LUCRAREA DE LABORATOR 3

Sistemul de criptare CAESAR CU CHEIE

Despre

În criptografie, sistemul CAESAR CU CHEIE este o variantă imbunătățită a vechiului sistem de criptare/decriptare CAESAR, pentru ai mări rezistență la atacul prin forță brută.

Descriere

Procesul criptografic CAESAR CU CHEIE constă în utilizarea unui cuvânt în calitate de cheie de criptare. Caracterele din care este compus cuvântul cheie sunt în limita alfabetului utilizat. Metoda constă în aşezarea cuvântului cheie la începutul alfabetului. Apoi se elimină la o altă apariţie caracterele identice înlocuindu-se cu litere din alfabet ce nu se găsesc şi în cuvântul cheie pentru a exclude utilizarea caracterelor identice. După care se scriu literele rămase din alfabet în ordine alfabetică. Criptarea şi decriptarea se fac numai în baza cuvântului cheie. Dacă cuvântul cheie este „MARTOR” atunci vom obține 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
M A R T O B C D E F G I J K L N P Q S U V W X Y Z

Exemplu

k=MARTOR S T U D E N T Q S U T O J S	crypt(m) = m + 1 mod 26 decrypt(m) = (m – 1 + mod 26) mod 26

Implementări

Pentru criptare/decriptare vom utiliza o funcție specială destinată generării unui keystream ce integrează cuvântul cheie în alfabet. Corpul acestei funcții precum și corpul funcției de criptare le găsiți anexate la moodle, sau va fi prezentat parțial la lecție de către profesor.

Sarcini de laborator

1. Crează corpul funcției CSK_encrypt
2. Verifică corectitudinea criptării:
   a) mesajul de criptare: student
   b) cheia: martor
   c) mesajul criptat: qsutojs
3. Crează corpul funcției CSK_keygen
4. Mută algoritmul de generare a keystream-ului în funcția CSK_keygen

Tema pentru acasă

Adaptează aplicația după modelul de mai jos:

1. Crează corpul funcției de decriptare CSK_decrypt
2. Modifică fișierul main.c în așa mod încât cele 3 funcții să fie localizate în fișierul csk.h
3. Modifică cele 3 funcții în așa mod încât variabilele des utilizate să fie localizate în fișierul vars.c
4. Adaugă o variabilă alfabet2 ce conține atât literele minuscule cât și cele majuscule plus toate cifrele, și fă-o disponibilă doar pentru această metodă de criptare.

Exemple de rulare

Criptarea

Unix/Linux

```
$ ./crypto -Ecsk STUDENT
key: MARTOR
enc: QSUTOJS
```

Windows

```
C:\Users> crypto.exe -Ecsk STUDENT
key: MARTOR
enc: QSUTOJS
```

Decriptarea

Unix/Linux

```
$ ./crypto -Dcsk QSUTOJS
key: MARTOR
dec: STUDENT
```

Windows

```
C:\Users> crypto.exe -Dcsk QSUTOJS
key: MARTOR
dec: STUDENT
```