Jegyzőkönyv

Biztonság és védelem az informatikában c. tárgy

10. feladat

Készítette:

Csomor Bence, TVIK4I

2021.04.21.

**Az Enigma, és az NTFS használata**

Az Enigma:

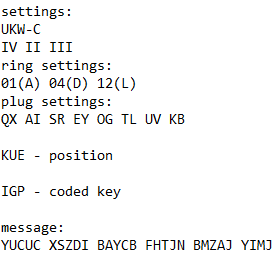
Az Enigma üzenetek sifrírozására (titkosítására, kriptográfiai kódolására, rejtjelezésére) és desifrírozására (visszafejtésére) használt, német gyártmányú, forgótárcsás, elektromechanikus berendezés. Az „Enigma“ szó a görög (αίνιγμα) szóból ered, melynek jelentése: rejtély, rejtvény.

A második világháború során a kódkönyvekkel a tárcsákat, a gyűrűket és a kapocstáblát állították be. Minden egyes üzenetnél az operátor véletlenszerű indulási pozíciót választott – mondjuk WZA, valamint egy véletlenszerű üzenetkulcsot, mondjuk SXT. Ezután a tárcsákat a WZA állásba fordította, és ezzel kódolta el az üzenetkulcsot, így az SXT-ből például UHL lett. Ezután az SXT indulópozíciót használva sifrírozta az üzenetet. A vevőnek átküldte az indulópozíciót (WZA), a sifrírozott üzenetkulcsot (UHL), majd a titkosított üzenetet. A vevő a napi beállításokat követően beállította a WZA indulópozíciót, és ezzel dekódolta az UHL üzenetkulcsot. Az így kapott SXT indítóállásba állítva a tárcsákat az üzenet titkosítását is vissza tudta fejteni. Ez az eljárás kiküszöbölte a Grundstellung-alapú kód kétszeresen ismételt elküldését, és bezárta a korábbi eljárás biztonsági rését.

Az üzenet, amit kódoltam és elküldtem az a következő volt:

„amit harman tudnak az mar nem titok”

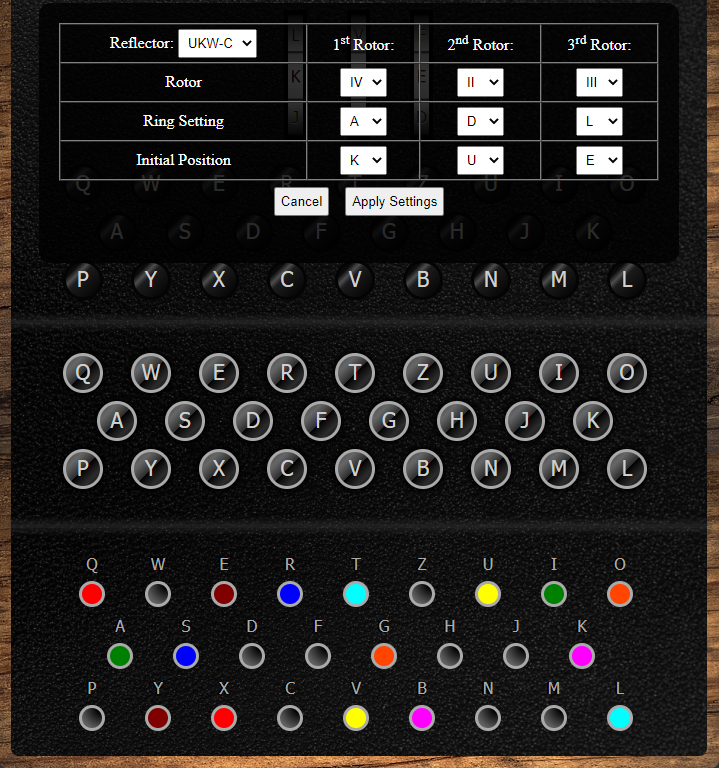
Elküldtem a beállításokat és az üzenetet is.



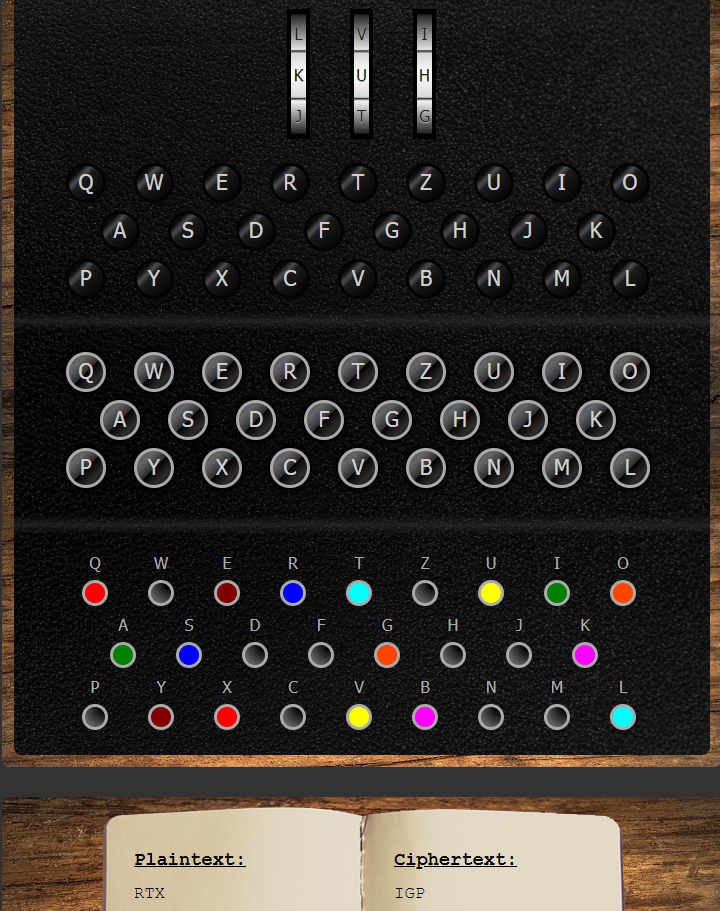
ezeket a beállításokat használva sikerült dekódolni az üzenetet az <https://www.101computing.net/enigma-machine-emulator/> segítségével.

Az első lépés az volt, hogy a beállítások után kódoltam a választott kulcsomat:

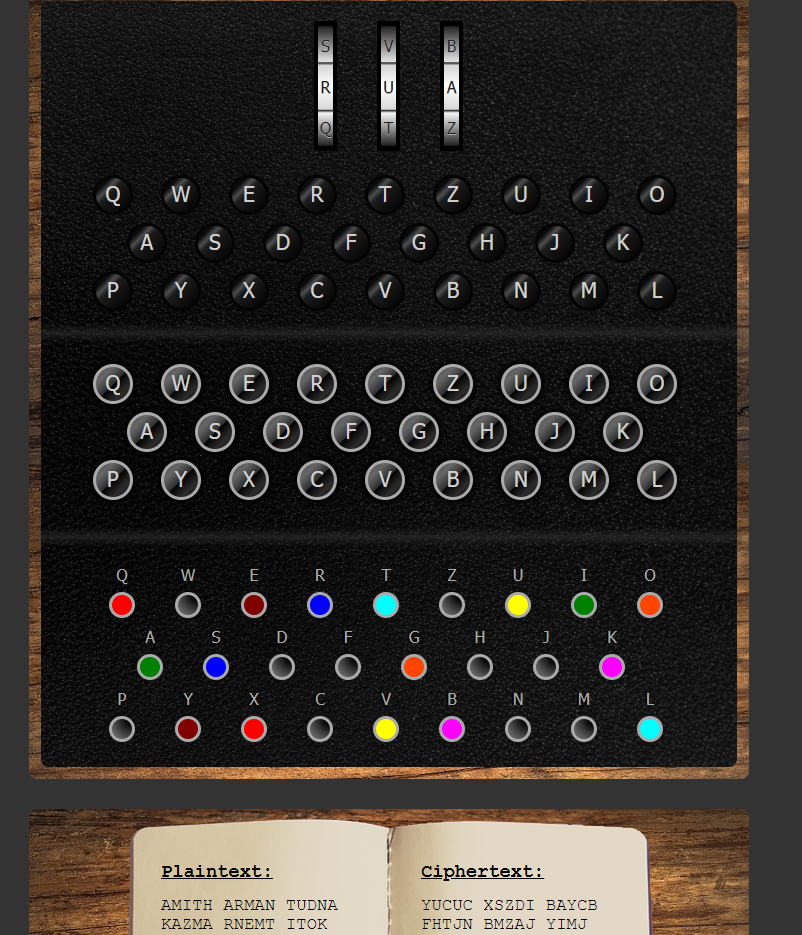
Beállítások:



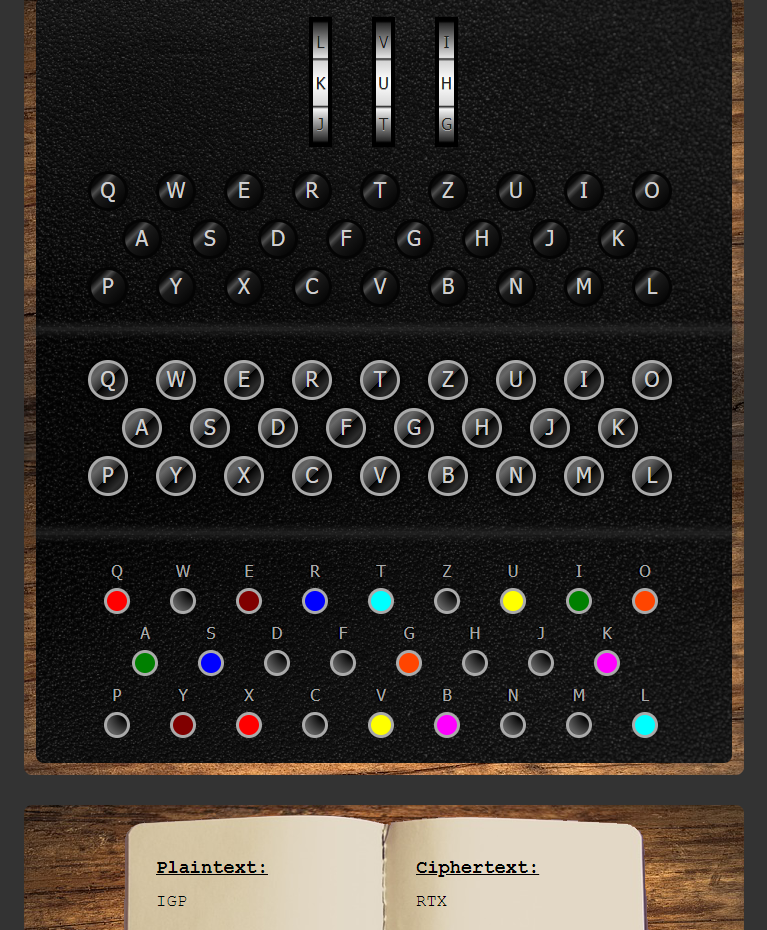
A kulcs az „RTX” volt. Ezt beírva kaptam az IGP kódot.



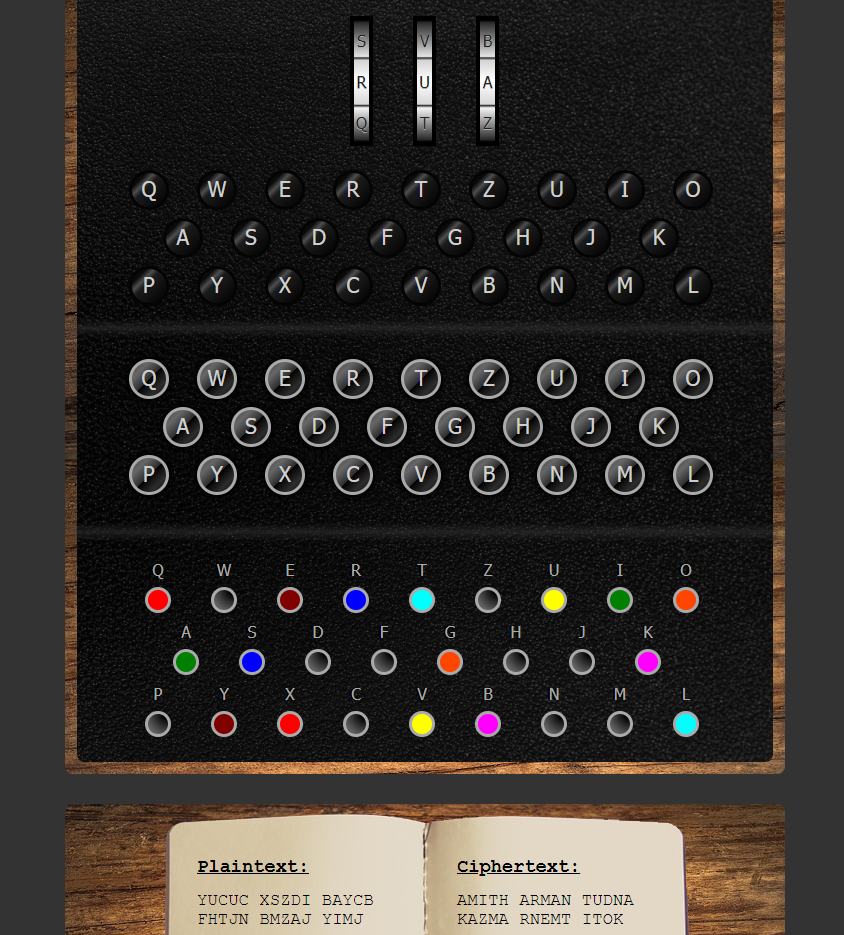
Ezután átállítottam a három tárgyát RTX-re és kódoltam az üzenetet:



Majd a kódokat elküldtem és a beállítások után a dekódolás egyszerű volt. Először a KUE állással be kellett írni az IGP kódot amire kiadta a kulcsot ami az RTX volt:



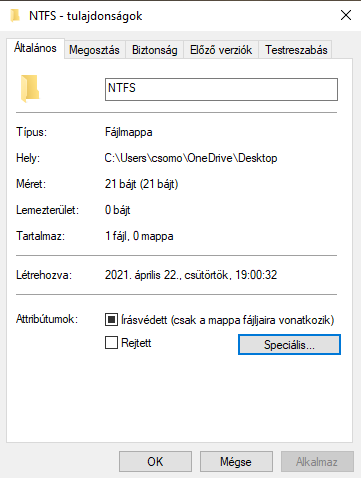
Utána az RTX állással be kellett írni a kódolt üzenetet, ami visszaadta az eredeti szöveget négy betűkre tagolva:



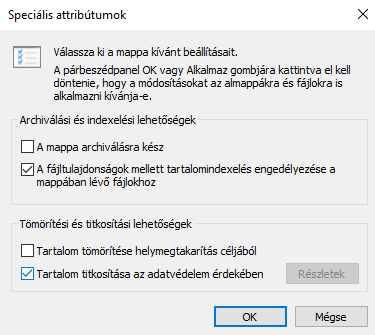
Windows NTFS-EFS titkosítás:

Az NTFS vagy New Technology File System (új technológiájú fájlrendszer) a Microsoft Windows NT szabványos fájlrendszere.

Létrehoztam egy NTFS nevű mappát, amiben létrehoztam egy text nevű szöveges dokumentumot.

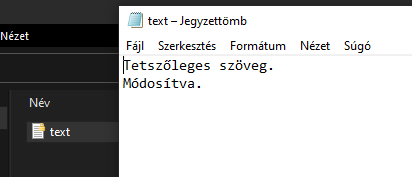


A mappára jobbklikkelve és a tulajdonságokra kattintva jön elő a fönt látható menü. Itt rákattintok a „Speciális…” gombra.



Ezen belül kipipálom a Tömörítés és titkosítási lehetőségeken belül a Tartalom titkosítása az adatvédelem érdekében négyzetet majd leokézom öket.

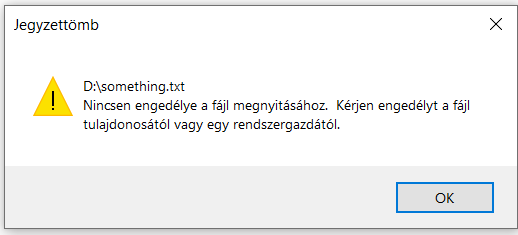
Beítam egy tetszőleges szöveget és módosítottam is a titkosítás után. Ez probléma nélkül sikerült.



Egy something nevű másik szöveges dokumentum mappába tétele után ez is titkosított lett, tehát minden, ami a titkosított mappába kerül, automatikusan titkosítva lesz.

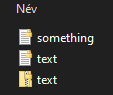


Következő lépésben a something fájlt átmásoltam egy pendrivera és egy másik gépen meg lett nyitva. Az eredmény alul látható:



Tehát más nem tudja megnyitni az én titkosított fájljaimat.

Végül tömörítettem a text szöveges dokumentumot. Ahogy látni, tömörítés után a tömörített mappa titkosított lesz, de ez csak azért, mert még a titkosított mappában van. Viszont a benne lévő text szöveges dokumentum már nem titkosított. Vagyis, ha nem a titkosított mappába tömörítjük akkor már nem lesz titkosított, akár az volt akár nem.



források:

<https://hu.wikipedia.org/wiki/Enigma_(g%C3%A9p)>