Lab #13

Introduction to Operating Systems CS-UY 3224 | CS-UY 3224G

Mirna Džamonja, email md5961@nyu.edu

Due 4th of December, 2023 at 5 PM Paris time. Please hand in through the *Assignments* option on *Brightspace.*

Question 1: *Ceasar ciphering code*

.

Explanation The Caesar Cipher is one of the simplest and oldest encryption techniques in the history of cryptography. It is a substitution cipher where each letter in the plaintext is shifted a certain number of places down or up the alphabet. The method is named after Julius Caesar, who seemed to have used it to encrypt his private correspondence. (It seems that his talents in the military science were higher than in secure messaging, as the code is not very secure).

The cipher works by choosing a fixed number called 'key' or 'shift' and shifting each letter of the alphabet by that many places in the alphabet, cycling back to the beginning if necessary. For example, if the shift is 3, then 'A' becomes 'D,' 'B' becomes 'E,' and so on. The alphabet wraps around, so 'Z' becomes 'C.'

Decryption is performed by shifting the letters in the opposite direction (subtracting the key).

Question. Discuss the security of the Caesar Cipher. How can it be cracked ? Come up with two different ways of improving its security.

To do at home and hand in: Your complete answer.

Question 2: *Programmation for Ceasar.*

1. Write a C program that implements the Ceasar ciphering code.
2. Write a C program that cracks the Ceasar ciphering code.
3. Write a C program that implements an improved version of the Ceasar ciphering code using one of the methods you designed in the first Question.

To do at home and hand in: Your C programs and the documentation .