Vigenére rejtjel

Török Dániel

Bevezetés az informatikába - 2021

Tartalom

[Program rövid leírása 1](#_Toc82788260)

[Vigenére rejtjel 1](#_Toc82788261)

[Ceasar kód 1](#_Toc82788262)

[Program célja 1](#_Toc82788263)

[Program működése 2](#_Toc82788264)

[Kódolás 2](#_Toc82788265)

[Dekódolás 2](#_Toc82788266)

[File kódolása 2](#_Toc82788267)

[File dekódolása 2](#_Toc82788268)

Program rövid leírása

Vigenére rejtjel

A Vigenére kód, vagy rejtjel egy viszonylag alapabbnak számító titkosítási módszer, mely a ceasar kódok sorozatára épül. Viszonylag elterjedtebb, mivel maga a kód könnyen megérthető, és alkalmazható.

Ceasar kód

A ceasar kód egy olyan betűsor, melyet az ABC alapján hozunk létre, méghozzá úgy, hogy egy bizonyos karakternél elvágjuk az ABC-t, majd a végét az elejére illesztjük, ezáltal az egészet úgymond eltoljuk.

Program célja

Olyan program írása volt a célom, mely a vigenére rejtjel logikáját felhasználva képes szöveget, vagy file-ok tartalmát letitkosítani, valamint dekódolni azokat. Továbbá fontosnak tartottam, hogy ne csak azokat a szövegeket tudjam titkosítani, melyek kizárólag az ABC elemeiből állnak, ezért kicsit bővítettem az alapértelmezett karakterek listáját, így a magyar ABC-n kívül a számokat, valamint a .,!?#$@, és a szóköz karakterek egyaránt felhasználhatók a kódolni kívánt szövegben.

Program működése

Kódolás

Ahhoz, hogy le tudjuk titkosítani a megadott szöveget, először is be kell kérni a felhasználótól egy jelszót, ami alapján létrehozzuk a ceasar sorokat az előre megadott karaktersorból.

Maga a kódolás rész az alábbi módon néz ki:

* Sorra veszi a megadott szövegben a karaktereket
* Az adott ceasar sorból kiválasztja az adott pozíciójú karaktert
* Ezt a karaktert hozzáfűzi a visszaadni kívánt stringhez

Dekódolás

Alapértelmezetten a programot két féle képpen lehet elindítani. A normál módú indítással lehet titkosítani a kívánt szöveget, viszont ha a –d kapcsolót használja az ember, akkor a program dekódoló funkciója indul el.

Maga a dekódolás ugyan azon az elven működik, mint a kódolás, természetesen az ellentétes irányba.

File kódolása

Ha egy bizonyos file tartalmát szeretnénk lekódolni, akkor erre a -f kapcsolóval van lehetőségünk. Ebben az esetben a program egyszerűen beolvassa a felhasználótól a kódolni kívánt file-t, tartalmát elmenti egy változóba, amelyen végrehajtja a korábban leírt kódolási folyamatot, majd létrehoz egy .VIG kiterjesztésű lekódolt file-t.

File dekódolása

Természetesen a -d és -f kapcsolók együttes használata lehetővé teszi, hogy egy .VIG kiterjesztésű lekódolt file-t dekódoljunk. Ugyan úgy, mint a file lekódolásánál, meg kell adni a szükséges file-t, majd a dekódolás alapján dekódolja, és az eredményt kiírja egy file-ba.