

Birzeit University

Department of Electrical & Computer Engineering

First Semester, 2022/2023

Computer Architecture

First Project – Text Message Encryption and Decryption

You are required to build a MIPS program 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 (Words length)

For example:

Given the following plain text message:

“Welcome to Linux lab”

Shift value = Max (7, 2, 5, 3) = 7

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 should print shift value
 - e. Ask user to input the name of the cipher text file
 - f. 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 should print shift value
 - 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. Code
2. At least 2 testing examples.

Notes:

- Write the code for the MIPS program to satisfy the requirements described above and name the file as SimpleEncryption.
- Make sure your code is clean and well indented; variables have meaningful names, etc.
- Make sure your code has enough comments inserted to add clarity.
- Work in groups of at most two students
- Deadline: Friday, 30 December, 2022 at 11:59pm. Please submit your project (code + test cases) through Ritaj as a reply to this message.
- This project is per group effort: instances of cheating will result in you failing the course.