail Fence Cipher

- Input
  - A given text file for plaintext
  - A given depth of the rail fence (not fixed, user input at the time of execution)
- Output
  - Encrypted ciphertext and decrypted plaintext
- See the requirements for submission

Requirements

a. You are given the flexibility to choose one of your favorite programming languages for implementation either in a Windows or Linux environment.

b. You must submit
   a) all the **source code** of your program
   b) **executable files and Makefile**(if using c/c++)
   c) **ReadMe file** that describes
      i. the use of your program
      ii. how to execute it

c. You will need to **demonstrate your project in class on Zoom on Apr 24. Otherwise, 10 out of total 20 points will be deducted from your project**.