LUCRAREA DE LABORATOR 7

Adăugarea operațiilor pe biți și dispersarea seed-ului pe hash la criptosistemul VIGENERE (v3)

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 de tip alfabet în unul de operații binare. În continuare, vom transforma sistemul de criptare VIGENERE într-un sistem fluid, cu parcurgere binară.

Descriere

Procesul criptografic este identic cu sistemul de criptare VIGENERE precedent, cu excepția excluderii alfabetului la procesul de parcurgere binară. Adică, constă în utilizarea unei din cele 3 operații binare: XOR, AND, OR. Deci, metoda constă în compararea binară a biților ASCII ale caracterelor mesajului cu cele ale cheie-i. La finisarea parcurgerii caracterelor în format binar, mai este parcurs și mesajul criptat pentru înlocuirea caracterelor speciale cu cele obișnuite. Plus, trebuie ca seed-ul de timp să fie dispersat random sau pseudo-random pe lungimea mesajului criptat. Criptarea și decriptarea trebuie să conțină algoritmii voștri personali. În lucrarea încărcată pe moodle trebuie să adăugați și exemplele matematice utilizate pentru criptare și decriptare.

Implementări

Pentru criptare/decriptare vom utiliza următoarele două funcții care fac toată treaba pentru noi și respectiv care sunt incluse în fișierul „vgb.h”. Celelalte funcții necesare pentru: parcurgerea binară, înlocuirea caracterelor speciale și dispersarea aleatorie a seed-ului, le efectuați de sine-stătător. Corpul acestor funcții precum și corpul funcției de criptare le găsiți anexate la moodle, sau vor fi prezentate parțial la lecție de către profesor.

Sarcini de laborator

1. Crează corpul funcției VGB_encrypt
2. Crează corpul funcției VGB_exclud
3. Crează corpul funcției de VGB_random

Tema pentru acasă

Adaptează aplicația după modelul de mai jos:

1. Crează corpul funcției de decriptare VGB_decrypt
2. Modifică fișierul main.c în așa mod încât toate funcțiile necesare să fie localizate în fișierul vgb.h
3. Modifică funcțiile în așa mod încât variabilele des utilizate să fie localizate în fișierul vars.c

Exemple de rulare

Criptarea

Unix/Linux

```
$ ./crypto -Evgb NUPOTVENIAZI
key: FOCAR
enc: $2a$06$6N6Yv2F8HGD.E4dSTWR4AOLscQRr
```

Unix/Linux

```
$ ./crypto -Evgb NUPOTVENIAZI
key: FOCAR
enc: $2a$06$.Ekr0KoiMcr1ToNrVFwWQ.dZMhQQ
```

Windows

```
C:\Users> crypto.exe -Evgb NUPOTVENIAZI
key: FOCAR
enc: $2a$06$6N6Yv2F8HGD.E4dSTWR4AOLscQRr
```

Windows

```
C:\Users> crypto.exe -Evgb NUPOTVENIAZI
key: FOCAR
enc: $2a$06$.Ekr0KoiMcr1ToNrVFwWQ.dZMhQQ
```

Decriptarea

Unix/Linux

```
$ ./crypto -Dvgm $2a$06$6N6Yv2F8HGD.E4dSTWR4AOLscQRr
key: FOCAR
dec: NUPOTVENIAZI
```

Unix/Linux

```
$ ./crypto -Dvgm $2a$06$.Ekr0KoiMcr1ToNrVFwWQ.dZMhQQ
key: FOCAR
dec: NUPOTVENIAZI
```

Windows

```
C:\Users> crypto.exe -Dvgm $2a$06$6N6Yv2F8HGD.E4dSTWR4AOLscQRr
key: FOCAR
dec: NUPOTVENIAZI
```

Windows

```
C:\Users> crypto.exe -Dvgm $2a$06$.Ekr0KoiMcr1ToNrVFwWQ.dZMhQQ
key: FOCAR
dec: NUPOTVENIAZI
```