Jegyzőkönyv

Biztonság és védelem az informatikában c. tárgy

9. feladat

Készítette:

Csomor Bence, TVIK4I

2021.04.14.

**Titkosítási gyakorlatok**

Szteganográfia:

A szteganográfia a rejtett üzenetek oly módon történő létrehozásának tudománya és művészete, hogy az üzenet létezéséről csak a címzett tudjon. A kriptográfia párja, ahol az üzenet, illetve a titkosított tartalom létét nem álcázzák, de a tartalmát csak megfelelő rejtjel segítségével olvashatja a fogadó.

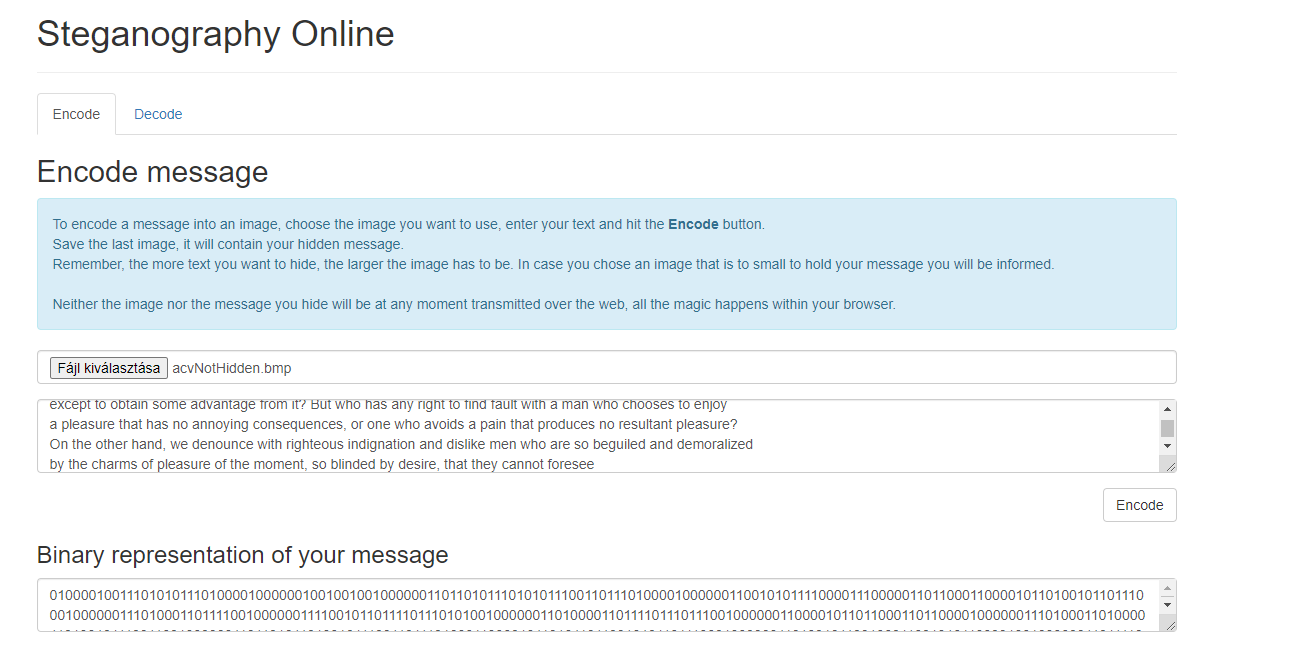
Egy 1080p Full HD 24 bites True Color kép esetén 1920\*1080\*24 bit = 6220800 byte a mérete, ami körülbelül 6 MB. Egy ilyen képnél, ha az utolsó három bitet felhaszmáljuk minden képpont esetén, akkor az mind a három színcsatorna felhasználásával 1920\*1080\*3\*3 bit = 2332800 byte rejthető el, ami közel 2 MB.

Ha egy A/4 – es oldal 30 sorból és egy sor 60 karakterből áll, ami 1800 karakter / oldal, akkor az 18662400 / 1800 = 10368 db A/4 – es oldal.

Adatrejtés:

A <https://stylesuxx.github.io/steganography/> oldalon online Szeganográfia érhető el.

Be kell illeszteni a használni kívánt képet és az elrejteni kívánt szöveget.



Ezután Láthatjuk az eredeti képet, a normalizáltat és az elrejtett szöveggel ellátottat is:

Eredeti kép:



Normalizált kép:



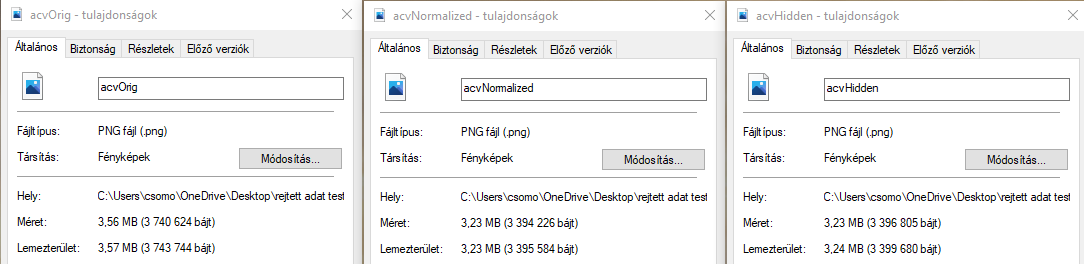
Rejtett szöveggel ellátott kép:



Én nem vélek felfedezni semmi szembetűnő változást a képekben.

Ha a méreteket nézzük akkor látszik, hogy a normalizált már előre kivette a feleslegesnek vélt területeket, hogy helyet csináljon a szövegnek.

Látható az is, hogy ez a pár soros szöveg aligha növelte meg a kép méretét. Ez azt jelenti, hogy a fentebb kiszámolt több mint tízezer A/4 es oldalnyi szöveghez képest ez semmi. Továbbá egy ekkora képben sokkal több szöveg elfér.



Titkosítandó szöveg: *„amit hárman tudnak, már nem titok”*

Ceacar-féle titkosítás:

A Caesar-kód vagy Caesar-rejtjel az egyik legegyszerűbb és legelterjedtebb titkosírási módszer. Ez egy helyettesítő rejtjel, ami azt jelenti, hogy minden egyes betűt az ábécében egy tőle meghatározott távolságra lévő betűvel kell helyettesíteni. Így például, ha mondjuk az eltolódás 3, az angol ábécében az A-t a D-vel, a B-t az E-vel stb. kell helyettesíteni. A magyar ábécére vonatkoztatva ez az A betű helyett C-t, az Á betű helyett CS-t jelent. Az elnevezését Julius Caesar után kapta, aki ennek a segítségével kommunikált tábornokaival.

Az eltolás legyen 7.

A kódolt üzenet: „dzspnw meüpdzsq wygyqdzsó, peü qíp wnwsó”

Kulcsszó használata (Vigenère-rejtjel):

A Vigenère-kód vagy Vigenère-rejtjel egy titkosítási módszer, amely különböző Caesar-kódok sorozatát használja, egy adott kulcsszó betűitől függően. Ez egy egyszerű fajtája a polialfabetikus rejtjeleknek.

Itt legyen a kulcsszó „aldi”.

amit hárman tudnak, már nem titok

aldi aldial dialdi, ald ial diald

AÁBCD.EÉFGH.IÍJKL.MNOÓÖ.ŐPQRS.TUÚÜŰ.VWXYZ

AÁBCD.EÉFGH.IÍJKL.MNOÓÖ.ŐPQRS.TUÚÜŰ.VWXYZ

LMNOÓ.ÖŐPQR.STUÚÜ.ŰVWXY.ZAÁBC.DEÉFG.HIÍJK

DEÉFG.HIÍJK.LMNOÓ.ÖŐPQR.STUÚÜ.ŰVWXY.ZAÁBC

IÍJKL.MNOÓÖ.ŐPQRS.TUÚÜŰ.VWXYZ.AÁBCD.EÉFGH

A kódolt ütenet: „aűla hmú

források: <https://hu.wikipedia.org/wiki/Szteganogr%C3%A1fia>

<https://hu.wikipedia.org/wiki/Caesar-rejtjel>