Elemi matematika 1.
TIKOSÍRÁSOK

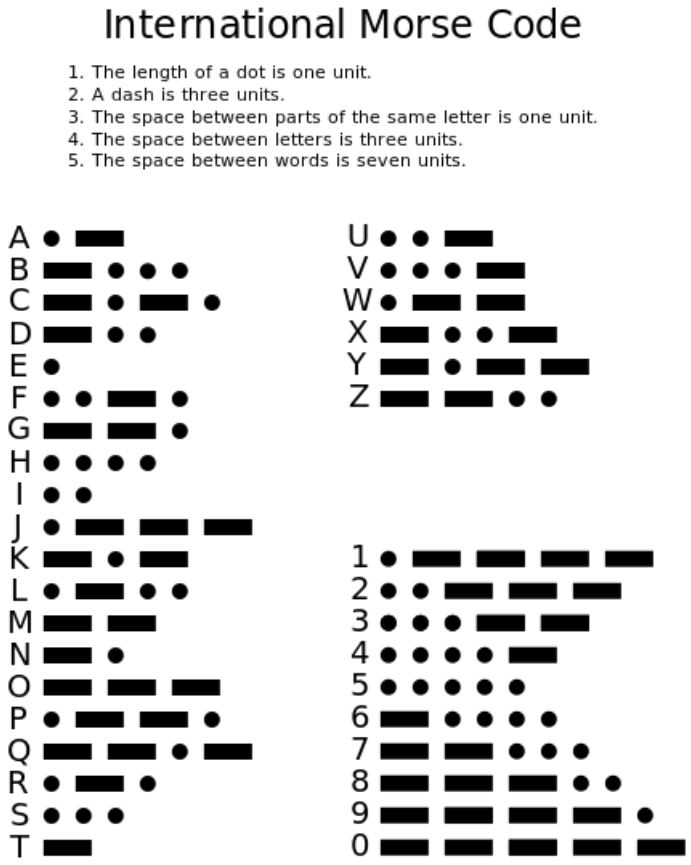
1. TITKOSÍTÁSOK?

A rövid idő alatt, nagy távolságra való üzenettovábbítás régóta fontos célja az embernek. A pontos továbbítás mellett általában az is kiemelten fontos, hogy a címzetten kívül más ne férhessen hozzá az üzenet tartalmához.

1. Feladat. Milyen „ősi" titkosítási, adattovábbítási módokat ismerünk?

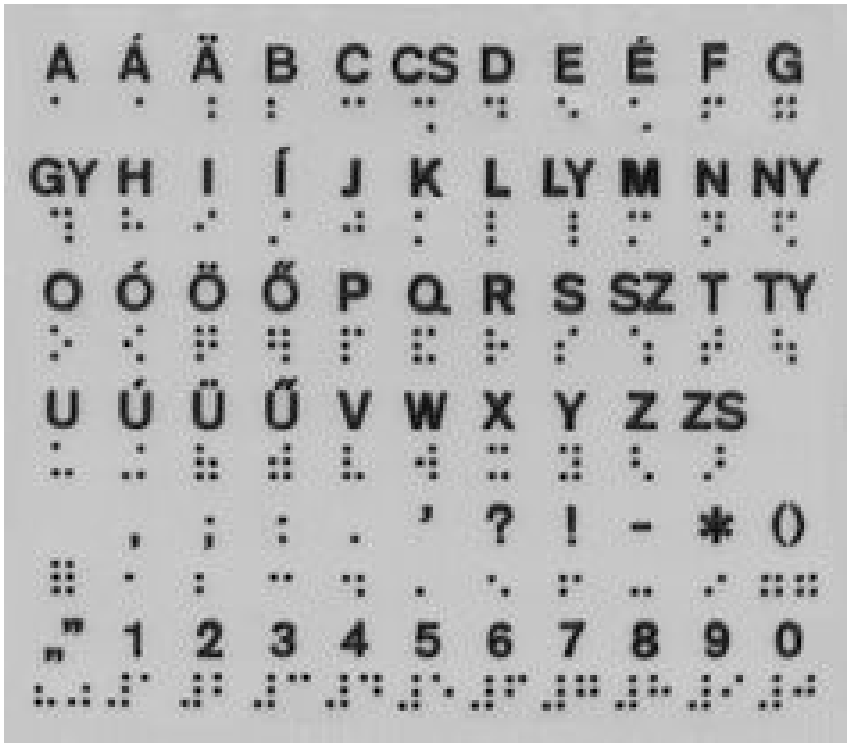
2. Feladat. Milyen, a mindennapokban használt „titkosításokat" ismerünk? (Itt titkosítás alatt értünk olyan üzenetkódolási eljárásokat is, amelyek célja nem a titkolózás, hanem épp ellenkezőleg, a mások számára történő hozzáférés, az üzenet gyors továbbítási lehetőségének biztosítása.)

3. Feladat. Milyen előnye, hátránya van az alábbi „titkosítási" eljárásoknak? Mi a közös bennük?



(a) Morse-abc
Mitől függhet az egyes betűkhöz tartozó jelsorozat hossza, bonyolultsága?

(b) Jelnyelv 

(c) Braille-írás 

2. Ládák, bírók, prímek

4. Feladat. A üzenetet akar küldeni B-nek. Van egy le- és feltörhetetlen lakattal záródó ládájuk, egyetlen hozzá tartozó kulccsal. Mit tegyenek?

5. Feladat. Mit tegyenek, ha B bizalmatlan, s szeretne megbizonyosodni arról, hogy az üzenet valóban A-tól jött, de van két az előzőhöz hasonló lakatjuk is?

6. Feladat. A és B sakkozik, a mérkőzést félbe kell szakítani. Mit tegyenek, hogy másnap igazságosan tudják folytatni a mérkőzést (Azt kell megakadályozni, hogy az, aki lépésre következne egész éjjel tudjon gondolkodni a következő lépésén, jelentős előnyhöz jutva ezzel.), ha

(a) személyesen, egy asztalnál ülve,

(b) online játszanak? (`PrimeQ[expr]`, `FactorInteger[n]`...)

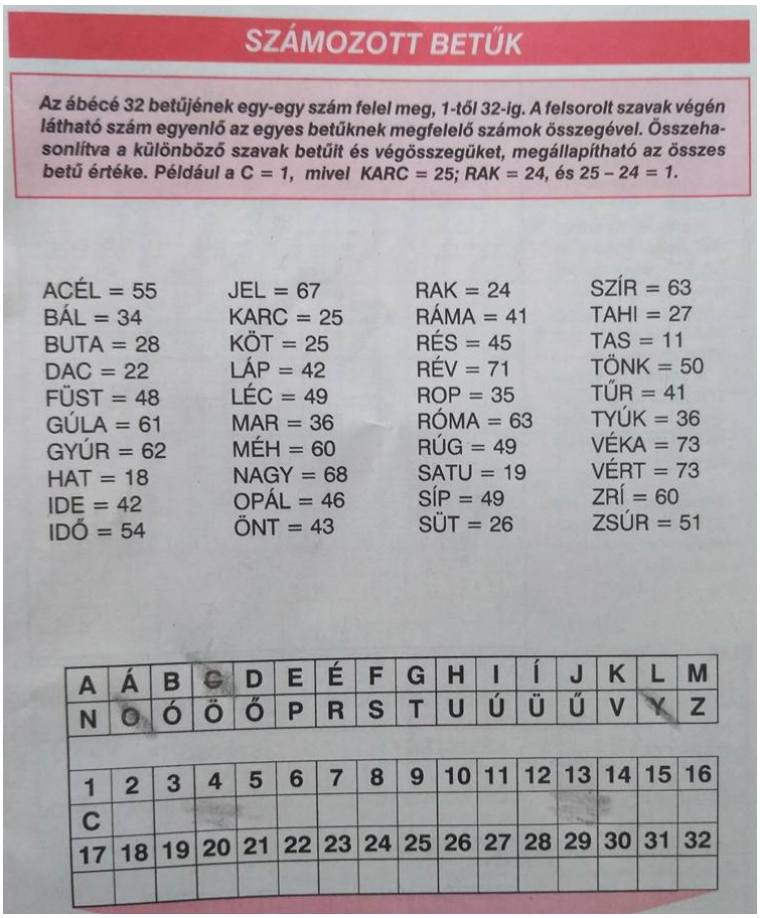
3. Számok kódolása

7. Feladat. A egy bináris (csak 0 és 1-ből álló) üzenetet akar küldeni B-nek. Az üzenet a következő: `01010011 01011010 01001001 01000001`. Ezt úgy titkosítja, egy reményeik szerint csak B által ismert kulccsal, hogy ehhez a kettes számrendszerbeli számhoz hozzáad `1011011101111`-et (ez a kulcs). B az összeget kapja.

(a) Hogyan tudja B visszafejteni az üzenetet?
(b) Mit küld A?
(c) Hogyan lehet csökkenteni a küldött üzenet hosszát, ha csak számokat továbbíthatunk?
(d) Hogyan lehet csökkenteni az üzenet megfejtésének esélyét?
(e) Mi lehetett az eredeti üzenet? (Tényles jelentéssel bíró szöveget várunk. Talán segít: `https://hu.wikipedia.org/wiki/ASCII`)

4. Rejtvények

8. Feladat. Oldjuk meg az alábbi rejtvényt!



SZÁMOZOTT BETŰK

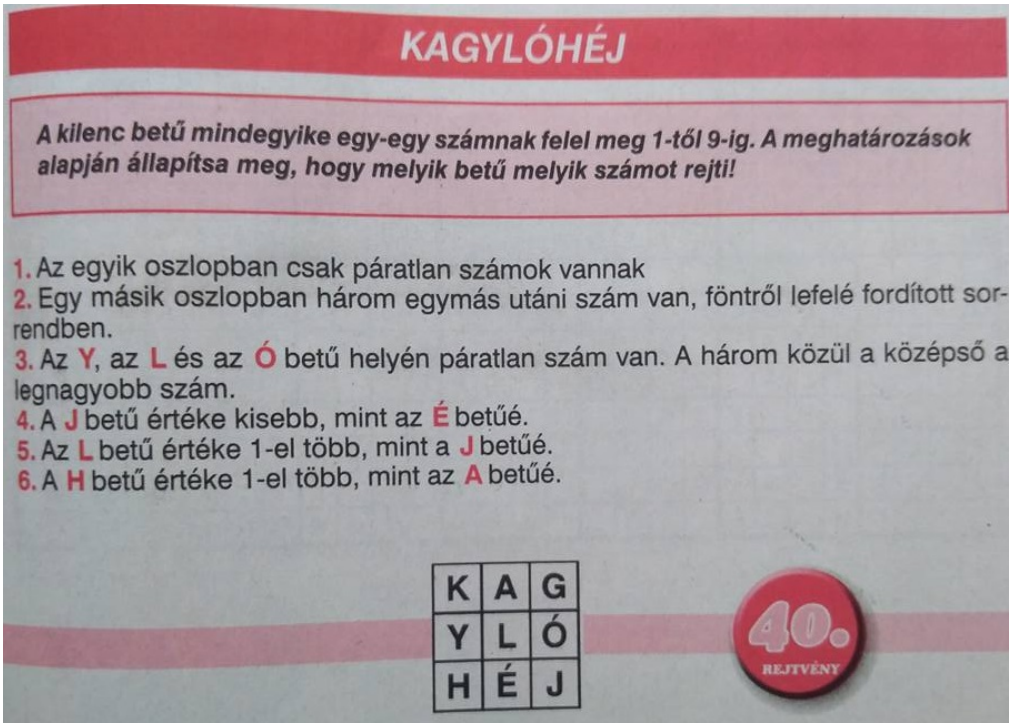
Az ábécé 32 betűjének egy-egy szám felel meg, 1-től 32-ig. A felsorolt szavak végén látható szám egyenlő az egyes betűknek megfelelő számok összegével. Összehasonlítva a különböző szavak betűit és végösszegüket, megállapítható az összes betű értéke. Például a C = 1, mivel KARC = 25; RAK = 24, és 25 – 24 = 1.

ACÉL = 55
BÁL = 34
BUTA = 28
DAC = 22
FÜST = 48
GÚLA = 61
GYÚR = 62
HAT = 18
IDE = 42
IDŐ = 54
JEL = 67
KARC = 25
KÖT = 25
LÁP = 42
LÉC = 49
MAR = 36
MÉH = 60
NAGY = 68
OPÁL = 46
ÖNT = 43
RAK = 24
RÁMA = 41
RÉS = 45
RÉV = 71
ROP = 35
RÓMA = 63
RÚG = 49
SATU = 19
SÍP = 49
SÜT = 26
SZÍR = 63
TAHI = 27
TAS = 11
TÖNK = 50
TŰR = 41
TYÚK = 36
VÉKA = 73
VÉRT = 73
ZRÍ = 60
ZSÚR = 51

A	Á	B	C	D	E	É	F	G	H	I	Í	J	K	L	M
N	O	Ó	Ö	Ő	P	R	S	T	U	Ú	Ü	Ű	V	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
C															
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

«Füles Logika»

9. Feladat. Oldjuk meg az alábbi rejtvényt!



«Füles Logika»

5. Helyettesítések, permutációk

A továbbiakban szükségünk lesz egy rögzített ábécére. Ez a következő: (kettős betűket az egyértelműség kedvéért nem használunk.)

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.

10. Feladat. Caesar-rejtjel: Kulcs: Az ábécé minden betűje helyett a következőt írjuk, az utolsó helyett az elsőt. (A szóközöket nem titkosítjuk, írásjeleket nem használunk, kis és nagy betűket nem különböztetünk meg.) (Caesarnál valójában $a = d$ volt a kulcs, ezt, az $a = b$ újítást Augustus vezette be.)

(a) Hogyan kódoljuk az `Elemi matematika` üzenetet?
(b) Mi az üzenet ha `uíulót űaéoéu`-t kaptunk?
(c) Mi a hátránya ennek a titkosításnak?
(d) Hányféle kulccsal titkosíthatunk?
(e) Megnehezíti-e az üzenet feltörését ha a kulcsot többször egymás után alkalmazva titkosítunk?
(f) Hogyan nehezíthető meg az üzenet feltörése?

11. Feladat. A Caesar-rejtjel egy módosítása: Az ábécé minden betűje helyett az ötödik bal oldali szomszédját írjuk (ciklikusan természetesen), továbbá minden hasznos karakter után beszúrjuk az ábécé soron következő betűjét hátulról kezdve. (A szóközöket nem titkosítjuk, írásjeleket nem használunk, kis és nagy betűket nem különböztetünk meg.)

(a) Titkosítsuk: `Este ma várom a Nemzetinél!`
(b) Mi az üzenet ha `tzvyíxaw övűűwüíúzuátgs`-t kapunk?

12. Feladat. Mi a közös a fenti két titkosításban? Miben különböznek? Hogyan nehezíthető a kódolás létrejötte mikéntjének a felismerése?

13. Feladat. Affin rejtjel: Legyen az ábécénk hosszúsága n és $C_{(a;b)}(x) = a \cdot x + b \pmod{n}$, ahol $(a; n) = 1$.

(a) Legyen az ábécénk: `a, b, c, d, e, f` és $C(x) = 5x + 1$.

0	1	2	3	4	5
a	b	c	d	e	f

Titkosítsuk a BAD DAD üzenetet.

(b) Milyen módon tudunk dekódolni? Fejtsük vissza az ABE EBE üzenetet.

(c) Miért szükséges az $(a; n) = 1$ feltétel? Próbáljuk meg a $C(x) = 2x+1$ rejtjellel titkosítani az ABC és DEF üzeneteket. Mit tapasztalunk?

(d) Mennyi itt a kulcsok száma? A jó titkosítás nagy számú kulcsot képes generálni.

14. Feladat. Helyettesítés kulcsszóval: Tekintsünk egy kulcsszót, pl. azt, hogy KULCSSZO. Szabaduljunk meg a többször előforduló betűktől: KULCSZO. Vegyük az ábécénket, majd az ábécénk betűinek rendre feletessük meg a KULCSZO karaktereit: a→ k, á→ u, b→ l, s.í.t. Amikor elfogy a kulcsszó, folytassuk a sort az ábécé a kulcsszó utolsó betűjét követő betűjével, kihagyva azokat a betűket, amik már szerepeltek.

15. Feladat. PA-LE-RI-NO-FU írás: Tekintsük a PA-LE-RI-NO-FU-KÖ-TÉ-SÜ kulcsot. Ha a szövegnek van olyan betűje ami itt szerepel, akkor helyette a párját írjuk. Ha a titkosítandó szöveg betűje itt nem szerepel, akkor nem változik.

(a) Kódoljuk: `Szeged`

(b) Dekódoljuk: `hndmlzkváüáihley`

«Grätzer József: Új Sicc»

16. Feladat. Vágásos permutálás: Vágjuk a szöveget 5 karakter hosszúságú egységekre (szóközöket, írásjeleket is beleértve) a végét szükség szerint szóközökkel kiegészítve, majd permutáljuk az egyes szakaszokat a $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix}$ kulcs segítségével.

(a) Dekódoljuk: `␣jobbra ívksnana ag edatantbebb, ojsb␣␣blzeerkemens vrezbes ,edev` (A szövegben a szöveg eleji, végi, és az esetleges többszörös szövegközi szóközöket ␣ jelöli, a többi helyen a szóköz a szóköz.)

(b) Hogyan tudja B dekódolni az üzenetet?

(c) Titkosítsuk: `viszem a régen kihízott nacim, viszem a kelet-német származású macim`

(d) Nehezíti-e az üzenet feltörését ha a kulcsot többször egymás után alkalmazva titkosítunk, vagy több kulcsot alkalmazva titkosítunk többször?

(e) Miben különbözik ez a titkosítás az előzőektől?

6. Rácsok

17. Feladat. Polübiosz fáklyatávírója: Az üzenet küldőjének mindkét kezében 5-5 fáklya van, s annyit tart fel a bal, illetve a jobb kezével, ahányadik sorában, illetve oszlopában van a továbbítandó karakter.

	1.	2.	3.	4.	5.
1.	a	f	m	r	y
2.	b	g	n	s	z
3.	c	h	o	t	
4.	d	i	p	u	
5.	e	l	q	x	

(a) Mik a módszer előnyei?
(b) Hányféleképp tölthető ki a táblázat 25 helye ezzel a 22 karakterrel?

18. Feladat. Bifid rejtjel: Polübiosz táblázatához hasonlót készítünk, kevert ábécével (i=j).

	1	2	3	4	5
1	B	G	W	K	Z
2	Q	P	N	D	S
3	I	O	A	X	E
4	F	C	L	U	M
5	T	H	Y	V	R

Az üzenet betűihez tartozó koordináta-párok tagjait (sor-oszlop) sorrendben egymás alá írjuk. Ezután a második sort az első sor után illesztjük. Az egymás melletti számpárokat koordinátapárként tekintve megkeressük a hozzájuk tartozó betűt a táblázatban. Ezek adják a kódolt üzenetet.

(a) Kódoljuk: `Meneküljetek!`
(b) Dekódoljuk: `LNKLEIREUITV`

19. Feladat. Találjunk ki a fenti táblázaton alapuló „saját" titkosírást.

20. Feladat. Vigenère-rejtjel (a „feltörhetetlen" kód): Caesar-kódok sorozatát használja, a változtatható hosszúságú kulcs miatt a monoalfabetikus Caesar-kóddal ellentétben polialfabetikus. Adott a következő táblázat.

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

Kell egy kulcs, pl: `MATEK`. A titkosítandó szöveget pl.: kulcs hosszúságú részekre daraboljuk, s ennek segítségével a szöveg minden betűjének megfeleltetjük a kulcs egy-egy betűjét, majd ezen betűpárokhoz (oszlop-sor) sorrendben kiválasztjuk a táblázat megfelelő betűjét, ez adja a rejtjelezett üzenetet.

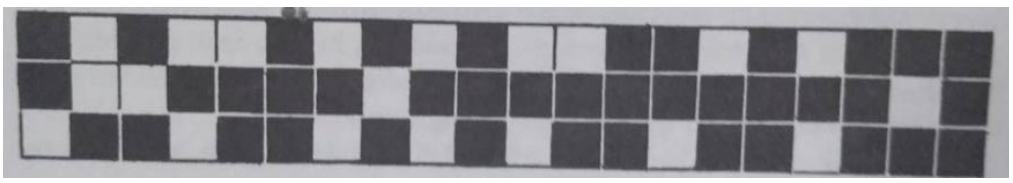
(a) Titkosítsuk a MATEK kulcs segítségével: `Plakátokon masíroznak az igazi...` .
(b) Hogyan kell megfejteni egy üzenetet?
(c) Baj-e, ha nyilvánosságra kerül a táblázat? Miért?
(d) Dekódoljuk: `pppjkitkjspeygmddjrrmrpo` ha tudjuk, hogy a kulcs `ELEFÁNT`.
(e) Mit kapunk (általánosan) ha a kulcs B?
(f) Mihez hasonlít ez a táblázat?
(g) Keressünk olyan üzenetet és kulcsot, amelyek csupa azonos betűből álló titkosítást eredményeznek.
(h) Hogyan érdemes megpróbálni feltörni a kódot?

21. Feladat. Polübiosz táblázata magánhangzópárokkal: A szövegben található magánhangzópárok sor-oszlop sorrendben kódolják a táblázat alapján az üzenetet, így csak annak magánhangzóit kell figyelnünk.

	1 A	2 E	3 I	4 O	5 U
1 A	A	B	C	D	E
2 E	F	G	H	I	J
3 I	K	L	M	N	O
4 O	P	Q	R	S	T
5 U	U	V	X	Y	Z

(a) Mik a módszer előnyei?
(b) Hányféleképp tölthető ki a táblázat 25 helye, illetve a sor és oszlop fejléce? Ezek mind ténylegesen különböző kulcsot adnak?
(c) Mit rejt a `Itt aludt aki eladott egy uborkagyalut, itthon csücsülök, unom.` üzenet?
(d) Kódoljuk: `Fekete szívem fekete sebbel feketét dobban, Csak te vagy színes, szinte látom, ahogy színed robban.`

22. Feladat. Egyszerű rács: Az üzenetet egy rácsba rejtjük, melynek kulcs ugyanezen rács ablakokkal ellátott változata. A fedett mezőket zavaró karakterekkel töltjük fel. Dekódoljuk az alábbi üzenetet.



5	J	X	O	B	C	B	A	R	G	O	L	E	M	T	L	Á	O	I	É
7	M	A	5	4	2	P	D	R	D	I	U	K	K	O	Ö	L	É	Á	V
S	Z	T	E	U	K	R	R	D	P	Ő	Á	Á	R	I	O	E	D	K	5

«Grätzer József: Új Sicc»

23. Feladat. Cardano-rács: (A XVI. századból származik, de még a XX. században is használták.) Jules Verne regényében Sándor Mátyás üzenete:

RHGAAZÜYGGRÉAFXSGMNTRÁREEZLFTÉSERÉOG.

A megfejtéshez a betűket táblázatba rendezzük:

R	H	G	A	A	Z
Ü	Y	G	G	R	É
A	F	X	S	G	M
N	T	L	Á	R	E
E	Z	L	F	T	É
S	E	R	É	O	G

Majd ráhelyezzük a kulcsként szolgáló rácsot, leírjuk a kilátszó betűket, majd a rácsot elforditva ezt ismételgetjük. http://slideplayer.hu/slide/2251755/

1. ábra. HAZRXTRÉÉ

2. ábra. GÉSNELTEG

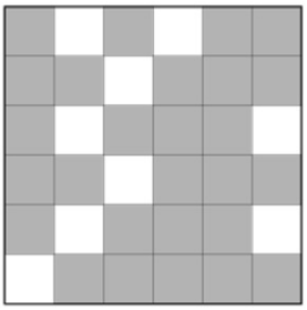
3. ábra. GÜFGÁZSRO

4. ábra. RÁYGAMLEF

Az üzenetet visszafelé olvasva: Fel Magyarország függetlenségéért! XRZAH

(a) Hogyan keletkezett az üzenet?
(b) Fejtsük meg az alábbi üzenetet!

E	J	E	U	S	T
Y	G	L	É	Á	N
Á	E	Y	S	É	S
C	N	V	D	Í	B
O	E	R	M	M	R
N	E	Ű	N	R	Á



(c) Egy $n \times n$-es rácson hány, egyszerre k betűt látni engedő (egyszerű) rács van?
(d) Forgató-rács olyan rács, amelyet 90°-onként elforgatva ablakaival pontosan egyszer lefedi a rács minden mezőjét. Hány ablakos egy forgató-rács egy $n \times n$-es rács esetében?
(e) Igazoljuk, hogy a forgató-rácsok száma egy $n \times n$-es rács esetében $4^{\frac{n^2}{4}}$.

«KöMaL, http://slideplayer.hu/slide/2251755/»

24. Feladat. Mik a „hagyományos” rejtjelezés problémái?

(a) kulcsminőség
(b) kulcs célba juttatása, kulcscsere
(c) kulcshasználat száma

(d) a legjobb az egyszer használatos, cserét nem igénylő véletlen kulcs.

25. Feladat. A fenti módszerek kombinációjával (pl. Vinegere és vágásos permutáció) állítsunk elő saját titkosírást!