Zabavimo se...


- Kako zapisati poruku da samo nama bude razumljiva?
- Znam! To je i Cezar radio...
- EDFLPR VH QD SRVDR!
NY TIMES
Naučimo šifrirati i dešifrirati tajne poruke!

(De)šifriranje

Ljubica Jerković

Sadržaj

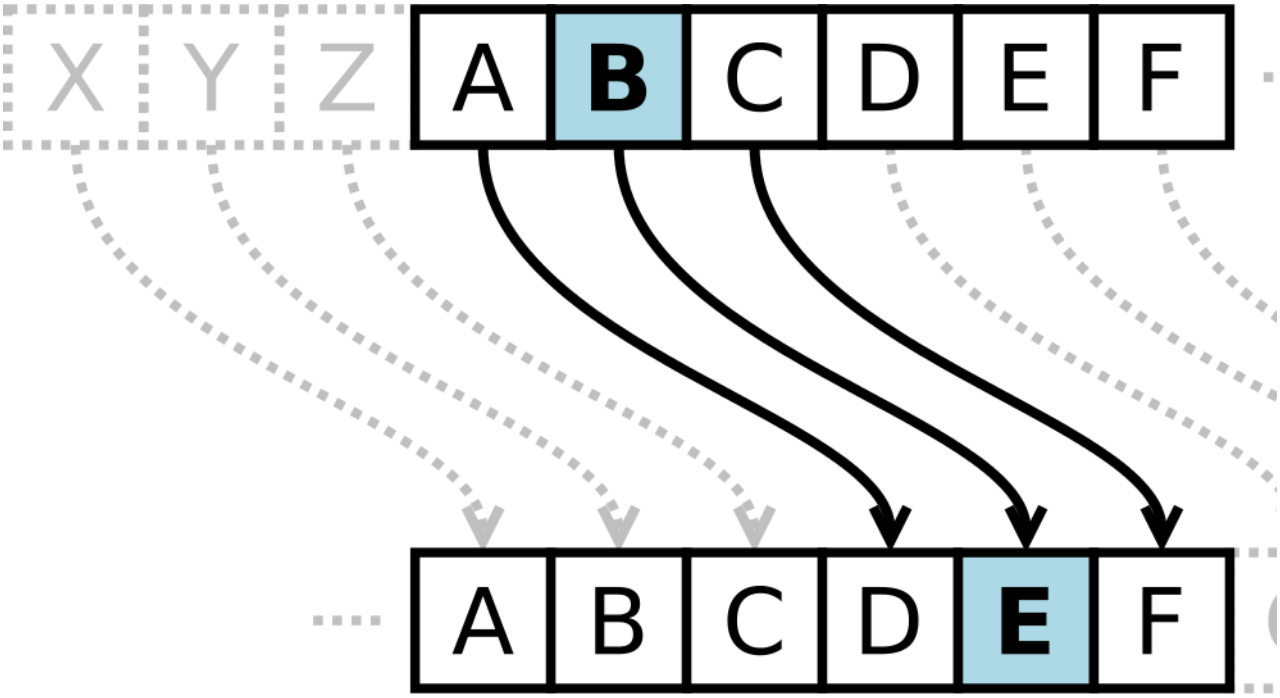
CEZAROVA ŠIFRA

Šifriranje je pisanje pomoću tajnih znakova (slova, brojeva ili nekih drugih simbola), a dešifriranje je "prevođenje" tajnog zapisa na razumljiv jezik. Šiframa se koriste vojnici, liječnici, bankari, prijatelji,...

Znate li da je i Julije Cezar koristio šifre u svojim tajnim porukama? Činio je to da ih neprijatelj ne odgonetne.

Kada je želio poručiti nešto povjerljivo, on je to pisao šifrirano tako što je mijenjao redoslijed slova u alfabetu i na taj način postizao da se nijedna riječ nije mogla prepoznati. Ako bi netko to želio dešifrirati i naći značenje, morao bi zamijeniti četvrto slovo alfabeta, dakle D s A i tako dalje za ostala.

Cezarova šifra je bila dosta učinkovita i sigurna u to vrijeme, ne samo zbog toga što je malo Cezarovih neprijatelja znalo latinski ili uopće bilo upoznato s pisanim jezikom, već i zbog nepoznavanja same postavke šifre, načina na koji je zadana.



Navedimo osnovne pojmove koje ćemo koristiti:

- otvoreni tekst je (jasna i nešifrirana) poruka koju želimo poslati
- šifriranje je postupak kojim se jasna poruka pretvara u nejasnu kako bi se sačuvala od onih kojima nije namijenjena
- šifrat (šifrirani tekst) je poruka (otvoreni tekst) koji smo promijenili postupkom šifriranja
- dešifriranje je postupak suprotan šifriranju
- ključ je način (de)šifriranja
- originalni tekst ćemo, zbog jednostavnosti, označavati malim tiskanim slovima, a šifrirani tekst velikim tiskanim slovima iako se oba teksta mogu označavati ili velikim ili malim slovima

U daljnim primjerima koristit ćemo se engleskim (međunarodnim) alfabetom od 26 slova. Ukoliko ćemo raditi s otvorenim tekstom na hrvatskom jeziku, onda ćemo:

- Č i Ć zamijeniti s C
- Đ, DŽ, LJ, NJ, Š, Ž redom s DJ, DZ, LJ, NJ, S, Z

CEZAROVA ŠIFRA S POMAKOM 3

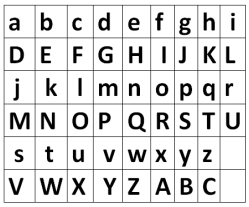
a	b	c	d	e	f	g	h	i	j	k	l	m
D	E	F	G	H	I	J	K	L	M	N	O	P
n	o	p	q	r	s	t	u	v	w	x	y	z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Razmisli kako bi Cezarovom šifrom s pomakom 3 šifrirali riječ " sunce "

i dešifrirali riječ " NDXERM " pa riješi kviz koji slijedi.

Kviz - Pomak 3

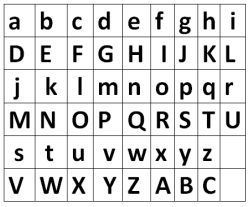
Šifriraj riječ " sunce " Cezarovom šifrom s pomakom 3.



a	b	c	d	e	f	g	h	i
D	E	F	G	H	I	J	K	L
j	k	l	m	n	o	p	q	r
M	N	O	P	Q	R	S	T	U
s	t	u	v	w	x	y	z	
V	W	X	Y	Z	A	B	C	

- [ ] VXQFH
- [ ] VXQHF
- [ ] VXFHQ
- [ ] VXHQF

Dešifriraj riječ " NDXERM " Cezarovom šifrom s pomakom 3.



a	b	c	d	e	f	g	h	i
D	E	F	G	H	I	J	K	L
j	k	l	m	n	o	p	q	r
M	N	O	P	Q	R	S	T	U
s	t	u	v	w	x	y	z	
V	W	X	Y	Z	A	B	C	

- [ ] kolica
- [ ] kauboj
- [ ] kamion
- [ ] krevet

Provjeri odgovore!

CEZAROVA ŠIFRA S POMAKOM 4

a	b	c	d	e	f	g	h	i	j	k	l	m
E	F	G	H	I	J	K	L	M	N	O	P	Q
n	o	p	q	r	s	t	u	v	w	x	y	z
R	S	T	U	V	W	X	Y	Z	A	B	C	D

Razmisli kako bi Cezarovom šifrom s pomakom 4 šifrirali riječ " sunce " i dešifrirali poruku " NE ZSPMQ XENRSTMW " pa riješi kviz koji slijedi.

Kviz - Pomak 4

Šifriraj riječ " sunce " Cezarovom šifrom s pomakom 4.

a	b	c	d	e	f	g	h	i
E	F	G	H	I	J	K	L	M
j	k	l	m	n	o	p	q	r
N	O	P	Q	R	S	T	U	V
s	t	u	v	w	x	y	z	
W	X	Y	Z	A	B	C	D	

- [ ] WRYGI
- [ ] WYRGI
- [ ] WYGRI
- [ ] WYRIG

Dešifriraj poruku " NE ZSPMQ XENRSTMW " Cezarovom šifrom s pomakom 4.

a	b	c	d	e	f	g	h	i
E	F	G	H	I	J	K	L	M
j	k	l	m	n	o	p	q	r
N	O	P	Q	R	S	T	U	V
s	t	u	v	w	x	y	z	
W	X	Y	Z	A	B	C	D	

- [ ] Ja volim matematiku
- [ ] Ja volim šifriranje
- [ ] Ja volim tajnopis
- [ ] Ja volim tajnosti

Provjeri odgovore!

CEZAROVA ŠIFRA S POMAKOM 7

a	b	c	d	e	f	g	h	i	j	k	l	m
H		J				N			Q			
n	o	p	q	r	s	t	u	v	w	x	y	z
		W		Y		A			D		F	

Koja slova nedostaju? Riješi kviz koji slijedi.

Istražujte malo ...

http://tools.zenverse.net/caesar-cipher/

Kviz - Pomak 7

Uparivanje odgovora

Slovu " b ", u tablici s pomakom 7, odgovara u šifriranom tekstu slovo : I

Slovu " k " , u tablici s pomakom 7, odgovara u šifriranom tekstu slovo : I

Slovu " s ", u tablici s pomakom 7, u odgovara u šifriranom tekstu slovo : I

Slovu " v " , u tablici s pomakom 7, odgovara u šifriranom tekstu slovo : I

Dešifriraj treću riječ u rečenici " RYPWAVNYHMPQH QL GUHUVZA AHQUVN WPZHUQH " Cezarovom šifrom s pomakom 7 te pokušaj dešifrirati i ostatak.

a	b	c	d	e	f	g	h	i
H		J				N		
j	k	l	m	n	o	p	q	r
Q						W		Y
s	t	u	v	w	x	y	z	
	A			D		F		

- [ ] Treća riječ je "pisanje".
- [ ] Treća riječ je "šiframa".
- [ ] Treća riječ je "znanost".
- [ ] Treća riječ je "izvrsno".

Provjeri odgovore!

ŠIFRIRANJE S KLJUČNOM RIJEČI I KLJUČNIM SLOVOM

Ovaj je način šifriranja vrlo sličan Cezarovom, a sastoji se u tome da se odabere neka riječ (u kojoj nema ponovljenih slova jer bi to dodatno otežalo stvar) i neko slovo, npr. ključna riječ MORE i ključno slovo G pa tablica izgleda na sljedeći način:

a	b	c	d	e	f	*g*	h	i	j	k	l	m
U	V	W	X	Y	Z	*M*	*O*	*R*	*E*	A	B	C
n	o	p	q	r	s	t	u	v	w	x	y	z
D	F	G	H	I	J	K	L	N	P	Q	S	T

Preostala se slova rasporede abecednim redom, počevši tamo gdje se završilo s ključnom riječi.

Koristeći tablicu s ključnom riječi MUDROST i ključnim slovom P dešifriraj poruku:

" RWPQJIPOJ IZGDF IQJWF, F YJ WPQJMJ DPQJHP. "

a	b	c	d	e	f	g	h	i	j	k	l	m
F	G	H	I	J	K	L	N	P	Q	V	W	X
n	o	*p*	q	r	s	t	u	v	w	x	y	z
Y	Z	*M*	*U*	*D*	*R*	*O*	*S*	*T*	A	B	C	E

ŠIFRE S BROJEVIMA

Ideja je da se slovo zamijeni s brojem pa se koristi sljedeća tablica:

a	b	c	d	e	f	g	h	i
0	1	2	3	4	5	6	7	8
j	k	l	m	n	o	p	q	r
9	10	11	12	13	14	15	16	17
s	t	u	v	w	x	y	z	
18	19	20	21	22	23	24	25	

Kao i kod Cezarove šifre i ovdje možemo koristiti pomak pa slijedi

tablica s brojevima s pomakom 3 :

a	b	c	d	e	f	g	h	i
3	4	5	6	7	8	9	10	11
j	k	l	m	n	o	p	q	r
12	13	14	15	16	17	18	19	20
s	t	u	v	w	x	y	z	
21	22	23	24	25	0	1	2	

Kviz - Šifre s brojevima

Šifriraj rečenicu: " Danas je lijep dan", koristeći tablicu s brojevima (bez pomaka).

a	b	c	d	e	f	g	h	i
0	1	2	3	4	5	6	7	8
j	k	l	m	n	o	p	q	r
9	10	11	12	13	14	15	16	17
s	t	u	v	w	x	y	z	
18	19	20	21	22	23	24	25	

- [ ] 3 0 13 0 18 9 3 11 8 9 4 15 3 1 13

a	b	c	d	e	f	g	h	i
0	1	2	3	4	5	6	7	8
j	k	l	m	n	o	p	q	r
9	10	11	12	13	14	15	16	17
s	t	u	v	w	x	y	z	
18	19	20	21	22	23	24	25	

- [ ] 3 0 13 0 18 9 3 11 9 8 4 15 3 0 13

a	b	c	d	e	f	g	h	i
0	1	2	3	4	5	6	7	8
j	k	l	m	n	o	p	q	r
9	10	11	12	13	14	15	16	17
s	t	u	v	w	x	y	z	
18	19	20	21	22	23	24	25	

- [ ] 3 0 13 0 18 9 4 11 9 8 4 15 3 0 13

a	b	c	d	e	f	g	h	i
0	1	2	3	4	5	6	7	8
j	k	l	m	n	o	p	q	r
9	10	11	12	13	14	15	16	17
s	t	u	v	w	x	y	z	
18	19	20	21	22	23	24	25	

- [ ] 3 0 13 0 18 9 4 11 8 9 4 15 3 0 13

a	b	c	d	e	f	g	h	i
0	1	2	3	4	5	6	7	8
j	k	l	m	n	o	p	q	r
9	10	11	12	13	14	15	16	17
s	t	u	v	w	x	y	z	
18	19	20	21	22	23	24	25	

Tablica prikazuje šifru s brojevima s pomakom 5

a	b	c	d	e	f	g	h	i
5				9				13
j	k	l	m	n	o	p	q	r
					19			22
s	t	u	v	w	x	y	z	
		25	0					

- Da
- Ne

Uparivanje odgovora

Slovu " d " u tablici s brojevima s pomakom 5 odgovara broj : 24

Slovu " n " u tablici s brojevima s pomakom 5 odgovara broj : 24

Slovu " t " u tablici s brojevima s pomakom 5 odgovara broj : 24

Slovu " x " u tablici s brojevima s pomakom 5 odgovara broj : 24

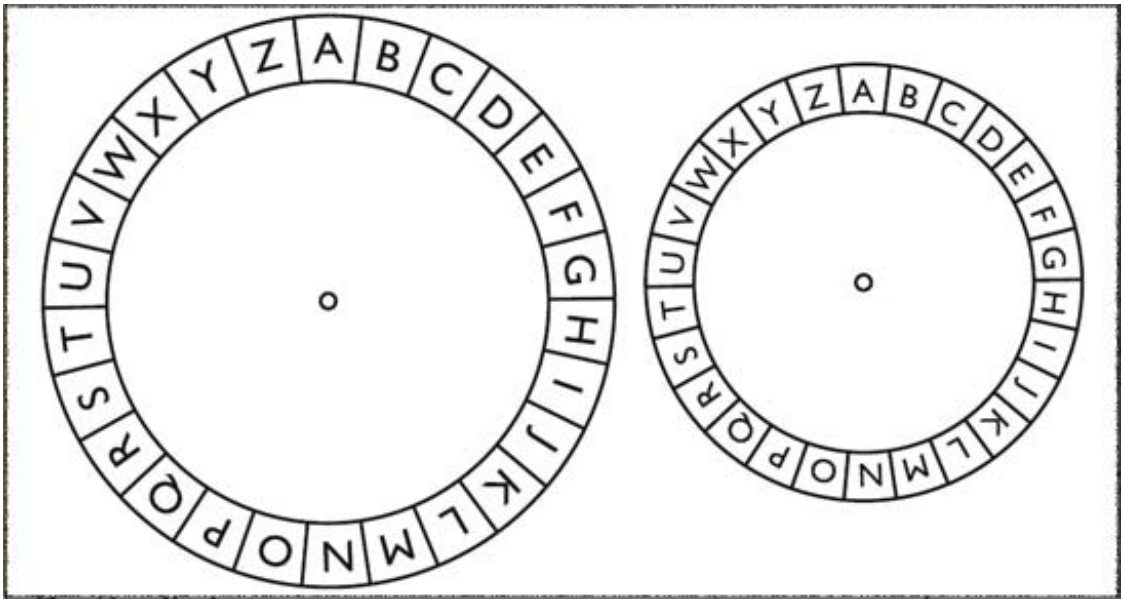
Provjeri odgovore!

CEZAROV KRUG

Može biti dosadno i nepraktično uvijek praviti tablice s pomakom pa je sve pojednostavljeno Cezarovim krugom.

Jednostavno se okretanjem odrede pozicije odgovarajućih slova. Vanjski krug odgovara otvorenom tekstu, a unutrašnji šifriranom.

Od kartona se izrežu krugovi, pričvrste čavlićem jedan za drugi i s donje strane se stavi komadić pluta da se ne ogrebemo.



Postoji i online verzija pa se zabavite ...

http://inventwithpython.com/cipherwheel/

JOŠ NEKA ŠIFRIRANJA...

(De)šifriranje može biti znatno zahtjevnije ako se koriste i neke druge tablice. Slova i brojevi, na primjer, ne moraju biti poredani po nekom redu, a moguće je koristiti i tablice u kojima se koriste i brojevi i slova.

Npr.

a	b	c	d	e	f	g	h	i	j	k	l	m
E	Y	Q	L	F	R	M	W	G	A	K	P	D
n	o	p	q	r	s	t	u	v	w	x	y	z
X	O	H	Z	J	S	V	B	U	C	T	N	I

Tablica 1.

a	b	c	d	e	f	g	h	i
8	11	3	16	21	12	23	4	0
j	k	l	m	n	o	p	q	r
15	17	9	5	22	10	2	25	1
s	t	u	v	w	x	y	z	
14	20	18	13	19	7	24	6	

Tablica 2.

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	A	B	C	D	E
n	o	p	q	r	s	t	u	v	w	x	y	z
F	G	H	I	J	K	L	M	N	O	P	Q	R

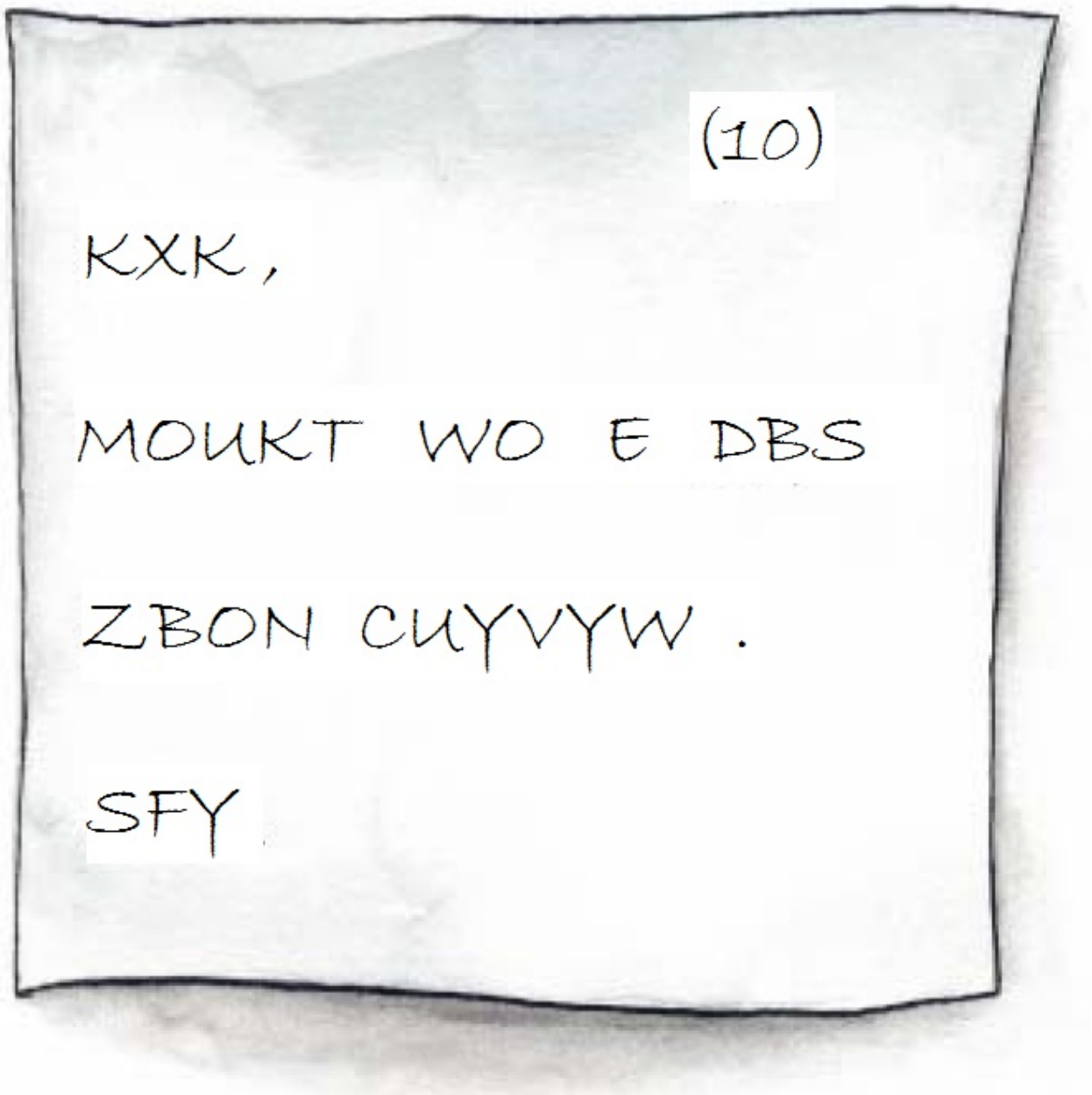
Tablica 3.

Koristeći, po izboru, jednu od tri navedene tablice šifriraj poruku:

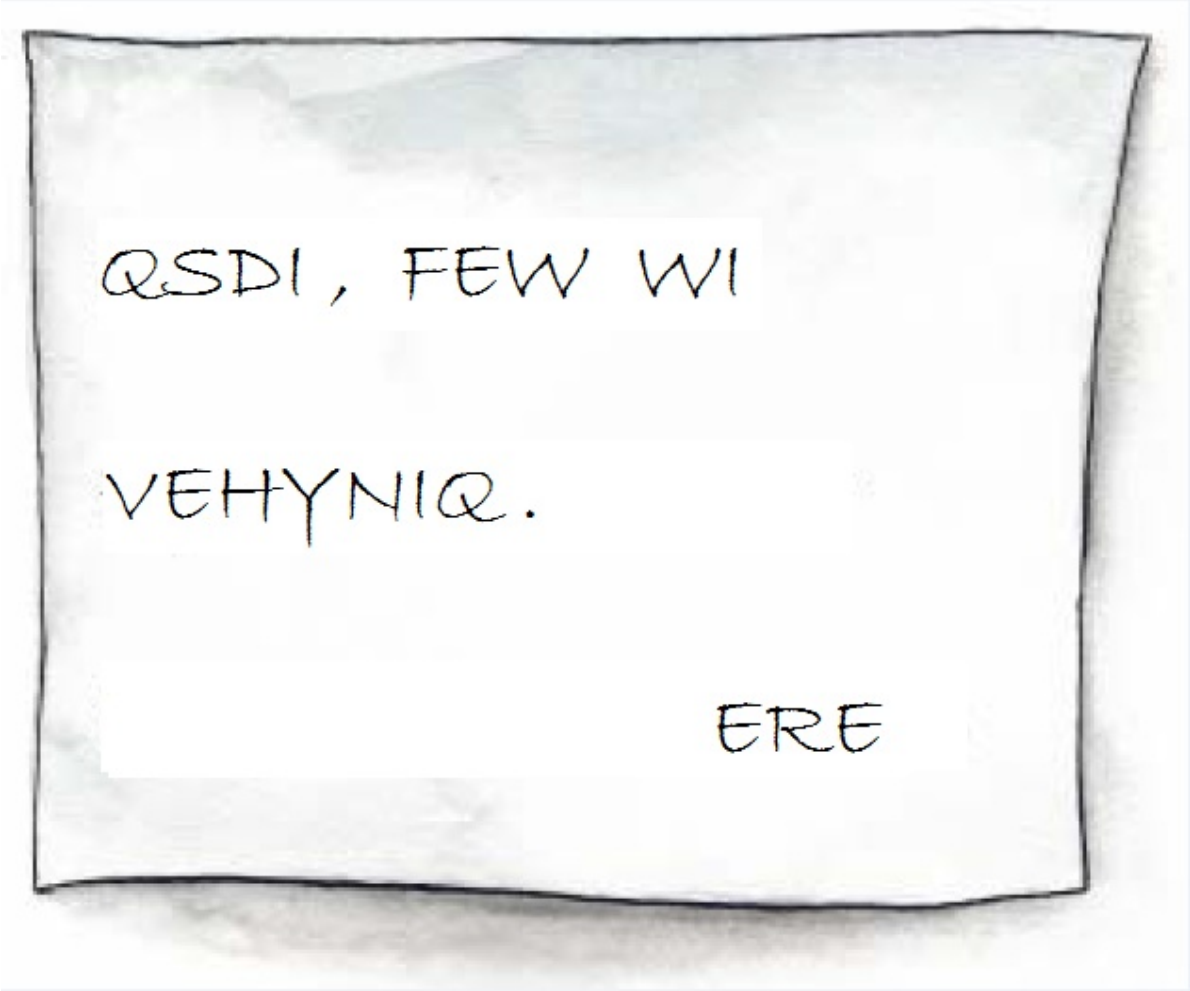
Mali princ

ZA KRAJ ...

Ivo je Ani poslao poruku i istaknuo da se radi o Cezarovoj šifri s pomakom 10 . Ana mu je odgovorila, isto Cezarovom šifrom, ali je zaboravila istaknuti pomak. Pomozi im da se razumiju i dešifriraj njihove poruke.



Ivo piše...



Ana odgovara...

Reference

1. 3.2 *Ljubica Jerković (author)*
2. (De)šifriranje *Ljubica Jerković (author)*
3. Kviz *Ljubica Jerković (author)*
4. Kviz *Ljubica Jerković (author)*
5. Kviz *Ljubica Jerković (author)*
6. Kviz *Ljubica Jerković (author)*
7. Kviz *Ljubica Jerković (author)*
8. Kviz *Ljubica Jerković (author)*
9. Kviz *Ljubica Jerković (author)*
10. Kviz *Ljubica Jerković (author)*
11. Kviz *Ljubica Jerković (author)*
12. Kviz *Ljubica Jerković (author)*
13. Kviz *Ljubica Jerković (author)*
14. Kviz *Ljubica Jerković (author)*
15. Kviz *Ljubica Jerković (author)*
16. Kviz *Ljubica Jerković (author)*
17. Kviz *Ljubica Jerković (author)*
18. Kviz *Ljubica Jerković (author)*
19. Kviz *Ljubica Jerković (author)*

20. Kviz *Ljubica Jerković (author)*
21. Kviz *Ljubica Jerković (author)*
22. Kviz *Ljubica Jerković (author)*
23. Kviz *Ljubica Jerković (author)*
24. Kviz *Ljubica Jerković (author)*
25. Kviz *Ljubica Jerković (author)*
26. Kviz *Ljubica Jerković (author)*
27. Kviz *Ljubica Jerković (author)*
28. Kviz *Ljubica Jerković (author)*
29. Kviz *Ljubica Jerković (author)*
30. Kviz *Ljubica Jerković (author)*
31. Kviz *Ljubica Jerković (author)*