Az objektumorientált fájlkezelés (Vigenère-kód)

A Vigenère-kód

A Vigenère-kódot, ami lényegében a Caesar-kód továbbfejlesztett változata, évszázadokon át feltörhetetlennek tartották. Az eljárást már Blaise Vigenère (1523-1596) [blez vizsöner] előtt feltalálták, ám széles körben az ő munkássága nyomán terjedt el.

Használatát legegyszerűbben egy példán érthetjük meg. A szöveg kódolásához ezúttal egy kulcsszó szükséges, amely legyen példánkban az ABC, a nyílt szöveg pedig a VISUALBASIC. A kulcsszót folyamatosan a nyílt szöveg alá írjuk, az egymás alá eső betűket pedig „összeadjuk”: Ha egy betűhöz az A-t adjuk, akkor az nem változik, ha a B-t, akkor az eggyel, ha a C-t, akkor kettővel, … ha a Z-t akkor 25-tel eltolódik. Így a kódolás eredménye: VJUUBNBBUID.

Ha a Vigenère-féle eljárást kézzel végezzük, hasznos segédeszköz lehet az ún. Vigenère-tábla, amely lényegében a karakterek „összeadó táblája”. A táblát a következő ábrán láthatjuk.

```
VISUALBASIC
+ABCABCABCAB
VJUUBNBBUID
```

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Ellenőrizzük mintapéldánk kódolását a Vigenère-tábla segítségével!

A Vigenère-féle kódoláshoz kétféleképpen írhatunk programot. Az egyik megoldás a Caesar-kódoláshoz készített program továbbfejlesztése, míg a másik egy új program írása a Vigenère-tábla felhasználásával. Ezúttal ez utóbbi megoldást

fogjuk követni. A XIX. század második felében ugyanis sikerült a Vigenère-féle eljárást feltörni, ekkor javasolta Étienne Bazeries (1846-1931) [étien bezirié], hogy az eljárás hatásfokának növelése érdekében készítsenek más táblákat is. Észrevehető ugyanis, hogy gyakorlatilag bármely olyan tábla, amelynek minden sorában és minden oszlopában minden betű pontosan egyszer szerepel, megfelelő. Programunk tehát lehetővé fogja tenni a táblák cseréjét is.

Új programunk grafikus felülete a Caesar-kódtól csak abban fog eltérni, hogy ezúttal a számláló helyett egy szövegmezőt veszünk fel. A szövegmező neve legyen *txtKulcsszó*.

A Vigenère-féle kódolás képernyője csak a txtKulcsszó mezőben tér el a Caesar kódtól.

Értelemszerűen a program fontos része lesz a tábla adatainak beolvasása, azonban a feladat összetettebb, így ezúttal nem élhetünk a *My* objektum segítségével. Az adatokat ugyanis nem egyetlen sztringbe fogjuk beolvasni, hanem egy *tábla* nevű vektorba, amelynek minden eleme a Vigenère-tábla egy-egy sorát fogja tartalmazni. A *tábla* vektort az űrlap minden részéről el kell érnünk, tehát az űrlap deklarációs részébe kerül:

```
Public Class Form1
    Private tábla(25) As String 'A sorokat 0-tól számozzuk
```

Az adatok beolvasására a *Form1_Load* eseménykezelő eljárásban kerül sor. Ehhez azonban meg kell ismerkednünk a fájlkezelés néhány fontos fogalmával.

Objektumorientált fájlkezelés

Az objektumorientált fájlkezeléshez kétféle objektumot kell létrehoznunk. Az egyik ahhoz szükséges, hogy hozzáférjünk a szükséges fájlhoz az operációs rendszer mappaszerkezetében, azaz a fájlt létrehozzuk és/vagy megnyissuk. Ez az objektum a *FileStream* [fájlsztrím] osztály egy példánya lesz.

A másik objektum **az adatok mozgatását végzi** a fájl és a programunk között. Ezt az adatok típusától és a mozgatás irányától függően négy osztályból választhatjuk. A *BinaryReader* [bájnöriríder] és a *BinaryWriter* [bájnörirájter] osztályok a fájlokból való olvasást, illetve a fájlokba való írást teszik lehetővé, akár bájton-