Kriptografija u nastavi matematike u osnovnoj školi

Ivan Nađ
Visoko učilište Algebra, Zagreb, Hrvatska; Fakultet hrvatskih studija, Sveučilište u Zagrebu, Zagreb, Hrvatska;
Osnovna škola Eugena Kvaternika, Velika Gorica, Hrvatska
ivan.nadjzg@gmail.com ; inad@racunarstvo.hr ; inad@hrstud.hr

Sažetak **- Nastavnici matematike se često u nastavi susreću s pomanjkanjem interesa i motivacije učenika za matematiku. Kako istraživanja pokazuju da rad nastavnika matematike utječe i na rad i motivaciju učenika, na nastavnicima je velika odgovornost da svojim pristupom i zalaganjem obogate nastavni proces novim sadržajima i aktivnostima koji bi bili motivirajući učenicima. U članku se opisuju šifre primjerene za rad u osnovnoj školi te predlažu nastavni sadržaji iz matematike u koje bi se te šifre mogle uključiti.**

Ključne riječi - kriptografija; matematika; motivacija u nastavi matematike; osnovna škola

I. OSNOVNO O KRIPTOGRAFIJI

Kriptografija je, prema [1], znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kojemu su namijenjene može pročitati.

Proces u kojem se poruka (takva se poruka u literaturi često naziva otvoreni tekst) koju pošiljatelj šalje primatelju transformira, često koristeći tzv. ključ, naziva se šifriranje. Rezultat šifriranja nazivamo šifrat.. Primatelju je ključ (ili način šifriranja ako se ključ ne koristi) unaprijed poznat te ga on koristi kako bi šifrat transformirao natrag u početnu poruku. Taj proces transformacije šifrata u početnu poruku naziva se dešifriranje. Ključ ima istu funkciju kao i obični ključ za vrata, zaključava (kada početnu poruku transformiramo u šifrat) i otključava (kada šifrat nazad transformiramo u početnu poruku).

Često se pri upoznavanju s kriptografijom, a pogotovo u nižim uzrastima na koje je usmjeren i ovaj rad, otvoreni tekst, šifrat i ključ pišu velikim tiskanim slovima, kako će biti i u ovom radu, prvenstveno usmjerenom na zabavne strane kriptografije i prijedloge za uključenje u nastavu.

II. ZAŠTO KRIPTOGRAFIJA?

Možda najbolji odgovor na to pitanje piše u samom uvodu članka „Kriptografija u školi“ [2]. U tom uvodu piše: „Kriptografija ima veliki potencijal kojim može obogatiti nastavu matematike. Može joj dati uzbudljivost, dramatičnost, dinamičnost, a kod učenika pobuditi znatiželju i kreativnost.“.

Primjeri iz kriptografije nastavnicima mogu pomoći obogatiti nastavni sat, dati mu dinamiku, promijeniti ustaljene načine na koje učenici usvajanju nastavne sadržaje. Pogotovo je to bitno ako uzmemo u obzir motivaciju i općeprihvaćeni stav među učenicima prema matematici u školi. Učenici često misle da je matematika

dosadan predmet te ju uče samo radi ocjene. To potvrđuju i rezultati istraživanja koje su 2006. godine na 374 učenika osmih razreda, u deset osnovnih škola grada Zagreba, provele Benček, Marenić [3]:

- 81.6% učenika se na nastavi matematike dosađuje
- 58.7% učenika uči matematiku samo radi ocjene
- tek nešto više od 15% učenika uči matematiku zbog zanimljivosti sadržaja.

U istom se istraživanju saznalo i da 72% učenika kaže da rad njihovih nastavnika matematike utječe i na rad njih samih. Zato nastavnici, kao voditelji nastavnog procesa, imaju značajnu ulogu da nastavu obogate novim načinima rada u razredu i sadržajima kao što je, primjerice, kriptografija, iako se kriptografija niti ništa slično s kriptografijom niti ne spominje u novom kurikulumu za nastavni predmet matematika [4], kako u redovnim tako niti u dodatnim sadržajima u osnovnoj školi.

Utjecaj kriptografije na motivaciju učenika proučavali su i Aydin, Güler i Sükrü Özdemir [5]. Eksperiment su provodili na učenicima iste generacije u tamošnjem 8.razredu (starosno odgovaraju 8.razredu naših učenika), podijeljenima u dvije grupe, eksperimentalnu grupu i kontrolnu grupu. Prije podjele u grupe su učenike testirali kako bi bili sigurni da učenici u obje grupe imaju podjednaka matematička znanja i vještine te podjednaku motivaciju za učenje matematike. U kontrolnoj grupi se nastava matematike odvijala na uobičajeni tradicionalni način, a u eksperimentalnoj grupi su, gdje je god to moglo biti ostvareno, kao motivaciju koristili različite kriptografske aktivnosti. Nakon tri tjedna eksperimenta, obje grupe su ponovno testirali te rezultate analizirali ANOVA testom hipoteza kako bi se uvjerili jesu li dobiveni rezultati statistički značajni. Pokazalo se da su rezultati, koji govore da je došlo do značajnog povećanja motivacije za učenje matematike, statistički značajni. Zanimljiv rezultat je i da je u kontrolnoj grupi motivacija ostala gotovo ista u odnosu na onu prije eksperimenta.

III. KRIPTOGRAFIJA U NASTAVI

Prema Borelli, Fioretto, Sgarro i Zuccheri [6], u školama sjeveroistočne Italije se, bez upotrebe ikakve tehnologije osim papira i olovke, na 300 učenika od sedam do deset godina počeo provoditi eksperimentalni program, a koji se djelomično provodi i danas zbog pozitivnih reakcija učenika i učitelja.

Učenici su bili podijeljeni u dvije skupine, kriptografe (šalju tajne poruke) i kriptoanalitičare (nastoje saznati što zapravo u tajnoj poruci piše, odnosno „razbiti ju“). Kriptografi su najprije započeli s šifriranjem u kojem su svako slovo poruke zamijenili slovom koje se nalazi određeni broj mjesta u abecedi dalje, tj. s Cezarovom šifrom. Primjerice, ako radimo pomak od jednog mjesta, onda bi riječ „MATKA“ bila šifrirana u riječ „NBULB“ (abeceda se ciklički nastavlja, tj. nakon zadnjeg slova abecede niz slova opet nastavljamo prvim slovom abecede, drugim slovom abecede itd.) Za dešifriranje su kriptoanalitičari svako slovo šifre, budući da su znali postupak šifriranja, slovo po slovo pomicali za isti broj mjesta u abecedi, sve dok metodom pokušaja i promašaja nisu došli do smislene poruke. Tu su kriptografi eksperimentirali i s više varijanti šifrata, koji uključuju i koji ne uključuju razmake među riječima kako bi zbunili kriptoanalitičare.

Kada im je to postalo prejednostavno, prešli su na iduću fazu u kojoj su unaprijed dogovorena slova u poruci (npr. drugo, peto i osmo) izbacili te ih u obrnutom redoslijedu napisali na kraju poruke. Primjerice, ako izbacimo drugo, peto i osmo slovo, onda bismo riječ „MATEMATIKA“ šifrirali u riječ „MTEATKAIMA“. Tu su također eksperimentirali s uključivanjem i neuključivanjem razmaka među riječima. Eksperimentirali su i s uključivanjem tzv. numeričkog ekvivalenta (udaljenosti slova u abecedi od prvog slova abecede) slova u abecedi umjesto samog tog slova.

U sljedećoj fazi, koja je bila ujedno i posljednja, zajednički su radili na dešifriranju tekstova od približno 300 znakova koristeći učestalost svakog slova u izrazima, tj. koristeći tzv. frekvencijsku analizum znajući da je riječ o Cezarovoj šifri. Učestalost (frekvenciju) slova su analizirali tako da su na običnom nešifriranom tekstu od 1000 riječi bilježili frekvencije svakog slova te onda izrađivali tablice s frekvencijama (histograme) jer je vrlo vjerojatno da najfrekventnija slova šifrata odgovaraju najfrekventnijim slovima u jeziku, pogotovo ako je šifrat nešto dulji. Primjerice, prema [1], u hrvatskom jeziku su najzastupljenija slova „A“,„I“,“O“ i „E“, a najmanje „H“ i „F“. Uočavali su i posebne odnose među slovima, tj. analizirali česte bigrame (parove slova) i trigrame (nizove od tri slova) te si i tako olakšavali kriptoanalizu, odnosno „razbijanje“ skrivene poruke. Primjerice, prema [1], u hrvatskom su jeziku najčešći bigrami „JE“,„NA“ i „RA“, a trigram „IJE“.

U ovom se eksperimentu također pokazalo da je došlo do povećanje motivacije učenika za učenje matematike. Ovakav eksperiment bi se vrlo lako mogao provesti i u nastavi kod nas već i to već u nižim razredima jer učenici na zanimljiv način ponavljaju slova abecede, odnose među slovima, riječi, izraze i slično.

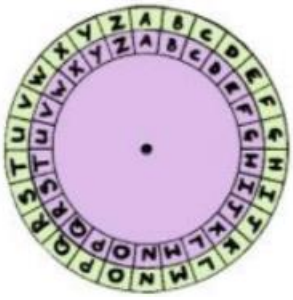
Otvoreni tekst	P	R	S	T	I
Numerički ekvivalent	21	22	23	25	12
Šifrat	S	Š	T	V	K
Numerički ekvivalent	23	24	25	27	14
Zadatak	Od zbroja numeričkih ekvivalenata slova šifrata oduzmi zbroj numeričkih ekvivalenata slova otvorenog teksta.				

TABLICA I. PRIMJER ZADATKA S CEZAROVOM ŠIFROM

Što se nastave matematike tiče, frekvencijska analiza može biti pomoć ili motivacija i pri usvajanju ili ponavljanju (stupčastih dijagrama, histograma, grafova, frekvencija i postotaka (relativnih frekvencija), a izražena je i korelacija s nastavom povijesti (povijesni značaj šifri) i hrvatskog jezika. Moguće je korelirati i s nastavom nekog stranog jezika ako učenicima dajemo tekst na nekom stranom jeziku, a time ih moguće i motivirati za upis izbornog drugog stranog jezika. Korelirati možemo i s nastavom informatike ako učenicima odlučimo dati tekst na računalima pa da, koristeći računala ili tablete, računaju frekvencije koristeći naredbe u nekom programu za obradu teksta, primjerice MS Excelu. Učenici mogu na računalima i izrađivati tablice i dijagrame, a što onda može i uštediti dosta vremena za izvođenje eksperimenta na satu matematike ili pak omogućiti drugačiji način prezentacije rezultata eksperimenta. Cezarovu šifru možemo, primjerice, iskoristiti kao motivaciju ili dodatno pojašnjenje funkcija.

Također, u petom i u nižim razredima možemo, primjerice, posebno zbrajati numeričke ekvivalente slova početne poruke i posebno numeričke ekvivalente slova šifrata te ta dva zbroja međusobno zbrajati, množiti, a ako je moguće i dijeliti i oduzimati ili kreirati zadatke s više računskih operacija.

Kako bi si učenici pri šifriranju i dešifrirali olakšali taj pomak po abecedi, na satu tehničke kulture mogu izraditi i naprave za šifriranje/dešifriranje, tzv. šifrarnike koji učenicima možemo predstaviti i kao ključeve jer se koriste kako za šifriranje, tako i za dešifriranje. Konkretnije, što se Cezarove šifre tiče, to bi bila dva diska s abecedom, odnosno dva papira kružnih oblika, spojena u središtu i na čijim su rubovima po cijelom opsegu ispisana slova abecede. Učenicima ovakav šifrarnik olakšava šifriranje i dešifriranje jer rotiranjem diskova automatski pomiču cijelu abecedu za isti broj mjesta.



Slika 1. Primjer šifrarnika s engleskom abecedom (preuzeto 6.4.2021. s:http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/shift.pdf)

Učenicima osnovne škole se lako može objasniti i uporaba Vigenéreove šifre, vrlo slične Cezarovoj šifri. Uzmimo kao primjer ključa riječ „VLAK“. Prvi korak je da analiziramo redne brojeve i numeričke ekvivalente slova ključa: „V“ je 28. slovo abecede pa je njegov numerički ekvivalent 27, „L“ je 16.slovo abecede s numeričkim ekvivalentom 15, „A“ je 1.slovo abecede s numeričkim ekvivalentom 0 i „K“ je 15.slovo abecede čiji je numerički ekvivalent 14.

U sljedećem koraku se onda svako slovo poruke koju želimo poslati, slično kao u Cezarovoj šifri, pomiče za određeni broj mjesta u abecedi u ovisnosti o ključu, i to prvo slovo poruke za 27 mjesta, drugo slovo poruke za 15 mjesta, treće slovo poruke za 0 mjesta, četvrto slovo poruke za 14 mjesta, peto slovo poruke ponovno za 27 mjesta, šesto slovo poruke ponovno za 15 mjesta itd.

Kao pomoć, učenici mogu izraditi i tzv. Vigenéreov kvadrat, odnosno tablicu u kojoj su u prvom retku ispisana sva slova abecede, u drugom retku sva slova abecede s pomakom za jedno mjesto (počinje se sa slovom „B“, nakon slova „Ž“ dolazi slovo „A“), u trećem retku sva slova abecede s pomakom za dva mjesta (počinje se sa slovom „C“, nakon slova „Ž“ dolaze slova „A“ i „B“) itd. Taj Vigenéreov kvadrat onda može učenicima pomoći pri šifriranju/dešifriranju jer je svaki idući redak kvadrata zapravo pomak za jedno mjesto u abecedi. Primjerice, ako za šifriranje treba napraviti pomak slova „E“ za 7 mjesta, samo pogledamo koje se slovo nalazi u retku s pomacima za 7 mjesta, a u istom stupcu kao slovo „E“ u prvom retku kvadrata, što bi ovdje bilo slovo „L“.

Prema [7], s učenicima se pri dešifriranju najbolje najprije usredotočiti na unaprijed poznatu duljinu ključa, a da sam ključ nije poznat. Primjerice, započnemo s ključem od četiri slova (učenici na početku znaju duljinu ključa), te onda radimo frekvencijsku analizu na svakom četvrtom slovu šifre, a i lakše je provesti kriptoanalizu jer onda znamo da, primjerice, 1.,5.,9.,13. itd. slovo otvorenog teksta je pomicano za isti broj mjesta.

Slika 2. Primjer Vigenéreovog kvadrata s engleskom abecedom (preuzeto 9.4.2021. s: https://upload.wikimedia.org/wikipedia/commons/thumb/9/9a/Vigen%C3%A8re_square_shad)

Što se nastave matematike tiče, aktivnosti u kojima bi se koristila Vigenéreova šifra mogu se onda svesti i na samo traženje ključa te povezivanje ključa s nekim nastavnim sadržajima. Uzmimo za primjer sat ponavljanja translacije. Možemo, primjerice, translatirati neki ΔABC za vektor s početnom točkom D i završnom točkom E, gdje je, primjerice, D(numerički ekvivalent prvog slova ključa, numerički ekvivalent drugog slova ključa) i E(numerički ekvivalent trećeg slova ključa, numerički ekvivalent četvrtog slova ključa), a ključ je riječ „ABAK“. Tako bi u ovom primjeru koordinate početne točke vektora translacije bile $D(1,2)$, a završne točke vektora translacije $E(1,15)$. Učenicima u ovom primjeru ne bi unaprijed bio poznat ključ, nego bi ga morali sami najprije pronaći provodeći kriptoanalizu nad nekim tekstom s poznatom duljinom ključa (u ovom primjeru je ključ duljine 4) i znajući da o kojoj je šifri riječ.

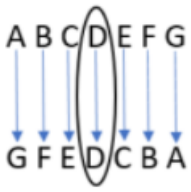
Vigenéreovu šifru možemo iskoristiti i tijekom ponavljanja ili obrade pravokutnog koordinatnog sustava u ravnini. Primjerice, dane su koordinate dvaju vrhova nekoga trokuta. Ako je ključ duljine 2, koordinate trećeg vrha mogu, primjerice, biti numerički ekvivalenti slova ključa. Ako je ključ dulji, možemo šifrirati oznake prvih dviju točaka i kao koordinate treće točke uzeti numeričke ekvivalente šifrata. Učenicima možemo dati i ključ te neki otvoreni tekst te reći da su koordinate treće točke zbrojevi numeričkih ekvivalenata otvorenog teksta i šifrata. Kada odrede koordinate nepoznatog vrha, učenici mogu takvom trokutu računati opseg, površinu, crtati mu osnosimetrične ili centralnosimetrične slike, određivati koordinate vrhova osnosimetričnih i centralnosimetričnih slika i slično. Naravno, slično možemo raditi s nekim drugim likovima.

Zadatke možemo svesti i na aritmetičke. Primjerice, učenicima možemo dati otvoreni tekst i ključ pa oni onda mogu promatrati što se događa kada na nekoliko primjera šifriranja oduzmu zbrojeve numeričkih ekvivalenata šifrata i otvorenog teksta. Kada uoče da je ta razlika uvijek ista, možemo im dati po nekoliko primjera otvorenog teksta i šifrata pa da u grupama pokušaju upariti šifrat s pripadajućim otvorenim tekstom promatrajući isključivo spomenutu razliku zbrojeva numeričkih ekvivalenata, odnosno i na ovaj način dešifriraju poruke.

Također, i ovdje je moguće s učenicima provoditi zadatke koji se svode na frekvencijsku analizu i sve već prethodno spomenute sadržaje u Cezarovoj šifri.

Atbash šifra je slična prethodnima i smatra se jednom od najjednostavnijih šifri. U ovoj se šifri svako slovo poruke mijenja nekim drugim slovom i to na način da se prvo slovo abecede mijenja zadnjim slovom abecede, drugo slovo abecede predzadnjim slovom abecede itd.

Slika 3. Atbash šifra



Slika 4. Atbash šifra i „abeceda“ s neparnim brojem slova

U abecedama s neparnim brojem slova bi slovo koje se nalazi točno u sredini abecede bilo nepromijenjeno, odnosno ne bi ga se mijenjalo nijednim drugim slovom.

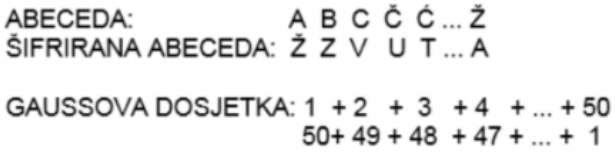
Kako je redoslijed slova u abecedi unaprijed poznat, ovdje se za šifriranje i dešifriranje ne koristi ključ te je stoga Atbash vrlo lagana šifra koja može poslužiti i kao uvod u kriptografiju, čak i prije Cezarove šifre, a u nižim razredima za ponavljanje abecede i redoslijeda slova u njoj. Učenici kasnije mogu i sami izrađivati vlastite abecede, mijenjati redoslijed slova i slično.

Što se matematike tiče, Atbash šifru, kao i Cezarovu, možemo iskoristiti za pomoć pri uvođenju pojma funkcije. Nadalje, učenici mogu zbrajati numeričke ekvivalente otvorenog teksta i šifrata (otvoreni tekst im jedan, a šifrat moraju pronaći) te uočiti vezu s Gaussovom dosjetkom jer se i ona uvodi tako da se broj ispod broja napiše isti niz brojeva, jedanput sortiran uzlazno, a u drugom retku sortiran silazno, kao što je primjerice na Slici 5.

Za razliku od prethodnih šifri, Polibijev kvadrat je šifra u kojoj se slova poruke ne mijenjaju nekim drugim slovima, nego se svako slovo mijenja dvama brojevima, tj. položajem tog slova u retku i stupcu kvadrata, odnosno tablice. Tako bi, koristeći Polibijev kvadrat na Slici 6., šifrirani oblik riječi „SLON“ bio „46 34 43 41“. Pri dešifriranju je vrlo učinkovita frekvencijska analiza.

Polibijev kvadrat učenicima možemo predstaviti i kao ključ, pogotovo ako ih u nekom trenutku oni sami izrađuju. Umjesto Polibijevog kvadrata s hrvatskom abecedom i dodatnim slovima, učenici mogu koristiti i Polibijev pravokokutnik koji se od spomenutog kvadrata jedino razlikuje što nema redak 6 s dodatnim slovima.

Ova šifra je odličan uvod u pravokutni koordinatni sustav u ravnini (usvajanje koordinata točaka/slova), jedino bi tada bilo uputno malo izmijeniti način šifriranja/dešifriranja, odnosno bilo bi dobro uputiti učenike da najprije pri zamjeni pišu brojeve iz stupaca pa tek onda iz redaka. Kako bismo bili još bliži pravokutnom koordinatnom sustavu, a i da spriječimo kasniju zbunjenost, Polibijev kvadrat možemo još malo izmijeniti pa da izgleda kao na Slici 7.



Slika 5. Usporedba Atbash šifre I Gaussove dosjetke

	1	2	3	4	5	6
1	A	B	C	Č	Ć	D
2	DŽ	Đ	E	F	G	H
3	I	J	K	L	LJ	M
4	N	NJ	O	P	R	S
5	Š	T	U	V	Z	Ž
6	Q	W	X	Y	α	β

Slika 6. Primjer Polibijevog kvadrata s hrvatskom abecedom i dodatnim slovima

U nastavi možemo koristiti i fragmentarnu (pigpen) šifru. Ova šifra je slična prethodnim šiframa, ali se slova poruke ne mijenjaju slovima ili brojevima nego simbolima. Poruka se šifrira tako da se u šifrarniku traži slovo po slovo i mijenja pripadajućim simbolom. Snaga ove šifre leži i u promjeni šifrarnika.

Primjerice, ako bismo koristili dani primjer šifrarnika na Slici 8., slovo „C“ bismo tada zamijenili simbolom „ “ , slovo „G“ simbolom „ “, a slovo „Y“ simbolom „ “ .

Ti šifrarnici također imaju ulogu ključeva jer o njima ovisi kako će poruka biti šifrirana/dešifrirana. Nastavnik može najprije sam kreirati šifrarnike, a zatim potaknuti učenike na kreiranje vlastitih. Nastavnik bi tu trebao pomoći učenicima da izbjegnu čestu grešku pri izradi ovakvih šifrarnika, a to je korištenje istog simbola za više različitih slova. Također je važno da sheme budu jednostavne i praktične za uporabu. Pri dešifriranju učenici i ovdje koriste frekvencijsku analizu (bez da im je poznat šifrarnik/ključ) pa se onda i ova šifra može koristiti kao pomoć ili motivacija pri usvajanju ili ponavljanju istih sadržaja kao i prije spomenutih uz primjere s frekvencijskom analizom.

Transpozicijska šifra, za razliku od prethodno spomenutih šifri, ne mijenja slova/simbole početne poruke nekim drugim slovima/simbolima, nego samo mijenja položaj slova unutar poruke, odakle i dolazi sami naziv ove šifre. Šifra je vrlo nesigurna za kratke poruke jer se slova poruka mogu ispremještati na mali broj načina.

6	A	B	C	Č	Ć	D
5	DŽ	Đ	E	F	G	H
4	I	J	K	L	LJ	M
3	N	NJ	O	P	R	S
2	Š	T	U	V	Z	Ž
1	Q	W	X	Y	α	β
	1	2	3	4	5	6

Slika 7. Primjer Polibijevog kvadrata s hrvatskom abecedom i dodatnim slovima, primjeren za uvođenje pravokutnog koordinatnog sustava u ravnini

Slika 8. Primjer jednog Pigpen šifrarnika s engleskom abecedom (preuzeto 9.4.2021. s: https://en.wikipedia.org/wiki/Pigpen_cipher)

S učenicima možemo započeti s takvim kratkim riječima kako bismo ih motivirali za dešifriranje složenijih poruka. Primjerice, možemo započeti koristeći riječ „MAČ“. Kombinacije koje možemo dobiti razmještanjem slova su „MČA, AČM, AMČ, ČAM i ČMA“.

Učenicima, nakon kratkog objašnjenja šifre, možemo dati bilo koju od tih kombinacija, primjerice šifrat „MČA“, sa zadatkom da ispremještaju slova dok ne dobiju smislenu riječ.

U osnovnoj, ali i srednjoj školi bi ovakvo ispisivanje svih kombinacija slova neke riječi moglo poslužiti pri uvođenju permutacija ili općenito kao motivacija pri proučavanju broja kombinacija. Primjerice, broj uređenih parova koji se mogu sastaviti od brojeva 2 i 4, tako da se brojevi ne ponavljaju je jednak broju kombinacija koje možemo dobiti šifriranjem riječi od 2 različita slova. Šifru možemo iskoristiti i kao motivaciju za uvođenje svojstava zbrajanja prirodnih brojeva. Učenici mogu zbrajati numeričke ekvivalente svih kombinacija (otvorenog teksta i šifrata) i uočiti da je zbroj, neovisno o poretku brojeva, uvijek isti. Dobro je učenicima dati i primjer otvorenog teksta u kojima se ponavljaju neka slova više puta i tu onda komentirati smislenost rezultata u šifratu, odnosno broja kombinacija.

Kako bi primatelj mogao dešifrirati poruku šifriranu ovom šifrom, način na koji su slova ispremještana mora biti unaprijed poznat i pošiljatelju i primatelju jer se sam broj mogućih kombinacija vrlo brzo povećava kako povećavamo broj slova u porucit, a i od nekog šifrata možemo premještanjem slova dobiti više smislenih riječi, npr. od šifrata „RESC“ možemo dobiti riječi „SRCE“ i „CRES“ ili pak od šifrata „ATRAV“ možemo dobiti riječi „VATRA“ i „TRAVA“. Taj način na koji mi želimo ispremještati slova učenicima možemo dati kao nekakvu uputu koja onda zapravo preuzima ulogu ključa, pogotovo na samim počecima dešifriranja.

Važno je da učenici uoče da pri dešifriranju ove šifre frekvencijska analiza ne pomaže. Učenici to mogu uočiti ako im damo dva primjera šifrata, jedan dobiven supstitucijskom, a drugi transpozicijskom šifrom, a koje oni onda mogu pokušati dešifrirati frekvencijskom analizom.

Nešto drugačija aktivnost je Tajni protokol. Pretpostavimo da ravnatelj škole želi saznati koliko vremena učitelji iz zbornice dnevno troše na popunjavanje pedagoške dokumentacije. Ako bi se anketiranje provelo javno, za pretpostaviti je da bi neki koji manje vremena u danu troše za popunjavanje pedagoške dokumentacije bili skloni uvećavati svoje vrijeme, a neki koji troše nešto više vremena bi bili skloni umanjiti svoje vrijeme. Zato prvi učitelj najprije zamisli neki broj, primjerice 222, njemu pribroji broj sati u danu koje troši na dokumentaciju i zbroj šapne drugom učitelju u nizu. Drugi učitelj u nizu na zbroj koji mu je dan pribraja svoj broj sati u danu te novi zbroj šapće trećem učitelju u nizu i tako svaki učitelj do zadnjeg svoj broj sati pribraja na prethodni zbroj kojeg je saznao od učitelja koji mu prethodi u nizu. Zadnji učitelj u nizu, nakon što pribroji svoj broj sati, ukupan zbroj šapće prvom učitelju u nizu koji od tog ukupnog zbroja oduzima zamišljeni broj, u našem primjeru oduzima 222. Ako podijelimo razliku s brojem učitelja u zbornici, lako dobivamo aritmetičku sredinu vremena kojeg učitelji utroše na popunjavanje pedagoške dokumentacije.

Tajni protokol u nastavi matematike možemo upotrijebiti za, primjerice, brzo prikupljanje numeričkih podataka, a koje učenici ne bi možda željeli izreći javno. Može poslužiti i kao odlična motivacija ili pak pri ponavljanju aritmetičke sredine. Već od nižih razreda se može koristiti za ponavljanje zbrajanja prirodnih brojeva, a u višim razredima i cijelih brojeva. Ovakva aktivnost je i odličan uvod u poučavanje kriptografije jer učenici saznaju nešto o prijenosu i tajnosti informacija, a što je oboje uistinu važno u kriptografiji.

IV. ZAKLJUČAK

Nastavnici mogu u nastavi matematike ovakve šifre kombinirati, dorađivati i dopunjavati svojim idejama. Dobro je i učenicima dati da sami kreiraju svoje šifre, time učenici osmišljavaju svoje algoritme, razvijaju kognitivne sposobnosti, uče se samostalnosti i suradnji, ali i argumentiranju svojeg mišljenja i rada. Kako su istraživanja pokazala da je motivacija učenika za učenje matematike značajan problem, svako obogaćivanje nastavnog procesa, ne samo kriptografijom, je uvijek dobrodošlo i učenici će ga zasigurno s odobravanjem dočekati.

LITERATURA

[1] https://web.math.pmf.unizg.hr/~duje/kript.html
A. Dujella, Kriptografija, skripta, (preuzeto 5.4.2021)

[2] M. Barun, A. Dujella, Z. Franušić, „Kriptografija u školi“, Poučak, Zagreb, 2008.

[3] A. Benček, M. Marenić, „Motivacija učenika osnovne škole u nastavi matematike“, Školske novine, Zagreb 2006.

[4] Ministarstvo znanosti i obrazovanja, “Odluka o donošenju kurikuluma za nastavni predmet matematike za osnovne škole i gimnazije u Republici Hrvatskoj”, Narodne novine NN 7/2019, Zagreb, 2019.

[5] N. Aydin, E. Güler, A. Sükrü Özdemir, „Effects of Cryptographic Activities on Understanding Modular Arithmetic“, Faculty Publications, Paper 5, 2011.

[6] M. Borelli, A. Fioretto, A. Sgarro, L. Zucherri, „Cryptography and Statistics: A Didactical Project”, Department of Mathematical Sciences, Trst (Italija) 2002.

[7] N. Koblitz, „Cryptography as a teaching tool“, Cryptologia, Vol.21, No.4, 1997.