IZ NASTAVNE PRAKSE

Kreativne radionice za širenje matematičkih vidika: Kriptografija

Suzana Antunović[1]

Matematika, ako se gleda na pravi način, ne posjeduje samo istinu, nego i iznimnu ljepotu. Ovo su riječi slavnog matematičara Bertranda Russella koje bi nas, profesore i nastavnike, trebale nadahnuti da svoje učenike i studente usmjerimo na to da matematiku promatraju na pravi način, s oduševljenjem i znatiželjom s kojom smo je i mi nekada promatrali. Učenici se često žale da je matematika dosadna, teška i da nema primjenu u stvarnom životu. Opterećeni su formulama, definicijama i zadatcima kojima ne vide svrhu, što stvara određeni otpor prema matematici. U ovom članku predstavljena je radionica koja se može prilagoditi različitim uzrastima, a cilj je da se učenicima na zanimljiv i pristupačan način približe grane matematike s kojima se rijetko imaju priliku susresti tijekom školovanja. Osmišljena je na način da učenici sudjeluju u aktivnostima dešifriranja koje su prilagođene njihovu uzrastu, bez potrebnog posebnog matematičkog predznanja, a matematiku prikazuju u potpuno novom svjetlu i omogućavaju širenje matematičkih vidika. Na taj način možemo učenike potaknuti da sami dolaze do određenih matematičkih spoznaja i oblikuju dijelove matematičkog svemira.

Uvod

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati. Sama riječ *kriptografija* grčkog je podrijetla i mogla bi se doslovno prevesti kao *tajnopis* [1].

Osnovni zadatak kriptografije je omogućiti dvjema osobama komuniciranje na način da treća osoba ne može razumjeti njihove poruke. Poruku koja se šalje nazivamo *otvoreni tekst* (engl. *plaintext*). Pošiljatelj transformira otvoreni tekst koristeći unaprijed dogovoreni *ključ* (engl. *key*). Taj postupak naziva se *šifriranje*, a dobiveni rezultat nazivamo *šifrat* (engl. *ciphertext*) ili *kriptogram*. Primatelj koji zna ključ kojim je šifrirana poruka može *dešifrirati* šifrat i odrediti otvoreni tekst [1].

[1]Suzana Antunović, Prirodoslovno-matematički fakultet Sveučilišta u Splitu

Jednu od najstarijih poznatih tehnika šifriranja podataka koristili su Spartanci oko 500. godine prije Krista. Skital je šipka određenog promjera na koju bi se omotala traka pergamenta. Kada bi se odmotala, tekst je djelovao nepovezano. Jedini način dešifriranja je da se traka namota na šipku istog promjera [2]. Ovo je bio jedan od prvih poznatih primjera transpozicijske šifre. U transpozicijskoj šifri slova u riječi ostaju ista, ali se mijenja njihova pozicija u riječi.

Slika 1. Skital, alat za podatke koji je korišten oko 500. g. prije Krista [4]

U srednjem vijeku arapski učenjaci primjenjivali su analizu frekvencija za razbijanje supstitucijskih šifri u kojima se slovo ili više njih mijenja nekim drugim simbolom, slovom ili brojem [3].

Tijekom Drugog svjetskog rata kriptografija je doživjela dramatičan procvat. Većina njemačke vojne komunikacije bila je šifrirana pomoću Enigme, uređaja koji se sastojao od kompleksnog sustava električnih rotora i priključnih ploča. Njegovo konačno dešifriranje koje je proveo Alan Turing i njegov tim u Bletchley Parku smatra se prekretnicom u ratu i razvoju računalnih znanosti i matematičke logike.

Danas je kriptografija temelj kibernetičke sigurnosti. Koristi se pri zaštiti e-pošte, šifriranju financijskih podatka i osiguravanju razgovora, često se oslanjajući na koncepte kao što su modularna aritmetika, faktorizacija na proste faktore i eliptične krivulje.

Radionica

Radionica opisana u ovom članku održana je u sklopu stemKa konferencije 2024. godine u Karlovcu. Cilj je bio upoznati učenike osmog razreda osnovne škole

Slika 2. Detalj s radionice „Šifre koje su promijenile svijet" održane za učenike prvog razreda srednje škole u sklopu stemKa konferencije u Karlovcu 2024. godine (uz dopuštenje autora)

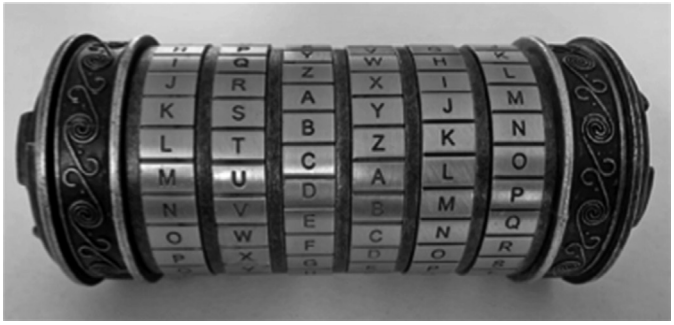
i prvog razreda srednje škole s nekim zanimljivim šiframa i omogućiti im da sami riješe danu zagonetku.

Pomoću Cezarove, masonske, *dancing men* i Vigenèreove šifre kodiran je sljedeći tekst:

Legenda kaže da su u Karlovcu dvije,
u vodama čistim one žive.
Magično biće, pola riba, pola žena,
tajanstvenu pjesmu pjeva.
Njeno ime je

_ _ _ _ _ _

Učenici su dobili tekst šifriran različitim šiframa i materijale za dešifriranje. Nakon što se dešifrira tekst, dobije se zagonetka čije je rješenje SIRENA ujedno i lozinka za otvaranje kripteksa kakvog prikazuje Slika 3. Kripteks je uređaj koji se sastoji od cilindara na kojima su navedena slova (engleske) abecede. Pravilan položaj cilindara oblikuje riječ koja otvara kripteks. Unutar njega moguće je staviti novu poruku ili sliku. Učenicima je također predloženo da detaljnije pregledaju kripteks i pokušaju shvatiti mehaniku rada, na koji način se postavlja šifra i na koji način pravilno postavljena šifra otvara kripteks. Radionicu je moguće provesti u grupama ili individualno.

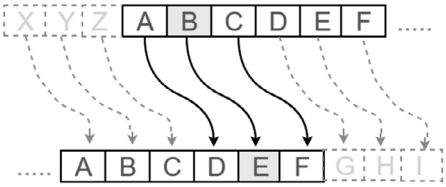


Slika 3. Kripteks je uređaj u koji je moguće pohraniti poruku, a za otvaranje je potrebna tajna riječ.

Vrste šifri

1. Cezarova šifra

Znameniti rimski vojskovođa i državnik Gaj Julije Cezar u svojoj se komunikaciji koristio šifrom u kojoj su se slova otvorenog teksta zamjenjivala slovima koja su se nalazila tri mjesta dalje u abecedi. Pretpostavljamo da se alfabet ciklički nastavlja, tj. da nakon zadnjeg slova Z ponovo dolaze A, B, C. Danas se Cezarovom šifrom nazivaju i šifre istog oblika s pomakom različitim od tri [1].



Slika 4. U Cezarovoj šifri slovo otvorenog teksta mijenja se slovom koje je pomaknuto za 3 mjesta u abecedi.

Za dešifriranje teksta koristi se Cezarov kotač koji je vrlo jednostavan za izradu. Predlošci za printanje dostupni su besplatno online na više mjesta, npr. [5]. Cezarov kotač koristi se na sljedeći način: unutarnji (manji) krug namjesti se na vanjski krug tako da slova A budu poravnata. Zatim se manji krug pomiče u smjeru suprotnom od kazaljke na satu za određeni broj mjesta (u ovom slučaju 11). Na taj se način slovo A na većem krugu poklopi sa slovom L na manjem krugu, što znači da slovo A u šifratu predstavlja slovo L u otvorenom tekstu.

Slika 5. Cezarov kotač koji se koristi za dešifriranje Cezarove šifre

Pomak: **11**

"Šifre koje su promijenile svijet"

ATVTCSP ZPOT SP HJ J ZPGADKRJ
SKXYT J KDSPBP RXHIXB DCT OXKT
RPGDQCD QXRT EDAP GXQP EDAP
OTCP IPYPCHIKTCJ EYTHBJ EYTKP
CYTCD XBT YT

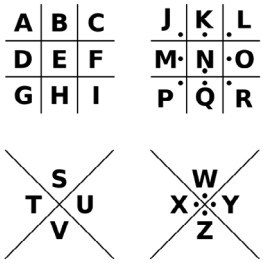
--- --- --- --- --- ---

Slika 6. Radni materijali za Cezarovu šifru koje su dobili sudionici radionice

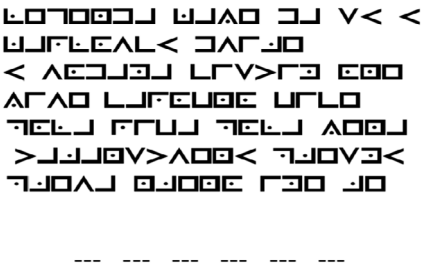
2. Masonska šifra

Riječ je o geometrijskoj supstitucijskoj šifri u kojoj se slova zamjenjuju geometrijskim oblicima, kako prikazuje Slika 7. Vjeruje se da su ovu drevnu šifru koristili vitezovi tijekom križarskih ratova. Početkom 18. stoljeća počeli su je koristiti masoni kako bi sačuvali tajnost svojih zapisa te za korespondenciju između vođa loža [6]. Na groblju crkve Svetog Trojstva u New Yorku nalazi se nadgrobni spomenik iz 1697. godine, na kojem je tekst *memento mori* šifriran masonskom šifrom. Vjeruje se da je to jedan od najranijih dokaza da su šifru koristili masoni.

Masonska šifra ponekad se naziva i „pigpen". Ime je dobila jer korišteni simboli izgledaju kao svinjci ili ograđeni prostori kakvi se mogu vidjeti na farmama. Svako slovo skriveno je unutar dijela rešetke koja podsjeća na jednostavan oblik ograde.



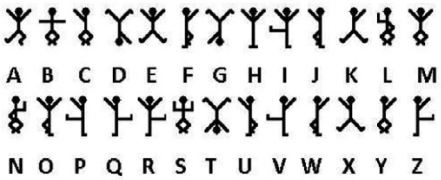
Slika 7. Masonska šifra [7]



Slika 8. Tekst šifriran pomoću masonske šifre

3. Dancing men

Dancing men je oblik zamjenske šifre koju je osmislio Arthur Conan Doyle 1903. godine i upotrijebio je u svojoj kratkoj priči o Sherlocku Holmesu *The Adventure of the Dancing Men*. Radnja priče fokusirana je na Hiltona Cubitta i njegovu suprugu Elsie, na čijem se imanju pojavljuju čudni crteži u obliku ljudi koji plešu. Cubitt traži pomoć Sherlocka Holmesa jer crteži postaju sve češći i zlokobniji. Holmes počinje analizirati crteže i shvaća da su oni zapravo zamjenska šifra - svaki plešući čovječuljak predstavlja slovo abecede. Verzija čovječuljka koji drži zastavicu označava da se slovo koje predstavlja nalazi na kraju riječi.



Slika 9. Abeceda šifre „dancing men" [8]

Holmesova metoda za dešifriranje izvrstan je primjer klasičnog razbijanja šifri pomoću logike i analize frekvencija. Na primjer, jedna poruka je imala isti simbol ponovljen tri puta zaredom. Holmes je pretpostavio da je vjerojatno riječ o slovu E

pošto je to najčešće korišteno slovo u engleskom jeziku. Zatim je usporedio koliko se često određeni simboli pojavljuju u svim porukama. Budući da su E, T, A, O, N najčešća slova u engleskom jeziku, logično je pretpostaviti da simboli koji se često pojavljuju odgovaraju nekom od tih slova.

Konačno, sve što je pretpostavio uvrštava se u poruke. Ukoliko se na taj način dobije smislena riječ ili tekst, znači da su pretpostavljena slova bila ispravna. U suprotnom se prilagođava tekst ovisno o kontekstu i smislenosti riječi.

Slika 10. Tekst šifriran pomoću dancing men šifre

4. Vigenèreova šifra

Vigenèreova šifra je polialfabetska supstitucijska šifra. U monoalfabetskoj šifri (poput Cezarove šifre) svako se slovo u otvorenom tekstu svaki put zamjenjuje istim slovom. Dakle, ako A jednom postane D, uvijek postaje D. Ali u polialfabetskoj šifri, isto slovo u otvorenom tekstu može biti šifrirano različitim slovima, ovisno o položaju u tekstu i ključu. To čini analizu frekvencije mnogo težom. Ova šifra stoljećima se smatrala šifrom koja se ne može dešifrirati i uvelike se koristila za osiguravanje vojnih i diplomatskih komunikacija.

Pokažimo proces šifriranja na primjeru riječi RAVNINA (Slika 11.)

- Korak 1: Poravnamo ključnu riječ (u ovom slučaju ključna je riječ *key*) s porukom. Ako je poruka duža od ključne riječi, ponavljamo ključnu riječ dok ne pokrijemo sva slova u otvorenom tekstu

  Poruka: R A V N I N A

  Ključna riječ: K E Y K E Y K

- Korak 2: Pretvorimo slova u otvorenom tekstu i ključnoj riječi u brojčane vrijednosti (A = 0, B = 1, ..., Z = 25). Koriste se vrijednosti od 0 do 25 jer standardna engleska abeceda ima 26 slova.

- Korak 3: Zbrojimo brojčane vrijednosti parova slova u poruci i ključnoj riječi i zbroj pogledamo modulo 26 jer pretpostavljamo da se abeceda ciklički ponavlja.
- Korak 4: Dobivene brojčane vrijednosti prebacimo u slova abecede na isti način kao u koraku 2.

Slovo u poruci	Vrijednost slova	Ključno slovo	Vrijednost ključa	Zbroj (mod 26)	Šifrirano slovo
R	17	K	10	(17 + 10) % 26 = 1	B
A	0	E	4	(0 + 4) % 26 = 4	E
V	21	Y	24	(21 + 24) % 26 = 19	T
N	13	K	10	(13 + 10) % 26 = 23	X
I	8	E	4	(8 + 4) % 26 = 12	M
N	13	Y	24	(13 + 24) % 26 = 11	L
A	0	K	10	(0 + 10) % 26 = 10	K

Slika 11. Primjer šifriranja riječi ravnina pomoću Vigenèreove šifre

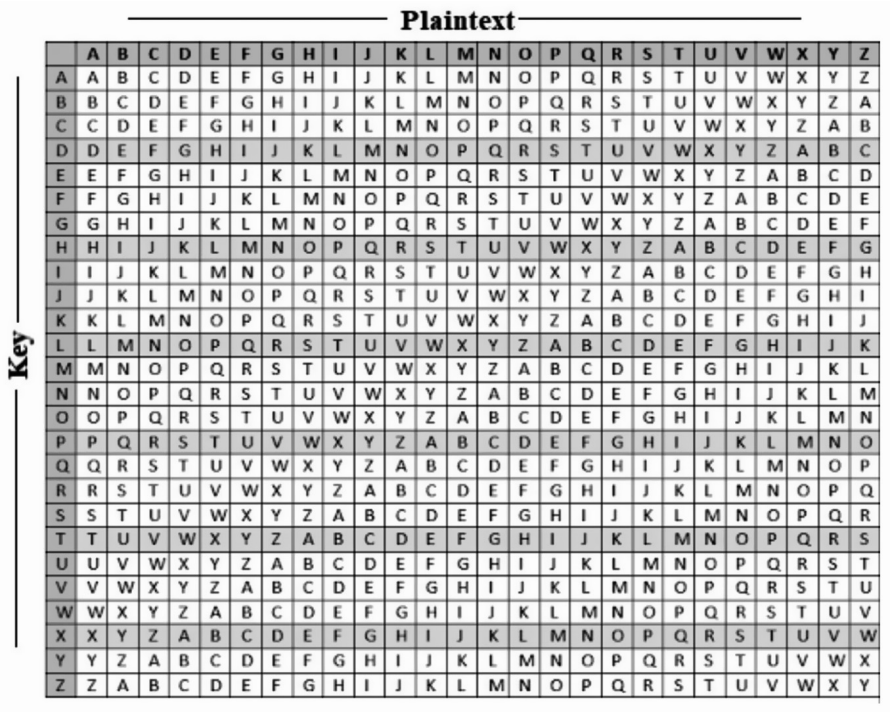
Za šifriranje i dešifriranje često se koristi *Vigenèreov kvadrat* kakav prikazuje Slika 12. Koristeći Vigenèreov kvadrat proces šifriranja obavljamo na sljedeći način. Slova u retcima predstavljaju slova ključne riječi, a slova u stupcima predstavljaju otvoreni tekst. Presjek retka sa slovom K iz ključne riječi i stupca sa slovom R iz otvorenog teksta (poruke) daje slovo B. To znači da će slovo R u otvorenom tekstu biti šifrirano slovom B. Zatim odredimo presjek retka sa slovom E iz ključne riječi i stupca sa slovom A iz otvorenog teksta RAVNINA. Dobiveni presjek je slovo E. Nastavljajući ovaj proces dobijemo da je traženi šifrat BETXMLK.

Pokažimo proces dešifriranja riječi BETXMLK, za koju znamo da daje otvoreni tekst RAVNINA, pomoću Vigenèreovog kvadrata. Poravnamo šifrat i ključnu riječ. Ako je šifrat duži, ključnu riječ ponavljamo.

Šifrat: B E T X M L K

Ključna riječ: K E Y K E Y K

U retku sa slovom K iz ključne riječi tražimo slovo B. Zatim pogledamo stupac u kojem se slovo B nalazi i dolazimo da zaključka da slovo B u šifratu predstavlja slovo R u otvorenom tekstu. U retku sa slovom E iz ključne riječi pronađemo slovo E iz šifrata i pogledamo kojem stupcu pripada. Nastavljamo postupak sve dok ne dešifriramo cijelu poruku.



	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 12. Vigenèreov kvadrat [9]

Zaključak

Ovakve radionice učenicima pružaju priliku da istraže matematičke pojmove koji se rijetko spominju u učionici i nisu dio standardnog gradiva. Također, mogu pomoći u stvaranju dinamičnijeg i uzbudljivijeg iskustva učenja. Cilj je potaknuti radoznalost i dublje razumijevanje uvodeći praktične aktivnosti i navodeći učenike da sami rješavaju probleme i donose zaključke o problemima i situacijama s kojima se možda nisu imali prilike ranije susresti. Učenici su imali prilike podijeliti svoje dojmove nakon radionice. Dojmovi su bili mahom pozitivni jer su svi, bez obzira na matematičku pozadinu, mogli sudjelovati u radionici. Istražujući klasične šifre, učenici ne samo da su se bavili matematičkim razmišljanjem na praktičan način, već su i otkrili kako rješavanje problema nadilazi tradicionalne vježbe u učionici.

Literatura:

1. A. Dujella i M. Maretić, Kritografija, Zagreb: Element, 2007.
2. M. L. M. Diepenbroek, *Myths and Histories of the Spartan scytale*: *A comprehensive review and reassessment of the extant sources describing the cryptographic Spartan device known as the scytale to challenge the view promoted by modern historians of cryptography that denies the scytale its deserved status as a vehicle for secret communication in the ancient world,* Univerity of Bristol, 2021.
3. L. D. Broemeling, „An account of early statistical inference in Arab cryptology," *The American Statistician*, vol. 65, no. 4, p. 255–257, 2021.
4. „Scytale, Wikipedia," https://en.wikipedia.org/wiki/Scytale#/media/File:Skytale.png (20. 2. 2007.)
5. „Science form Scientists," https://www.sciencefromscientists.org/wp-content/uploads/2019/03/caesar-wheel-DIY.pdf
6. W. K. MacNulty, Freemasonry: symbols, secrets, significance, London: Thames & Hudson, 2006.
7. „Pigpen cipher, Wikipedia," https://en.wikipedia.org/wiki/Pigpen_cipher#/media/File:Pigpen_cipher_key.svg (5. 11. 2021.)
8. „Even Wiki". https://evil.fandom.com/wiki/The_Dancing_Men
9. B. Infinity, „Vigenere cypher in Phyton," https://www.boardinfinity.com/blog/vigenere-cipher-in-python/