LUCRAREA DE LABORATOR 1

Aplicația shell personalizată de criptare

Despre

În criptografie, aplicațiile shell personalizate de criptare, sunt utilizate pentru crearea cheilor și pentru criptarea datelor private, preponderent de către administratorii de sistem și/sau de către utilizatorii preocupați de securitatea datelor personale. Aceste aplicații, urmăresc totalmente principiile de utilizare ale uneltelor shell.

Descriere

Procesul criptografic este absent și înlocuit temporar cu afișarea: „encrypt function” și „decrypt function”, la apelarea funcțiilor „CSR_encrypt” și respectiv „CSR_decrypt”. Funcția „main” conține scheletul necesar pentru dezvoltarea aplicației de criptare: variabile locale înlocuitoare pentru vectorul de argumente, ramificații de utilizare pentru contorul de argumente și loguri de eroare pentru ramificațiile prezente. Utilizatorul va introduce numele aplicației urmat de tipul criptării și de mesajul supus criptării sau decriptării, conform modelului de mai jos.

```
nameofapp -PROCESStypeofencryption message
```

Exemplu

`$ crypto -Ecsr message` `encrypt function`	funcția de criptare
`$ crypto -Dcsr message` `decrypt function`	funcția de decriptare
`$ crypto` `crypto: no option and message`	ramificația 1
`$ crypto -Ecsr` `crypto: no option or message`	ramificația 2/1

`$ crypto message` `crypto: no option or message`	ramificația 2/2
`$ crypto -Egdf message` `crypto: illegal option: -Egdf`	ramificația 3

Implementări

Pentru criptare/decriptare vom utiliza următoarele două funcții care sunt incluse temporar în fișierul „main.c”. Corpul funcției „CSR_encrypt” și „CSR_decrypt” doar afișează ce vor face în viitor funcțiile respective.

Sarcini de laborator

1. Crează corpul funcției main
2. Utilizează argumentele shell:
   a) argc
   b) argv
3. Crează variabilele înlocuitoare pentru vectorul de argumente
4. Crează funcțiile:
   a) CSR_encrypt
   b) CSR_decrypt
5. Utilizează logurile de eroare (în total 3)
6. Verifică corectitudinea funcționării aplicației după modelul de mai sus

Tema pentru acasă

Adaptează aplicația după modelul de mai jos:

1. Modifică cazul (argc==2) în așa fel încât să deosebească opțiunea de mesaj și să poată afișa următoarele:
   a) no option (dacă este introdus doar mesajul)
   b) no message (dacă este introdusă doar opțiunea)
2. Mai adaugă un caz care afișează:
   a) to many strings
3. Adaugă încă 2 loguri de eroare (în total 5)

Exemple de rulare

Criptarea

Unix/Linux

```
$ ./crypto -Ecsr mesaj
encrypt function
```

Windows

```
C:\Users> crypto.exe -Ecsr mesaj
encrypt function
```

Decriptarea

Unix/Linux

```
$ ./crypto -Dcsr mesaj
decrypt function
```

Windows

```
C:\Users> crypto.exe -Dcsr mesaj
decrypt function
```

Ramificațiile

Unix/Linux

```
$ ./crypto -Ecsr
./crypto: no message
$ ./crypto message
./crypto: no option
$ ./crypto -Ecsr message1 message2
./crypto: to many strings
```

Windows

```
C:\Users> crypto.exe -Ecsr
crypto.exe: no message
C:\Users> crypto.exe message
crypto.exe: no option
C:\Users> crypto.exe -Ecsr message1 message2
crypto.exe: to many strings
```