Upotreba operatora Xor

Šema šifrovanja koju smo prikazali dovoljno je „bezbedna" za tekstualne fajlove zato što pomera ASCII vrednosti samo za jedan. Međutim, treba biti jako pažljiv ako se ASCII vrednosti pomeraju za više od nekoliko jedinica, a rezultat upisuje kao tekst u tekstualni fajl. Imajte na umu da drastično pomeranje ASCII vrednosti (na primer, kada biste na svaku ASCII vrednost dodavali 500) ne bi kao rezultat imalo ispravne ASCII vrednosti koje se kasnije mogu dešifrovati. Na primer, ako bi ASCII vrednosti za slovo "A" (65) dodali 500, rezultat bi bio 565. Funkcija Chr tu vrednost ne bi mogla da prevede u slovo, već bi dala rezultat *null*, koji kasnije ne bi mogao da se dešifruje. Drugim rečima, nikada više ne biste mogli da povratite prvobitni sadržaj, on bi bio zauvek izgubljen.

Jedno od rešenja ovog problema bi bilo da se slova u fajlu, prilikom šifrovanja prevedu u brojeve, kako bi dešifrovanje bilo moguće bez obzira koliko bi brojevi postali veliki (ili mali). Tu bi se za šifrovanje mogle koristiti bilo neke matematičke operacije - množenje, logaritmi i tako dalje - jedino bi bilo važno da postoji obrnuta operacija.

Visual Basic već sadrži jednu od najboljih alatki za šifrovanje numeričkih vrednosti. To je *operator Xor* koji izvršava operaciju „ekskluzivno ili" na samim bitovima koji čine broj. Da bismo videli kako funkcioniše operator Xor, iskoristićemo prozor Immediate gde se upisane naredbe odmah i izvršavaju. Prozor Immediate ćete otvoriti tako što ćete u Visual Basicovom meniju View izabrati komandu Immediate Window. Ako u prozor Immediate upišete:

```
print asc("A") Xor 50
```

i pritisnete taster Enter, Visual Basic će numerički rezultat 115 prikazati odmah ispod naredbe. Ako upišete:

```
print 115 Xor 50
```

Visual Basic će prikazati rezultat 65, ASCII vrednost slova A (vaše prvobitno slovo). Drugim rečima, rezultat operacije Xor može da se vrati na prvobitnu vrednost - ako se ponovo primeni ista operacija. Ovo zanimljivo ponašanje funkcije Xor se koristi u mnogim popularnim algoritmima šifrovanja. Tako će dešifrovanje vaših tajnih fajlova biti mnogo teže.

Šifrovanje teksta operatorom Xor

Sada isprobajte program Encrypt2 videćete kako radi operator Xor.

1. Kliknite na dugme Open Project na liniji alatki i otvorite projekat Encrypt2 u folderu \Vb6Sbs\Less12.
2. Kliknite na dugme Start na liniji alatki da biste pokrenuli program.
3. Za šifrovani fajl upišite sledeći tekst (ili nešto što sami želite):

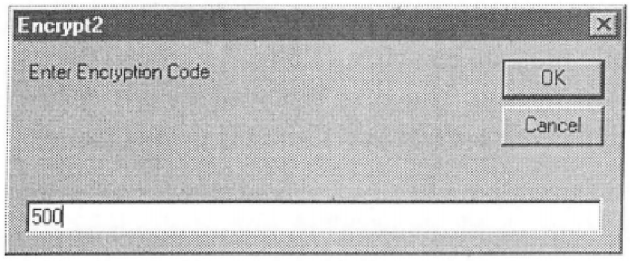
   Rothair's Edict (Lombard Italy, c. 643)

   296. On Stealing Grapes. He who takes more than three grapes from another man's vine shall pay six soldi as composition. He who takes less than three shall bear no guilt.

❹ U meniju File kliknite na komandu Save Encrypted File i sačuvajte fajl u folderu \Vb6Sbs\Less12 pod imenom **oldlaws.txt**.

Program zahteva da unesete tajni broj, šifru koja će se koristiti za šifrovanje i kasnije dešifovanje. (Zapišite broj – trebaće vam za dešifrovanje fajla.)

❺ Upišite **500** ili neki drugi broj i pritisnite taster Enter.



Visual Basic šifruje tekst operatorom Xor i rezultat upisuje na disk kao niz brojeva. Na ekranu nećete videti nikakvu promenu, ali budite uvereni da je program na disku napravio šifrovani fajl. (Možete da proverite nekim programom za obradu teksta.)

❻ Obrišite tekst iz polja tako što ćete ga označiti mišem i pritisnuti taster Del.

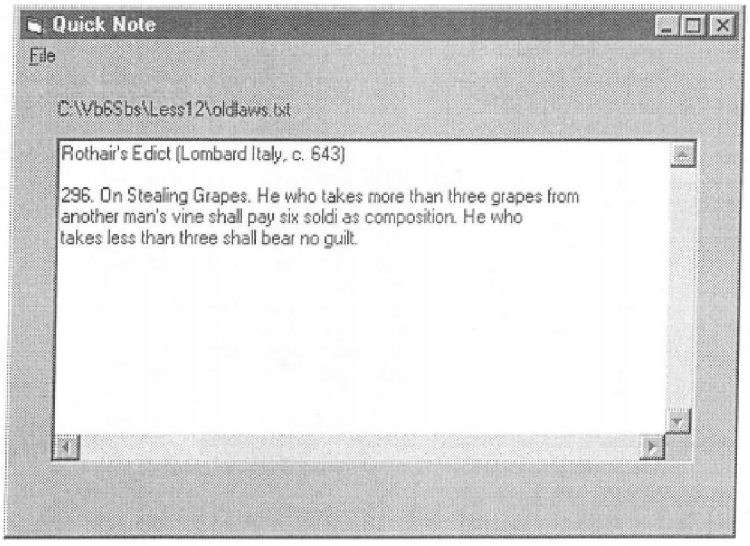
Sada ćete vratiti prvobitni izgled tekstá.

❼ U meniju File kliknite na komandu Open Encrypted File.

❽ Dva puta brzo kliknite na ime fajla oldlaws.txt, u okvir za dijalog upišite broj **500** i kliknite na dugme OK. (Ako ste na početku vežbe upisali neki drugi broj, upišite njega.)

Program otvara fajl i vraća prvobitni izgled teksta pomoću operatora Xor i šifre koju ste odredili.

❾ U meniju File kliknite na komandu Exit da biste zaustavili program.



Analiza programskog koda za šifrovanje

Operator Xor se koristi u obe procedure događaja - za objekte mnuOpenItem i mnuItemSave. Do sada su vam već poznate ove rutine koje se pozivaju iz menija. Konkretno, procedura događaja za objekat mnuItemSave sledećim naredbama prvo zahteva od korisnika da unese vrednost koja će se koristiti za šifrovanje, a zatim pomoću te vrednosti šifruje fajl:

```
code = InputBox("Upišite vrednost za šifrovanje", , 1)
If code = "" Then Exit Sub  'ako je kliknuto dugme Cancel, napustiti proceduru
Form1.MousePointer = 11    'prikazati peščani sat
charsInFile% = Len(txtNote.Text) 'utvrditi dužinu stringa
Open CommonDialog1.FileName For Output As #1 'otvoriti fajl
For i% = 1 To charsInFile%  'za svaki znak u fajlu
   letter$ = Mid(txtNote.Text, i%, 1) 'učitati sledeći znak
   'pretvoriti u broj funkcijom Asc , a zatim šifrovati operatorom Xor
   Print #1, Asc(letter$) Xor code; 'upisati fajl na disk
Next i%
Close #1            'na kraju zatvoriti fajl
```

Operator Xor se koristi za konvertovanje pojedinačnog slova iz otvorenog polja za tekst u samoj naredbi Print #1 koja zatim šifrovani znak upisuje na disk. (Da biste videli obrnuti postupak, otvorite proceduru događaja za objekat mnuOpenItem.) Kao što rekoh, ovi fajlovi nisu više tekstualni nego numerički i garantovano će zbuniti svakoga ko zabada nos u tuđe poslove. Na primer, na sledećoj slici je šifrovani fajl koji je napravila prethodna rutina za šifrovanje, prikazan Windowsovim Notepadom. (Omogućio sam Word Wrap da biste videli sve znakove.) Mada sadržaj fajla izgleda besmisleno, sada umete da rešite takve šifre. Samo pazite da ne izgubite vrednost za dešifrovanje!