

Šifriranje u nastavi

Često razmišljamo na koji način potaknuti dječiju znatiželju, maštu i kreativnost jer ih to tjera na intenzivan rad, a kad su u pitanju najmlađi učenici mislim da niko od njih neće odbiti ulogu detektiva.



Veoma je važno potaknuti dječiju znatiželju, maštu, kreativnost i motivirati ih da uče u uvjerenju da uče upravo ono što žele i zato što to oni žele.

U svakodnevnom životu svima nam je privlačno nešto što pobuđuje maštu, tjera nas na intenzivan rad, a kad su u pitanju najmlađi učenici mislim da nitko od njih neće odbiti ulogu detektiva.

Cijela jedna nauka, **kriptografija**, se bavi proučavanjem šifriranja i dešifriranja poruka, odnosno proučava načine sigurnog komuniciranja.

Šifriranje je postupak kojim običnu poruku, koju svi mogu pročitati, pretvaramo u "tajnu poruku" pomoću šifre ili koda.

Šifrirana poruka jednostavno je poruka koja je pretvorena u tajni kod tako da se može prenijeti na siguran način. To se postiže korištenjem matematičkih algoritama koji mijenjaju sadržaj izvorne poruke, čineći je tako da je mogu čitati samo određene osobe.

Dešifriranje je suprotan proces od šifriranja. Poruku je potrebno dešifrovati da bismo razumjeli njen sadržaj. To činimo pomoću ključa ili pravila koja smo unaprijed dogovorili sa pošiljaocem tajne poruke.

Iako kriptografija nije uvrštena u obaveznu nastavu, lako je primjenjiva u nastavi i doprinosi razvijanju logičkog načina razmišljanja.

Neke od jednostavnih šifri koje se lako mogu koristiti u nastavi, u bilo kojem dijelu časa su: Cezarova šifra, Pig Pen šifra, Polibijev kvadrat, Atbaš šifra i dr.

1. Šifriranje **Cezarovom šifrom** ima dugu historiju i datira još od Julija Cezara. Koristio je šifriranje da zaštiti poruke od vojne važnosti i smatra se da je koristio još mnogo drugih supstitucionih šifri. Šifriranje se vrši tako što kod ove šifre, slova abecede ili azbuke zamjenjujemo slovima koja se nalaze tri mjesta dalje od njih u alfabetu (A → D, B → E, itd), ako koristimo oblik $n=3$, odnosno $+3$ (često se koriste i $+5, +7, \dots$). Nakon zadnjeg slova Z, ponovo dolaze slova A, B, C, . . .

Originalna šifra koristi engleski alfabet.

abeceda:	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	+3
šifrovana abeceda:	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	

Zadatak:

Sa razmakom $n=5$ ($+5$) šifrovati sljedeću poruku: VENI VIDI VICI.

Rješenje :

abeceda :	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	+5
šifrovana abeceda :	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	
tekst:	v e n i v i d i v i c i	
šifrovani tekst:	A J S N A N I N A N H N	

2. **Pig Pen šifra** je poznata već nekoliko stoljeća. Dobila je ime zbog svog izgleda, odnosno po načinu na koja se slova odvajaju linijama kao svinje u svinjcu. To je monoalfabetska šifra gdje su slova zamijenjena simbolima koji su dijelovi rešetke. Zapisi o njenom korištenju sežu još iz 18.vijek, njome su se koristili masoni pa je poznata i kao masonska šifra.

Osnovni oblik ove šifre ne sadržava sva slova abecede. Tekst šifriramo tako što svako slovo zamijenimo crtežom odjeljka u kojem se to slovo nalazi.




A	B	C
D	E	F
G	H	I

J	K	L
M	N	O
P	R	S

~~T

Š

U

V~~

~~Z

Č

Ć

Ž~~

SLOVO	ZNAK	SLOVO	ZNAK	SLOVO	ZNAK
A	┐	G	└	O	◻
B	└	H	┐	P	└
C	┌	I	┐	R	◻
Č	➤	J	┐	S	┐
Ć	◀	K	◻	Š	➤
D	┐	L	◻	T	∨
DŽ	◻A	U	◻	U	<
Đ	Δ	M	◻	V	∧
E	◻	N	◻	Z	∨
F	┐	NJ	◻	Ž	◻

$\vee \square \cdot$ $\vee \sqcap \sqcap$ $\cdot \square$ $\vee \sqcap \vee \sqcap$ $\cdot \sqcap \cdot \square \square \cdot < \cdot$ $\cdot < < \cdot \sqcap$

(Primjeri zadataka i prilagođene šifre su preuzeti sa skolskiportal.hr)

Polibije je starogrčki i rimski historičar. Usavršio je metodu svojih prethodnika kojom se mogu slati skrivene poruke. Njegova metoda zove se Polibijeva ploča ili Polibijev kvadrat. Polibijev kvadrat preteča je telegrafije i steganografije.

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

55-14-42-11-51-34 ZDRAVO

4. **Atbaš šifra** je veoma stara supstitucijska šifra koja je originalno napravljena da se koristi u hebrejskom alfabetu. Ustvari, u knjizi proroka Jeremije se nalazi nekoliko riječi koje su šifrirane Atbaš šifrom. Smatrano je da je to jedna od najjednostavnijih šifri za upotrebu, budući da prati jednostavne supstitucijske metode. Prvo slovo alfabeta je zamijenjeno posljednjim, drugo slovo je zamijenjeno drugim od kraja i tako dalje.

Engleski alfabet može biti zamijenjen abecedom ili azbukom.

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

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

PIGPEN

šifra

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	

otvoreni tekst

M A L A

šifrat

┐ ┘ └ ┘

Cezarova šifra

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

UDCUHG → razred

Kada želiš da šifriraš riječ "razred" (+3) od slova "R" brojiš 3 slova u abecedi ili azbuci i upisuješ treće (...R- s,t,u) slovo "U".

Tako šifriraš svako slovo (A-b,c,d; ...Z-a,b,c (poslije "z" se kreće ispočetka abeceda); ...R-s,t,u; ...E-f,g,h;...D-e,f,g).

			а	б	в	г	д	ђ	е	ж	з	и	ј	к	л	љ	м	н	њ	о	п	р	с	т	ћ	у	ф	х	ц	ч	џ	ш	
←	А	Б	В	Г	Д	Ђ	Е	Ж	З	И	Ј	К	Л	Љ	М	Н	Њ	О	П	Р	С	Т	Ћ	У	Ф	Х	Ц	Ч	Џ	Ш	А	Б	В

ЋГКЋИЖ → разред

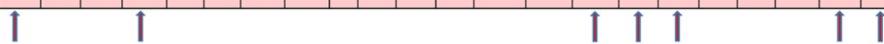
Polibijev kvadrat

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Ђ
2	Е	Ж	З	И	Ј	К
3	Л	Љ	М	Н	Њ	О
4	П	Р	С	Т	Ћ	У
5	Ф	Х	Ц	Ч	Џ	Ш

ЗДРАВО → 23 15 42 11 13 36

Afine šifra

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22



16- 15- 22- 4- 17- 1- 21 → POZDRAV

Atbaš šifra

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



G H A T F Z B → POZDRAV

Tags

Istraživanje i stvaranje

Igra i rad

Collections

Metodika i didaktika

Autorski tekstovi