CSCI 4900_6600 Project

Symmetric Encryption/Decryption

Part 1 (50 points + bonus if any) – Encryption/Decryption using Polyalphabetic Ciphers **(Due on July 28th 11:30 pm, 2017)**

- Input
  - A given plaintext or ciphertext (assume only 26 letters, no special characters, numbers and punctuations)
  - 3 substitution ciphers, M1,M2,M3
    - M1 – left shift 3 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 I B J W P E S C X H T M Y A U O L R G Z N
    - M3 – right shift 5 letters
  - cycling pattern
    - n=3: M1,M2,M3; M1,M2,M3;
- Output
  - Encrypted ciphertext or decrypted plaintext
- See the requirements for submission
- Bonus (extra 10 points) – optional
  - Your program can handle encrypt/decrypt a given message with special characters, numbers and punctuations
  - You can decide how to encrypt and decrypt the special characters, numbers and punctuations (You can define your own cipher if you want!).
  - Please detail this part in the ReadMe file

Part 2 (50 points + bonus if any) – Encryption/Decryption using Rail Fence Cipher with depth 4 **(Due on Aug. 10th 11:30 pm, 2017)**

- Input
  - A given plaintext or ciphertext
  - Depth = 4
- Output
  - Encrypted ciphertext or 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 Windows or Linux environment.
b. You must submit

a) all the source code of your **daemon program**
b) **executable files**
c) **Makefile** (if use c/c++)
d) **ReadMe file** that describes
    i. the use of your program
    ii. how to run it

c. You need to demonstrate your project in class at the end of the semester.
d. Bonus (extra 5 points) – optional
    a) If you implement a GUI for either Part 1 or Part 2 or both.
    b) Please detail this part in the ReadMe file.