LUCRAREA DE LABORATOR 5

Sistemul de criptare VIGENERE

Despre

În criptografie, sistemul VIGENERE a fost elaborat de către baronul francez Blaise Vigenere (1523-1596) diplomat la curtea regelui Henry III. A fost considerat mult timp unul din cele mai bune sisteme de criptare. În prezent există multe variațiuni ale acestui sistem.

Descriere

Procesul criptografic VIGENERE 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. La finisarea caracterelor din care este formată cheie se reia cuvântul cheie de la început. Evident că criptarea și decriptarea se fac numai în baza cuvântului cheie. Dacă cuvântul cheie este„FOCAR” vom obține următoarea configurare prezentată mai jos.

Exemplu

k=FOCAR N U P O T V E N I A Z I S I R O K A S P I R E W	$crypt(m) = m_i + k_i \bmod 26$ $decrypt(m) = (m_i - k_i + 26) \bmod 26$

Implementări

Pentru criptare/decriptare vom utiliza următoarele două funcții care fac toată treaba pentru noi și respectiv care sunt incluse în fișierul „vgn.h”. Corpul acestei funcției de criptare îl găsiți în fișierul anexat la moodle.

Sarcini de laborator

1. Crează corpul funcției VGN_encrypt
2. Verifică corectitudinea criptării:
   a) mesajul de criptare: nupotveniazi
   b) cheia: focar
   c) mesajul criptat: sirokaspirew

Tema pentru acasă

Adaptează aplicația după modelul de mai jos:

1. Crează corpul funcției de decriptare VGN_decrypt
2. Modifică fișierul main.c în așa mod încât cele 2 funcții să fie localizate în fișierul vgn.h
3. Modifică cele 2 funcții în așa mod încât variabilele des utilizate să fie localizate în fișierul vars.c
4. Adaugă o variabilă alfabet3 ce conține toate caracterele incluse în variabila alfabet2 plus și caractere speciale. Și fă-o disponibilă doar pentru această metodă de criptare.

Exemple de rulare

Criptarea

Unix/Linux

```
$ ./crypto -Evgn NUPOTVENIAZI
key: FOCAR
enc: SIROKASPIREW
```

Windows

```
C:\Users> crypto.exe -Evgn NUPOTVENIAZI
key: FOCAR
enc: SIROKASPIREW
```

Decriptarea

Unix/Linux

```
$ ./crypto -Dvgn SIROKASPIREW
key: FOCAR
dec: NUPOTVENIAZI
```

Windows

```
C:\Users> crypto.exe -Dvgn SIROKASPIREW
key: FOCAR
dec: NUPOTVENIAZI
```