Birzeit University

Department of Electrical & Computer Engineering

Second Summer Semester, 2019/2020

ENCS313 Linux Laboratory

Shell Scripting Project – Text Message Encryption and Decryption

---

You are required to build a shell script that does simple encryption/decryption algorithm based on Caesar cipher algorithm for English- based text messages.

Caesar cipher
The Caesar cipher is one of the earliest methods in cryptography. In this method, the message is hidden from unauthorized readers by shifting the letters of a message by an agreed number. It uses the substitution of a letter by another one further in the alphabet. Upon receiving the message, the recipient would then shift the letters back by the same number agreed upon earlier.

Encryption example: Assume shift value = 3

Plain text	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Caesar cipher (+3)	DEFGHIJKLMNOPQRSTUVWXYZABC

Decryption example:

Decrypt GFRGHA with shift value = 3.
To decrypt G, take the alphabet and look 3 letters before: D. So, G is decrypted with D.
To decrypt X, loop the alphabet: before A: Z, before Z: Y, before Y: X. So, A is decrypted X.
So, GFRGHA is decrypted to DCODEX.

Here we need to update Caesar method by making dynamic shifting value. The shift value calculated as following: Shift value = Max ((sum of characters frequencies for each word in the text) mod 26).

For example:
Given the following plain text message:
“Welcome to Linux lab”

The frequency of each character is:
F(w) = 1, F(e) = 2, F(l) = 3, F(c) = 1, F(o) = 2, F(m) = 1, F(t) = 1, F(i) = 1, F(n) = 1, F(u) = 1, F(x) = 1, F(a) = 1, F(b) = 1

Shift value = Max { [(1+2+3+1+1+1), (1+2), (3+1+1+1+1), (3+1+1)] mod 26} = 9

Procedure:

1. The program will ask user to choose between encryption and decryption (e.g. e for encryption and d for decryption)
2. If the user enters ‘e’:

a. The program should print on the screen “Please input the name of the plain text file”
b. The program should remove none alphabet characters
c. Convert all characters to lower case
d. After that, the program must print the sum of word characters frequencies
e. After that, the program should print shift value
f. Ask user to input the name of the cipher text file
g. The program will write the generated cipher text on the cipher file

3. If the user enters ‘d’:
    a. The program should print on the screen “Please input the name of the cipher text file”
    b. After that, the program must print the sum of word characters frequencies
    c. After that, the program should print shift value
    d. Ask user to input the name of the plain text file
    e. The program will write the generated plain text on the plain text file

Submission:

Please submit the following:

1. Shell script program
2. Report: the report must include:
    a. The code, idea, and a screen shot of each task. For example: for the task “Convert all characters to lower case” you need to add code + description + screen shot of the output
    b. At least 2 testing examples.

Notes:

- Write the code for the shell script to satisfy the requirements described above and name the script as SimpleEncryption.
- Make sure your code is clean and well indented; variables have meaningful names, etc.
- Make sure your script has enough comments inserted to add clarity.
- Work in groups of at most two students
- Deadline: Monday, 17 August, 2020 at 11:59pm. Please submit your project (code + report) through Ritaj as a reply to this message.
- This project is per group effort: instances of cheating will result in you failing the lab.