A. 808. Keressük meg az összes páronként relatív prím a, b, c pozitív egészt, melyekre

$$a^2 + 3b^2c^2 = 7^c.$$

Javasolta: *Nikolai Beluhov* (Bulgária)

Beküldési határidő: 2021. november 10.
Elektronikus munkafüzet: `https://www.komal.hu/munkafuzet`

❄

„Titkos üzenet száll a széllel” I.*

Előzmények dióhéjban

Amióta ember él a Földön, akadtak olyanok, akiknek voltak titkaik. Ezeket persze csak egy vagy néhány emberrel szerették volna megosztani. A titoktartás akkor kezdett nehézkessé válni, amikor az a bizonyos másik messze volt, üzenni kellett neki. Hamar rájöttek, hogy az üzenet elrejtése nehézkes, mert ha valaki megtalálja az üzenetet, vége a titoknak. Az üzenet értelmét kellett elrejteni. hogy fellelése esetén ne lehessen kihámozni a tartalmát. (Ma már tudjuk, hogy inkább arra kell törekedni, hogy ne legyen érdemes a titkosított tartalmat visszaalakítani, hiszen a megoldási technikák idő- és erőforrásigénye miatt talán a megfejtés időpontjára az üzenet elavul, vagy a megfejtés többe kerül, mint amekkora hasznot az üzenet hozhat.)

Első lépésként a nyelvi rendszertől kell megszabadulni, vagyis a kis- és nagybetűk megkülönböztetésétől, a szóközöktől és az írásjelektől. Az üzenet olvashatóságát ezek alig rontják, viszont a megfejtőnek sokat segítenének.

A kialakuló titkosítási módszereket két nagy csoportba sorolhatjuk:

- Az üzenet eredeti karaktereit megtartjuk, csak valamilyen szabályszerűség szerint megváltoztatjuk a sorrendjüket, ez az úgynevezett *keverő módszer.*
- Az üzenet eredeti karaktersorrendjét megtartjuk, csak az egyes karaktereket cseréljük le egy szabálynak megfelelően, ezt nevezzük *cserélő módszernek.*

A mai számítógépek kapacitása mellett a keverő módszernek nem sok értelme van, a gép pillanatok alatt végigpróbálhat néhány tízezer keverési lehetőséget. Az értelmes keverési módok száma nagyságrendileg ebbe a tartományba esik.

A legegyszerűbb cserélő technikák már Julius Caesar korában is elavultnak voltak mondhatók, hiszen arab tudósok már időszámításunk kezdete előtt rájöttek az így titkosított – úgynevezett *monoalfabetikus* módszer – megfejtésére.

A titkosítási módszer hiányában is lehetséges volt az így titkosított üzenet megfejtése. A visszafejtésre azért volt lehetőség, mert a nagybetűs írással, a szóközök

*A cím a TNT együttes *Titkos üzenet* című dalának szövegét idézi.

és írásjelek törlésével sem sikerül teljesen megszabadulnunk a nyelvi rendszertől. Az egyes nyelvek szavai ugyanis nem véletlen számú, véletlenszerűen kiválasztott betű véletlen sorrendben egymás mögé írásával keletkeznek. Például szinte minden szóban illik lennie legalább egy magánhangzónak, sőt hosszabb szót nehézkes is kimondani egy magánhangzóval (a magyar nyelvből talán a *brrr* hangutánzó szót lehet felhozni ellenpéldának [bár biztos van olyan nyelvész, aki élénken tiltakozna a brrr szónak minősítésén], de a fagylalt cseh verziója, a *zmrzlina*, vagy a Csorba tó szlovák neve *Štrbské pleso* is szinte kimondhatatlan.)

Minden nyelvre jellemző, hogy eltérő gyakorisággal használja az egyes betűket, azok gyakorisági sorrendje jellemző az adott nyelvre. A hosszabb – egy-két oldalas – üzenetben az egyes kódok előfordulásait megszámolva, és ezeket összehasonlítva a nyolc-tíz leggyakoribb betűt helyettesítő kód megfejthető. Ezek visszaállításával olyan szórészletek keletkeznek, amelyekből a nyelv ismeretében a többi kód is kideríthető és az üzenet elolvasható.

A monoalfabetikus módszert tehát az tette megfejthetővé, hogy a szöveg adott betűjéből mindig ugyanaz a titkos betű (kód) lett, és a nyelvek az egyes betűket más-más gyakorisággal használják, így egy rejtjelezett szövegnél a szóba jöhető titkosítási módok száma a milliós nagyságrendbe esik. A fennmaradó kódok és betűk párosítása és a szöveg elejének összevetése az adott nyelv szótárával a mai számítógépeknek nem okoz gondot. Ráadásul, ha a titkos üzenet betűgyakoriságai megegyeznek a valódi betűgyakorisággal, akkor azonnal tudjuk, hogy azt keverő módszerrel titkosították. Minket éppen ezért a betűgyakoriság-elemzést hiábavaló próbálkozássá tevő *polialfabetikus* titkosítási módok érdekelnek.

A Bellaso kifejlesztette Vigenère-kódolás pont egy ilyen titkosírás. A fentiek alapján érthető, miért kellett Napóleonnak egy új, biztonságosabb titkosítási mód – a főként hadműveletekkel kapcsolatos – üzenetei megóvására.

Vigenère-kódolás

A technika története tele van tévedésekkel. A Napóleon által használt, akkor modernnek számító titkosítási módszert *Blaise de Vigenère* találmányának tartják, holott a módszert 1553-ban már publikálta *Giovan Battista Bellaso* egy művében. Vigenère csak továbbfejlesztette. Igazán nem szép a történelemtől, hogy az igazi megalkotót a névtelenség homálya rejti, míg a továbbfejlesztő neve válik ismertté, gondoljunk csak *Amerigo Vespucci* és *Kolumbusz Kristóf* esetére vagy a *Thomas Savery* és *Thomas Newcomen* által tervezett gőzgépre, amelynek szabadalmát végül 1769-ben *James Watt* kapta meg, netán a jól ismert *Bolyai–Lobacsevszkíj* elsőségi vitára a hiperbolikus geometria kapcsán.

Ennyi bevezető után ideje rátérnünk a módszer ismertetésére.

A kódolási módszer

A módszer megértéséhez három dologra lesz szükségünk:

- A nyelvi rendszerétől megfosztott, úgynevezett *nyers* üzenetre,
- a kódoláshoz szükséges *kulcsra,* ami egy hosszabb-rövidebb szövegdarab,
- és a Vigenère-táblára, ami egy betűtáblázat.

Lássunk is egyből egy példát, azon egyszerűbb megérteni.

- A nyers szöveg legyen a címben is szereplő dalszövegrészlet (Titkos üzenet száll a széllel) nyelvi rendszerétől megfosztott változata:

TITKOSÜZENETSZÁLLASZÉLLEL.

- A kulcs vagy *sifré* szerepére a KÖMALINFORMATIKA jelsorozatnál mi sem lehetne kézenfekvőbb.

Írjuk le a nyers szöveget, fölé pedig betűnként a kulcsot; ha hamarabb elfogynának a kulcs betűi, mint a nyers szövegé, ismételgessük a kulcsot, amíg szükséges.

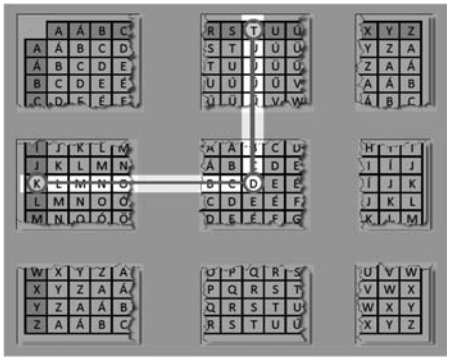
kulcs:	K	Ö	M	A	L	I	N	F	O	R	M	A	T	I	K	A	K	Ö	M	A	L	I	N	F	O
nyers:	T	I	T	K	O	S	Ü	Z	E	N	E	T	S	Z	Á	L	L	A	S	Z	É	L	L	E	L

Végül lássuk a Vigenère-táblát:

	A	Á	B	C	D	E	É	F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z
A	Á	B	C	D	E	É	F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z	A
Á	B	C	D	E	É	F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á
B	C	D	E	É	F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B
C	D	E	É	F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B	C
D	E	É	F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B	C	D
E	É	F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B	C	D	E
É	F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B	C	D	E	É
F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B	C	D	E	É	F
G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B	C	D	E	É	F	G
H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B	C	D	E	É	F	G	H
I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B	C	D	E	É	F	G	H	I
Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B	C	D	E	É	F	G	H	I	Í
J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B	C	D	E	É	F	G	H	I	Í	J
K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B	C	D	E	É	F	G	H	I	Í	J	K
L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B	C	D	E	É	F	G	H	I	Í	J	K	L
M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B	C	D	E	É	F	G	H	I	Í	J	K	L	M
N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B	C	D	E	É	F	G	H	I	Í	J	K	L	M	N
O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B	C	D	E	É	F	G	H	I	Í	J	K	L	M	N	O
Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B	C	D	E	É	F	G	H	I	Í	J	K	L	M	N	O	Ó
Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B	C	D	E	É	F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö
Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B	C	D	E	É	F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő
P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B	C	D	E	É	F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P
Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B	C	D	E	É	F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q
R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B	C	D	E	É	F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R
S	T	U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B	C	D	E	É	F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S
T	U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B	C	D	E	É	F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T
U	Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B	C	D	E	É	F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U
Ú	Ü	Ű	V	W	X	Y	Z	A	Á	B	C	D	E	É	F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú
Ü	Ű	V	W	X	Y	Z	A	Á	B	C	D	E	É	F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü
Ű	V	W	X	Y	Z	A	Á	B	C	D	E	É	F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű
V	W	X	Y	Z	A	Á	B	C	D	E	É	F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V
W	X	Y	Z	A	Á	B	C	D	E	É	F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W
X	Y	Z	A	Á	B	C	D	E	É	F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X
Y	Z	A	Á	B	C	D	E	É	F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y
Z	A	Á	B	C	D	E	É	F	G	H	I	Í	J	K	L	M	N	O	Ó	Ö	Ő	P	Q	R	S	T	U	Ú	Ü	Ű	V	W	X	Y	Z

A felső sorba és az első oszlopba az egybetűs ábécé kerül. A táblázatba soronként egy-egy betűvel eltolva ismétlődik a fenti ábécé, ha annak a végére érünk, folytatjuk az ábécé újrakezdésével.

A titkosításra előkészített sorok egymás alatti betűpárjaiból indulunk ki: a kulcs megfelelő betűjét a bal szélen, a nyers szöveg betűjét pedig felül keressük meg, és az adott sor és oszlop találkozásánál lévő betű lesz a nyers szöveg adott betűjének titkosított párja.



A mi példánknál elsőként a K szerint titkosítjuk a T-t, az ábra mutatja, hogy a titkos karakter a D lesz. Írjuk ezt a betűt a betűpár alá.

Hajtsuk végre a műveletet az összes betűre.

kulcs:	K	Ö	M	A	L	I	N	F	O	R	M	A	T	I	K	A	K	Ö	M	A	L	I	N	F	O
nyers:	T	I	T	K	O	S	Ü	Z	E	N	E	T	S	Z	Á	L	L	A	S	Z	É	L	L	E	L
titkos:	D	V	É	L	X	A	I	F	R	E	P	U	M	I	M	M	Ü	Ő	E	A	P	T	W	K	X

Figyeljük meg, hogy ennél a kódolási módszernél tényleg kútba esik a betűgyakoriságon alapuló megfejtés, hiszen a nyers szöveg 1., 3. és 12. betűje is T, de a titkos párjuk D, É és U lesz, valamint a titkos szöveg M betűit a nyers szöveg S, Á és L betűjéből kapjuk.

A visszafejtés

Ez valóban egyszerű. A fenti példát nézve a következőt kell tenni: írjuk fel a kulcsot és a titkos üzentet, ugyanúgy, mint az előbb a kulcsot és a nyers szöveget. Először a kulcs K sorában kell a táblában megkeresnünk a D betűt, majd ennek az oszlopnak a tetején levő betűt, ami nálunk T, beírjuk alájuk és lépünk tovább a következőre. Az Ö sorában megkeressük a V betűt, majd az oszlop tetején látható I betűt rögzítjük és így tovább.

kulcs:	K	Ö	M	A	L	I	N	F	…
titkos:	D	V	É	L	X	A	I	F	…
visszafejtett:	T	I	T	K	O	S	Ü	Z	…

Mindebből látható, hogy a kulcs birtokában nem nagyobb munka a visszafejtés, mint a titkosítás. Arról, hogy megfejthető-e az ilyen kód a kulcs hiányában, a cikk következő részében olvashattok. De addig is érdemes nekilátni a cikkhez tartozó, ebben a számban megjelenő feladatnak. Megemlítendő, hogy a 2005. október 27-ei emelt szintű informatika érettségi programozás feladata is ezzel a témakörrel foglalkozott.

Tóth Tamás