Házi feladat terv

A program:

A feladat egy olyan titkosító program létrehozása, amely képes tetszőlegesen hosszú szöveg titkosítására.
A program kétféle titkosítást lesz képes alkalmazni, az egyik a Caesar titkosítás, a másik pedig a XOR (kizáró vagy) alapú titkosítás. Mindkét esetben lesz egy kulcs, mely segítségével a titkosított szöveg visszaalakítható eredeti formájába.

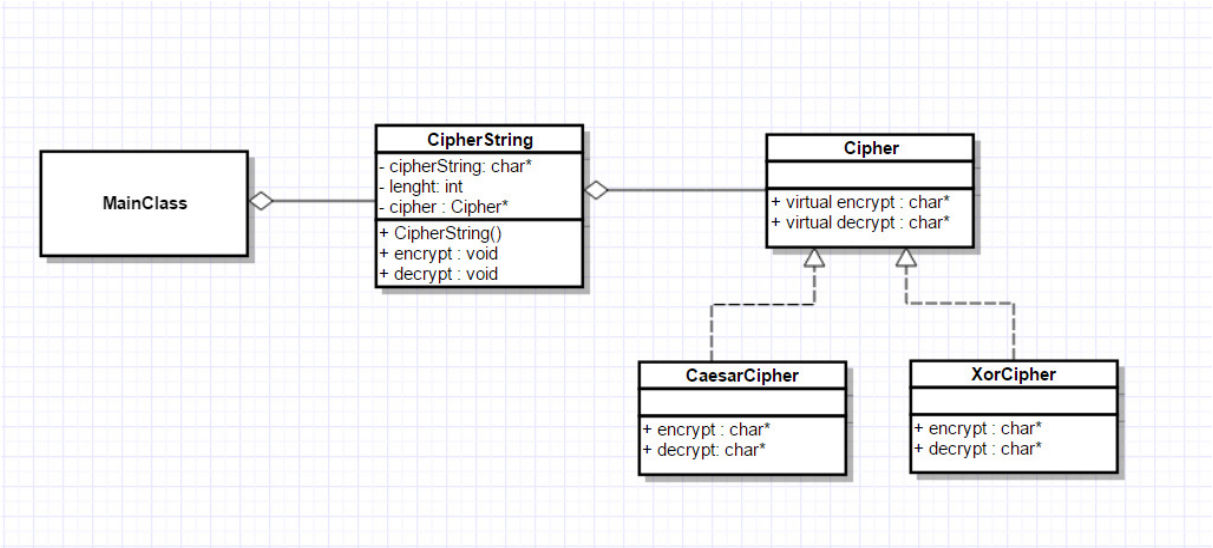
A program működése:

A program indításakor menü fogja fogadni a felhasználót. A menüben lehetősége van a felhasználónak választani a kétfajta titkosítás közül, illetve még a kilépési opciót is választhatja.
Ha a felhasználó már titkosította a szöveget, lehetősége lesz a szöveg visszaállítására is.

Titkosítási módszerek:

Caesar titkosítás: A cserélő algoritmusok lényege, hogy adott betűt egy másikkal helyettesítünk, így kapunk egy értelmetlen szöveget, ami már titkos tartalmú. A Caesar titkosítás esetén a csere szabály az, hogy minden betűhöz az ABC szerint elfoglalt pozíciója alapján tetszőleges hellyel arrébb található karaktert rendeljük (ez a szám a kulcs): A -> D, B -> E, C -> F … Körbeérés után pedig az X, Y, Z betűkhöz az A, B, C betűket rendeljük.
XOR alapú titkosítás: Ezen titkosítási algoritmus a Boole algebra XOR műveletének következő azonosságain alapul:
A XOR B = C
C XOR B = A
Titkosításra ez úgy használható fel, hogy az A változó jelenti az adat egy titkosítandó bitjét, B a hozzá tartozó kulcs egy bitjét, C pedig a kimenetként kapott titkosított bitet.
A titkosítás menete úgy fog zajlani, hogy a betűket összexoroljuk a kulccsal, vagy a kulcs egy részével, és így fog előállni a titkos szöveg. Visszafejtésnél szintén ugyanez a művelet fog végrehajtódni.

A program osztálydiagramja:



Somogyi Balázs
CAXOZ9