PANNON

ENIGMA

kód

Informatikai programozási kódtörő verseny 2018

Általános iskolások részére

KÓDVETŐK
digitális oktatási műhely

www.kodvetok.com

SZÉCHENYI 2020

MAGYARORSZÁG KORMÁNYA

Európai Unió
Európai Szociális Alap

BEFEKTETÉS A JÖVŐBE

A kiadvány, a rendezvény és a verseny az **EFOP-3.4.4-16-2017-00002** azonosítószámmal ellátott

"*A felsőoktatásba való bekerülést elősegítő készségfejlesztő és kommunikációs programok megvalósítása, valamint az MTMI szakok népszerűsítése a Pannon Egyetemen*"

elnevezésű projekt keretében valósulhatott meg.

Jelen kiadvány elérése: http://math.uni-pannon.hu/~szalkai/PEnigmaFuzet.pdf

A füzetet A/5 méretű (kicsinyített) nyomtatásra terveztük.

A **Pannon Enigma** verseny

2018.

Feladatok, megoldások, elemzések

dr. Szalkai István

2018. július. 30.

Tartalom

Bevezetés

A **"Pannon Enigma"** azaz a PEnigma verseny rendhagyó módon keletkezett. Általános iskolás tanulóknak országos internetes verseny titkosírások megfejtéséből, a történeti hűség megtartása mellett, nem túl nehéz és nem túl könnyű feladatokon keresztül, a matematika és a számítástechnika és a tanulók ötletességének alapos felhasználásával, a nyelvek és a matematika és a számítástechnika fontosságának kiemelésével. Mindezt (betűrendben) a **Kódvetők Csapata** (http://www.kodvetok.com) és a **Pannon Egyetem MIK** (http://mik.uni-pannon.hu/) közösen ötlötte ki, vállalta fel, és vitte végbe 2018. tavaszán, egyesek szerint sikerrel! (Lásd: https://www.kodvetok.com/enigma és https://mik.uni-pannon.hu/index.php/hu/szervezet/hirek-osszes/...kodtoro-verseny.html).

Véletlenül épp a legelső feladat sikerült a legnehezebbre, pontosabban igényelte a leghosszabb kitartó, precíz, aprólékos munkát a versenyzőktől - de a verseny időzítése folytán épp erre a feladatra volt a legtöbb idejük. Ennek ellenére országosan majdnem ezer tanuló illetve csapat nevezett be, bár a finisben már csak kb. 30 megoldás érkezett. A lezajlott verseny feladatait, megoldásait és alapos elemzéseit közöljük ebben a kis füzetben, de a feladatokat megtaláljuk a https://www.kodvetok.com/enigma címen is.

Matematikai szempontból nem adhattunk nehéz problémákat a versenyzőknek, de az aprólékos (egyszerre monoton és ötleteket is igénylő) munka a kora ókortól a 21. századig mind az igazi *siffírozás* és *desiffírozás* (chiffrer & dechiffrer, azaz kódolás és dekódolás) jellemzője, és még lesz is pár ezer évig! Tehát pedagógiailag is (talán) jól sikerültek a feladatok. Ebben a kis füzetecskében igyekeztünk arra is rávilágítani, hogy a számítógépeket hogyan lehet titkosírásokhoz felhasználni, de néha a papír-olló-fogaskerék megoldások egyszerűbbek. Jómagam néha már-már a **Bletchley_Parkban** éreztem magam ... (https://hu.wikipedia.org/wiki/Bletchley_Park , https://hu.wikipedia.org/wiki/Bletchley_Park_Múzeum). Érdemes még elolvasni **R.P.Feynman** fizikus (1918-1988) *Tréfál, Feynman úr?* önéletrajzi regényének első fejezetét, ahol szakmai szemszögből írja le sikereit titkosírások és kódolt zárak feltöréséről: https://www.libri.hu/konyv/richard_phillips_feynman.trefal-feynman-ur.html https://moly.hu/konyvek/richard-p-feynman-trefal-feynman-ur , ...

Mint említettük, néha papír-olló-ceruza is használható számítógép helyett (pl. 1,2,6,7 feladatoknál). Egy háborús helyzetben melyik romlik el előbb, melyiket lehet hamarabb kijavítani vagy pótolni - tehát melyik is a jobb túlélőkészlet ?

Sok versenyző panaszolta a német nyelv szükségességét, hiszen napjainkban a nyelvtanulóknak csak 10%-a tanul németül. Ezt nem csak történeti hűség miatt választottuk (hiszen 100 évvel ezelőtt még a tudomány világnyelve is a német volt), hanem egyrészt a mai Európában is szükség van erre a nyelvtudásra, másrészt olvassuk el a legutolsó feladat utáni legutolsó megjegyzést a 38. oldalon. Mert ez is a túlélőkészlet egyik eleme!

Ezt a füzetet elsősorban tanítók és tanárok részére készítettük, de természetesen diákok is forgathatják, esetleg tanári segítséggel. Bevezetésképpen ajánljuk még a wikipédia rövid, összefoglaló oldalát: http://hu.wikipedia.org/wiki/A_kriptográfia_története

A feladatok megszövegezésében, többszöri ellenőrzésében, rengeteg alapos megbeszélésében, észrevételek és tanácsok felvetésében az alábbi kollégák vettek részt (betűrendben):

Süle Péter, Szakmáry Ákos és **jómagam**.

Veszprém, 2018. július 30.

Dr. Szalkai István
Pannon Egyetem, Veszprém, Matematika Tanszék
szalkai@almos.uni-pannon.hu

1. Feladat

Az ellenség a következő titkosírást használja: 31 betűs abc:
("_" a szóköz jele), a betűk értékei / kódjai:

		1									2									3
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0
_	a	á	b	c	d	e	é	f	g	h	i	j	k	l	m	n	o	ö	p	q	r	s	t	u	ü	v	w	x	y	z

- Első lépésben az eredeti szöveg első betű értékével ciklikusan eltolja az összes betűt (értékeiknek megfelelően). Tehát pl. ha az első betű g (=9), akkor minden betű értékéhez 9 -et adunk és az így kapott kódnak megfelelő betűt írjuk le az illető betű helyett. Ha az összeadáskor 30-nál nagyobb számot kapunk, akkor az összegből levonunk 31-et (ún. ciklikus vagy "mod 31" hozzáadás).
- A második lépésben az előzőleg kapott betűsorozat második betűjének értékével toljuk el, de csak azokat a betűket, amelyek a második betűtől jobbra állnak és magát a második betűt is, az előző bekezdésben említett módon.
- Az i -edik lépésben a legutoljára kapott betűsorozat i -edik betűjének értékével toljuk el, de csak azokat a betűket, amelyek az i -edik betűtől jobbra állnak és magát az i -edik betűt is.
- Az utolsó lépésben csak a legutolsó betűt toljuk el önmagával.

Például: a málna (5-betűs) szó kódolása:

```
1. lépés:  m=15  miatt  1-5. betűket 15-tel eltoljuk (mod 31):      zoy_n
2. lépés:  o=17  miatt  2-5. betűket 17-tel eltoljuk (mod 31):      zbmoá
3. lépés:  m=15  miatt  3-5. betűket 15-tel eltoljuk (mod 31):      zbzao
4. lépés:  a= 1  miatt  4-5. betűket  1 -el eltoljuk (mod 31):      zbzáö
5. lépés:  ö=18  miatt az 5. betűt   18 -al eltoljuk (mod 31):      zbzád
```

Feladat: dekódolja az alábbi üzenetet, amelyet a fenti módon titkosítottak:

znnseppdgqekfmz

Az 1. feladat megoldása

i) Dekódolásnál nyilván vissza kell tolnunk a szöveg jobb felénél álló betűket - jobbról balra haladva - , de mennyivel?

Mivel az eltolást meghatározó **?** betűhöz (az *i* -edik lépésben az *i* -edik betűhöz) éppen *önmagát* adtuk (kódja kétszeres lett), és így lett a végeredmény **ω** (az adott látható betű, `abc...xyz` valamelyike), ezért olyan **?** betűt kell keresnünk, amelynek kódjának kétszerese egyenlő az adott helyen a titkos szövegben éppen a helyén álló szám kódjával:

? + ? = ω (kódja). (1)

Ilyen **?** betűt könnyű találni, ha a végeredmény **ω** kódja páros. Ha pedig **ω** kódja *páratlan*, akkor ez csak úgy keletkezhetett, hogy **?+?** kiszámolásakor az eredmény 30-nál nagyobb lett, és kódoláskor levontunk **31** -et (mert a karakterek kódjai 0 és 30 között vannak!). Tehát, ha **ω** kódja *páratlan*, akkor ezt a levont 31-et kell pótolnunk, vagyis a

? + ? = ω + 31 (2)

egyenletet kell megoldanunk! Ez esetben ω+31 páros, tehát ? könnyen kiszámolható.

Például, ha a dekódolásnál a már eddig visszafejtett kód közepe **...könvqoy...**, és most a **v=26** betűnél kell visszafejtenünk, akkor olyan ? betűt kell keresnünk, amelyre **?+?=26** vagy **?+?=26+31=57**, ahonnan **?=13=k** , tehát a **v** betűből és a tőle jobbra levő betűkből (esetleg 31-el növelve) le kell vonnunk 13 -at. Ezért a kapott (előző) betűsorozat: **...könkécn...** .

Könnyen ellenőrizhetjük, hogy a **málna** szót így visszafejtve pontosan a fenti kódoláskor kapott betűsorozatokat kapjuk meg, fordított sorrendben.

ii) Mind kódoláskor mind dekódoláskor (a feladat megoldásakor) sok betűnek sokszor kell különböző eltoltjait kitalálnunk. A betűk eltolását megkönnyíti, ha a diák két **kartonpapír csíkra** számolóléc ("logarléc") módjára felírja az `abc`-t, ügyelve arra, hogy a betűk közötti távolság mindig ugyanannyi legyen, majd a két csíkot egymás alá téve eltolja, és máris leolvashatja a betűk eltolt értékeit (alább a **h** betűvel toltuk el az alsó `abc` -t):

```
_abcdefghijklmnopqrstuvwxyz_abcdefghijklmnopqrstuvwxyz
   <=    _abcdefghijklmnopqrstuvwxyz    =>
```

Ha nincs kéznél papír és olló, akkor bármely szövegszerkesztőbe gépeljük be az `abc` -t két sorban, de `monospaced` (**egyenlő közű**) betűtípussal, mint például `CouierNew` vagy `Lucida Console`, hiszen eltoláskor lényeges, hogy a betűk szélességei *ugyanakkorák* legyenek! Az alsó sort a `Space` vagy `Del` gombokkal tologathatjuk jobbra-balra. (Ezeket a "trükköket" részletesen ismertetjük a x) megjegyzésben, a füzet 45-49. oldalain pedig kivágható ábrákat is közlünk.)

A 31-es levonás/hozzáadás is elvégezhető ezeken az eszközökön, hiszen a felső papíron (betűsorozatban) egymás után kétszer írtuk fel az abc-t: a fenti ábrán például **x+h-31=e** látszik.

iii) Tehát a feladat megoldása: Az éppen vizsgált betűt aláhúztuk, zárójelben a "?+?=ω" illetve a "?+?=ω+31" egyenlet megoldását írtuk:

```
15.                  znnseppdgqekfmz     ( m+m=z )
14. /vissza m- el/   znnseppdgqekfmm     ( t+t=m )
13. /vissza t- el/   znnseppdgqekftt     ( c+c=f )
12. /vissza c-vel/   znnseppdgqekcpp     ( s+s=k )
11. /vissza s- el/   znnseppdgqeskxx     ( b+b=e )
10. /vissza b-vel/   znnseppdgqbphüü     ( h+h=q )
09. /vissza h-val/   znnseppdghug_mm     ( q+q=g )
```

```
08. /vissza q-val/    znnseppdqrcqivv    ( ö+ö=d )
07. /vissza ö-vel/    znnseppöáboáuff    ( ü+ü=p )
06. /vissza ü-vel/    znnsepüufgtfzll    ( ü+ü=p )
05. /vissza ü-vel/    znnseü_zlmyldqq    ( b+b=e )
04. /vissza b-vel/    znnsbsxwijviáoo    ( i+i=s )
03. /vissza i-vel/    znnition_am_see    ( f+f=n )
02. /vissza f- el/    znfbmbgftuétlyy    ( f+f=n )
01. /vissza f- el/    zf_véva_mnzmerr    ( m+m=z )
00. /vissza m- el/    munition_am_see
```

Eredmény: **`munition_am_see`** **(**lőszer a tónál**).**

Megjegyzések

iv) Eredetileg a `znnseppdgqekönvgjoiwéwsk` titkos szöveget terveztük kitűzni, de túl hosszúnak bizonyult. Próbálja meg kedves Olvasó ezt az üzenetet dekódolni, a megoldást a füzet végén ismertetjük.

v) A `31` szám időnkénti hozzáadása/elvétele amiatt szükséges, mert a használt betűk kódjai `0` és `30` között vannak. Tulajdonképpen minden számoláskor a kapott eredmények `31` -el való osztási **maradékát** kellett vennünk, amit a számelméletben a ≡ és `mod 31` jelekkel jelölnek. Ekkor az (1) és (2) egyenleteket egységesen a

$$? + ? \equiv \omega \pmod{31} \qquad (3)$$

formában írhatjuk.

Érdekes, hogy a megoldás `03.` sorában már megjelent a megfejtés nagy része, majd eltűnt és a végére ismét előtűnt. Ennek oka az, hogy az utolsó 3 sor eltolás mértéke `m+f+f=15+8+8=31≡0` (`mod 31`), természetesen ennek hatása csak a 3. betűtől érvényes.

vi) Az (1) és (2), azaz a (3) egyenleteknek azért van minden **ω** esetén *pontosan egy* megoldása, mert a modulus (vagyis `31`) *páratlan* szám! Ezt érdemes, mint szakköri matekfeladatot végiggondolni! Többek között tehát **csúszó-eltolás** kódolás esetén mindig *páratlan sok* betűt (karaktert) használjunk!

vii) A http://math.uni-pannon.hu/~szalkai/csuszokod.zip címen egy egyszerű programomat találja a kedves Olvasó, amellyel bármilyen hosszú (legfeljebb 100 karakternyi) szövegeket lehet kódolni és dekódolni, amely természetesen a *részletszámolásokat* is kiírja mind a képernyőre mind egy szöveges állományba (fájlba). Így tetszőleges szöveg(ek) feladatható(k) és megoldhatók, ellenőrizhetők, tanulmányozhatóak. Sajnos a program betűkészlete rögzített, a feladatban ismertetett `31` betű.

viii) A feladat alapja nyilván a **Cézár kódolás**: https://hu.wikipedia.org/wiki/Caesar-rejtjel (Kr.e. 100-44). Egy kicsit nehezebb feladványt szerettem volna alkotni (sikerült), tudomásom szerint a feladatban leírt *eltolásos* "**csúszókód**" sehol sem használt módszer. A Cézár kódolás egy sikeres továbbfejlesztése a **Vigenère**-kódolás: https://hu.wikipedia.org/wiki/Vigenère-rejtjel (amelyet 1553 körül talált fel **Bellaso**), amelyet csak **Euler**nek (1707-1783) sikerült feltörnie, matematikai megfontolásokkal, módszere azonban hosszú kulcsok esetén fáradságos.

ix) Az általunk közölt feladat, ha már rájöttünk az (1) és (2) egyenletekre és megoldásukra, már csak aprólékos "pepecselés". Azonban nagyon kell vigyáznunk: ha egy betűnél elrontjuk akár a kódolást akár a dekódolást, a hiba tovább "gyűrűzik", kijavítani nem tudjuk sőt észre sem vesszük, csak a legvégén, amikor értelmetlen szöveget kaptunk! Mivel a szöveg hosszával *négyzetesen* növekszik a "pepecselés", ezért rövidítettük le az eredeti, (iv) pontban közölt) szöveget.

x) A megoldás elején a ii) pontban ismertetett **kartonpapír** és `monospaced` betűkészlet-tologatási módszereket érdemes kicsit közelebbről is megismernünk, hiszen számtalan "eltolásos" (azaz összeadási) feladatnál lehetnek segítségünkre.

Tehát, az `abc` -t `monospaced` betűtípussal (pl. `CourierNew` vagy Notepad) gépeltük (https://en.wikipedia.org/wiki/Typeface#Proportional_font , https://en.wikipedia.org/wiki/Typeface#Monospaced_typefaces.)
A piros sort a `Space/Del` gombokkal jobbra - balra tologathatjuk, és a felső kék sorban leolvashatjuk a piros betű eltolt értékét, ha előtte az eltolni kívánt értékhez állítottuk a piros _ (szóköz) jelet (a vízszintes vonal felett levő számok csak a kék betűk értékét mutatják):

```
          1         2         3         4         5         6
012345678901234567890123456789012345678901234567890123456789012
_aábcdeéfghijklmnoöpqrstuüvwxyz_aábcdeéfghijklmnoöpqrstuüvwxyz
 _aábcdeéfghijklmnoöpqrstuüvwxyz
```

Például a **málna** szó eltoltja az **m=15** értékkel **zoy_n** mert

```
          1         2         3         4         5         6
012345678901234567890123456789012345678901234567890123456789012
_aábcdeéfghijklmnoöpqrstuüvwxyz_aábcdeéfghijklmnoöpqrstuüvwxyz
               _aábcdeéfghijklmnoöpqrstuüvwxyz
```

A **kartonpapír** és `monospaced` módszerekkel *tetszőleges* betű- (karakter-) sorozathoz magunk is készíthetünk számolási segédeszközöket, legalábbi elég hosszú papírcsík és monitor esetén! Ajánlom a honlapomon található skálákat (többféle betűkészlettel), amelyeket a mellékelt "szabásminta" segítségével kényelmes számolólécet készíthetünk magunknak (és füzetünk végén is mellékeltünk pár kivágható skálát): http://math.uni-pannon.hu/~szalkai/Csuszokod-loglec4.doc ,
http://math.uni-pannon.hu/~szalkai/Csuszokod-loglec4.pdf .
Ilyen segédeszközöket természetesen a világháborúkban széles körben használtak, persze nem papírból: https://upload.wikimedia.org/wikipedia/commons/f/fa/Cryptographic_sliding_rule-IMG_0533.jpg .

xi) A gyakori `±31` problémát elkerülendő nagyszerű ötlet, ha az `abc` -ket két kör kerületére írjuk (pl. macisajt dobozára). Sajnos a jobboldali ábra csak 27 betűt tartalmaz, de füzetünk végén egy 31 részes, kivágható szabásmintát közlünk.

xii) Összeadás-kivonás nem csak Cézár kódolásnál jelentkezik, hanem az Élet rengeteg más területén, pl.: öröknaptár és x nap múlva milyen nap lesz: **Szalkai:** *Öröknaptárt számoló léc* http://math.bme.hu/~hujter/180517.doc ,
http://math.uni-pannon.hu/~szalkai/Loglec-Naptar-2huen.pdf
http://math.uni-pannon.hu/~szalkai/Loglec-Naptar-2huen.doc
http://math.uni-pannon.hu/~szalkai/Log-orokNaptar-171105-elt-HUEN.png
abszolút és relatív hangmagasság a Kodály-féle szolmizációban
https://hu.wikipedia.org/wiki/Kodály-módszer , http://leewm.freeshell.org/origami/chord-ruler.pdf
https://hu.wikipedia.org/wiki/Szolmizáció ,
időzónák, napfelkelte és -nyugta http://leewm.freeshell.org/origami/timezone.pdf
fényképezés : http://math.uni-pannon.hu/~szalkai/Zenith-el-300.jpg ,
https://hu.wikipedia.org/wiki/Mélységélesség , https://hu.wikipedia.org/wiki/Fényképezőgép
törtek összeadása http://www.evilmadscientist.com/article.php/inchadder ,
https://www.evilmadscientist.com/2007/make-your-own-1952-fraction-of-an-inch-adding-machine
és **kedvenc** (mindennapi) **problémám**: ha a *h* magas árbóc tetejéről éppen megpillantjuk a *t* magas világítótornyot, akkor milyen messze vagyunk a kikötőtől: https://arxiv.org/abs/1612.03955 ,
http://www.animatedsoftware.com/elearning/DigitalSlideRule/index.html
http://www.animatedsoftware.com/elearning/DigitalSlideRule/DigitalSlideRule.swf
http://www.oughtred.org/jos/pages/JOS_2018_Vol_27_1_Cover.jpg .
Lásd még: http://db.komal.hu/scan/1977/04/97704146.g4.png , https://arxiv.org/abs/1612.03955 ,
és *Make Your Own Slide Rule*, J. of Oughtred Society http://www.oughtred.org/journal.shtml (megjelenés alatt).

2. Feladat

Derítsd ki, hogy kitől származott a lenti elfogott üzenet és mi volt az üzenet tartalma magyarul és latinul is! Az üzenetről annyit már sikerült kideritenünk, hogy annak küldője „Caesar titkosítást” alkalmazott, ahol az eltolás mértéke 4.
(A feladat megoldásához az angol abc-t használd.)

Az elfogott üzenet a következő: Epie megxe iwx!

Az elfogott üzenet, latinul:

Az elfogott üzenet jelentése magyarul:

Az üzenet szövegében megtalálható alakzat nevéről elhíresült magyar játék feltalálásának évszámát osszuk el az eddig megrendezésre került világbajnokságok számával:

Az utolsó érték a Pannon Enigma kód része!

A 2. feladat megoldása

A betűk eltolását megkönnyíti, ha két kartonpapírcsíkra felírjuk az `abc`-t (ügyelve arra, hogy a betűk közötti távolság mindig ugyanannyi legyen), és a két csíkot eltolva és egymás alá téve máris leolvashatjuk a betűk eltolt értékeit. Ha nincs kéznél papír és olló, bármely szövegszerkesztőbe gépeljük be az abc-t két sorban, **de** `monospaced` **(egyenlő közű)** betűtípussal, mint például `Couier New` vagy `Lucida Console`, hiszen (valóságos) eltoláskor lényeges, hogy a betűk szélességei (azaz a közöttük levő távolságok) *ugyanakkorák* legyenek! Az alsó sort az `insert space` vagy `del` gombokkal tologathatjuk jobbra-balra:

```
      _abcdefghijklmnopqrstuvwxyz_abcdefghijklmnopqrstuvwxyz
<-    _abcdefghijklmnopqrstuvwxyz    ->
```

(A "kartonpapír-csík" és "szövegszerkesztő" módszereket részletesen ismertettük az 1. feladat megoldása után, és a füzet végén kivágható ábrát is közlünk.)

A 2. feladatban csak egyetlen eltolás volt +4 -el, és angol abc -t használtunk:

```
           1         2         3         4         5         6
0123456789012345678901234567890123456789012345678901234567890123456789012
_abcdefghijklmnopqrstuvwxyz_abcdefghijklmnopqrstuvwxyz
    _abcdefghijklmnopqrstuvwxyz
```

Az betűket: "**epie megxe iwx**" szöveg betűit a felső sorban keressük, alattuk látjuk az eredeti "**alea iacta est**", magyarul: "*A kocka el van vetve.*"

A **Rubik-kocka** feltalálásának éve **1974**, az eddigi világbajnokságok száma **9**, a hányados 1974/9 =

= **219,333**... .

Megjegyzések

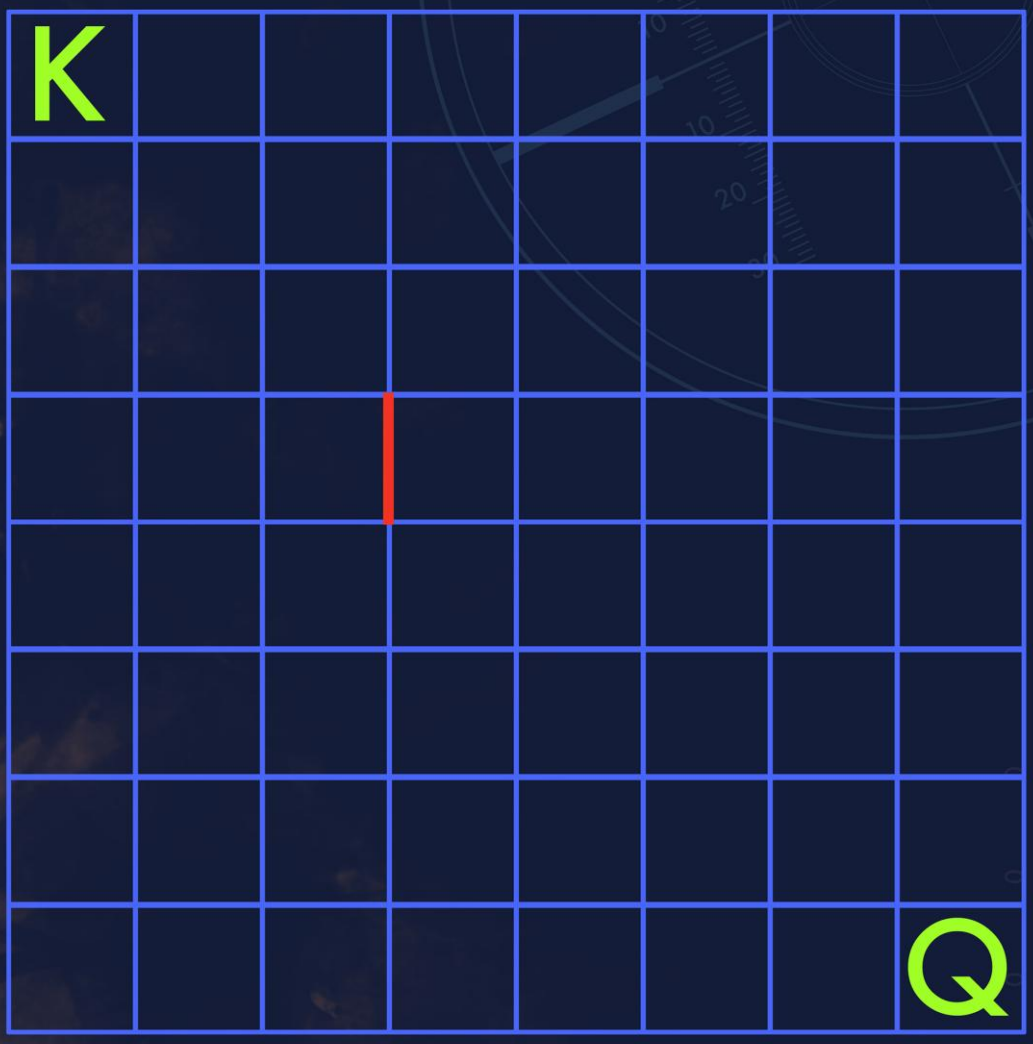
i) A feladat szövegéből nem derül ki, hogy a szóközt is hozzászámoljuk a karakterkészlethez (27 karakter), vagy csak az ékezet nélküli betűket (26 karakter). Szerencsére ez most nem lényeges, mert a kódolt "`epie megxe iwx`" szövegben nincs `a,b` vagy `c` betű, (azaz az eredeti szövegben nincs `x,y` vagy `z` betű).

ii) Lásd még az 1. feladathoz írt x) és xi) megjegyzéseket is, valamint az alábbi olvasnivalókat:

http://hu.wikipedia.org/wiki/Caesar-rejtjel , https://hu.wikipedia.org/wiki/Vigenère-rejtjel

3. Feladat

Hányféleképpen juthat el a király a sakktábla bal felső (K) mezőjéről a jobb alsó (Q) mezőre, ha minden lépésben csak le egyet vagy csak jobbra egyet léphet. A király, az ábrán látható vastag piros vonalon nem léphet át a szomszédos egyik mezőről a másikra.

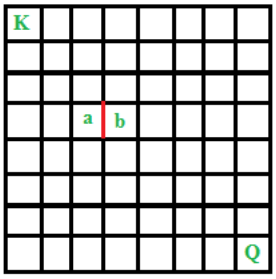


A 3. feladat megoldása

I. megoldás:

Általános iskolások számára a legegyszerűbb - és *szinte minden feladathoz használható módszer* az úgynevezett **"összeszámlálós módszer":** a játéktábla (táblázat, gráf) minden mezőjére, lépésről lépésre, kiszámoljuk és ráírjuk, hogy erre a mezőre hányféleképpen lehet eljutni. A "start" mezőre nyilván 1 -est írunk. Minden további "aktuális" mező esetén meg kell keresnünk azokat a "megelőző" mezőket (esetleg csak egy van ilyen), amelyekről egy lépésben eljuthatunk az "aktuális" mezőre, és ezen "megelőző" mezőkre írt számok *összege* adja az "aktuális" mezőre írandó számot. Az alábbi, bal oldali ábrán néhány számot kiszámoltunk, az egész tábla kiszámolása ajánlott házi feladat. (Végeredmény a II. megoldás végén.)

K 1	1	1	1	1
1	2	3	4	5
1	3	6	10	6
1	4	10	10	16
1	5	15	25	41
1	6	21	46	87



A lehetséges útvonalak számai

Ha nincs "megelőző" mező (néha előfordul), akkor az "aktuális" mezőre nyilván 0 -át kell írnunk.

A módszer természetesen csak akkor működik, ha a táblán nem lehet körbemenni - de ekkor a feladatnak sem lenne értelme. (A módszer alapötlete hasonlít Dijksra útkereső algoritmusához, pl. [0],[1].)

A fenti ábrán a Pascal háromszöget vélhetjük felfedezni, legalábbis a piros vonaltól balra felfelé, aminek folytatódását a piros vonal megakasztja (mint szirt a patak folyását). Ez utóbbi észrevétel nem meglepő, teljesen érthető.

A Pascal háromszögön pedig érdemes eltűnődnünk, még ha nem is érezzük meglepőnek. Speciális, például *téglalapháló* (vagy háromszög-, hatszögháló stb.) elrendezésű táblázatnál kombinatorikai eszközökkel össze is számolhatjuk a lehetséges útvonalakat (az "összeszámlálós módszer" nélkül), mint alább a II. megoldásban. (Más elrendezések megoldásait például [2] -ben találjuk.)

II. megoldás:

Ha nem lenne a piros vonalon a tiltás, akkor minden útvonalon pontosan 7-et kell **L**E és **J**OBBRA lépni, összesen 14 -et. Az **L** és **J** lépések sorrendje egyértelműen határozza meg az útvonalakat, számuk pedig *ismétléses permutáció*:

$$P_{14}^{7,7\,(ism)} = 14! / (7!*7!) = 3432 .$$

A piros tiltás miatt a következő útvonalak *szűnnek meg*: elmegyünk a piros vonal bal széléig, az **a** mezőig (3xLE és 2xJOBBRA), átmegyünk a piros vonalon, majd onnan, a **b** mezőtől a szokásos módon a Q mezőig (4xLE és 4xJOBBRA). Az ilyen utak száma, az előző gondolatmenettel:

$$P_5^{3,2\,(ism)} * P_8^{4,4\,(ism)} = 5!/(3!*2!) * 8!/(4!*4!) = 700$$

Tehát maradt 3432 - 700 = **2732** lehetőség.

Megjegyzések

iv) *Mindkét módszert* érdemes gyakorolni különböző táblákon és különböző feltételekkel. Például:

3B.Feladat:

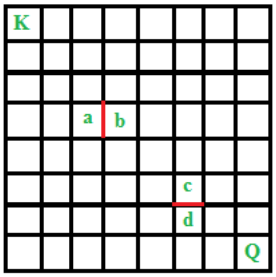
Hányféleképpen juthat el a király a sakktábla bal felső (K) mezőjéről a jobb alsó (Q) mezőre, ha minden lépésben

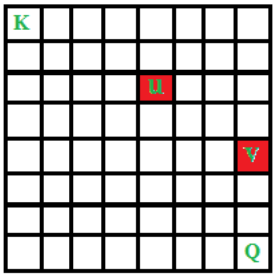
a) csak jobbra és lefelé egyet-egyet léphet (korlátozás nélkül),

b) csak jobbra, lefelé és *átlósan jobbra-le* egyet-egyet léphet,

c) csak jobbra és lefelé egyet-egyet léphet, de a baloldali ábrán látható vastag piros vonalakon nem léphet át a szomszédos egyik mezőről a másikra,

d) csak jobbra és lefelé egyet-egyet léphet, de a jobboldali ábrán nem léphet rá a piros mezőkre?





A feladat néhány változata

vi) Az a) feladat egy klasszikus feladvány, nagyon sok feladatgyűjteményben és a Neten is megtalálható (pl. [2] vagy http://www.piok.hu/rpg/images/Dokumentumok/Matek/11/kombinatorika_11.pdf), a számolást a II. megoldás elején ismertettük, a végeredmény **3432.**

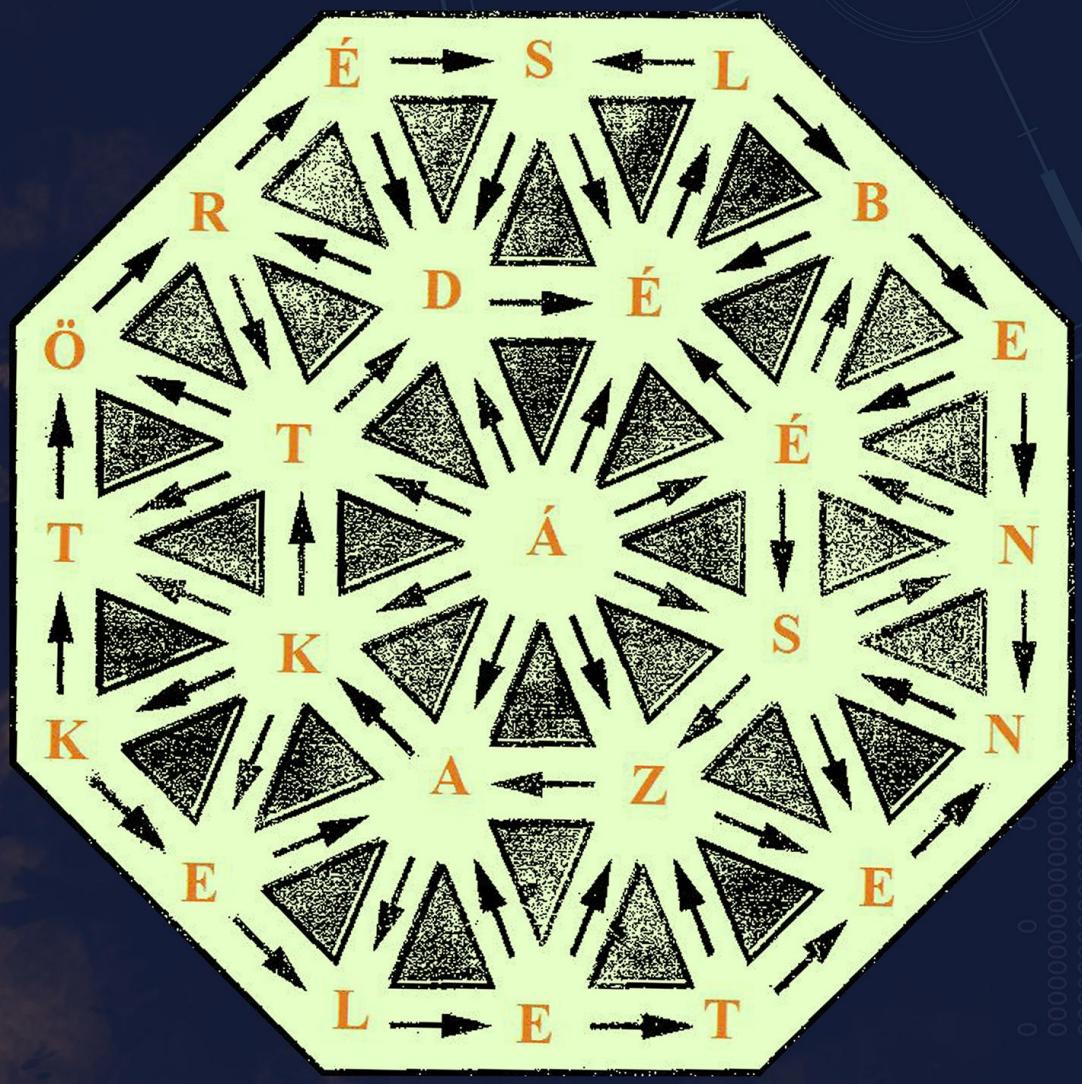
vii) A b) és c) feladatok megoldását füzetünk legvégén ismertetjük, a d) feladat házi feladat. Ha egy táblán több tiltott átjáró vagy mező is van, akkor a *logikai szitaformulát* ("tartalmazás és kizárás elve") kell használnunk.

Ez az oldal szándékosan üres.

4.

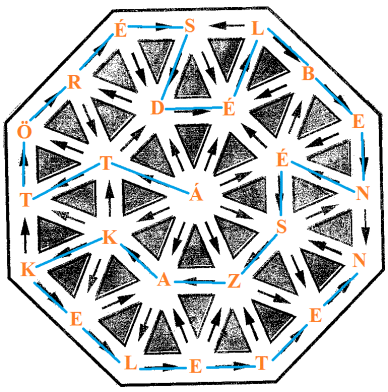
Feladat

A tengeralattjárók újabb üzenetváltását fogtuk el, tudjuk valahol támadásra készülnek, a mondat tartalmazza az időpontot is. Azt kiderítették matematikusaink, hogy a karaktersorozat az alábbi ábrába rendezhető. Az ábra középső betűjétől indulva a nyilak mentén olvassuk össze az összes betűt pontosan egyszer (ezt Hamilton útnak nevezik). A kapott betűsorozat lesz a Kód negyedik részlete, amit természetesen szóközök nélkül kell használni.



A 4. feladat megoldása

Mindössze próbálgatni kell a betűk összeolvasását:



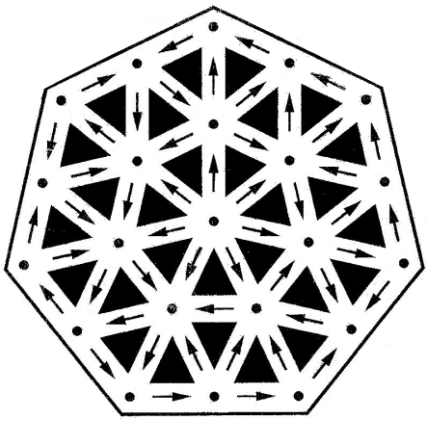
A megoldás

Vagyis a megfejtés: " **ÁTTÖRÉS DÉLBEN ÉSZAKKELETEN** "

Megjegyzések

i) A feladatot nagyban megkönnyítette, hogy egy értelmes mondatot (kifejezést, szavakat) kellett keresnünk. Ha a kódolt üzenet csak egy jelsorozat lett volna, nem csak nehezebb, hanem veszélyesebb is lett volna ez a feladat: a legtöbb gráfban több Hamilton út is lehetséges - melyik a jó?

ii) Rejtvényújságokban rengeteg hasonló feladatot találhatunk, gyakorlásképpen az alábbi megfejtését füzetünk végén találja az Olvasó:



Egy hasonló feladat

iii) A feladat kerettörténete ("*kiderítették matematikusaink, hogy a karaktersorozat, az ábrába rendezhető*") meseszerű, sőt nem is igaz! Azonban manapság, a modern titkosírási módszerek nagyon sok **NP-teljes**[*)] probléma nehézségét használják fel titkosírások készítéséhez. Erről például Lovász László - Gács Péter könyvének http://web.cs.elte.hu/~lovasz/kurzusok/complexity.pdf 219-220. oldalain olvashatunk.

[*)] azaz **reménytelenül nehéz**: a legjobb matematikusoknak, programozóknak, szuperszámítógépeknek több milliárd (!) évre van szükségük a megoldáshoz !

5. Feladat

Az ügynökökkel a tartótisztek Kavaho nyelven beszélnek, melyet rajtuk kívül senki sem ért. A Kavaho nyelvben nincs semmilyen ragozás vagy elöljárószó, a szavaknak szótári alap alakját használják, a szavakat betűrendben írják le a mondatokba, csak nagybetűk vannak, a szavak között szóköz van, a mondat végén pont (szóköz nélkül). Öt mondatot már sikerült megfejtenünk:

1: KEW KIMA KOGH KOJI. =
Nagy ajtóban virág eldugva.

2: KAGA KEV KEW KIMA KMALE KOGH KUJU. =
Eldugott hideg vonat öt ajtójára virág esett.

3: KEV KEW KIMA KMALE KOJI KTI KUCE KUG KUJU. =
Holnap esik öt virág királyra eldugni hat nagy vonatot.

4: KAGA KEV KIMA KOGH KTI KUCE KUJU. =
Öt eldugott király holnapi hideg vonat ajtóra.

5: KAGA KEV KMALE KOGH KOJI KUCE KUG. =
Hat nagy ajtó leesett öt hideg királyra.

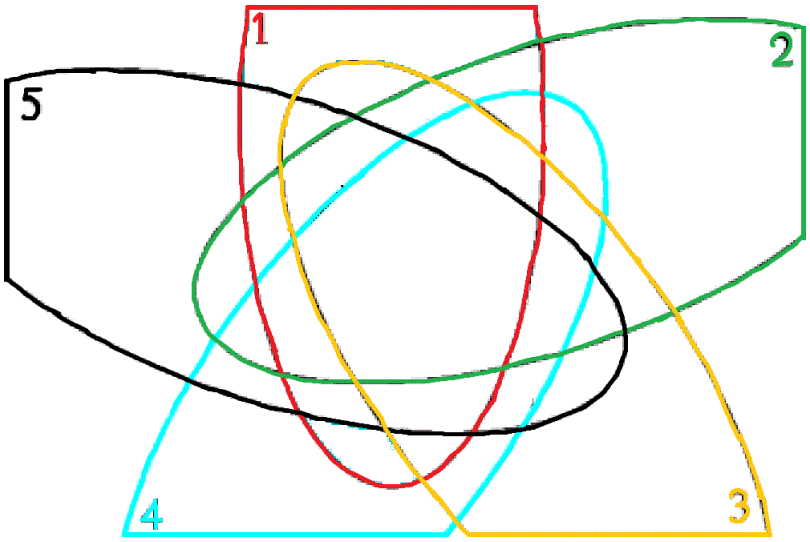
(A magyar mondatokba a szórend és a ragozás a fordítás után került bele, tehát például az "eldugni", "eldugtunk", "eldugott" , ... szavak a Kavaho nyelvben ugyanazzal a szóval vannak jelölve.)

Feladat: Fordítsuk le az alábbi (félrevezető) üzenetet a Kavaho nyelvre:

Eldugtunk öt nagy hideg királyt.

Az 5. feladat megoldása

Mivel a *Kavaho* nyelvben a szavak ABC rendben vannak egymás után, ezért minden mondat egy *halmaz*: a benne levő szavak halmaza. Tehát írjuk be a halmazábrába, hogy a szavak melyik mondatban szerepelnek, és megkapjuk a kavaho-magyar szótárt: *a megfelelő szavak ugyanazokban a mondatokban (halmazokban) szerepelnek* !



Venn diagram 5 halmazra

Az ábra helyett/mellett használhatunk táblázatokat is:

KAVAHO	KAGA	KEV	KEW	KIMA	KMALE	KOGH	KOJI	KTI	KUCE	KUG	KUJU
1.mondat											
2.mondat											
3.mondat											
4.mondat											
5.mondat											
bináris											

MAGYAR	ajtó	eldug	esik	hat	hideg	holnap	király	nagy	öt	virág	vonat
1.mondat											
2.mondat											
3.mondat											
4.mondat											
5.mondat											
bináris											

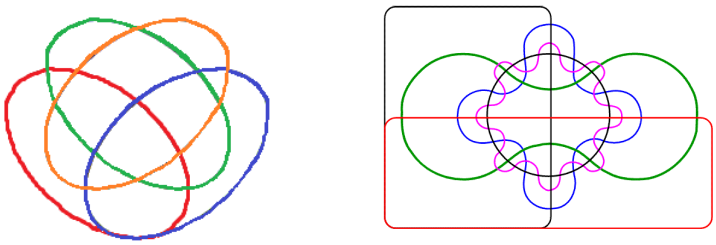
Az oszlopok (szavak) összehasonlítását megkönnyíti, ha az oszlopokat kettes számrendszerben felírt számoknak tekintjük, és - neveltetésünk révén - átírjuk tízes számrendszerbe, a "bináris" feliratú sorba. Ehhez használhatjuk az `Excel` függvényeit, például: "**=B4+B5*2+B6*4+B7*8+B8*16**". A táblázatot most azért hagytuk üresen, hogy az Olvasó gyakorolni tudja megoldási ötletünket, a kitöltött táblázatot és a feladat megoldását füzetünk végén ismertetjük.

Megjegyzések

iii) A Zrínyi Ilona matematikaverseny 1998. évi megyei versenyén hasonló feladat szerepelt:

"*Tifling országban anka nyelven beszélnek. Négy mondat fordítását megadjuk ankául:*
(1) "Leesett a kifli." = "*Ham bam.*" (2) "Szeretem a levest." = "*Vele memme.*"
(3) "Leesett a fáról." = "*Bam fam.*" (4) "Szeretem a kakaót." = "Dudu memme."

Hogyan mondhatják ankául a "Szeretem összeszedni a fáról leesett almákat." *mondatot*:
a) "*Memme venne fam bam ma.*" b) "*Memme ham fam bam ma.*"
c) "*Vele dudu fam bam ham.*" d) "*Memme venne ham bam ma.*"
e) "*Dudu venne bam fam al.*"



Venn digram 4 és 6 halmazra

iv) Ehhez a feladathoz is ajánljuk a Venn diagramokat és a táblázatot. A baloldali ábrán 4, a jobboldalin 6 halmaz ábráját látjuk. Körökkel nem lehet háromnál több halmaz Venn diagramját felrajzolni, de ellipszisekkel, téglalapokkal, sokszögekkel (ez Branko Grünbaum tétele), és egyéb "szép" síkidomokkal *akárhány* halmazból álló Venn digram elkészíthető. Néhány cím: http://hu.wikipedia.org/wiki/Venn-diagram, http://www.combinatorics.org/files/Surveys/ds5/VennIrreducible.html , http://www.combinatorics.org/files/Surveys/ds5/VennEJC.html , http://en.wikipedia.org/wiki/Venn_diagram .

v) A feladatban szereplő "Kavaho" nyelv kitalált, tulajdonképpen mind Zrínyi, mind a PEnigma feladatok szövegei halandzsák. Azonban tény, hogy a XX. század több háborújában sok rádióüzenetet valamilyen nagyon ritka élő nyelven, például *baszk, csaktó, komancs, navaho* közvetítettek. Hát mi ezért beszéltünk "kavaho" nyelven. További olvasnivalók: https://hu.wikipedia.org/wiki/Kódbeszélő , https://ru.wikipedia.org/wiki/Шифровалъщики-навахо , https://en.wikipedia.org/wiki/Code_talker , http://ru.wikipedia.org/wiki/Радисты-шифровалъщики .

Ez az oldal szándékosan üres.

6. Feladat

Programozott robot torpedó

A németek elindítottak egy robot torpedót, előre beépített, rögzített programmal, amit lehallgattunk:

FOR i=1 TO 8 ELORE;
BAL; FOR i=1 TO 6 (ELORE, ELORE, JOBB);
BAL, ELORE, JOBB, ELORE, BAL, ELORE, JOBB, ELORE;
ELORE, BAL, ELORE, JOBB, ELORE, JOBB, ELORE;
FOR i=1 TO 7 (BAL, ELORE, ELORE);
FOR i=1 TO 3 (JOBB, ELORE, BAL, ELORE);
ELORE, BAL, ELORE, JOBB, ELORE, ELORE;
FOR i=1 TO 5 (ELORE, JOBB, ELORE, BAL, ELORE);
BAL, BAL, ELORE, ELORE, ELORE;
FOR i=1 TO 4 (ELORE, BAL, ELORE, JOBB, ELORE);
FOR i=1 TO 4 (ELORE, JOBB);
FOR i=1 TO 11 ELORE;
BUMM!

1. A robot csak É-D és K-Ny irányban halad, minden utasított ELORE lépése ugyan olyan hosszú és egy óráig tart, és arrafelé történik, amerre éppen a hajó orra áll, minden fordulása (BAL, JOBB) 90°-os, amelyek ideje elhanyagolható.

2. Így az angolok felosztották a térképet 26x26 akkora négyzetre, hogy a robot egyik négyzet középpontjából a vele szomszédos négyzet középpontjába, pontosan 1 óra alatt (=egy ELORE lépés) jut el. A négyzeteket a sakktáblához hasonlóan **A01, ...,Z26** -tal jelölik (egy nagybetű és két számjegy): Nyugatról Keletre A, B, ..., Z ; Északról Délre 1,2,...,26. Az biztos, hogy a robot csak ebben a keretben mozog!

3. A robot pontos indítási helye és iránya ismeretlen, de időpontját a szonárok pontosan érzékelték.

4. Indítása után pontosan **1** nappal (24 órával) felderítő repülőgépek az **N15** négyzet közép-pontjában látták, és éppen **Kelet** felé tartott, de ekkor a robot megint alámerült és eltűnt.

5. A fenti észlelés után pontosan **+1** nappal indult el Amerikából a Speciális Hatástalanító Század (SHSz), amely sajnos csak pontosan **két** nap múlva ér a térség bármelyik négyzetébe. A térségben rengeteg a kereskedelmi hajó, a **BUMM** parancsra a robot legalább tíz értékes hajót fog elsüllyeszteni!

6. Melyik következik be előbb? A beküldendő **Pannon Enigma kódrészlet** a következő (idéző-jelek nélkül): "#***" ahol:
- ha az SHSz időben érkezik, akkor # egy + karakter, és *** annak a négyzetnek a kódja, ahol a robotot az SHSz hatástalanítja,
- ha az SHSz elkésett, akkor # egy - karakter, és *** annak a négyzetnek a kódja, ahol a robot felrobbantja a kereskedelmi hajókat.

Siess, számolj pontosan, az idő telik, a torpedó halad a célpontja felé!

A 6. feladat megoldása

Sajnos a feladatba gépelési hiba csúszott: a 4. pontban "Kelet" helyett "Délre" a helyes irány, vagyis a 4. pont helyesen :

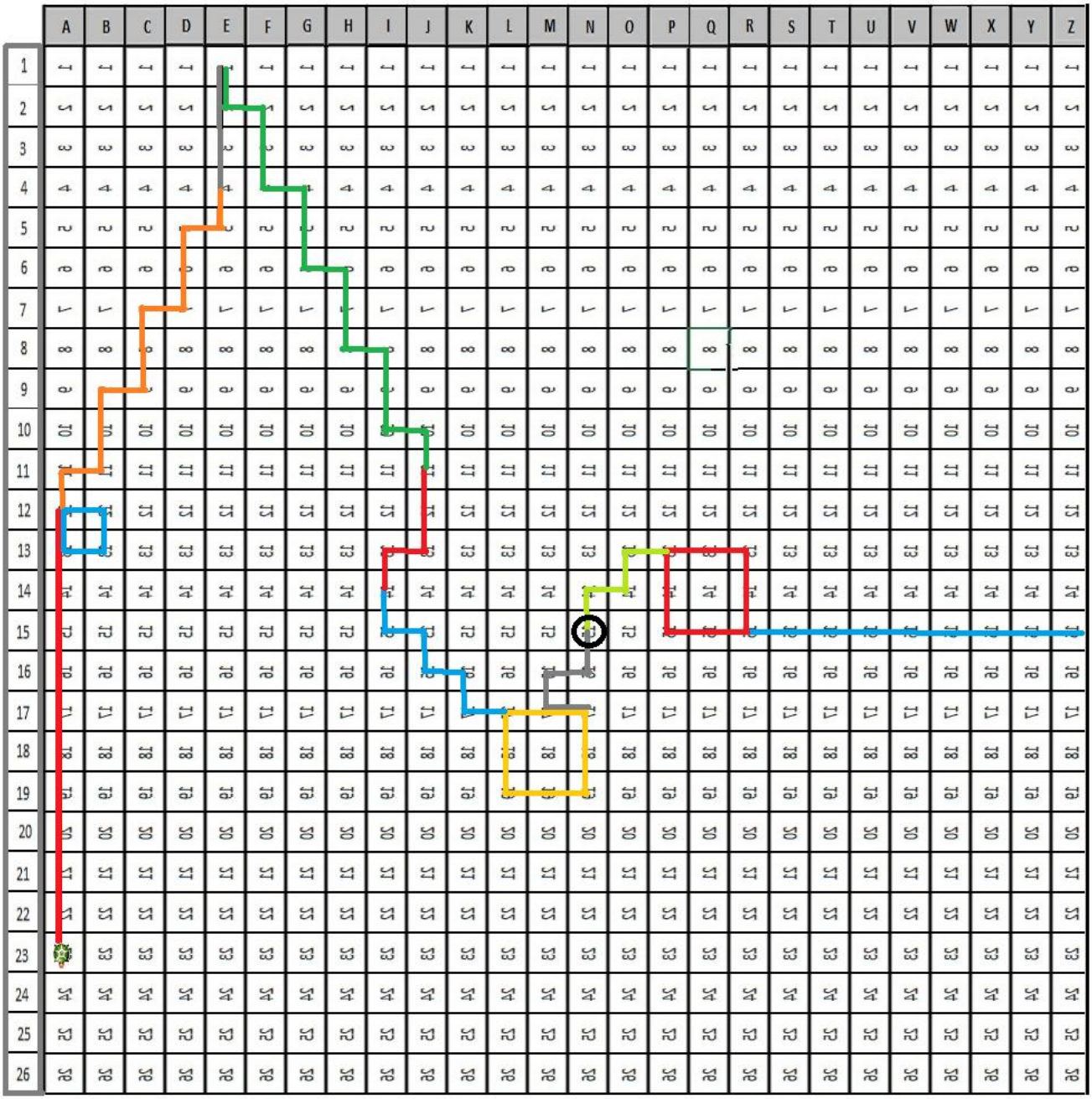
```
4. Indítása után pontosan 1 nappal (24 órával) felderítő repülőgépek az N15
négyzet középpontjában látták és éppen DÉL FELÉ tartott, de ekkor a robot
megint alámerült és eltűnt.
```

A feladat "legegyszerűbb" megoldása, ha egy hatalmas csomagolópapírra felrajzoljuk a 26×26 méretű négyzethálót ("sakktáblát"), és egy kis modellel (radír, faragó) követjük a torpedó útját.
(Ez bizony nagyon komoly módszer még manapság is a katonai felsőbb vezetésben.)

Hadműveleti irányítóközpont a II. világháborúban
https://en.wikipedia.org/wiki/Operational_level_of_war (nagyobb méretben)

Az indulási helyet ugyan nem ismerjük, de nem is szükséges, ugyanis nekünk elég az `N15` négyzetből indulni, mégpedig a program 25. órájától. Tehát meg kell keresnünk a program 25-dik órára vonatkozó utasítását: 4. sor első, `ELORE` utasítása, és csak innen követjük a torpedó útját.

A közismert `LOGO` programot is használhatjuk, természetesen a 96. órára is nagyon kell figyelnünk.



A torpedó útja a LOGO programmal

Az egyes színek a program különböző sorait jelölik (lásd a füzet végén az a) változat megoldásánál).

Tehát a megoldás: az **A22** mezőben sikerül hatástalanítani a torpedót, vagyis a kód: **+A22** .

Megjegyzések

iii) A nagyméretű térkép (csomagolópapír) valóban jó társasjáték volt családomban: egyikünk olvasta a parancsokat, másikunk vezette a torpedót, harmadik számolta az órákat és ellenőrzött, csapatépítő tréningnek nagyon ajánlom másoknak is!

iv) Érdekes módon néhány versenyző a feladat téves kitűzése ellenére is helyesen oldotta meg a feladatot. Egyikük a "sakktábla" szó hallatán azonnal a szabványos betűzésre gondolt (A1=bal alsó =délnyugati mező), nem gondolta végig a feladat ("angolok") számozását. Így az elgépelés és az ő figyelmetlensége

kiegyenlítette egymást. Más tanulók egyszerűen ide-oda forgatták a táblát, amíg meg nem tudták oldani a feladatot és megvédeni a kerekedelmi hajókat. Szemfülesség, életrevalóság nem csak egy versenyen feltétele a túlélésnek!

v) A II. világháborúban valóban létezett német programozott torpedó, bár nem ilyen bonyolult programmal, hanem csak oda-vissza járt párszáz métert, kicsit arrébb, amíg el nem talált egyet a mátrix alakban haladó kereskedelmi hajók közül (forrás: National Geographic).

vi) Alább közöljük a feladat pár nehezített és könnyített változatát, további gyakorlás céljából. A legnehezebbel kezdjük, mert a könnyebb változat elolvasása is nagymértékben segíti a többi feladat megoldását. Az összekötő szövegből csak azokat a részeket ismételjük meg, amelyek eltérnek az eredeti feladat kitűzésétől. A megoldásokat a füzet végén ismertetjük.

d) változat:

```
FOR i=1 TO 4 ELORE;
BAL; ELORE;
FOR i=1 TO 6 (ELORE, ELORE, JOBB);
BAL, BAL, ELORE;
FOR i=1 TO 3 (ELORE, JOBB);
JOBB, JOBB; FOR i=1 TO 3 ELORE;
FOR i=1 TO 4 (JOBB; FOR j=1 TO i ELORE;);
FOR i=1 TO 7 (BAL, ELORE, ELORE);
ELORE; BAL;
FOR i=1 TO 4 (JOBB; FOR j=1 TO 10 ELORE;);
FOR i=1 TO 8 ELORE;
BUMM!
```

3. A robot pontos indítási helye és iránya ismeretlen, de időpontját a szonárok pontosan érzékelték.
4. Indítása után pontosan **1** nappal (24 órával) felderítő repülőgépek a **P11** négyzet középpontjában látták, de irányát nem tudták megállapítani, majd ez után pontosan még **egy** nappal a **P10** négyzetben is észlelték, de ekkor a robot megint alámerült és eltűnt.

c) változat:

```
FOR i=1 TO 8 ELORE;
BAL; FOR i=1 TO 6 (ELORE, ELORE, JOBB);
BAL, ELORE, JOBB, ELORE, BAL, ELORE, JOBB, ELORE;
ELORE, BAL, ELORE, JOBB, ELORE, JOBB, ELORE;
FOR i=1 TO 7 (BAL, ELORE, ELORE);
FOR i=1 TO 3 (JOBB, ELORE, BAL, ELORE);
ELORE, BAL, ELORE, JOBB, ELORE, ELORE;
FOR i=1 TO 5 (ELORE, JOBB, ELORE, BAL, ELORE);
BAL, BAL, ELORE, ELORE, ELORE;
FOR i=1 TO 4 (ELORE, BAL, ELORE, JOBB, ELORE);
FOR i=1 TO 4 (ELORE, BAL);
FOR i=1 TO 11 ELORE;
BUMM!
```

Ugyanaz, mint a d), csak a program egyszerűbb: nem írtam bele egymásba skatulyázott ciklusokat. Természetesen a 4. bekezdésben a megadott mezők megváltoznak: P11 és P10 helyett **N15** és **I14** írandó.

b) változat:

Ez a kitűzött változat, programja megegyezik a c) változat programjával.

a) változat:

Marad a c) változat programja, de megadjuk a pontos indítási helyet és időt: **Z15** mező, 1944.05.09., 07:00', iránya Észak felé.

7. Feladat

A rács - elromlott az enigma

A német titkosszolgálat (Abwehr) rendszeresen tájékoztatja ügynökeit és az úton lévő hajók kapitányait az újabb tengeralattjáró-flottakötelékek kihajózásáról (bevetéséről). Az ENIGMA hálózat elromlott, ezért visszatérnek a régebbi „rácsos" titkosítási módszerhez. Az üzenetet fogadók, kódpárokat kapnak, amelyek segítségével össze tudják állítani azt a forgatható rácsot, amit ráheyezve a náluk lévő karakterekkel feltöltött 8x8-as kódtáblára azok a betűk „maradnak" csak olvashatóak, amelyek kiadják az üzenet valós szövegét.
Az Abwehr vezetése a saját kódoló katonáiban (küldők) sem bíznak meg, ezért a tisztek azt találták ki, hogy matematikai példákba rejtve küldik Berlinből Kielbe (a haditengerészet központjába) a koordinátákat.
Az angol ügynökök megszerzik a feladatokat és birtokában vannak a kódtáblának is!

Számold ki az egyenleteket, állítsd fel a rácsot, fejtsd meg az üzenetet!
Vigyázz, az üzenet német nyelvű, így tartalmaz a magyartól eltérő betűket is ezenkívül az elkészült rácsot többféleképpen is ráteheted a szövegre!

A beküldendő kód-részlet:
A titkos (német nyelvű) üzenet, de a német helyesírásnak megfelelő szóközökkel és a mondat végén pont (egyéb írásjel nincs a mondatban).

Kódtábla:

E	H	N	E	D	I	R	U
N	N	N	E	T	Ä	E	C
H	N	U	S	N	R	N	D
A	Z	S	E	C	W	T	H
A	E	S	N	E	W	C	Z
H	O	O	I	B	T	G	O
O	C	T	H	N	E	T	E
A	E	L	F	B	A	U	A

Feladatok (ereményül a koordinátákat kapjuk, ne feledd: $1 \le x \le 8$; $1 \le y \le 8$):

1) $x^3 = y$ & $x^3 \neq x$
2) $x+y = 15$ & $x+1 = y$
3) $x+y = 11$ & $x-y = -3$
4) $3x = y$ & $x = y-4$
5) $x*y = (x+1)*(y-1) = 3*(x+y-1)$
6) $2x+y = 7$ & $3x+2 = y$
7) $x^2+y^2 = 89$, $x>y$
8) $2*x*y = 50$
9) $3x+4y = 25$ & $4x+3y = 24$
10) $x^2-3y^2 = 1$, $y>1$
11) $3x = y$ & $x+2 = y$
12) $3x = 2y$ & $x = y-1$
13) $x = 2y$ & $x+y = 9$
14) $x = y^3 -1$
15) $x-2y = 1$ & $2x+y = 7$
16) $x = 2*(y+1)^2$

KÓDUETŐK digitális oktatási műhely

www.kodvetok.com/enigma

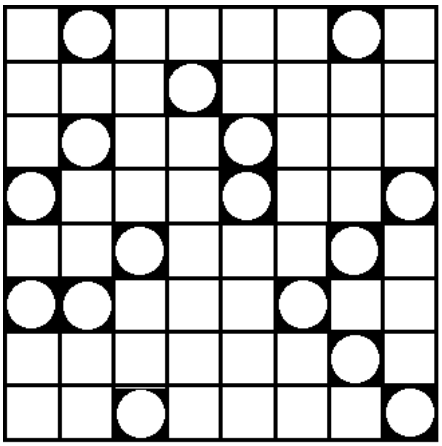
A 7. feladat megoldása

i) Először az egyenletrendszereket kell megoldanunk. Mivel $1 \le x \le 8$ és $1 \le y \le 8$, ezért általános iskolások akár próbálgatással is meg tudják oldani ezeket.

A **megoldások:**

(2,8), (7,8), (4,7), (2,6), (5,6), (1,5), (5,5), (8,5), (3,4), (7,4), (1,3), (2,3), (6,3), (7,2), (3,1), (8,1),

tehát a rács:



A 7. feladat dekódoló rácsa

ii) A köröknél kell lyukakat vágnunk a kartonpapír rácsra, amelyeken láthatóak lesznek az olvasandó betűk, amikor a rácsot (régiesen *rostélyt*) ráhelyezzük a szövegre. A betűket természetesen soronként olvassuk össze. (A kinyomtatott füzet 49. oldalán levő kivágható rács mérete megegyezik az előző oldalon levő szöveg méretével.)

A **forgatható rács** elnevezés arra utal, hogy a megfelelő betűk kiolvasása után a rácsot középpontja körül negyed fordulattal (90^o-kal) *többször* is el kell forgatnunk ahhoz, hogy a kódolt szöveg többi betűjét is el tudjuk olvasni. Megegyezés kérdése, hogy jobbra vagy balra forgatjuk a rácsot, tehát ezt is próbálgatnunk kell, azonban bármely forgásirány esetén már csak a kapott négy szövegrészletet kell sorbatennünk. Ráadásul, mint a kartonpapír rácsoknál, azt sem tudjuk, hogy melyik a rács színe és fonákja, vagyis lehet, hogy még tükröznünk is kell a rácsot, mielőtt a szövegre helyezzük, tehát legalább 8 lehetőséget kell kipróbálnunk!

A fentiekből következik, hogy ha a tanuló véletlenül összekeverte az x és y koordinátákat, semmi baj nem történik, hiszen a rács amúgy is forgatandó és tükrözendő!

Javasoljuk az Olvasónak, hogy a fenti rácsot valóban vágja ki papírból (a 49. oldalról), és próbálgasson, keresse meg a feladat megoldását.

A megoldást a füzet végén közöljük!

Megjegyzések

iii) Ha nincs kéznél papír és olló, akkor használhatunk rajzoló programot is (pl. Paint), amivel a fenti átlátszó (transparent) rácsot közvetlenül ráhelyezhetjük a feladat szövegére, forgathatjuk és tükrözhetjük. A *Powerpoint* pogram segítségével is készíthető és megoldható ilyen feladat, mint **Süle Péter** kollégám meg is tette: http://math.uni-pannon.hu/~sulep/index_html_files/Forgathato_racs.ppsx .

iv) A megoldások feltöltésénél sok tanuló csak a szöveg első 16 betűjét küldte be. Nem vették észre, hogy ez *nem* egy teljes mondat. Tehát nem forgatták el a rácsot, csak kiolvasták a 16 betűt, pedig erre a feladat szövege igyekezett utalni. A titkosírásokban valóban létezik és használtak **egyszerű rácsot** is, amit csak egyszer kell rátenni a szövegre. Ennek használata azért nehézkes, mert előtte a letakart betűk helyére egy értelemes (félrevezető) szöveget kell írni, és a küldhető titkos szöveg (hasznos információ) is elég rövid.

v) Rácsokról sok helyen olvashatunk. Például:
https://hu.wikipedia.org/wiki/A_kriptográfia_története#Cardano_rejtjelező_rácsa . A rácsokat valóban **G. Cardano** matematikus javasolta és vizsgálta először. Dénes Tamás: *Cardano és titkosírás* cikkét is ajánljuk, amely a KöMaL 2001/6 számának 325-335.oldalain jelent meg:
http://db.komal.hu/scan/2001/09/MAT0106.PS.png.3 , http://db.komal.hu/scan/2001/09/MAT0106.PS.png.4 ,
http://db.komal.hu/scan/2001/09/MAT0106.PS.png.5 , http://db.komal.hu/scan/2001/09/MAT0106.PS.png.6 ,
http://db.komal.hu/scan/2001/09/MAT0106.PS.png.7 , http://db.komal.hu/scan/2001/09/MAT0106.PS.png.8 ,
http://db.komal.hu/scan/2001/09/MAT0106.PS.png.9 , http://db.komal.hu/scan/2001/09/MAT0106.PS.png.10 ,
http://db.komal.hu/scan/2001/09/MAT0106.PS.png.11 , http://db.komal.hu/scan/2001/09/MAT0106.PS.png.12 ,
http://db.komal.hu/scan/2001/09/MAT0106.PS.png.13

Ajánljuk még Révay Zoltán: *Titkosírások* könyvét is, Zrínyi Katonai Kiadó 1978.

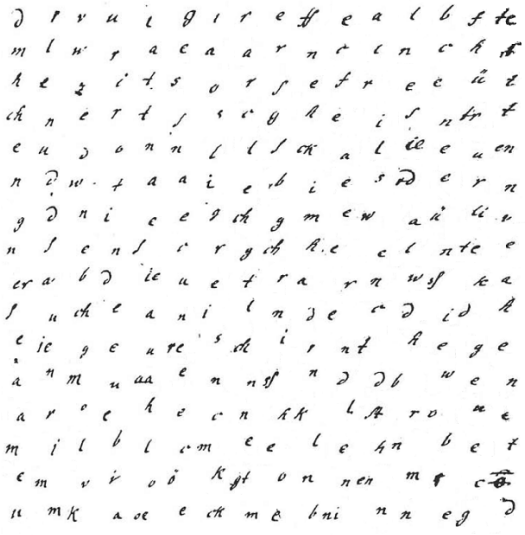
vi) Könnyű gyakorló **feladatok** a következők, megoldásukat a füzet hátulján vagy a [2] feladatgyűjteményben találjuk:

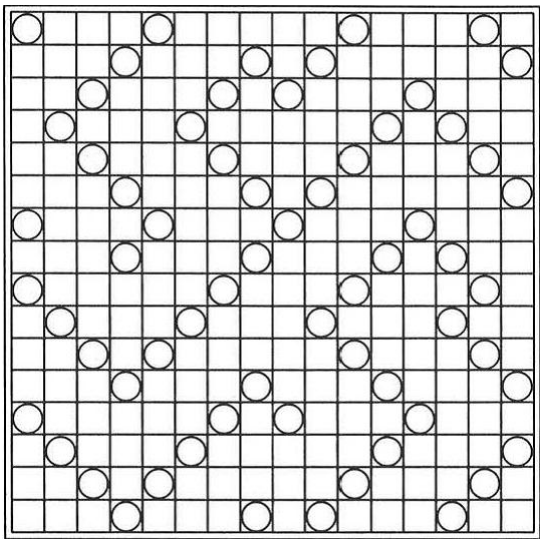
Hogyan tervezzünk saját rácsot?

Hányféle különböző $2n \times 2n$ méretű rács készíthető (n^2 számú ablakkal), és ez kb. mennyi $n = 6,8,16,$ ... esetén?

vi) Annak ellenére, hogy irodalmi alkotásokban gyakran szerepel a **forgatható rács** és használatának bemutatása (lásd alább), hiszen eléggé látványos, a gyakorlati életben alig használták (mert használata és a kulcs tárolása körülményes, pl. http://hu.wikipedia.org/wiki/A_kriptográfia_története).

vii) Pár évvel ezelőtt mégis matematikusok fejtettek meg több hónapi munkával és számítógép segítségével egy több évszázados, forgatható ráccsal készült régi szöveget, a felfedezésről és a megoldásról a https://www.tandfonline.com/doi/abs/10.1080/0161-119591883854#.VK-P8yuG8y0 és a közérthetőbb http://kripto.blog.hu/2015/01/09/grille címeken olvashatunk.
Az eredeti szöveget és a kulcsot az Olvasó szórakozására idemásoljuk, a megfejtést füzetünk végére írtuk.





Egy többszáz éves titkos szöveg és a megfejtett rács

viii) Legismertebb **Jules Verne** ("Verne Gyula") *Sándor Mátyás* című regénye, melyet számos helyen megtalál az Olvasó, mint például: Szépirodalmi Könyvkiadó, Budapest, 1960, http://mek.oszk.hu/03200/03220/03220.pdf , https://hu.wikipedia.org/wiki/Sándor_Mátyás_(regény) vagy megnézhetjük az 1979 -ben készült filmet is (2.rész), melynek körülbelül 7'00"-8'40" és 24'30"-27'35" részeiben láthatjuk a rács használatát: https://www.youtube.com/watch?v=Ia_RnM3tyqU .

ix) Erdemes még fellapoznunk **Grätzer József:** *Sicc (Szórakoztató Időtöltések, Cseles csalafintaságok)* című könyvét is, amely nem csak a rácsokról ír érdekes és hasznos tudnivalókat (első kiadás 1935, azóta több tucatnyi kiadást ért meg): https://hu.wikipedia.org/wiki/Sicc_... , vagy könyvesboltokban: https://moly.hu/konyvek/gratzer-jozsef-sicc , https://www.libri.hu/konyv/gratzer_jozsef.uj-sicc.html , https://www.antikvarium.hu/konyv/gratzer-jozsef-sicc-6345 , https://bookline.hu/product/.... .
Ajánlom még Grätzer József *Fejtorna* (1932) könyvét is: http://mek.oszk.hu/15300/15379/index.phtml .

Grätzer Józsefet "*A Rejtvénykirály*" -nek hívták, **Karinthy Frigyes** személyi titkára volt az 1920-as években: https://hu.wikipedia.org/wiki/Grätzer_József . György fia matematikus, István fia pedig bűvész-mester lett.

8.

Feladat

Egy nagy magyar író műve

A titkosításban gyakran használnak irodalmi műveket, sőt egész könyveket is. Belátható, minél ritkábbak ezek a művek (de elérhetőek) annál "erősebb", biztonságosabb kódot tudunk használni.
Elfogtunk egy üzenetet!
Annyit tudunk, hogy jelen feladatunkban egyik nagy írónk művét választották és megvan a megoldó kulcs is.
Beküldendő kódrészlet: a titkos üzenet, a megfejtésben kapott szöveg, de ügyeljünk a kis- és nagy betűkre, ékezetekre, szóközökre is!

Az üzenet szövege: (az idézőjelek nem része a szövegnek, karakterszám 1-1083)

"Édes néném, még kédnek semmi levelét nem vettem, amely nem igen jól esik nekem. De az igen jól esett, látván a köszvény, hogy nem becsüllik, a fejdelmet elhagyá, aki is ma a tatár hám látogatására mene, ugyan a tatár hám lován. Igen nagy barátsággal fogadta. Azt gondoltam elsőben, hogy majd elrabolnak bennünket; már csak azt néztem, hogy melyik kötöz meg. De ezek igen emberséges emberek; jó szívvel beszélgettek volna velünk, de oly kevés idő alatt nem leheténk tatárokká. A fejdelem elbúcsúzván a hámtól, mi is megköszönvén csak főintéssel ötatárságoknak jó akaratjokot, a szállásra menénk, és az urunknál egy szép paripát hagyának. Gondolom, hogy holnap ide hagyjuk ezt a puszta kies szomorú lakóhelyet, mivel a császár veres hintója elérkezett, amelyet urunk után küldöttek. Veresnek azért hívom, mert kívül veres posztóval vagyon béborítva, de a hintó nevet nem érdemli, mert csak kocsi. Aztot pedig négy fejér szokta húzni vagy vonni. Azokot pedig az ügettetéssel nem terhelik, mivel már azt el is felejtették, annyira megöregedtek; nyolcvan esztendőt csak adhatni a négynek."
(forrás: Magyar Elektronikus Könyvtár)

A fenti közismert levél sorai (karakterei) között fontos titkos információ rejlik. Az alábbi matematikai képletek megadják azoknak a betűknek (vagy szóközöknek) a sorszámait, amely betűket és szóközöket összeolvasva, a megadott sorrendben az üzenetet megkapjuk.

Képletek:

A*A*C+F+C , B*F*F+(C*A-B)/2 , E*E*F-B*B*C-F , (B+C)*(E+D)*C+C*F-(A+B) , B*B*C*A+B*B*F , D*E*E , (E+B*B)*B*B*A , (B*F+D-B)*(F-C)*D , A*A*A+(B+D)*F+B*D+D-B , E*E*F+B*D , B*(A*D*F+A-E) , (B+C)*(E+D)*C+C*F-B , (B*F*A)+(A-B*B)/(E-C) , C*(F-D) , (A*B+B+D)*(B*F+D) , F*(C-B)*(C+D)+(A-E) , E*(E*F+A+B-D) , F*F*(F-B)-B*B*D , D*(E*F+B)*(E/D)+B*D , A*(E-D)*(A-B)+B-D , (F+B)*(F+C)*D-(F+D+D)*(B+D) , ((F+D)*F-D)*(B+D) , B*(A*(A+C)+D) , A*A*A+B*B*F , A*(A*(B+D)-D) , B*B*F-C , A*(A+C)+D , F*(A+C)-F-B , B*B*E*(C+D)+A-F , B*D*F*F+C*(B*D+B) , A*B*F+D*D , A*(A*(A-B)+F-A)-C , A*F*B*D-(B+C+D) , A*(A*(A-B)+F-A) , (F-C)/B , (A-B)*((A-B)*(A-B)*B+C) , A*A*B*D+F-D , A*(B*A*B+A-F)+F , B*B*F*F-E .

Azt is tudjuk, milyen értékekkel kell számolnunk.

Start:

A=10, B=2, C=7, D=3, E=9 , F=11.

KÓDVETŐK
digitális oktatási műhely

A 8. feladat megoldása

Először is tanácsos a szöveget táblázatba rendeznünk, hogy a betűket könnyebben meg tudjuk számolni:

```
          12345678901234567890123456789012345678901234567890
----------+---------+---------+---------+---------+---------+--
0001-0050  Édes néném, még kédnek semmi levelét nem vettem, a
0051-0100  mely nem igen jól esik nekem. De az igen jól esett
0101-0150  , látván a köszvény, hogy nem becsüllik, a fejdelm
0151-0200  et elhagyá, aki is ma a tatár hám látogatására men
0201-0250  e, ugyan a tatár hám lován. Igen nagy barátsággal
0251-0300  fogadta. Azt gondoltam elsőben, hogy majd elraboln
0301-0350  ak bennünket; már csak azt néztem, hogy melyik köt
0351-0400  öz meg. De ezek igen emberséges emberek; jó szívve
0401-0450  l beszélgettek volna velünk, de oly kevés idő alat
0451-0500  t nem leheténk tatárokká. A fejdelem elbúcsúzván a
0501-0550   hámtól, mi is megköszönvén csak főintéssel őtatár
0551-0600  ságoknak jó akaratjokot, a szállásra menénk, és az
0601-0650   urunknál egy szép paripát hagyának. Gondolom, hog
0651-0700  y holnap ide hagyjuk ezt a puszta kies szomorú lak
0701-0750  óhelyet, mivel a császár veres hintója elérkezett,
0751-0800   amelyet urunk után küldöttek. Veresnek azért hívo
0801-0850  m, mert kívül veres posztóval vagyon béborítva, de
0851-0900   a hintó nevet nem érdemli, mert csak kocsi. Aztot
0901-0950   pedig négy fejér szokta húzni vagy vonni. Azokot
0951-1000  pedig az ügettetéssel nem terhelik, mivel már azt
1001-1050  el is felejtették, annyira megöregedtek; nyolcvan
1051-1100  esztendőt csak adhatni a négynek
----------+---------+---------+---------+---------+---------+-
```

Ha kockás papír helyett ezt is számítógéppel oldanánk meg, akkor csak **Monospaced** betűtípust használhatunk: az ilyen betűkészletekben minden betű (vízszintes) *szélessége ugyanannyi*, mint a régi írógépeknél. Ez alapján tudjuk a betűket egymás alá helyezni táblázatba, ilyen betűtípusok például a `Courier New` vagy a `Typewriter`. A szöveget nem kell begépelnünk, hiszen a feladatlapon szerepel a forrás: MEK, vagyis http://mek.oszk.hu/00800/00880/html/mikes1.htm .

A képletek "megfejtése" csak kitartó, precíz számolgatást követelt a tanulóktól. Alább az értékek mellé írtuk a szöveg megfelelő betűit ("_" a szóköz jele):

A*A*C+F+C	0718 = **c**	(B+C)*(E+D)*C+C*F-B	0831 = **v**
B*F*F+(C*A-B)/2	0276 = **s**	(B*F*A)+(A-B*B)/(E-C)	0223 = **o**
E*E*F-B*B*C-F	0852 = **a**	C*(F-D)	0056 = **n**
(B+C)*(E+D)*C+C*F-(A+B)	0821 = **p**	(A*B+B+D)*(B*F+D)	0625 = **á**
B*B*C*A+B*B*F	0324 = **a**	F*(C-B)*(C+D)+(A-E)	0551 = **s**
D*E*E	0243 = **t**	E*(E*F+A+B-D)	0972 = **_**
(E+B*B)*B*B*A	0520 = **ö**	F*F*(F-B)-B*B*D	1077 = **é**
(B*F+D-B)*(F-C)*D	0276 = **s**	D*(E*F+B)*(E/D)+B*D	0915 = **j**
A*A*A+(B+D)*F+B*D+D-B	1062 = **s**	A*(E-D)*(A-B)+B-D	0479 = **f**
E*E*F+B*D	0897 = **z**	(F+B)*(F+C)*D-(F+D+D)*(B+D)	0617 = **é**
B*(A*D*F+A-E)	0662 = **e**	**(**(F+D)*F-D**)***(B+D)	0755 = **l**

B*(A*(A+C)+D)	0346 = **k**	A*(A*(A-B)+F-A)-C	0803 = **_**
A*A*A+B*B*F	1044 = **o**	A*F*B*D-(B+C+D)	0648 = **h**
A*(A*(B+D)-D)	0470 = **r**	A*(A*(A-B)+F-A)	0810 = **í**
B*B*F-C	0037 = **_**	(F-C)/B	0002 = **d**
A*(A+C)+D	0173 = **a**	(A-B)*((A-B)*(A-B)*B+C)	1080 = **n**
F*(A+C)-F-B	0174 = **_**	A*A*B*D+F-D	0608 = **á**
B*B*E*(C+D)+A-F	0359 = **D**	A*(B*A*B+A-F)+F	0401 = **l**
B*D*F*F+C*(B*D+B)	0782 = **V**	B*B*F*F-E	0475 = **.** /pont/
A*B*F+D*D	0229 = **I**		

Tehát összeolvasva : **"Csapatösszevonás_éjfélkor_a_DVI_hídnál."**

Megjegyzések

i) Mint a legtöbb programnyelvben, az `Excel` -ben is van olyan függvény, amely megkeresi egy adott karaktersorozat adott sorszámú elemét (karakterét). Tehát **Mikes Kelemen** fenti levélrészletét bemásoljuk például az **A2** cellába (ekkor már bármilyen betűtípus megfelelő), és minden elrejtett betű esetén (azaz 39-szer) kiadjuk a **KÖZÉP(A2;x;1)** parancsot, ahol **x** a keresett karakter sorszáma (a fenti négyjegyű számok). Hát, a rengeteg kis képlet kiszámolását én inkább fejben vagy zsebszámológéppel számolgatnám ki (39-szer), minthogy begépeljem és programozzam `Excel` -ben vagy más nyelven.

ii) Bármilyen meglepő, a fenti "**könyvkód**" titkosírási módszer a könyvnyomtatás feltalálásától egészen a második világháború végéig használatban volt és egyszerűsége ellenére nagyon biztonságos. A két félnek mindössze egy könyv ugyanazon kiadású példányaira van szüksége (és persze titokban tartania): a két könyv minden oldalának mindegyik sorában ugyanazok a betűk, szavak állnak. A küldő egyszerűen megkeresi a betűket, szavakat (össze-vissza) a könyvben, és csak az oldalak, és sorok és a sorokon belül a betűk sorszámát küldi el, általában a fenti számolós matematikai műveletek nélkül. Lásd még: http://hu.wikipedia.org/wiki/A_kriptográfia_története "3.4. A könyvkódok" fejezet.

iii) Mikes Kelemen levelét nem csak azért választottuk, mert a szöveget azonnal lehet tölteni számítógépünkre a MEK honlapjáról (http://mek.oszk.hu/00800/00880/html/mikes1.htm), hanem titkon azt reméljük, hogy így talán többen kedvet kapnak elolvasására. Nem csak **Antoine Marie Jean-Baptiste Roger de Saint-Exupéry** foglalkozott művészettel a fronton, számos más művész is kénytelen volt kettős életet élni akkoriban !

Ez az oldal szándékosan üres.

9.

Feladat

Billentyű

A háború előrehaladtával a német hadsereg (Wehrmacht) folyamatosan tökéletesítette az Enigma gépet, de az angolok sorozatban fejtették meg az üzeneteket. Ezért most kézzel, emberi fantáziával kódolnak a gépek helyett.

Minden szót külön-külön kódolnak. Egy szó kódolása során a szó minden betűje helyett a billentyűzeten a billentyűtől jobbra fel, vagy balra fel, vagy jobbra le, vagy balra le lévő billentyűt nyomják meg. Egy szón belül ez az irány állandó, tehát ha a legelső betű helyett jobbra lefelé lévő billentyűt választjuk, akkor ennek a szónak az összes betűje helyett jobbra lefelé szomszédját nyomjuk meg. A következő szónál megváltoztathatjuk ezt az irányt, de ugyanezt is választhatjuk. Ha a billentyűzet szélén kellene túllépnünk, akkor aláhúzás (_) jelet nyomunk!

Például a málna szót a következő négy féle módon kódolhatjuk:
jobbra fel: kúpjw
balra fel: jpihq
jobbra le: __._y (két aláhúzás a pont előtt)
balra le: _-,_í

Vigyázat! Egy kód több szót is kódolhat a különböző irányok miatt,
például a kúpjw sorozat kódolhatja a következőket is:
balra le: málna
jobbra le: nincs ilyen szó
balra fel: ióöu2
jobbra fel: oűüi3

Feladat

Dekódoljuk az alábbi titkos üzenetet. Az egyszerűsítés miatt az üzenet magyar nyelvű és magyar nyelvű billentyűzetet használtunk, az írásjeleket külön szóként írtuk (pl. a vesszőt és a pontot nem az előző szó végéhez "ragasztottuk", hanem külön egybetűs szóként írtuk).

xőfbáx sdéy_f.y i3oo k modp,g-df-m w7 -xhy,k gőh-f 3643e_hi35 é

Beküldendő PEnigma kód: A magyar nyelvű üzenet. Ügyeljünk a helyesírásra!

A feladatban a következő billentyűzetkiosztást használtuk:

https://hu.wikipedia.org/wiki/Billenty%C5%B1zetkiosztás#/media/File:HU_Keyboard_Layout_V1_EN_Legend.svg

KÓDVETŐK
digitális oktatási műhely

www.kodvetok.com/enigma

A 9. feladat megoldása

Mint a bevezető sorok jelzik, minden kódolt szónál négy irányban lehet dekódolni. Ezeket a lehetőségeket a tanulók végigpróbálgatják (minden szónál legfeljebb 4 lehetőség) , és az értelmes szavak adják a megfejtést. A "_" jelek ugyan ismeretlen, kitalálandó karaktereket jelentenek, de a szövegkörnyezetből ezek a betűk kitalálhatóak.

Alább megadjuk a helyes dekódoló irányokat (BF = balra fel, ...) és a kapott szöveget:

```
BF      JF        JL  JL JF          BL  BF      BF     JL          JL
xőfbáx  sdéy_f.y  i3oo k modp,g-df-m w7  -xhy,k  gőh-f  3643e_hi35  é
sürgős  erős*tés  kell , körülz*rt*k az  északi  tüzér  ezred*nket .
sürgős  erősítés  kell , körülzárták az  északi  tüzér  ezredünket .
```

Tehát a megfejtés:

"Sürgős erősítés kell , körülzárták az északi tüzér ezredünket ."

Megjegyzések

i) Még Magyarországon sem egységes a Magyar billentyűzet kiosztása (főleg laptopoknál), erről a **Wikipédián** is olvashatunk: https://hu.wikipedia.org/wiki/Billentyűzetkiosztás#Magyar , és ezért adtuk meg az általunk használt billentyűzet képét: https://hu.wikipedia.org/wiki/Billentyűzetkiosztás#/.....svg

ii) Ha a kódolás ügyetlen, akkor a dekódolásnál lehetetlen megkülönböztetni a pontot (.) és a vesszőt (,), és egyéb félreértések is lehetségesek. A * -gal jelölt karaktereket ki kell találni, azonban a kódolás iránya leszűkíti a találgatások számát, hiszen * karakterek csak a billentyűzet szélén levő betűről történő "leeséskor" keletkezhetnek.

iii) A feladatot nehezíthetjük, ha hosszabb szöveget írunk, esetleg nem magyar (akár ismeretlen) nyelven, ami még életszerűbbé tenné a feladatot. Az alábbi hosszabb kódolt üzenet megoldását füzetünk végén találhatja az Olvasó:

xőfbáx sdéy_f.y i3oo k modp,g-df-m w7 -xhy,k gőh-f 3643e_hi35 k dwqi
dmgádf__áxp, nhfbíf_ím _s é ip5 jwü kűpgw d.vlb_ í ,éygsdp_m -x q6
őp4pk9e745_jo é s,ckvfh_m db_ 3h8tjq o_rt_74646 é l,pyy_í_mő éd_ív_ é

iv) A feladat valóban kitalált. Azonban valóban történtek kísérletek arra, hogy bizonyos kulcsokat a gépírók szabadon, össze-vissza gépelve találjanak ki. Azonban a gépírók általában váltott kézzel írnak a billentyűzet jobb- és bal oldalán, ezét az így előállított kódok is megfejthetők lettek, többek között a statisztikai elemzés módszerével.

10.

Feladat

Soknyelvű - a betörés

Az angol hírszerzők megszereztek egy Enigma készüléket, amivel egy üzenetet több nyelven titkosítottak (egy keresztrejtvényben), így lehetőségünk van arra, hogy megfejtsük a kódot, ami tartalmazza a központi gép helyét. Tervünk, ha sikerül, be tudunk törni az adatbázisukba és az eddigi kódrészletek megadásával megfejthetjük a PANNON ENIGMA kódját.

Az alábbi keresztrejtvény piros * jelű függőleges oszlopát írd be a

http://kodvetok.mik.uni-pannon.hu/***************

web címbe a csillagok helyére (egyik nyelven sem értelmezhető szó!).

Siess: a leggyorsabb versenyző nyeri a fődíja!

A keresztrejtvény: a megadott szavakat írd be a * -ok helyére (minden * egy-egy betű). Névelőket, ékezeteket és ragozást nem használtak, mindent kisbetűvel írtak.

A ciril betűk latin betűs átírására az alábbi táblázatot használták:

а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
A	**B**	**V**	**G**	**D**	**E**	**E**	**ZS**	**Z**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**R**	**Sz**	**T**	**U**	**F**	**H**	**C**	**Cs**	**S**	**S**	**-**	**Ü**	**-**	**E**	**Ju**	**Ja**

Vigyázat: a Ж, С, Ч, Ю és Я betűket a keresztrejtvényben két-két betűvel (két-két *) jelölték, a Ъ és Ь betűk helyett pedig egyetlen betűt (*-ot) sem írtak, a kemény és lágy betűket sem jelölték!

A keresztrejtvény:

*******	nap (égitest, oroszul),
******	főzni (németül),
******	vonat (lengyelül),
*****	barát (nem szerzetes, olaszul),
*****	ember (franciául),
***	víz (franciául),
********	őrmester (angolul),
*******	szív (testrész, oroszul),
****	nyolc (portugálul),
******	alszik/aludni (franciául),
******	kedd (szlovákul),
*******	sebesült (oroszul),
********	grófnő (angolul),
*****	felhő (németül),
****	erdő (németül).

Köszönjük, hogy velünk játszottál!

KÓDVETŐK digitális oktatási műhely

www.kodvetok.com/enigma

A 10. feladat megoldása

Az internet világában sokféle online szótár elérhető, tehát ez a feladat alkalmas volt a *gyorsaság* mérésére a döntőben. Alap-szavakat rejtettünk el, tehát a félreértéseket kizárhattuk.

A megfejtés:

`szolnce`	nap (égitest, oroszul): `солнце`
`kochen`	főzni (németül),
`pociag`	vonat (lengyelül),
`amico`	barát (nem szerzetes, olaszul),
`homme`	ember (franciául),
`eau`	víz (franciául),
`sergeant`	őrmester (angolul),
`szerdce`	szív (testrész, oroszul): `сéрдце`
`oito`	nyolc (portugálul),
`dormir`	alszik (franciául),
`utorok`	kedd (szlovákul),
`ránenüj`	sebesült (oroszul): `páненый`
`countess`	grófnő (angolul),
`wolke`	felhő (németül),
`wald`	erdő (németül),

tehát összeolvasva:

`occimuretronull`

vagyis az internetcím: http://kodvetok.mik.uni-pannon.hu/occimuretronull

(A honlap még megjelenik, de nem működik, legutoló hozzáférés 2018. június 13.)

Megjegyzések

i) A feladat és a keresztrejtvény inkább a háborút lezáró, a különböző anyanyelvű katonák barátkozását illusztrálja, de a feladat a szerverre való "bejutás", a megoldások feltöltése volt.

ii) Soha ne feledjük (még a fordítógépek korszakában sem): *Ahány nyelvet beszélsz, annyi embert érsz.* Nagyon sok titkosírás megfejtésének egyik fő eszköze a sok nyelv ismerete (szavak, nyelvtan, statisztika) volt. Egy nagyon tanulságos történet (TV riport egy túlélővel, kb. 20 évvel ezelőtt) a következő: 1944-45 telén orosz katonák magyar hadifoglyokat kísértek hosszú heteken keresztül. Utánpótlás hiányában meg kellett szabadulniuk a hadifoglyoktól, tehát falhoz állították őket és felhúzták a puskák ravaszait. Hirtelen jött ötlettől az egyik egyetemista kilépett, és hangosan, hosszan rákezdte:

" *Я вас люблю (к чему лукавить?), Но я другому отдана; Я буду век ему верна.* ..... "

(**Puskin**: Anyegin, részlet).

A katonák elcsodálkoztak: "*ezek a vad magyarok nem csak beszélnek oroszul, hanem irodalmi költemé-nyeket is elszavalnak*?", és leeresztették puskáikat ...

Ez az oldal szándékosan üres.

Megoldások

1B. Feladat:

```
24.                    znnseppdgqekönvgjoiwéwsk   (s+s=k)
23. /vissza s -el /    znnseppdgqekönvgjoiwéwss   (i+i=s)
22. /vissza i -vel/    znnseppdgqekönvgjoiwéwii   (y+y=w)
21. /vissza y -al /    znnseppdgqekönvgjoiwéykk   (p+p=é)
20. /vissza p -vel/    znnseppdgqekönvgjoiwphüü   (y+y=w)
19. /vissza y -al /    znnseppdgqekönvgjoiyrjww   (r+r=i)
18. /vissza r -el /    znnseppdgqekönvgjorf_see   (u+u=o)
17. /vissza u -val/    znnseppdgqekönvgjuxméykk   (e+e=j)
16. /vissza e -vel/    znnseppdgqekönvgeösgatéé   (q+q=g)
15. /vissza q -val/    znnseppdgqekönvqoyáqjböö   (k+k=v)
14. /vissza k -val/    znnseppdgqekönkécnqézrdd   (f+f=n)
13. /vissza f -el /    znnseppdgqeköfdzwfjzskxx   (g+g=ö)
12. /vissza g -vel/    znnseppdgqekgzwrözbrkcpp   (s+s=k)
11. /vissza s -el /    znnseppdgqesöfdzwfjzskxx   (b+b=e)
10. /vissza b -vel/    znnseppdgqbpmdáwudgwphüü   (h+h=q)
 9. /vissza h -val/    znnseppdghugdvtolvzog_mm   (q+q=g)
 8. /vissza q -val/    znnseppdqrcqnebxüehxqivv   (ö+ö=d)
 7. /vissza ö -vel/    znnseppöáboáypnhéptháuff   (ü+ü=p)
 6. /vissza ü -vel/    znnsepüufgtfcüsnküynfzll   (ü+ü=p)
 5. /vissza ü -vel/    znnseü_zlmylh_xsp_csldqq   (b+b=e)
 4. /vissza b -vel/    znnsbsxwijviéxüpnxapiáoo   (i+i=s)
 3. /vissza i -vel/    znnition_am_wolfdorf_see   (f+f=n)
 2. /vissza f -el /    znfbmbgftuétpge_xgk_tlyy   (f+f=n)
 1. /vissza f -el /    zf_véva_mnzmiaytqadtmerr   (m+m=z)
 0. /vissza m -el /    munition_am_wolfdorf_see .
```

Tehát a megoldás: **munition_am_wolfdorf_see (**lőszer a farkasfalu tónál**) .**

Megjegyzés: Vegyük észre, hogy ez a hosszabb *kódolt* szöveg eleje tartalmazta a kitűzött, rövidebb kódolt szöveget (vagyis a rövidebb szöveg **kezdőszelete** a hosszabbnak), és ennek megfelelően a visszafejtett, *kódolt* hosszabb szövegnek is eleje a rövidebb szöveg. Gondoljuk meg, hogy a kódolás folyamata miatt ez így van rendjén.

3B. Feladat:

b) Minden **Á** átlós jobbra-le lépés feleslegessé tesz / kizár egy **L** és egy **J** lépést. Tehát, ha az átlós lépések száma **i** , akkor az **L** és **J** lépések száma 7-**i** , az összes lépés száma pedig i+7-i+7-i=14-i . Továbbá ezen esetekben **Á, L** és **J** lépéseink sorrendjének száma kell, amik ismét ismétléses permutációk. Részletesebben:

ha 0 db Á lépésünk van (i=0), akkor $m_0 = P_{14}^{7,7\,(ism)} = 14! / (7!*7!) = 3\,432$,
ha 1 db Á lépésünk van (i=1), akkor $m_1 = P_{13}^{1,6,6\,(ism)} = 13! / (1!*6!*6!) = 12\,012$,
ha 2 db Á lépésünk van (i=2), akkor $m_2 = P_{12}^{2,5,5\,(ism)} = 12! / (2!*5!*5!) = 16\,632$,
ha 3 db Á lépésünk van (i=3), akkor $m_3 = P_{11}^{3,4,4\,(ism)} = 11! / (3!*4!*4!) = 11\,550$,
ha 4 db Á lépésünk van (i=4), akkor $m_4 = P_{10}^{4,3,3\,(ism)} = 10! / (4!*3!*3!) = 4\,200$,
ha 5 db Á lépésünk van (i=5), akkor $m_5 = P_9^{5,2,2\,(ism)} = 9! / (5!*2!*2!) = 756$,
ha 6 db Á lépésünk van (i=6), akkor $m_6 = P_8^{6,1,1\,(ism)} = 8! / (6!*1!*1!) = 56$,

ha 7 db Á lépésünk van (i=7), akkor $m_7 = P_7^{7,0,0\ (ism)} = 7!\ /\ 7! = 1$,
összesen: $m_0 + ... + m_7 =$ **<u>48 639</u>** .

c) Tehát a király a **K** mezőből kíván eljutni a **Q** mezőre az a) feladathoz hasonlóan, de az "**a**" mezőről nem léphet át a "**b**" mezőre, és hasonlóan a **c** mezőről sem léphet át a **d** mezőre. Ez azt jelenti, hogy az a) részben kapott megoldásból ki kell vonnunk azokat az útvonalakat, amelyek vagy az **a-b**, *vagy* a **c-d** közötti piros vonalon áthaladnak. Tehát

(megoldás **c)** = (megoldás **a)** - (áthalad **a-b** -n) - (áthalad **c-d** -n) + (áthalad **a-b** -n *és* **c-d** -n is)

hiszen azon útvonalakat majdnem kétszer vontuk ki, amelyek áthaladnak mind **a-b** -n és **c-d** -n is!

a-b -n áthaladó útvonalak: eljut K -ból **a** -ba (akárhogyan), majd akárhogyan továbbmegy b -ből Q -ba. Ezekre pedig használhatjuk az a) rész gondolatmenetét a K-a és b-Q kisebb méretű sakktáblákra, tehát

a-b -n áthaladók = (K-a)*(b-Q) = $P_5^{2,3\ (ism)} * P_8^{4,4\ (ism)} = 5!/(2!*3!) * 8!/(4!*4!) = 700$,

c-d -n áthaladók = (K-c)*(d-Q) = $P_{10}^{5,5\ (ism)} * P_3^{2,1\ (ism)} = 10!/(5!*5!) * 3!/(2!*1!) = 756$,

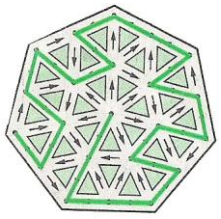
a-b -n *és* **c-d** -n áthaladók = (K-a)*(b-c)*(d-Q) = $P_5^{2,3\ (ism)} * P_4^{2,2\ (ism)} * P_3^{2,1\ (ism)} =$

$= 5!/(2!*3!) * 4!/(2!*2!) * 3!/(2!*1!) = 180$,

tehát

(megoldás **c)** = 3432 - 700 - 756 + 180 = **<u>2156</u>** .

4B. Feladat:



5. Feladat:

KAVAHO	KAGA	KEV	KEW	KIMA	KMALE	KOGH	KOJI	KTI	KUCE	KUG	KUJU
1.mondat	o	o	x	x	o	x	x	o	o	o	o
2.mondat	x	x	x	x	x	x	o	o	o	o	x
3.mondat	o	x	x	x	x	o	x	x	x	x	x
4.mondat	x	x	o	x	o	x	o	x	x	o	x
5.mondat	x	x	o	o	x	x	x	o	x	x	o
bináris	26	30	7	15	22	27	21	12	28	20	14

MAGYAR	ajtó	eldug	esik	hat	hideg	holnap	király	nagy	öt	virág	vonat
1.mondat	x	x	o	o	o	o	o	x	o	x	o
2.mondat	x	x	x	o	x	o	o	o	x	x	x
3.mondat	o	x	x	x	o	x	x	x	x	x	x
4.mondat	x	x	o	o	x	x	x	o	x	o	x
5.mondat	x	o	x	x	x	o	x	x	x	o	o
bináris	27	15	22	20	26	12	28	21	30	7	14

Tehát:

ajtó =KOGH(27), eldug =KIMA(15), esik =KMALE(22), hat =KUG (20),
hideg=KAGA(26), holnap=KTI (12), király=KUCE (28), nagy=KOJI(21),
öt =KEV (30), virág =KEW (7), vonat =KUJU (14).

És így a megfejtés (a Kavaho szavakat betűrendbe kell tennünk!):

`Eldugtunk öt nagy hideg királyt. =` **`KAGA KEV KIMA KOJI KUCE.`**

6.B Feladat

Minden programsor után írtuk az eltelt időt **összesítve**.

d) változat:

```
FOR i=1 TO 4 ELORE;                                          =  4
BAL; ELORE;                                                +  1  =  5
FOR i=1 TO 6 (ELORE, ELORE, JOBB);                         + 12  = 17
BAL, BAL, ELORE;                                           +  1  = 18
FOR i=1 TO 3 (ELORE, JOBB);                                +  3  = 21
JOBB, JOBB; FOR i=1 TO 3 ELORE;                            +  3  = 24 /"P11 négyzet"/
FOR i=1 TO 4 (JOBB; FOR j=1 TO i ELORE;);  +1+2+3+4 =      + 10  = 34
FOR i=1 TO 7 (BAL, ELORE, ELORE);                          + 14  = 48 /"P10 négyzet"/
ELORE; BAL;                                                +  1  = 49
FOR i=1 TO 4 (JOBB; FOR j=1 TO 10 ELORE;);                 + 40  = 89
FOR i=1 TO 8 ELORE;                                       +7 +1  = 96 /USA/ +1
BUMM!                                                      = ez már nem lesz !
```

A legfőbb baj, hogy nem tudjuk a robot indítási helyét és irányát, a 24. és 48. órák végén sem jegyezték fel az irányát, csak a helyeket, ezért a következő nyomozást ajáljuk.

Egyik lehetséges megoldás, hogy a **P11** négyzetből elindítjuk a robotot *valamilyen irányban*, a program hatodik sorától a nyolcadik soráig (25-48.órák), és megnézzük, hogy a robot így a **P10** négyzetbe jutott-e. Ha igen, akkor folytathatja útját, és megkaphatjuk a megoldást. Ha nem, akkor visszamegyünk a **P11** négyzetbe, és a robotot más irányban indítjuk el, ismét a program hatodik sorától a nyolcadik soráig (24-48.órák). A négy égtáj valamelyike jó lesz, tehát a diáknak legfeljebb csak négyet kell próbálkoznia.

A következő **trükkel** megszüntethetjük a próbálkozásokat. Készítsünk egy legalább 26×26 négyzetből álló, a térképpel megegyező négyzetekre osztott, **átlátszó papírra** (pl. pausz vagy átütő) négyzetrácsot, erre *ne* írjuk fel az A…Z és 01…26 koordinátákat. Az átlátszó papír *valamelyik* négyzetéről (pl. közepéről) indítsuk el a robotot a program negyedik sorától a hatodik soráig (24-48.órák). Természetesen jelöljük meg az indulási helyet és irányt (24.óra) és a 48. órában elfoglalt négyzetet és irányt is. Ekkor az átlátszó rajzot tegyük az eredeti térképre úgy, hogy a 24. órában elért négyzet éppen a térkép **P11** négyzetére essen, a 48. órában elfoglalt mező pedig pontosan a **P10** négyzetre. Így megkapjuk a számunkra legfontosabb információt: a robot merre néz a **P10** négyzetben a 48. órában. Ezután folytathatjuk a robot útját a program *kilencedik sorától* !

A végeredmény és a beküldendő **Penigma** kód:

c) változat:

Aprobléma (két négyzet de irány nélkül) és megoldása ugyanaz, mint a d) esetben.
Mivel a robot útja a 24. óra után ugyanaz, mint az a) és b) esetben, ezért a végeredmény és a beküldendő **Penigma** kód is ugyanaz: **+A22** .

b) változat:

A legfőbb baj, hogy nem tudjuk a robot indítási helyét és irányát, de ez nem is kell. Ugyanis a felderítés szerint a 24. óra végén az **N15** négyzetben van és Dél felé néz. Vagyis a program első három sorát nem kell elolvasnunk, a robot mozgását a negyedik sortól kell figyelemmel követnünk. Innen a megoldás ugyanaz, mint az a) esetben, a beküldendő **Penigma** kód is ugyanaz: **+A22** .!

a) változat:

Tehát tudjuk, hogy az indulási mező Z15, irány Észak (↑). Mindössze csak a programot kell végig lépegetnünk, és a 96**.** órában megnézni, hol és mi fog történni. A [ ] zárójelekbe beírtuk annak a mezőnek a kódját, ahol a robot lesz a parancssor végrehajtása után, és a nyilak (↑,↓,→,←) mutatják, hogy a robot ekkor merre néz.

```
[Z15↑]
FOR i=1 TO 8 ELORE;                                    [R15↑]          8.óra
BAL; FOR i=1 TO 6 (ELORE, ELORE, JOBB);                [P13→]         20.
BAL, ELORE, JOBB, ELORE, BAL, ELORE, JOBB, ELORE;      [N15→]         24.
ELORE, BAL, ELORE, JOBB, ELORE, JOBB, ELORE;           [N17↓] +  4   = 28
FOR i=1 TO 7 (BAL, ELORE, ELORE);                      [L17←]+ 14   = 42
FOR i=1 TO 3 (JOBB, ELORE, BAL, ELORE);                [I14←]      +  6   = 48
ELORE, BAL, ELORE, JOBB, ELORE, ELORE;                 [J11←]      +  4   = 52
FOR i=1 TO 5 (ELORE, JOBB, ELORE, BAL, ELORE);         [E01←]       + 15   = 67
BAL, BAL, ELORE, ELORE, ELORE;                         [E04→]      +  3= 70
FOR i=1 TO 4 (ELORE, BAL, ELORE, JOBB, ELORE);         [A12→]       + 12   = 82
FOR i=1 TO 4 (ELORE, JOBB);                            [A12→]      +  4   = 86
FOR i=1 TO 11 ELORE;     ### 10 lépés után:            [A22→]       + 10   =96.óra
                         ### robot megsemmisítve!                   /USA BUMM/
BUMM!                                          = ### ez már nem lesz !!!
```

Tehát a beküldendő **Penigma** kód: **+A22** .

7.A Feladat

Az ábrán látható rácsot úgy kell elforgatnunk, hogy a jobb alsó sarokban levő lyuk (köz) a bal felső sarokba kerüljön, tükröznünk nem kell. Az összeolvasott mondat, német helyesírással (szóközökkel):

`Ein und zwanzig neue Unterseeboote fahren nach Schottland nächste Woche ab.`

(Huszonegy új tengeralattjáró indul el a jövő héten Skócia felé.)

7.B Feladat

Az könnyen kiszámolható, hogy egy $2n \times 2n = 4n$ méretű rácsból n helyen kell ablakot vágnunk, hogy a négy forgatás alatt mind a $4n$ betűt el tudjuk olvasni. Arra kell ügyelnünk, hogy a négy forgatás során egyik ablak se kerüljön olyan kis négyzetre, amelyre már egy másik ablak valamikor "rákerült". Ezt az ütközést kettő módon is el tudjuk kerülni.

Egyik megoldás, hogy ha választunk egy ablakot, akkor azonnal forgassuk el a rácsot és jelöljük meg, hogy a választott ablak a négy forgatás folyamán mely másik (négy) kis négyzetre fog kerülni. Ezután olyan ablakot (kis négyzetet) választunk, amely különbözik az eddig kiválasztott és megjelölt kis négyzetektől, ennek is megjelöljük a forgatáskor elfoglalt helyeit, és így tovább.

Másik megoldás: könnyen észrevehetjük, hogy a nagy négyzet bal felső, $n \times n$ méretű negyede (az alábbi ábrán a fekete betűk) a forgatások folyamán három másik, szintén $n \times n$ méretű negyedekbe fognak kerülni, ezeket a negyedeket különböző színekkel jelöltük. Sőt, az azonos betűk (**A,B,C**,...) csak egymás között vándorolnak: az A betűk csak A betűvel jelölt kis négyzetekre kerülhetnek, stb. Tehát saját rácsunkat a következő módon tervezzük és készítjük el: kivágjuk a négy **A** betű közül az egyiket (bármelyiket), kivágunk pontosan egy **B** betűt (bármelyiket), és így tovább.

```
ABCDEUPKFA
FGHIJVQLGB
KLMNOWRMHC
PQRSTXSNID
UVWXYYTOJE
EJOTYYXWVU
DINSXTSRQP
CHMRWONMLK
BGLQVJIHGF
AFKPUEDCBA
```

7.C.Feladat

Tekintsük a nagy, négyzet $2n \times 2n$ -es bal felső részén levő n^2 kis négyzetet. Ezek elforgatottjai egyszeresen kiadják a nagy négyzet összes négyzetét. Továbbá, ha ezen n^2 kis négyzet bármelyikét helyettesítjük az ő $+90^o$, $+180^o$ vagy $+270^o$ -os elforgatottjával, akkor szintén jó rácsot kapunk, sőt így az összes rácsot megszerkeszthetjük. Tehát a készíthető rácsok száma 4^{n^2} (kitevőben n^2).

Például: $4^{2\wedge 2} = 256$ (4×4 -es rácsok), $4^{3\wedge 2} = 262\ 144$ (6×6 -os rácsok), $4^{4\wedge 2} = 4\ 294\ 967\ 296$ (8×8 -as rácsok), ...

7.D Feladat

"*die franszosen sind laut eingegangener erkundigung und nach richt von camberg abmarchiret es sollen aber dem verlaut nach andere an deren stelle einrucken vielleicht fürchten sie das en gelische bier welches ihnen wohl übel bekommen durfte wan es recht getruncken wird ich wünschet dass sie die rechte maass be kommen mögten [Trennungszeichen] koenig*."

9.B Feladat

```
BF     JF       JL  JL JF         BL  BF     BF    JL        JL JL
xőfbáx sdéy_f.y i3oo k modp,g-df-m w7 -xhy,k gőh-f 3643e_hi35 k dwqi
sürgős erős*tés kell , körülz*rt*k az északi tüzér ezred*nket , csak
sürgős erősítés kell , körülzárták az északi tüzér ezredünket , csak

 BF           JF       JF BL JL  BL  BL    BF    JF JF       BF JL
dmgádf__áxp, nhfbíf_ím _s é ip5 jwü kűpgw d.vlb_ í ,égygsdp_m -x q6
ejtőer**ősök juthat*ak *e . két nap múlva elfog* a lőszerü*k és az
ejtőernyősök juthatnak be . két nap múlva elfogy a lőszerünk és az

 BL           BL JF       BF   JL    BL         BL JF         JF    BL
őp4pk9e745_jo é s,ckvfh_m db_ 3h8tjq o_rt_74646 é l,pyy_í_mő éd_ív_ é
élelmiszer*nk . elfogtu*k eg* enigma k*df*zetet . plüss*a*kó őr*ag* .
élelmiszerünk . elfogtunk egy enigma kódfüzetet . plüssmackó őrnagy .
```

Jelölések:

JL = jobbra le, JF = jobbra fel, ... (a dekódolás lépései),
 * = ismeretlen, kitalálandó karakter

Hivatkozások

[0] **Wikipédia**, https://hu.wikipedia.org

[1] **Szalkai István:** *Diszkrét matematika és az algoritmuselmélet alapjai*, Veszprémi Egyetemi Kiadó, 2001, ISBN 0 202001 000700. Javított kiadás: 2006, ISBN 0202006000194.

[2] **Szalkai István:** *Diszkrét matematika feladatgyűjtemény* Veszprémi Egyetemi Kiadó, 1997.

Tolóka (csúszka):

. kivágni . . CUT . . . . . .

abcdefghijklmnopqrstuvwxyz
aábcdeéfghijklmnoöpqrstuüvwxyz
aábcdeéfghiíjklmnoóöőpqrstuúüűvwxyz

. kivágni . . CUT . . . . . .

A **test** a következő oldalon van.

Ez az oldal szándékosan üres.

. kivágni . . CUT . . . .

_zyxwvutsrqponmlkjihgfedcba_zyxwvüutsrqpöonmlkjihgféedcbáa_

_zyxwvüutsrqpöonmlkjíihgféedcbáa_zyxwvüutsrqpöonmlkjíihgféedcbáa_

_zyxwvűüúutsrqpőöóonmlkjíihgféedcbáa_zyxwvűüúutsrqpőöóonmlkjíihgféedcbáa_

10987654321098765432109876543210987654321098765432109876543210980123456

- hajtani - FOLD -

- hajtani - - FOLD -

1 2 3 4 5 6

0123456789012345678901234567890123456789012345678901234567890123456789

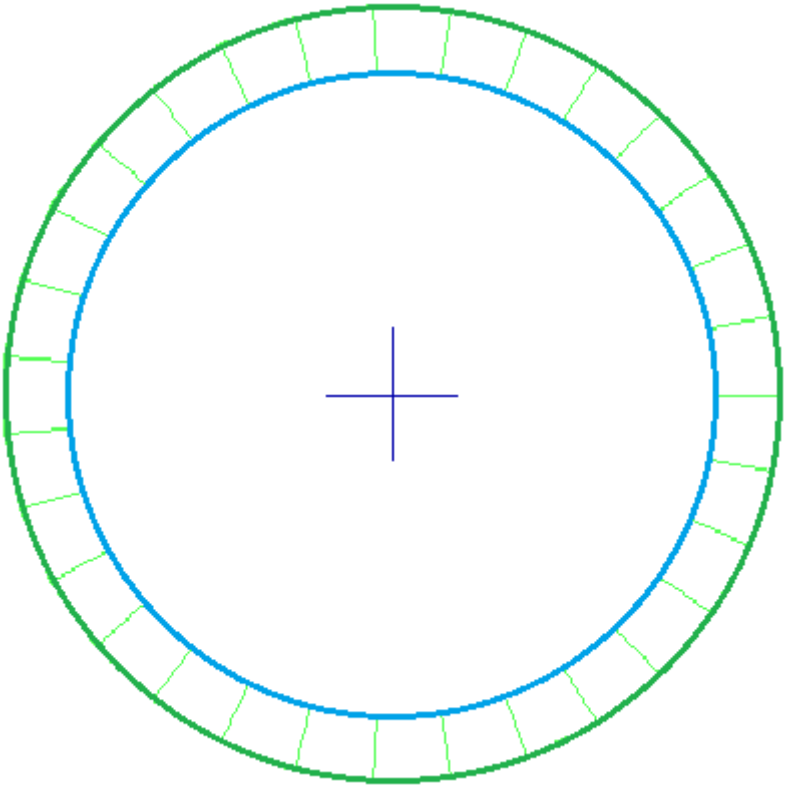
_abcdefghijklmnopqrstuvwxyz_abcdefghijklmnopqrstuvwxyz_

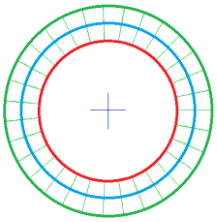
_aábcdeéfghijklmnoöpqrstuüvwxyz_aábcdeéfghijklmnoöpqrstuüvwxyz_

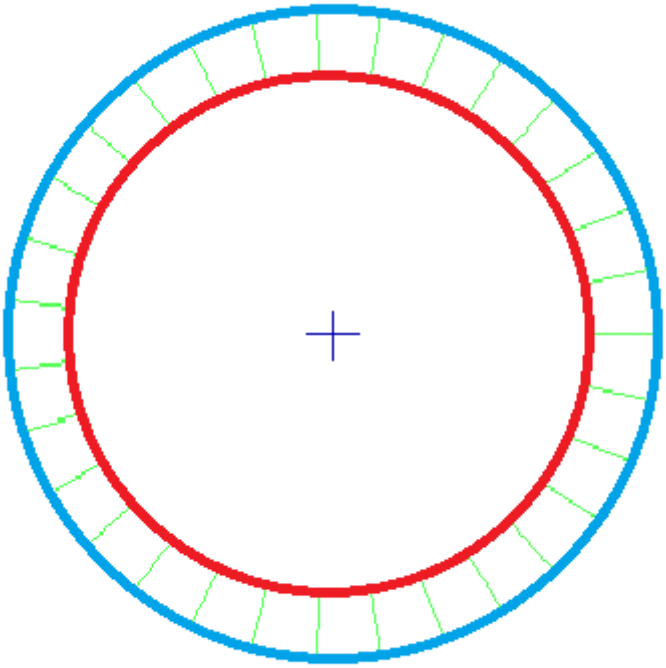
_aábcdeéfghiíjklmnoóöőpqrstuúüűvwxyz_aábcdeéfghiíjklmnoóöőpqrstuüvwxyz_

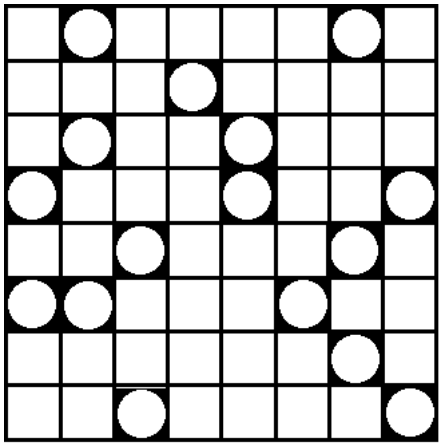
. kivágni . . CUT . . . .

Ez az oldal szándékosan üres.









Az 1. feladat dekódoló köre

A 7. feladat dekódoló rácsa

Ez az oldal szándékosan üres.

Ez az oldal szándékosan üres.

Bevezető:

1940-et írunk, a második világháború korát. A német fasiszta hadsereg elfoglalta Európát, a dunkerque-i kudarc után az Egyesült Királyság egyedül áll szemben az óriási méretű náci haderővel. Megpróbálják elfoglalni a brit szigeteket, de hősies harc árán megállítják a német erőket. A fasiszta hadvezetés taktikát vált, és több száz modern tengeralattjárót állít szolgálatba az Atlanti-óceánon, azzal a szándékkal, hogy elzárja a külvilágtól a brit szigeteket. A tengeralattjárókra, titkosító berendezéseket, az ENIGMA-kat helyezik el, amik segítségével farkas falkákban vadásznak a brit hajó-karavánokra. Sikerrel. Szinte felfoghatatlan pusztítást visznek végbe. Angliában, Skóciában és Írországban fogytán vannak a készletek, már csak korlátozott mennyiségben, jegyre kapnak az emberek élelmiszert, felüti a fejét a kétségbeesés.

Az angol katonai kódfejtők a Bletchley parkban (a brit kódfejtők központja) hiába próbálják megfejteni a titkosított német üzeneteket, nem járnak sikerrel, hiába dolgoznak ott a legkiválóbb tudósok, mégsem boldogulnak. Ekkor lép színre Alan Turing, aki belátja az emberi elme korlátosságát, ezért egy számítógépet tervez, majd épít, amivel 1942-ben megfejtik a tengeralattjárók üzeneteit. Onnantól kezdve nincs előnyük a német hajóknak, elfogják és elsüllyesztik azokat.
A hadi szerencse megfordul!

Mentsd meg Angliát a pusztulástól! Törd fel az ENIGMA kódját!
Állítsd meg a tengeralattjárók farkasfalkáit!

A puskázás nem tilos, sőt ajánlott, de vigyázz, lehet, hogy más rosszul oldotta meg a feladatokat és akkor Te sem tudsz regisztrálni!

A játékmenet:

Elhelyeztünk az Interneten egy kód-sorozatot: valahol, valamit, ezt neveztük el PANNON ENIGMA-nak. Amit meg tudsz fejteni, de csak akkor, ha megszerezted azt a kódsorozatból álló megfejtő kulcsot, amivel fel lehet törni (megfejteni). Ezenkívül kapsz még egy információt a feladványok eredményeként, azt, hogy hol van elrejtve a PANNON ENIGMA.

A megfejtő kulcs megszerzése: két hetente publikálunk egy feladványt, ami lehet egy kódfejtés, keresztrejtvény, matematikai példa, programozási feladat vagy kevésbé ismert történelmi rejtvény. Egy biztos, a megfejtéshez számítógépet kell használnod! Minden rejtvény megoldása egy kódrészletet tesz hozzá a kulcshoz. A kódrészleteket, sorba rendezve, összefűzve kiadják azt a kulcsot, amire szükséged van!

Mikor összeállítottad a megfejtő kulcsodat, az utolsó heti feladvány eredménye tartalmazza azt a „helyet" ahol használni kell azt, tehát megtalálhatod a PANNON ENIGMA-t. Már csak az a dolgod, hogy a helyes megoldó kulcsot használva törd fel és regisztráld magad a PANNON ENIGMA-ban.

KÓDVETŐK
digitális oktatási műhely

www.kodvetok.com/enigma