Vigenére rejtjel

Török Dániel

Bevezetés az informatikába - 2021

Tartalom

[Program rövid leírása 1](#_Toc83036905)

[Vigenére rejtjel 1](#_Toc83036906)

[Ceasar kód 1](#_Toc83036907)

[Program célja 1](#_Toc83036908)

[Program működése 2](#_Toc83036909)

[Kódolás 2](#_Toc83036910)

[Dekódolás 2](#_Toc83036911)

[File kódolása 2](#_Toc83036912)

[File dekódolása 2](#_Toc83036913)

[Jelszó megadása 2](#_Toc83036914)

[Kimenet 2](#_Toc83036915)

[File kódolása 3](#_Toc83036916)

[File dekódolása 3](#_Toc83036917)

Program rövid leírása

Vigenére rejtjel

A Vigenére kód, vagy rejtjel egy viszonylag egyszerűnek 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

Az általam megírt program, a vigenére rejtjel logikáját felhasználva képes szöveget, vagy file-ok tartalmát titkosítani, valamint dekódolni azokat. Továbbá fontosnak tartottam, hogy a megírt program ne csak azokat a szövegeket tudja titkosítani, melyek kizárólag az ABC elemeiből állnak, ezért kibővítettem az alapértelmezett karakterek listáját. A magyar ABC-n kívül a számok, a szóköz karakter valamint a különleges karakterek (.,!?#$@) egyaránt felhasználhatóak a kódolni kívánt szövegben

Program működése

Kódolás

Ahhoz, hogy le tudjuk titkosítani a megadott szöveget, először 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 string-hez

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 titkosítani, akkor erre a –f kapcsolóval van lehetőségünk. Ebben az esetben szükséges megadni a kapcsoló után a file nevét, melyet titkosítani szeretnénk. A program ennek a file-nak a tartalmát elmenti egy változóba, amelyen végrehajtja a korábban leírt kódolási folyamatot. Az eredményt kiírja egy .vig kiterjesztésű file-ba.

File dekódolása

Ha egy .vig kiterjesztésű file tartalmát szeretnénk dekódolni, akkor a –f kapcsolóval meg kell adni a programnak az adott file-t, majd a –d kapcsolóval dekódoló módban tudjuk elindítani a programot. A végeredményt ebben az esetben szintén egy file-ba menti a program.

Jelszó megadása

Alapértelmezetten ha elindítjuk a kódot, az első dolog amit a program bekér az a jelszó. Ha program indításnál a –p kapcsolót használjuk, akkor azzal meg tudjuk adni, hogy mi legyen ez a jelszó. Ezen kívül –s kapcsolóval lehetőségünk van jelszó file megadására, így a jelszót be tudjuk olvasni egy fileból is.

Kimenet

Program indításánál a felhasználónak lehetősége van megadni a kimeneti file nevét. Erre a programnak nincs feltétlen szüksége, így ha ez nem történik meg, akkor generál magának egy elnevezést. A kimeneti file neve az alábbi elven jön létre a különböző esetekben.

File kódolása

* Ha nincs megadva kimeneti file, akkor a program a bemeneti file nevéhez fűz egy .vig végződést.
* Ha van kimeneti file megadva, akkor egyértelműen az lesz a kimeneti file neve

Maga a program ragaszkodni fog ahhoz, hogy a kimeneti file kódolás esetén .vig-re végződjön, így ha a megadott kimeneti file nem .vig-re fégződik, akkor azt hozzáfűzi a végéhez.

File dekódolása

* Ha nincs megadva kimeneti file, akkor a program a bemeneti file nevéről levágja a .vig végződést (feltéve, hogy vig file-ról van szó)
* Ha a bemeneti file nem egy vig file, és nincs megadva kimeneti file, akkor a bemeneti file nevéhez hozzáfűzi a .org végződést.
* Ha van kimeneti file megadva, akkor az lesz a kimeneti file neve