LUCRAREA DE LABORATOR 2

Sistemul de criptare CAESAR

Despre

În criptografie, sistemul CAESAR este considerat ca fiind unul din primele sisteme de criptare cunoscute. Conform istoricului Suetoniu, acest sistem a fost folosit de Iulius Caesar cu deplasarea 3 în corespondenţa sa, iar nepotul sau Imperator Augustus folosea acelaşi sistem cu deplasarea 1.

Descriere

Procesul criptografic CAESAR constă în utilizarea unui număr întreg în calitate de cheie de criptare. Numărul cheie poate fi în limita alfabetului latin, deci între 0 şi 25. Deci, metoda constă în rescrierea alfabetului latin permutat ciclic începând de la numărul cheie. Criptarea şi decriptarea se fac numai în baza numărului cheie. Dacă numărul cheie este 6 atunci vom obţine următoarea configurare prezentată mai jos.

A B C D E F G I J K L M N O P Q R S T U V W X Y Z
G I J K L M N O P Q R S T U V W X Y Z A B C D E F

Exemplu

k=6 N U P O T V E N I A Z I T A V U Z B K T O G F O	crypt(m) = m + k mod 26 decrypt(m) = m – k mod 26

Implementări

Pentru criptare/decriptare vom utiliza următoarele două funcţii care fac toată treaba pentru noi şi respectiv care sunt incluse în fişierul „csr.h”. Corpul funcţiei „CSR_encrypt” îl găsiţi în fişierul anexat la moodle, sau va fi prezentat parţial la lecţie de către profesor.

Sarcini de laborator

1. Crează corpul funcţiei CSR_encrypt
2. Verifică corectitudinea criptării:
   a) mesajul de criptare: nupotveniazi
   b) pasul: 6
   c) mesajul criptat: tavuzbktogfo
3. Crează o dublură a funcţiei CSR_encrypt cu numele CSR_enc_math
4. Utilizează formula matematică de criptare în funcţia CSR_enc_math
5. Verifică corectitudinea criptării după modelul de mai sus

Tema pentru acasă

Adaptează aplicaţia după modelul de mai jos:

1. Crează corpul funcţiilor de decriptare CSR_decrypt şi CSR_dec_math
2. Modifică fişierul main.c în aşa mod încât cele 4 funcţii să fie localizate în fişierul csr.h
3. Modifică cele 4 funcţii în aşa mod încât variabila letters să fie localizată în fişierul vars.c

Exemple de rulare

Criptarea

Unix/Linux

```
$ ./crypto -Ecsr NUPOTVENIAZI
key: 6
enc: TAVUZBKTOGFO
```

Windows

```
C:\Users> crypto.exe -Ecsr NUPOTVENIAZI
key: 6
enc: TAVUZBKTOGFO
```

Decriptarea

Unix/Linux

```
$ ./crypto -Ecsr TAVUZBKTOGFU
key: 6
dec: NUPOTVENIAZI
```

Windows

```
C:\Users> crypto.exe -Ecsr TAVUZBKTOGFU
key: 6
dec: NUPOTVENIAZI
```