A Playfair-féle titkosítási eljárást[1] a fizikai tanulmányainkból ismert Charles Wheatstone találta ki 1854-ben, de azt barátjáról, a módszert népszerűsítő Lord Playfairről nevezték el. Magát az eljárást már az első világháború előtt feltörték, azonban az ausztrálok még a II. világháborúban is használták. (Akkoriban, számítógépek nélkül, a feltöréshez szükséges idő még hosszabb volt, mint amennyi ideig az információ titkosnak számított.)

Az eljárás alapját egy 5×5-ös táblázat alkotja, amely az angol ábécé betűit tartalmazza (az angol ábécé 26 betűs, így ebből egyet, esetünkben a Q-t, el kell hagyni). Természetesen ezt a táblát csak a küldő és fogadó fél ismerheti.

A titkosítandó szöveget (példánkban FINOM IZ) betűpárokra tagoljuk, szükség esetén az utolsót egy megválasztott jellel (a feladatban legyen X) kiegészítjük. Hasonló módon járunk el, ha a betűpár két eleme azonos, például az AA betűpárt AX AX betűpárokká alakítjuk át.

Az eljárás a betűpárokhoz rendel betűpárokat az alábbiak szerint:

- Ha a két betű a táblázatban egy sorban van, akkor azokat a tőlük eggyel jobbra lévő betű rejtjelezi. Az utolsó oszlopban lévő betűt az adott sor első betűje követi (FI $\rightarrow$ RN).
- Ha a két betű egy oszlopban van, akkor azokat az alattuk lévő betű rejtjelezi. Az utolsó sorban lévő betűt az adott oszlop első betűje követi. (NO $\rightarrow$ VN).
- Végül, ha a két betű különböző sorban és különböző oszlopban van, akkor tekintsük azt a „betűtéglalapot", amelyben a két betű egy „átló" két végpontja. A betűket ekkor a saját sorukban, a téglalap másik csúcsánál lévő betűkkel helyettesítjük. (MI $\rightarrow$ KF).

K	O	M	A	L
I	N	F	R	T
P	V	E	S	Y
B	Z	C	X	G
J	D	W	H	U

F	I
R	N

N	O
V	N

M	I
K	F

Z	X
C	G

A program első parancssori argumentuma egy karakter, amely megadja, hogy a felhasználó az adatokat rejtjelezni vagy visszafejteni szeretné-e (R/V), második a Playfair-rejtjelező táblázatot sorfolytonosan tartalmazó fájl neve, a harmadik a rejtjelezendő/visszafejtendő adatokat tartalmazó fájl neve, a negyedik pedig a kimeneti fájl neve legyen.

Feltételezhetjük, hogy a bemeneti adatok csak az angol ábécé fentieknek megfelelő nagybetűit tartalmazzák. A programot úgy készítsük el, hogy a rejtjelezendő/visszafejtendő állomány mérete tetszőleges, akár több GB-os is lehet.

Beküldendő egy `i385.zip` tömörített állományban a program forráskódja és dokumentációja, amely tartalmazza a megoldás rövid leírását, és megadja, hogy a forrásállomány melyik fejlesztő környezetben fordítható.

Letölthető fájlok (egy lehetséges Playfair-rejtjel, valamint egy lehetséges rejtjelezendő fájl): `kod.txt`, `be.txt`.

[1] *Forrás:* `https://hu.wikipedia.org/wiki/Playfair-rejtjel`.