Birzeit University

Department of Electrical & Computer Engineering

Summer Semester, 2021/2022

ENCS3130 Linux Laboratory

Shell Scripting Project – Text Message Encryption and Decryption

---

You are required to build a shell script that does simple encryption/decryption algorithm for text messages with only alphabet characters. This encryption/decryption is based on the use of XOR logic gate.

Encryption process:
The process for the encryption algorithm can be summarized in the following steps:

Step 1: Generate key. The key will be generated as following:

Key = Max[(sum of characters index in the word) mod 256]

The character index is the order of the character in the English alphabet. I.e. The character index of "A" or "a" is 1, and the character index of "W" or "w" is 23. As an example for key generation, if the file contains the sentence "Welcome to Linux lab" then the key will be:

Key = Max [(23+5+12+3+15+13+5) mod 256 , (20+15) mod 256 , (12+9+14+21+24) mod 256 , (12+1+2) mod 256] = 80

Step 2: The key will then be represented as 8-bit binary number.

Step 3: for each character in the text file compute the XOR between the key generated and the ASCII code of the character. The result will be 8-binary digit.

Step 4: for each 8-bit binary result, swap the first 4-bit with the last four bit. For example: 10001100 become 11001000.

Step 5: at the end, swap the first 4-bit with the last four bit of the key and add it as the last character of the generated file.

Decryption process:
The process for the decryption algorithm can be summarized in the following steps:

Step 1: get key (the las character in the encryption file) and swap the first 4-bit with the last four bit

Step 2: for each character in the encrypted file, swap the first 4-bit with the last for bit.

Step 3: Do the XOR between the key and each character from the encrypted file.

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 raise an error if the file contains any non-alphabet characters
    c. After that, the program must print the value of the key in decimal and binary
    d. Ask user to input the name of the cipher text file
    e. 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 value of the key
    c. Ask user to input the name of the plain text file
    d. 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 "Generate key" 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, 12 August, 2022 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.