Kriptografija u nastavi matematike

Jajetić, Sara

Sveučilište Josipa Jurja Strossmayera u Osijeku

Fakultet primijenjene matematike i informatike

Sveučilišni diplomski studij Matematika i informatika,
modul: nastavnički

Kriptografija u nastavi matematike

Diplomski rad

Mentor:

izv. prof. dr. sc. Ljerka Jukić Matić

Student:

Sara Jajetić

Osijek, 2024.

Sadržaj

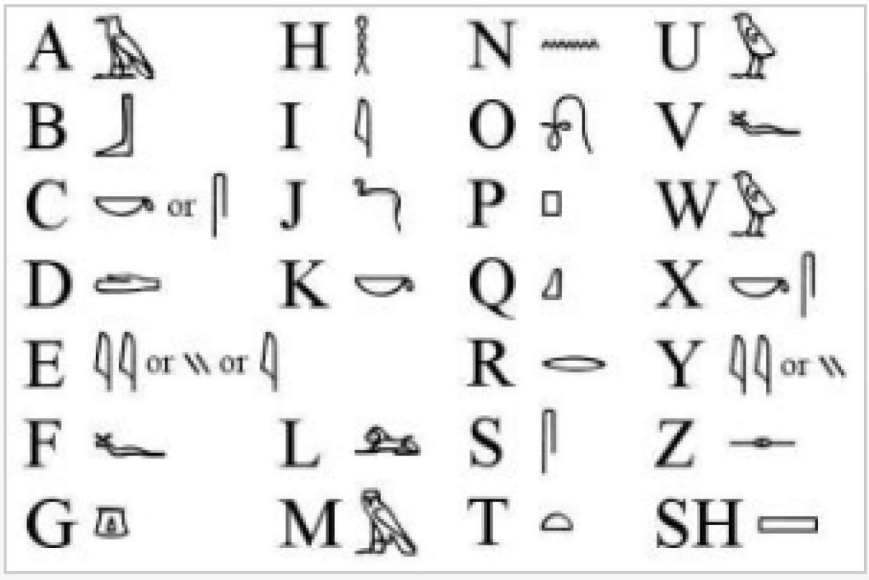
1 | Uvod

Kriptografija kao znanost je opširan pojam koji se spominje u raznim djelatnostima, filmovima, igrama, zanimanjima, a također i u školama. Kriptografija se može pojavljivati u raznim predmetima koje učenici uče u školama. Jedan od tih je i matematika. Sama poveznica između kriptografije i matematike je dakako opsežna. No, njihova povezanost u osnovnim i srednjim školama se najčešće izvodi u obliku radionica kroz poučan i zabavan način za učenike, ali isto tako i učitelje ili nastavnike. Sam cilj tih radionica je učenike upoznati sa samom kriptografijom, ali i na neki način to prikazati kroz igru gdje je cilj da učenici uz svoje znanje, sposobnosti i međusobno komuniciranje dođu do pojedinih rješenja.

Drugo poglavlje ovog rada daje uvid u razvoj same kriptografije kroz povijest te neke načine na koje su tada "slali" skrivene poruke. Nakon toga, u trećem poglavlju detaljno su opisani osnovni pojmovi u kriptografiji. Pomoću njih lakše je proučavati i koristiti se određenim metodama šifriranja i dešifriranja. U četvrtom poglavlju opisane su neke od metoda šifriranja i dešifriranja koja se mogu koristiti u raznim radionicama za učenike osnovnih i srednjih škola. Kroz primjere su opisani načini šifriranja te sam smisao pojedinih metoda. U petom poglavlju spominju se primjeri radionica u nastavi matematike gdje je opisano kako može neka radionica izgledati te što je potrebno da ona sadržava. U zadnjem poglavlju spominju se neki korisni savjeti za izradu radionica koji mogu uvelike pomoći učiteljima ili nastavnicima prilikom osmišljavanja pojedinih radionica.

2 | Kriptografija kroz povijest

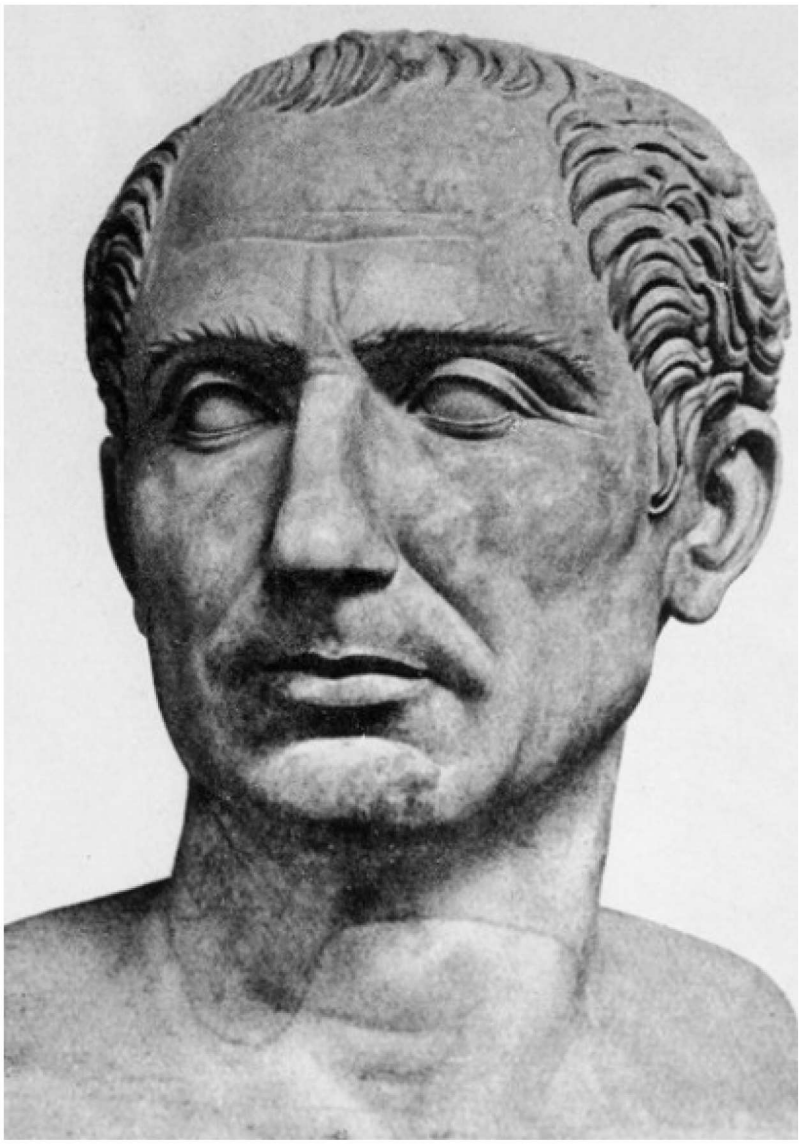
Pojam *kriptografije* prvi puta pojavljuje se još davne 2000. godine prije Krista. Tada se pojavljuju hijeroglifi kojima stari Egipćani ukrašavaju svoje grobnice. Hijeroglifi predstavljuju sličice koje obilježavaju nekakve stvari ili pojave. Ovaj sustav bio je neusavršen kôd za zamjenu znakova te time nije bio pretjerano pouzdan, no u to vrijeme bio je od velike koristi [6].



Slika 2.1: Hijeroglifi (prema [7])

U godinama obilježenim ratovima, sve veća potreba dolazi za skrivanjem poruka. Kroz povijest, ljudi su bili domišljati za smišljanjem poruka. Pojedine vojskovođe obrijale bi glavu glasnika te poruke napisali na nju. Nakon što bi glasniku narasla kosa, poslali bi ga na određeno odredište radi prijenosa poruke. Pojedini su se koristili upotrebom tinte iz raznih biljaka te pomoću njih skrivali svoje poruke. Kinezi su poruke pisali na svili koju bi zgužvali i natopili voskom. Spartanci su pomoću drvenog štapa slali poruke tako što bi namotali traku na štap te okomito na njoj napisali poruku. No, sve ove metode su se mogle lako otkriti te bi time stvarale opasnost. Tada se zapravo pojavljuje prava kriptografija koja ima tzv. proces *šifriranja* ili *kodiranja*. Njezin smisao je da poruka postane nerazumljiva tako što se slova isprepliću po nekom određenom pravilu između pošiljatelja i primatelja [5].

Supstitucija kao oblik šifriranja pojavljuje se još u hebrejskim tekstovima. Upravo je hebrejska šifra jedna od ranih poznatih supstitucijskih šifra gdje se svako slovo teksta zamijeni nekim drugim slovom. Jedna od najvažnijih metoda supstitucije je Cezarova šifra. Iako se sam Cezar dosta bavio tom metodom u Galskom ratu te ju je pokušavao na što bolji način iskoristiti, mnogi učenjaci smatrali su da se supstitucijska šifra ne može razbiti zbog velikog broja mogućih ključeva. Nakon određenog vremena, počinje razvoj kriptoanalize na istoku zahvaljujući velikom procvatu gramatike, lingvistike, matematike i statistike te su Arapi bili prvi koji su opisali tehniku kriptoanalize i time dokazali da se supstitucijska šifra vrlo lako može koristiti i pomoći u pojedinim stvarima [6].



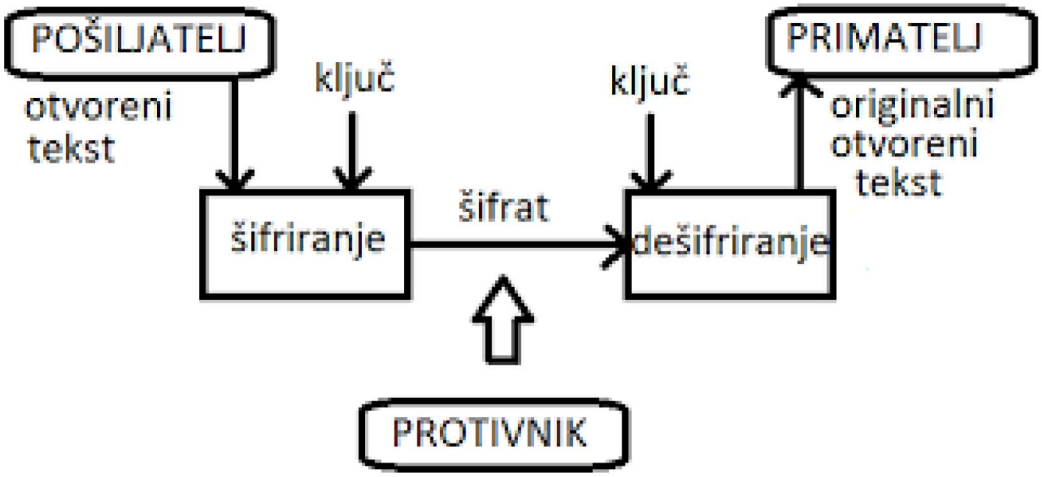
Slika 2.2: Gaj Julije Cezar (prema [8])

Kasnije kroz povijest dolazi do sve većeg razvoja šifriranja i uvođenja nekakvih novih metoda. Time se otežao posao kriptoanalitičarima, no s vremenom bi se i to poboljšalo. Poznate ličnosti koje su kroz povijest doprinijele razvoju kriptografije su: Alberti, Trithemius, Vigenère, Babbage, Playfair, Wadsworth, Jefferson, Enigma [5].

3 | Osnovni pojmovi u kriptografiji

Sama riječ *kriptografija* grčkog je podrijetla i u doslovnom prijevodu znači *tajnopis*. Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u oblicima čitljivim samo onima kojima su i namijenjene. Podrazumijeva se da će poruka biti isporučena nepromijenjena te da ju neće moći pročitati i razumijeti oni za koje nije namijenjena.

Cilj kriptografije je omogućiti komunikaciju između pošiljatelja (osoba koja šalje poruku) i primatelja (osoba kojoj je poruka namijenjena) tako da to komuniciranje u obliku poruka između te dvije osobe bude potpuno nerazumljivo nekoj trećoj osobi. U kriptografskoj literaturi, osobe između kojih se vrši komunikacija, tj. pošiljatelj i primatelj, uobičajeno nazivaju se *Alice* i *Bob*. Osoba do koje ne bi smjela doći poruka naziva se *Eva* ili *Oscar*. Poruka koju pošiljatelj želi poslati primatelju naziva se *otvoreni tekst*. Pošiljatelj najprije šifrira otovreni tekst s nekakvim unaprijed dogovorenim *ključem*. Tako se dobiva *šifrat* ili *kriptogram* koji se šalje nesigurnim komunikacijskim kanalom. Kada dođe u ruke neke druge osobe (koja nije primatelj) biva nerazumljiv te ju ta osoba ne može dešifrirati jer nema ključ. Na kraju, šifrat dolazi primatelju koji ga dešifrira pomoću ključa te dobiva otvoreni tekst [2].



Slika 3.1: Shema klasične kriptografije (prema [1])

Kriptoanaliza ili *dekriptiranje* je znanstvena disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka, a da se pri tome ne moraju poznavati pravila šifriranja i ključa.

Kriptografija i kriptoanaliza zajedno čini znanstvenu granu *kriptologiju*.

Kriptografski algoritam ili *šifra* je matematička funkcija, točnije sastoji se od dvije funkcije pri čemu se jedna koristi za šifriranje, a druga za dešifriranje.

Skup svih mogućih vrijednosti ključeva nazivamo *prostorom ključeva*.

Kriptosustav sastoji se od kriptografskog algoritma, otvorenih tekstova, šifrata te prostora ključeva. Oni se dijele po načinu na koji se obrađuje otvoreni tekst, tajnosti i javnosti ključa te tipu operacija koje se koriste pri šifriranju.

Način obrade otvorenog teksta temelji se prema podjeli na *blokovne šifre* i *protočne šifre*. Tajnost i javnost ključa odnosi se na podjelu na sustave s *tajnim* i sustave s *javnim* ključem. Tip operacija koje se koriste pri šifriranju dijeli se na *supstitucijske šifre* i *transpozicijske šifre* [2].

4 | Metode šifriranja i dešifriranja

Postoje razne metode šifriranja i dešifriranja s kojima se učenici mogu susresti u nastavi matematike i time kroz igru, razmišljanje i međusobne dijaloge naučiti mnoge korisne stvari, a ujedno se i zabaviti te razviti intelektualne vještine. Neke metode odgovaraju svim uzrastima učenika (bilo to osnovna ili srednja škola). No, postoje i metode koje nisu odgovarajuće za učenike nižih razreda osnovne škole zbog same zahtjevnosti i pojedinih pojmova koji njima u toj dobi nisu razumljivi. Također, postoje metode koje su predviđene za učenike srednjih škola zbog same zahtjevnosti i težeg postupka prilikom dešifriranja.

4.1 Cezarova šifra

Cezarova šifra jedna je od najpoznatijih i najranijih šifri. Nazvana je po Juliju Cezaru koji ju je koristio pri komunikaciji sa svojim generalima. Njezina osnova je supstitucija jednog slova s nekim drugim slovom. Postoji nekoliko tipova Cezarovih šifra koje su prilagođene pojedinom uzrastu učenika.

4.1.1 Originalna Cezarova šifra

Originalnu Cezarovu šifru koristio je sam Cezar u svojim ratovima prilikom komuniciranja sa svojim generalima i prijateljima.

Postupak šifriranja: svako slovo zamijeni se sa slovom koje se nalazi tri mjesta dalje u alfabetu. Tako slovo A zamijenimo slovom D, slovo B slovom E, a zadnja tri slova zamijenimo s početna tri slova, odnosno slovo X sa slovom A, Y s B te Z sa C. Tako bi se tekst MATEMATIKA (gledajući englesku abecedu) pomakom za tri mjesta u desno šifrirao u PDWHPDWLND, a tekst LAMPA šifrirao bi se u ODPSD [5].

Otvorena 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
Šifrirana 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

Slika 4.1: Originalna Cezarova šifra (prema [5])

4.1.2 Cezarova šifra s proizvoljnim pomakom

Postupak je isti kao u Originalnoj Cezarovoj šifri samo što pomak ne mora biti za tri mjesta, već za neki drugi broj. Npr. tekst JABUKA (gledajući englesku abecedu) s pomakom za pet mjesta u desno šifrira se u OFGZPF, a tekst LOPTA u QTUYF.

Otvorena 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
Šifrirana 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

Slika 4.2: Cezarova šifra s pomakom za pet mjesta

Isto tako kada bi se tekst JABUKA (gledajući englesku abecedu) s pomakom za osam mjesta šifriralo u desno, dobilo bi se RIJCSI. Tekst LOPTA šifriralo bi se u TWXBI.

Otvorena 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
Šifrirana abeceda	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

Slika 4.3: Cezarova šifra s pomakom za osam mjesta

4.2 Atbash šifra

Atbash šifra vrlo je stara supstitucijska šifra koja je izvorno razvijena za uporabu u hebrejskoj abecedi. Iako nije baš pouzdana metoda, u ono vrijeme bila je od velike koristi i značaja. Temelji se na tome da prvo slovo abecede zamijeni sa zadnjim slovo, drugo s predzadnjim itd. Ukoliko abeceda otvorenog teksta ima neparan broj slova, slovo koje se nalazi na $(n+1) : 2$ mjestu šifrirat će se u isto to slovo, dok u abecedi otvorenog teksta koja ima paran broj slova (engleska, hrvatska), niti jedno slovo neće se šifriranjem preslikati u to isto slovo. Npr. riječ HRANA (gledajući englesku abecedu) šifrirat će se u SIZMZ, a riječ LIVADA u OREZWZ [4].

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

Slika 4.4: Atbash šifra (prema [4])

4.3 Afina šifra

Afina šifra može se predstaviti tek učenicima sedmog razreda jer oni tada bivaju upoznati s pojmom *afine funkcije* $x \mapsto ax + b$. Postupak šifriranja je sljedeći: dobiva se tzv. ključ npr. $(5, 6)$ i riječ koju želimo šifrirati, npr. RIJEKA. Svako slovo alfabeta zamijenimo numeričkim ekvivalentom. Tada svaku koordinatu množimo s 5 te dodajemo 6. Ukoliko dobivena vrijednost je veća ili jednaka od 26 (toliko ukupno ima slova u engleskom alfabetu), tada tu vrijednost dijelimo s 26 i gledamo ostatak pri tom dijeljenju. Konačan rezultat zamijenimo s tim ostatkom. Time dobivamo: $(17, 8, 9, 4, 10, 6) \rightarrow (91, 46, 51, 26, 56, 6) \rightarrow (13, 20, 25, 0, 4, 6)$. Odnosno, riječ RIJEKA (gledajući englesku abecedu) odgovara šifratu NUZAEG. Ukoliko bi se gledala riječ LOPTA s istim tim ključem, rješenje tog šifriranja bilo bi JYDXG [2].

	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
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
y	6	11	16	21	0	5	10	15	20	25	4	9	14	19	24	3	8	13	18	23	2	7	12	17	22	1
	G	L	Q	V	A	F	K	P	U	Z	E	J	O	T	Y	D	I	N	S	X	C	H	M	R	W	B

Slika 4.5: Afina šifra s ključem (5,6) (prema [2])

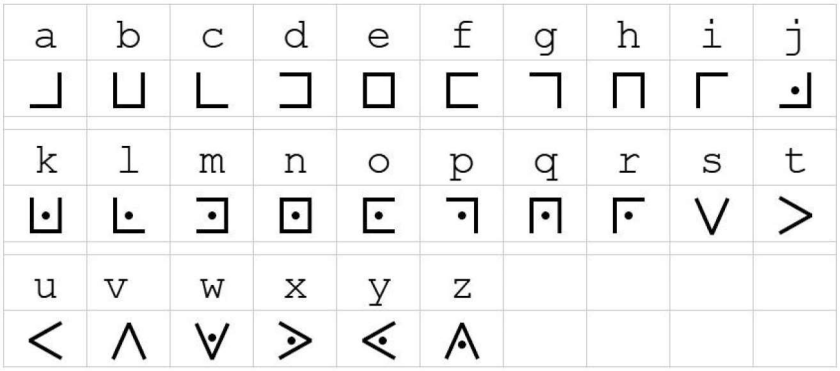
Kada bi se riječ RIJEKA (gledajući englesku abecedu) šifrirala uz ključ (7,4), rješenje bi bilo TIPGWE. Ukoliko bi se gledala riječ LOPTA s istim tim ključem, rješenje tog šifriranja bilo bi DYFHE.

	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
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
y	4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19	0	7	14	21	2	9	16	23
	E	L	S	Z	G	N	U	B	I	P	W	D	K	R	Y	F	M	T	A	H	O	V	C	J	Q	X

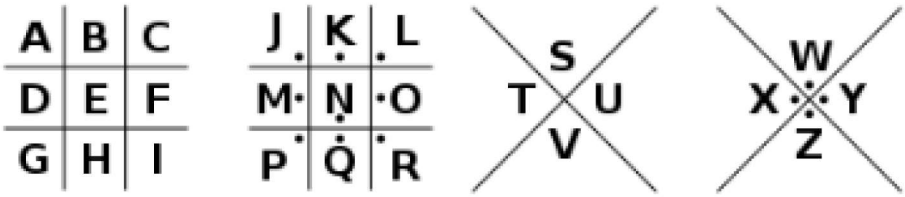
Slika 4.6: Afina šifra s ključem (7,4)

4.4 Fragmentarna šifra

Fragmentarna šifra (Pigpen šifra) nastala je u 18. stoljeću kada su masoni čuvali tajnost svojih spisa. Po njima ta šifra često nosi naziv i *masonska šifra*. Kod ove šifre je specifično što ona ne zamjenjuje jedno slovo drugim, nego na mjesto slova stavlja druge simbole. Riječ BUBA kada se šifrira (gledajući englesku abecedu) postaje $\sqcup < \sqcup <$ [4].



Slika 4.7: Fragmentarna šifra (prema [4])



Slika 4.8: Pigpen šifra (prema [4])

4.5 Playfairova šifra

Playfairova šifra je blokovska šifra gdje se parovi slova šifriraju tako da rezultat ovisi o oba slova. Algoritam se bazira na 5 × 5 matrici koja sadrži slova abecede. Postoje dvije vrste Playfairove šifre: bez upotrebe ključa i s upotrebom ključa [5].

4.5.1 Playfairova šifra bez ključa

Kod *Playfairove šifre bez ključa* matrica nastaje popunjavanjem slovima abecede po redovima. Zato ne postoji ključ. Kako je matrica 5 × 5 oblika, što znači da ima 25 slovnih mjesta, a engleska abeceda sastoji se od 26 slova, po dogovoru se poistovjećuju slova I i J. U slučaju da je otvoreni tekst na hrvatskom jeziku, poistovjećujemo V i W da bi se izbjegli mogući nesporazumi kod dešifriranja.

Postupak šifriranja:
Otvoreni tekst podijeli se na blokove koji se sastoje od samo dva slova. Nijedan blok ne smije sadržavati dva jednaka slova. Kako duljina teksta ne bi trebala biti parna, tada se između jednakih slova umeće novo slovo X (ono se najrjeđe koristi u svim jezicima). Bitno je da zadnji blok sadržava dva slova. To se osigurava tako što se slovo X doda na kraj bloka. Nakon podijele otvorenog teksta na blokove, pošiljatelj poruke uzima prvi blok i traži položaj unutar matrice riječi.

Postoje tri različita načina podijele položaja unutar matrice riječi. Ukoliko se slova nalaze u:

- istom retku, onda se svako slovo zamijeni s prvim njegovim slovom udesno;
- istom stupcu, onda se svako slovo zamijeni s prvim njegovim slovom ispod;
- nekom drugom položaju, onda se gleda pravokutnik čiji vrhovi čine ta dva slova. Redoslijed poretka ta dva vrha ovisi o samom bloku i to tako da najprije dođe ono slovo koje se nalazi u istom retku kao prvo slovo u početnom bloku [5].

Kada bi se šifrirao tekst TVOJA JE MASKA CRVENA, kao rješenje dobilo bi se QYTOD FB PCQFE BSZALC.

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

Slika 4.9: Matrica riječi (prema [5])

Otvoreni tekst: TVOJA JE MASKA CRVENA

Rastav na blokove: TV | OJ | AJ | EM | AS | KA | CR | VE | NA

Niz blokova: TV OJ AJ EM AS KA CR VE NA

Šifrirani tekst: QY TO DF BP CQ FE BS ZA LC

Slika 4.10: Playfairova šifra bez ključa

4.5.2 Playfairova šifra s ključem

Playfairova šifra s ključem je metoda kod koje matrica slova ovisi o ključu koji može biti ili neka proizvoljna riječ ili neka fraza. Matrica se popunjava po redovima i to tako da se prvo zapišu slova ključa (izbacuju se slova koja se ponavljaju), zatim se redom zapisuju preostala slova krenuvši od početka abecede (pazeći da ne zapišemo slova koja se pojavljuju kod ključa). Postupak šifriranja je isti kao i kod Playfairove šifre bez ključa.

Kada bi se uz ključ TAJNA šifrirao tekst LEINA MASKA JE SIVA, kao rješenje dobilo bi se RLNBK KNQQD EL RNWT.

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

Slika 4.11: Matrica riječi uz ključ (prema [5])

Otvoreni tekst: LEINA MASKA JE SIVA

Rastav na blokove: LE|IN|AM|AS|KA|JE|SI|VA

Niz blokova: LE IN AM AS KA JE SI VA

Šifrirani tekst: RL NB NK NQ QD EL RN WT

Slika 4.12: Playfairova šifra s ključem

4.6 Vigenerèova šifra

Vigenerèova šifra prvi puta se spominje sredinom 16. stoljeća kada ju je opisao Giovan Battista Bellaso. Kasnije u 19. stoljeću, zasluge su pogrešno pripisane Bellasovom istovremeniku, francuskom diplomatu i kriptografu Blaiseu de Vigenèreu. Tri stoljeća su mnogi vjerovali da je ovu šifru nemoguće razbiti. Sredinom 19. stoljeća Friedrich Kasiski prvi je objavio opću metodu dešifriranja Vigenerèove šifre.

Način šifriranja jako je sličan Cezarovom načinu šifriranja. Glavna razlika i karakteristika je ta što se kod Vigenerèove šifre pojavljuje ključ koji je sačinjen od bloka slova, odnosno neke kraće riječi. Zato je Vigenerèova šifra primjer blokovne šifre [2].

Postupak šifriranja je sljedeći:
npr. zadana je riječ INSTALACIJA koja se šifrira Vigenerèovom šifrom uz ključ ROSA. Prvo se mora svakome slovu (u ovome slučaju engleske abecede) dodijeliti pozicija. Odnosno A se nalazi na poziciji 0, B na poziciji 1, C na poziciji 2,..., Z na poziciji 25 (engleske abecede).

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Slika 4.13: Pozicija slova u engleskoj abecedi

Gledaju se slova kod zadanog ključa. Slovo R nalazi se na poziciji broj 17 engleske abecede, slovo O na poziciji broj 14, slovo S na poziciji broj 18 te slovo A na poziciji broj 0 u engleskoj abecedi. Svako slovo zadane riječi šifrira se u odnosu na jedno slovo iz zadanog ključa (kao što je prikazano na slici 4.14).

I	N	S	T	A	L	A	C	I	J	A
R	O	S	A	R	O	S	A	R	O	S
Z	B	K	T	R	Z	S	C	Z	X	S

Slika 4.14: Vigenerèova šifra

Svako slovo se pomiče u desno onoliko kolika je pozicija njegovog pripadnog slova u ključu. Odnosno, slovo I se pomiče za 17 mjesta udesno jer se slovo R nalazi na poziciji broj 17 engleske abecede. Slovo N pomiče se za 14 mjesta udesno jer se slovo O nalazi na poziciji 14 engleske abecede. Analogan je postupak i za ostala slova.

Šifriranjem riječi INSTALACIJA pomoću Vigenerèove šifre uz ključ ROSA dobiva se rješenje ZBKTRZSCZXS. Dešifriranje je analogno šifriranju samo se pomičemo unazad (tj. ciklički u lijevo).

Da bi se pojednostavnilo šifriranje ovom metodom, koristi se Vigenèreov kvadrat. Presjek stupca slova koje treba šifrirati iz zadane riječi i retka slova iz zadanog ključa daje rješenje šifriranog slova. Za dešifriranje se koristi analogan postupak.

	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

Slika 4.15: Vigenerèov kvadrat (prema [9])

4.7 Beaufortova šifra

Beaufortova šifra nastala je u 19. stoljeću. Opisao ju je irski časnik u Britanskoj kraljevskoj mornarici Sir Francisa Beaufort. Njezin način šifriranja jako je sličan Vigenèreovoj šifri [2].

Riječ MAJICA šifrirat će se u riječ ZUBDSK (vidi slika 4.16) pomoću Beaufortove šifre uz ključ LUK. Nakon što se svakom slovu zadane riječi koja se šifrira (u ovome slučaju engleske abecede) dodijeli redni broj (vidi slika 4.13) kao kod Vigenèreove šifre, tada se svako slovo zadanog ključa pomiče ulijevo za onoliko kolika je pozicija dodijeljenog slova iz zadane riječi koja se šifrira.

Slovo L pomaknut će se za 12 mjesta ulijevo jer se slovo M iz zadanog teksta za šifriranje nalazi na poziciji 12 u engleskoj abecedi. Slovo U pomaknut će se za 0 mjesta ulijevo jer se slovo A nalazi na poziciji 0 u engleskoj abecedi. Slovo K pomaknut će se za 9 mjesta ulijevo jer se slovo J nalazi na poziciji 9 u engleskoj abecedi. Slovo L pomaknut će se za 8 mjesta ulijevo jer se slovo I nalazi na poziciji 9. Slovo U pomaknut će se za 2 mjesta ulijevo zbog pozicije slova C te slovo K pomaknut će se za 0 mjesta ulijevo zbog slova A (vidi slika 4.16).

L	U	K	L	U	K
M	A	J	I	C	A
Z	U	B	D	S	K

Slika 4.16: Beaufortova šifra

Da bi se pojednostavnilo šifriranje ovom metodom, koristi se Beaufortov kvadrat. Presjek stupca slova koje treba šifrirati iz zadane riječi i retka slova iz zadanog ključa daje rješenje šifriranog slova.

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

Slika 4.17: Beaufortov kvadrat

4.8 Ostale metode

Postoje i razne ostale metode od kojih se također mogu smisliti pojedine radionice. Neke su teže i kompliciranije od prethodno navedenih, ali sam način na koji su nastale je poučan. Naime, nisu sve metode primjerene da se provode u svim razredima osnovne škole. Neke su toliko lagane da mogu i učenici razredne nastave koristiti se njima, odnosno dešifrirati pojedine zadatke. No, postoje metode koje su primjerene isključivo učenicima viših razreda osnovne škole te učenicima srednjih škola. Neke od tih metoda su: Jednokratna bilježnica, Bifid šifra, Stupčana transpozicija, Šifra s uzorkom, Savršeni kôd i mnoge druge. Za rješavanje i dešifrianje pjedinog otvorenog teksta koji je šifriran u nekoj od ovih metoda, ponekad je potrebno i biti dobar matematičar te dobro poznavati i služiti se nekim matematičkim zakonima i definicijama. No, kako se kriptografija najčešće provodi u obliku radionica u nastavi matematike gdje učenici moraju dešifrirati određene riječi i doći do konačnog rješenja, mnogim učenicima koji i nisu toliko dobri u matematici ovo može dosta pomoći za promišljanje o pojedinim problemima iz matematičkog aspekta. Grupni rad i dobra komunikaciju među ostalim učenicima dovodi do pozitivnog ozračja i ugodne atmosfere.

5 | Primjeri radionica u nastavi matematike

Učitelj ili nastavnik koji provodi s učenicima radionicu o kriptografiji i pojedinim metodama šifriranja i dešifriranja, trebao bi na početku objasniti teorijske osnove svake od tih metoda šifriranja, tj. kako su nastale, koja je metoda dešifriranja i princip dolaženja do rješenja.

5.1 Radionica za osnovnu školu

Primjer teksta zadatka jedne radionice za osnovnu školu (7. i 8. razred) u kojoj se spominju neke od prethodno objašnjenih metoda šifriranja:

Riti je učiteljica zadala zadatak da odgonetne sljedeću šifru uz koju je dobila par napomena: ***PDWHPDWLND L PIRKGLTIZURQZ V< QYYJ****. Rita se nikako ne može snaći te joj treba pomoć. Pomozi Riti doći do konačnog rješenja. Napomene su sljedeće:*

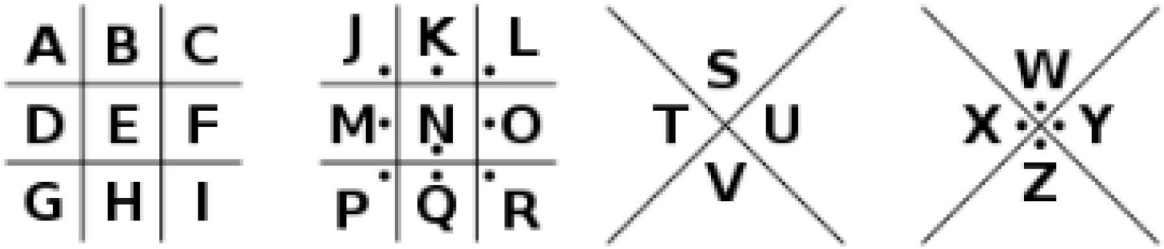
1) ***PDWHPDWLND L*** *dešifriraj pomoću Cezarove šifre (pomak za tri mjesta). Ispod otvorene abecede, ispiši šifriranu abecedu.*

Otvorena 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

2) ***PIRKGLTIZURQZ*** *dešifriraj pomoću Atbash šifre. Ispod otvorene abecede, ispiši šifriranu abecedu.*

Otvorena 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) ***V<*** *dešifriraj pomoću Fragmentarne šifre (Pigpen šifre).*



4) ***QYYJ*** *dešifriraj pomoću Afine šifre uz ključ (5,6). Ispod otvorene abecede, ispiši šifriranu abecedu.*

Otvorena 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

Rješenje radionice: MATEMATIKA I KRIPTOGRAFIJA SU COOL.

5.2 Radionica za srednju školu

Primjer teksta zadatka jedne radionice za srednju školu (3. i 4. razred) u kojoj se spominju neke od prethodno objašnjenih metoda šifriranja:

Noi je nastavnica zadala zadatak da odgonetne sljedeću šifru uz koju je dobio par napomena: ***LBUDLBYOFE KD QFFBLC. URDPDOBRKFDJK DW IYMZ.*** *Noa nikako ne može dešifrirati te mu treba pomoć. Pomozi Noi doći do konačnog rješenja. Napomene su sljedeće:*

1) ***LBUDLBYOFE KD QFFBLC*** *dešifriraj pomoću Playfairove šifre bez ključa. Rastavi šifrirani tekst na blokove. Prilikom dešifriranja, koristi se obrnutom metodom od šifriranja.*

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

2) ***URDPDOBRKFDJK*** *dešifriraj pomoću Vigenerèove šifre uz ključ KAVA. Prilikom dešifriranja, koristi se obrnutom metodom od šifriranja.*

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

3) ***DW IYMZ*** *dešifriraj pomoću Beaufortove šifre uz ključ MAK. Prilikom dešifriranja, koristi se obrnutom metodom od šifriranja.*

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Rješenje radionice: MATEMATIKA JE LAGANA. KRIPTOGRFAIJA JE COOL.

6 | Savjeti za izradu radionica

Prilikom planiranja i izrade radionica o kriptografiji, svaki učitelj ili nastavnik trebao bi pripaziti na par stvari. Neke od tih stvari su:

- uzrast učenika,
- znanje učenika,
- teorijska podloga,
- dostupno vrijeme,
- težina zadataka,
- zanimljivost zadataka,
- ugodna atmosfera.

Prvo i osnovno na što bi se trebalo pripaziti su sama uzrast učenika te njihovo znanje o matematici. Nisu sve metode šifriranja i dešifriranja prilagođene za sve uzraste učenika. Kod nekih je potrebno znanje nekih pojmova, definicija te same strukture prilikom izračunavanja pojedinih rješenja. Zbog toga na to treba ponajviše pripaziti.

Dakako, prilikom provođenja same radionice o kriptografiji u nastavi matematike, na početku treba dobro proći teorijsku podlogu samih metoda šefriranja i dešifriranja te tako učenike uvesti u samu temu radionice. Najbolje je to napraviti kroz nekakve primjere prikazane na prezentaciji te time uz razgovor s učenicima dobiti povratnu informaciju o onome što su čuli te jesu li to dobro shvatili.

Nikako se ne smije zanemariti dostupno vrijeme za izvedbu radionice jer time se nekada treba ograničiti broj zadataka i općenito sama težina zadataka kako bi uz uvodni dio teorije o samim metodama učenici uspjeli na zanimljiv i samostalan način (ili u grupama) riješiti pojedine zadatke za koje im uvijek trebaju biti dostupni učitelji ili nastavnici kako bi im pripomogli.

Osim o samom broju i težini zadataka, ti zadaci bi trebali biti zanimljivi te time i samo atmosferu unutar razreda činiti ugodnom. Za to se dakako treba pripremiti sam učitelj ili nastavnik te biti maštovit prilikom osmišljanja zadataka.

Literatura

[1] A. Bajac *Radionice klasične kriptografije u osnovnoškolskoj matematici*, Odjel za matematiku, Sveučilište u Rijeci, Diplomski rad, 2020.
https://repository.math.uniri.hr/islandora/object/mathri%3A178/datastream/PDF/view

[2] J. Bogović, *Kriptografija u nastavi matematike*, PMF-MO, Sveučilište u Zagrebu, Diplomski rad, 2021.
https://repozitorij.unizg.hr/islandora/object/pmf:9803/datastream/PDF/view

[3] A. Dujella, M. Maretić, *Kriptografija*, Element, Zagreb, 2007.

[4] K. Gradištanac, *Elementi kriptografije u nastavi*, Fakultet za odgojne i obrazovne znanosti, Sveučilište Josipa Jurja Strossmayera u Osijeku, Diplomski rad, 2018.
https://core.ac.uk/download/pdf/197870521.pdf

[5] J. Macanić, *Kriptografija u školi*, Fakultet primijenjene matematike i informatike, Sveučilište Josipa Jurja Strossmayera u Osijeku, Diplomski rad, 2012.
https://www.mathos.unios.hr/~mdjumic/uploads/diplomski/MAC06.pdf

[6] Singh, S. (2003). Šifre: kratka povijest kriptografije. Zagreb: Mozaik knjiga.

[7] https://www.kgz.hr/hr/dogadjanja/hijeroglifi-za-pocetnike/38524

[8] https://www.enciklopedija.hr/clanak/cezar-gaj-julije

[9] https://hr.wikipedia.org/wiki/Vigen%C3%A8reova_%C5%A1ifra

Sažetak

Mnogi smatraju kriptografiju pretečom današnje tehnologije pošto je kroz nju bila prikazivana komunikacija između pošiljatelja i primatelja kroz razne šifre. Danas se kriptografija pojavljuje u vrlo običnim, ali također i u neobičnim situacijama. Jedan od primjera je film Da Vincijev kôd. Također, kriptografija se može pojavljivati i u nastavi matematike. Iako nije uvrštena u obaveznu nastavu matematike, učitelji i nastavnici svojim učenicima mogu sate učiniti zanimljivijima kroz razne zadatke i mozgalice u obliku radionica gdje se naglasak stavlja na to kako nešto dešifrirati. Učenicima će takvi oblici sata biti vrlo korisni te uz zabavu, morat će se potruditi i dobro promisliti kako odgonetnuti pojedine šifre.

Ključne riječi

kriptografija, matematika, šifriranje, dešifriranje, pošiljatelj, primatelj, ključ, kriptoanaliza, kriptosustav, radionice, učenici

Cryptography in the teaching mathematics

Summary

Many consider cryptography to be the forerunner of today's technology because it was used to show communication between sender and receiver through various codes. Today, cryptography appears in very ordinary, but also in unusual situations. One example is the movie The Da Vinci Code. Also, cryptography can appear in mathematics lessons. Even though it is not included in the compulsory teaching of mathematics, teachers can make the lessons more interesting for their students through various tasks and brain teasers in the form of creative projects where the emphasis is placed on how to decipher something. Students will find such forms of lessons very useful, and in addition to having fun, they will have to make an effort and think carefully about how to decipher individual codes.

Keywords

cryptography, mathematics, encryption, decryption, sender, recipient, key, cryptanalysis, cryptosystem, workshops, students

Životopis

Rođena sam 3.6.1999. godine u Požegi. Završila sam Osnovnu školu Mitnica u Vukovaru te sam tokom svog osnovnoškolskog obrazovanja dva puta bila druga na Županijskom natjecanju iz matematike. Nakon završetka osnovne škole, upisujem Gimnaziju Vukovar (opći smjer) gdje se u tom periodu školovanja odlučujem za studiranje matematike. Srednju školu završavam u lipnju 2018. godine te iste godine u srpnju upisujem Prijediplomski studij Matematika na Odjelu za matematiku u Osijeku, sadašnjem Fakultetu primijenjene matematike i informatike. Nakon završetka tog studija s temom završnog rada "Rješavanje sustava nelinearnih jednadžbi primjenom Newtonove metode", u rujnu 2022. godine upisujem Sveučilišni diplomski studij Matematika i informatika, modul: nastavnički na istom fakultetu.