Zaštita teksta šifrovanjem

Sada, kad ste stekli malo iskustva sa ASCII vrednostima, možete da pređete na rutine za šifrovanje koje u dokumentima menjaju ASCII vrednosti i „zabrljaju" tekst tako da neovlašćeni ne mogu da ga pročitaju. Taj postupak, koji se zove *šifrovanje*, matematički menja znakove u fajlu tako da postanu nečitki za slučajnog posmatrača. Naravno, da bi šifrovanje bilo uspešno, mora postojati i način dešifrovanja, inače biste samo uništavali fajlove umesto da ih štitite. U sledećoj vežbi je prikazano kako se string bezbedno šifruje i dešifruje. Sada ćete pokrenuti program Encrypt da bise videli kako funkcioniše jedan jednostavan način šifrovanja.

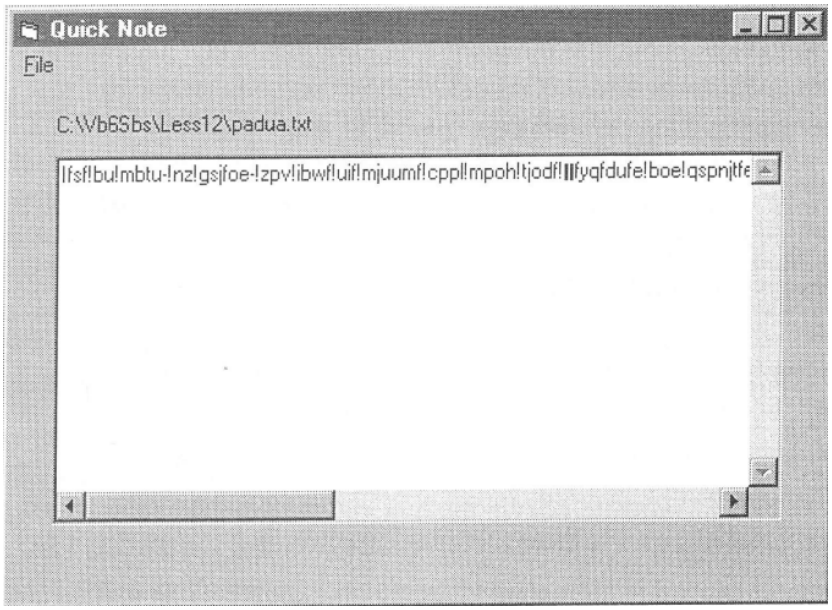
Šifrovanje teksta promenom ASCII vrednosti

1. Kliknite na dugme Open Project na liniji alatki i otvorite projekat Encrypt u folderu \Vb6Sbs\Less12.
2. Kliknite na dugme Start na liniji alatki da bi se program pokrenuo.
3. Upišite sledeći tekst, ili neki vlastiti, u polje za tekst.

   Here at last, my friend, you have the little book long since
   expected and promised, a little book on vast matter,
   namely, "On my own ignorance and that of many others."

   Francesco Petrarca, c. 1368.
4. U meniju File kliknite na komandu Save Encrypted File i sačuvajte fajl u folderu \Vb6Sbs\Less12 pod imenom **padua.txt**.

   Prilikom upisivanja tekstualnog fajla na disk, program menja ASCII vrednosti i prikazuje rezultat u polju za tekst na sledeći način:

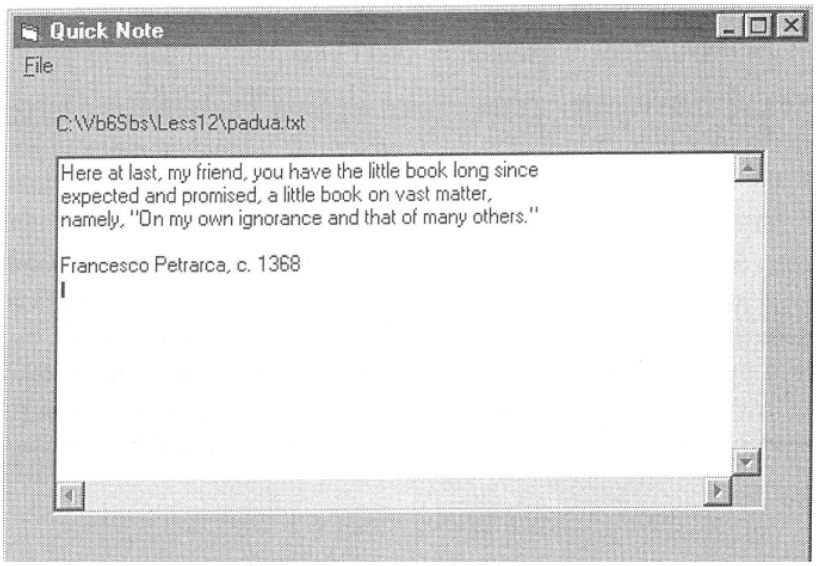


Ako fajl otvorite pomoću Microsoftovog Worda ili nekog drugog programa za obradu teksta, videćete isti rezultat – znakovi u fajlu su šifrovani da bi se sprečilo neovlašćeno čitanje.

❺ Da biste fajl vratili u prvobitni oblik, izaberite komandu Open Encrypted File u meniju File i otvorite fajl padua.txt iz foldera \Vb6Sbs\Less12.

Fajl se ponovo pojavljuje u prvobitnom obliku, kao na sledećoj slici.

❻ U meniju File kliknite na komandu Exit i zaustavite program.



Analiza programa Encrypt

❶ U prozoru Code otvorite proceduru događaja za objekat mnuItemSave u kojoj se nalazi programski kôd za šifrovanje čiji ste rezultat upravo posmatrali.

Iako možda deluje misteriozno, to je veoma jednostavna šema šifrovanja. Funkcijama Asc i Chr i petljom For, jednostavno sam ASCII vrednosti svakog znaka u polju dodavao jedan isti broj, a zatim sačuvao rezultat u navedenom fajlu.

```
'sačuvati tekst šemom šifrovanja (ASCII vrednost + 1)
encrypt$ = ""  'inicijalizirati string za šifrovani tekst
charsInFile% = Len(txtNote.Text) 'utvrditi dužinu stringa
For i% = 1 To charsInFile%   'za svaki znak u fajlu
   letter$ = Mid(txtNote.Text, i%, 1) 'pročitati sledeći znak
   'utvrditi ASCII vrednost znaka i dodati joj jedan
   encrypt$ = encrypt$ & Chr(Asc(letter$) + 1)
Next i%
Open CommonDialog1.FileName For Output As #1 'otvoriti fajl
Print #1, encrypt$          'upisati šifrovani tekst u fajl
txtNote.Text = encrypt$      'prikazati šifrovani tekst
```

Ključna naredba je:

```
encrypt$ = encrypt$ & chr(Asc(letter$) + 1)
```

U ovoj naredbi se utvrđuje ASCII vrednost tekućeg slova, vrednosti se dodaje 1, nova vrednost se prevodi u slovo i ono se dodaje na kraj šifrovanog stringa. U poslednja dva reda ove rutine se string encrypt$ upisuje u fajl i prikazuje u polju za tekst.

❷ Sada otvorite proceduru događaja za objekat mnuOpenItem da biste videli kako se tekst u programu dešifruje.

Programski kôd je skoro identičan, jedino što se ovde broj 1 umesto da se sabere oduzima od ASCII vrednosti slova.

```
'sada dešifrovati string oduzimanjem jedinice od ASCII vrednosti
decrypt$ = ""  'inicijalizirati string za dešifrovani tekst
charsInFile = Len(AllText$)  'utvrditi dužinu stringa
For i% = 1 To charsInFile   'jednom za svaki znak
   letter$ = Mid(AllText$, i%, 1)  'uzeti slovo funkcijom Mid
   decrypt$ = decrypt$ & Chr(Asc(letter) - 1) 'oduzeti 1
Next i%                  'i napraviti novi string
txtNote.Text = decrypt$     'zatim prikazati dešifrovani string
```

Ovakvo jednostavno šifrovanje je dovoljno da bi se sakrile informacije iz tekstualnih fajlova. Međutim, tako jednostavna šema se lako otkriva. Traženjem mogućih zamena za uobičajene znakove, kao što je razmak, određivanjem pomeraja ASCII vrednosti, da bi se vratio prvobitni znak, i pokušajem da se isti pomeraj vrednosti primeni na ceo tekst, čovek sa iskustvom u šifrovanju bi brzo dešifrovao ceo fajl. Osim toga, ova vrsta šifrovanja ne sprečava zlonamernog korisnika da fizički ošteti fajl - na primer da ga obriše, ako nije zaštićen na sistemu, ili da ga izmeni na razne načine. Međutim, ako je potrebno da samo na brzinu sakrijete informacije, ovaj jednostavan način je sasvim dovoljan.