LUCRAREA DE LABORATOR 6

Optimizarea criptosistemului VIGENERE (v2)

Despre

În criptografie, sistemele fluide sunt cele mai utilizate în prezent din cauza nivelului mărit de variațiuni posibile. Există mai multe posibilități de a transforma un sistem cu chei statice într-un sistem cu chei dinamice. În continuare, vom transforma sistemul de criptare VIGENERE într-un sistem fluid, adăugându-i variabila ce conține timpul de execuție în momentul criptării.

Descriere

Procesul criptografic este identic cu sistemul de criptare VIGENERE plus timpul de execuție. Adică, constă în utilizarea unui cuvânt cheie utilizat la criptare și decriptare. Cuvântul cheie poate fi doar în limita alfabetului utilizat. Deci, metoda constă în adunarea numărului de rând al caracterului mesajului cu numărul de rând al caracterului cuvântului cheie și cu timpul de execuție. La finisarea caracterelor din care este formată cheie se reia cuvântul cheie de la început, timpul de execuție rămâne același. Evident că criptarea se face numai în baza cuvântului cheie ales de utilizator și în baza timpului de execuție inițial adăugat la algoritm în mod aleatoriu, iar decriptarea se face în baza cuvântului cheie și în baza timpului de execuție utilizat la criptare. Prin urmare, la criptare este important de afișat pe lângă mesajul criptat și timpul de execuție. Dacă cuvântul cheie este„FOCAR” vom obține următoarea configurare prezentată mai jos.

Exemplu

k=FOCAR time=1644485555 N U P O T V E N I A Z I D T C Z V L D A T C P H	$crypt(m) = m_i + k_i + time \bmod 26$ $decrypt(m) = (m_i - k_i - (time \bmod 26))+26*2) \bmod 26$

Implementări

Pentru criptare/decriptare vom utiliza următoarele două funcții care fac toată treaba pentru noi și respectiv care sunt incluse în fișierul „vgm.h”. 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 VGM_encrypt
2. Verifică corectitudinea criptării:
   a) mesajul de criptare: nupotveniazi
   b) cheia: focar
   c) seed-ul: 1644485555
   d) mesajul criptat: dtczvldatcph
3. Scoate seed-ul implicit după verificare
4. Automatizează procesul de generare a seed-ului

Tema pentru acasă

Adaptează aplicația după modelul de mai jos:

1. Crează corpul funcției de decriptare VGM_decrypt
2. Modifică fișierul main.c în așa mod încât cele 2 funcții să fie localizate în fișierul vgm.h
3. Modifică cele 2 funcții în așa mod încât variabilele des utilizate să fie localizate în fișierul vars.c
4. Utilizează alfabet2 ca variabilă de bază pentru acest algoritm

Exemple de rulare

Criptarea

Unix/Linux

```
$ ./crypto -Evgm NUPOTVENIAZI
key: FOCAR
enc: DTCZVLDATCPH
tms: 1644485555
```

Windows

```
C:\Users> crypto.exe -Evgm NUPOTVENIAZI
key: FOCAR
enc: DTCZVLDATCPH
tms: 1644485555
```

Decriptarea

Unix/Linux

```
$ ./crypto -Dvgm DTCZVLDATCPH
key: FOCAR
tms: 1644485555
dec: NUPOTVENIAZI
```

Windows

```
C:\Users> crypto.exe -Dvgm DTCZVLDATCPH
key: FOCAR
tms: 1644485555
dec: NUPOTVENIAZI
```