

Elemi matematika 1.

TITKOSÍRÁSOK

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.)

Megoldás.

- (a) Morse-abc,
- (b) jelnyelv,
- (c) Braille-írás,
- (d) vonalkód, QR-kód

International Morse Code

1. The length of a dot is one unit.
2. A dash is three units.
3. The space between parts of the same letter is one unit.
4. The space between letters is three units.
5. The space between words is seven units.

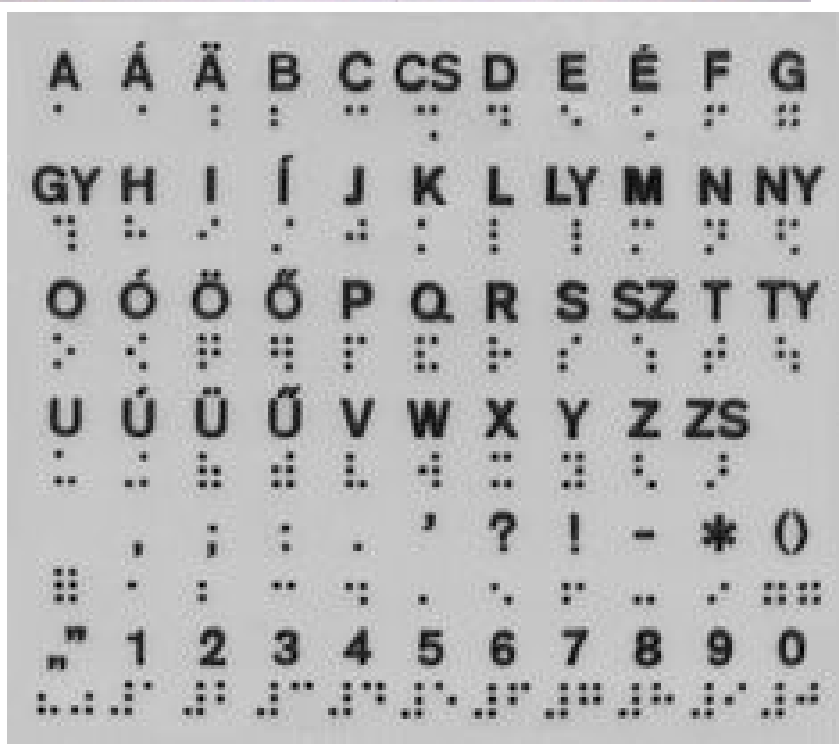
A	• —	U	• • —
B	— • • •	V	• • • —
C	— • — •	W	• — —
D	— • •	X	— • • —
E	•	Y	— • — —
F	• • — •	Z	— — • •
G	— — •		
H	• • • •		
I	• •		
J	• — — —		
K	— • —	1	• — — — —
L	• — • •	2	• • — — —
M	— —	3	• • • — —
N	— •	4	• • • • —
O	— — —	5	• • • • •
P	• — — •	6	— • • • •
Q	— — • —	7	— — • • •
R	• — •	8	— — — • •
S	• • •	9	— — — — •
T	—	0	— — — — —

3. Feladat. (a) Morse-abc

Mitől függhet az egyes betűkhöz tartozó jelsorozat hossza, bonyolultsága?



(b) Jelnyelv



(c) Braille-írás

Megoldás.

- (a) Morse-abc: Megállapodás szerint a morzekód olyan jelek és szünetek szabályszerű sorozatából áll, amelyeket adás kezdete vezet be és adás vége vagy vétel jelcsoport zár le. A morzekód csak nagybetűket, számokat és írásjeleket használ: nem tesz különbséget a kis- és a nagybetűk között. Emellett: rövid jel (ti 1 egység hosszú); hosszú jel (tá 3 egység hosszú); rövid szünetjel (jelköz 1 egység hosszú); hosszú szünetjel (betűköz 3 egység hosszú); nagyon hosszú szünetjel (szóköz és mondatköz 7 egység hosszú). Az egyes betűk jelhossza, bonyolultsága annál kisebb, minél gyakrabban fordulnak elő (angol) szövegekben pl: E, I, T stb. Az egyes nyelvek (magyar, cseh, arab, görög, amerikai stb.) saját Morse-abc-t használnak.

- (b) Jelnyelv: Országoként, nyelvenként különbözik, a hasonló jelek ellenére. Tulajdonképpen egy valódi, természetes nyelv.
- (c) Braille-írás: 6 vagy 8 pontos hibajavító kódolás, a karaktereken kívül más jelek közvetítésére is alkalmas, nyelvenként eltérő.

A felsorolt eljárások többsége többek számára is hozzáférhetővé az üzenet. Mindegyike helyettesítéses, egy rögzített ábécé jeleit felelteti meg kölcsönösen egyértelműen egy másik jelrendszer jeleinek.

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]...`)

Megoldás.

- (a) Aki lépne leírja lépését egy papírra, amit egy független bíró, széf, stb. őriz.
- (b) A lépést előre tisztázott módon kódolják, pl. megfeleltetnek a sakktábla minden mezőjének egy kétjegyű számot, így a lépést egy négyjegyű szám megmásíthatatlanul őrzi. Ezt a négyjegyű számot A kiegészíti egy 1000 jegyű prímmé, és vesz egy másik, pl. ennél nagyobb 1000 jegyű prímet, s a szorzatot elárulja B-nek, valamint persze azt is, hogy lépését a kisebbik tényező első négy jegye rejti. Ekkor B adott idő alatt nem tudja megtalálni a felbontást, A nem tudja megváltoztatni a lépését, B pedig összeszorzással gyorsan ellenőrizni tudja, helyesek-e a tényezők, A tényleg azt lépi-e amit kódolt.

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>)

Megoldás.

- (a) A kapott számból kivonja a kulcsot, a kapott számot hátulról kezdve 8 karakter hosszú egységekre bontja, ha szükséges az elején 0-val kiegészítve.
- (b) 1010011010110100110000000110000

- (c) Az üzenetet adó kettes számrendszerbeli számot átírjuk tízes számrendszerbe, és azt küldjük. (Ekkor $1398425921+5871 = 1398431792$.)
- (d) Pl.: az üzenet karaktereit fordított sorrendben küldjük.
- (e) 7 bites ASCII-ban: SZIA (csupa nagybetűvel).

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

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

Megoldás.

«FÜLES LOGIKA»


9. Feladat. Oldjuk meg az alábbi rejtvényt!

KAGYLÓHÉJ

A kilenc betű mindegyike egy-egy számnak felel meg 1-től 9-ig. A meghatározások alapján állapítsa meg, hogy melyik betű melyik számot rejtli!

1. Az egyik oszlopban csak páratlan számok vannak
2. Egy másik oszlopban három egymás utáni szám van, föntről lefelé fordított sorrendben.
3. Az **Y**, az **L** és az **Ó** betű helyén páratlan szám van. A három közül a középső a legnagyobb szám.
4. A **J** betű értéke kisebb, mint az **É** betűé.
5. Az **L** betű értéke 1-el több, mint a **J** betűé.
6. A **H** betű értéke 1-el több, mint az **A** betűé.

K	A	G
Y	L	Ó
H	É	J



4	1	8
3	7	5
2	9	6

Megoldás.

«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.)

- Hogyan kódoljuk az Elemi matematika üzenetet?
- Mi az üzenet ha uíulót ũaéoéu-t kaptunk?
- Hányféle kulccsal titkosíthatunk?
- Megnehezíti-e az üzenet feltörését ha a kulcsot többször egymás után alkalmazva titkosítunk?
- Hogyan nehezíthető meg az üzenet feltörése?

11. Feladat. Mi a hátránya ennek a titkosításnak?

Megoldás. Könnyen feltörhető. A karakterkészletből, a szavak hosszából (ez elkerülhető, ha minden egybeírunk), a karaktergyakoriságokból beazonosítható a nyelv, sőt a karaktergyakoriságokból az is, hogy melyik karakter mit rejt, így nem csak a nyelv van meg, de maga az üzenet is.

12. Feladat. Hogyan védhető ki a karaktergyakoriság árulkodó volta?

13. 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 *tzvxyíaw övűüüüúzuátgs-t* kapunk?

- 14. Feladat.** (a) Mi a közös a fenti két titkosításban?
 (b) Miben különböznek?
 (c) Hogyan nehezíthető a kódolás létrejötte mikéntjének a felismerése?

15. 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.

Megoldás.

- (a) A B képe $5 \cdot 1 + 1 \equiv 0$, azaz A. Az A képe $5 \cdot 0 + 1 \equiv 1$ vagyis B. A D képe pedig $5 \cdot 3 + 1 \equiv 4$, vagyis E. Így ABE EBE.
 (b) Meg kell keresni a függvény inverzét, $y = 5x + 1$ -ből $x = 5(y - 1)$ lesz. (Az 5 most önmaga inverze.)
 (c) Mindkettőből BDF lesz, így nem visszafejthető.
 (d) $\varphi(n) \cdot (n - 1)$.

16. 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: $a \rightarrow k$, $\acute{a} \rightarrow u$, $b \rightarrow l$, s.i.t. Amikor elfogy a kulcsszó, folytassuk a sort az ábécé a kulcsszó utolsó betűjét követő betűjével, kihagyva azokat a betűket, amik már szerepeltek. Pl.:

Létezik egy nagyon egyszerű módszer arra, hogy szinte végeláthatatlan mennyiségű könnyen megjegyezhető kódot generáljunk az ezzel a módszerrel történő rejtjelezéshez. Elég kiválasztani egy bármilyen *kulcsszót* (ez akár mondat is lehet), elhelyezni a rejtjel-ábécé elején, és a kulcsszó utolsó betűje után befejezni a sort a hagyományos ábécé sorrendben következő betűivel, eltávolítva az ismétlődő betűket. Példaként vegyük a JANUARY CIPHER (Januári rejtjel) kulcsmondatot. Először megszabadulunk a szóköztől és az egyforma betűktől, és a JNUYCIPHE kulcsszót kapjuk. Ezután a rejtjel-ábécénk így fog kinézni:

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

17. 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: hndmlzkväuáihley

«GRÄTZER JÓZSEF: ÚJ SICC»

18. Feladat. EGY PÉLDA POLIALFABETIKUS KÓDOLÁSRA: 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

DIGRAFIKUS REJTJELEK (BIGRAMMÁK)

19. 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?

20. 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**

21. Feladat. Találjunk ki a fenti táblázaton alapuló „saját” titkosírást.

Megoldás. Ilyesmi a négy négyzet rejtjel, vagy pl. a Playfair-titkosírás: A szöveget betűpárookra bontjuk, majd:

- (a) Ha a két betű ugyanaz, az első után X-et szúrunk be
 (b) Ha egy sorban/oszlopban vannak, akkor a közvetlen utánuk álló betűket írjuk
 (c) Különben az általuk kifeszített téglalap másik átlójában álló betűket (rögzített sorrendben).

22. 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 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?

Megoldás.

	p	l	a	k	á	t	o	k	o	n	m	a	s	í	r	o	z	n	a	k	a	z	i	g	a	z	i	
(a)	m	a	t	e	k	m	a	t	e	k	m	a	t	e	k	m	a	t	e	k	m	a	t	e	k	m	a	
	b	l	t	o	k	f	o	d	s	x	y	a	l	m	b	a	z	g	e	u	m	z	b	k	k	l	i	

- (b) Megfejtéséhez a titkosított üzenetet kulcs hosszúságú részekre daraboljuk, s ennek segítségével a szöveg minden betűjének megfeleltetjük a kulcs egy-egy betűjét, majd a kulcsbetű által jelzett sorban megkeressük az üzenet karakterét, és leírjuk annak oszlopazonosítóját.
- (c) Nem, mert a kulcs nélkül nem sokat ér.

	l	é	l	e	k	v	a	g	y	o	k	é	l	n	i	s	z	e	r	e	t	n	é	k
(d)	e	l	e	f	á	n	t	e	l	e	f	á	n	t	e	l	e	f	á	n	t	e	l	e
	p	p	p	j	k	i	t	k	j	s	p	e	y	g	m	d	d	j	r	r	m	r	p	o

(e) A Caesar-rejtjelet.

(f) Véges csoportok Cayley-táblázata.

(g) ...

(h) Babage: Megkeressük az ismétlődő betűket s megnézzük hány karakter múlva ismétlődnek. Ezek nagy valószínűséggel azok, amik azonos módon lettek kódolva, tehát a kulcs hossza osztója a távolságnak, a távolságok legnagyobb közös osztójának. Ezek után, ha a kulcsszó n hosszú, csak n darab monoalfabetikus kóddal van dolgunk amik külön-külön, például gyakoriságelemzéssel támadhatók.

23. Feladat. POLÜBIOSZ TÁBLÁZATA MAGÁNHANGZÓPÁROKKAL: A szövegben található magánhangzópárok sor-oszlop sorrendben kódolják a táblázat alapján az üzenetet, így csak annak magánhangzóit kell figyelniük.

	1	2	3	4	5
	A	E	I	O	U
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	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 uborkagyálut, itthon csücsülök, unom. üzenet?

(d) Kódoljuk: Fekete szívem fekete sebbel feketét dobban, Csak te vagy színes, szinte látom, ahogy színed robban.

Megoldás.

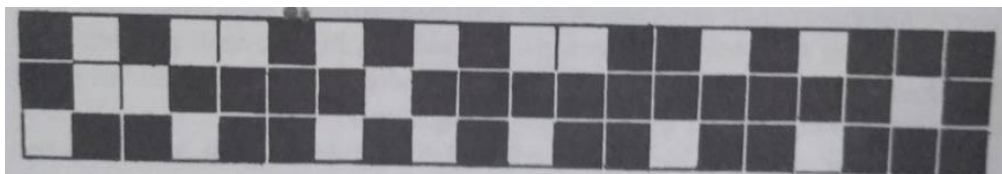
(a) A táblázat könnyen újrendezhető.

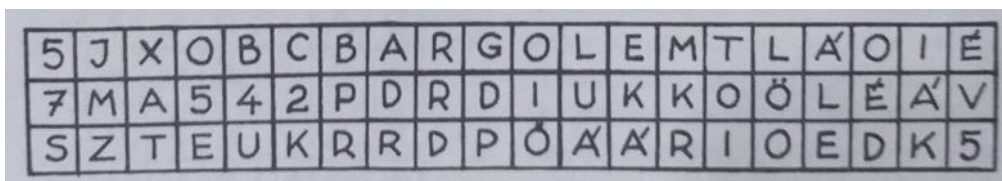
(b)

(c) A magánhangzópárok: ia ua ie ao eu oa au io üü öü. (Úgy tűnik, az utolsó o-nak nincs párja, ő felesleges.) Ezek rendre: kuldj penzt.

(d) Az ea au ia au ou au oo uu eo ue au ii, ... magánhangzó párokra kell szöveget fűzni.

24. 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.





«GRÄTZER JÓZSEF: ÚJ SICC»

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

RHGAAZÜYGGREÁFXSGMNTRÁREEZLFTÉSERÉOG.

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 elfordítva ezt ismételtjük. <http://slideplayer.hu/slide/2251755/>

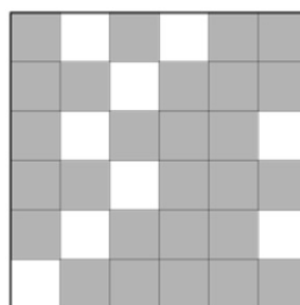


1. ábra. HAZRXTRÉÉ 2. ábra. GÉSNELTEG 3. ábra. GÜFGÁZSRO 4. ábra. RAYGAMLEF

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/](http://slideplayer.hu/slide/2251755/)»

26. 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.

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