Kriptografija u nastavi matematike

Bogović, Josipa

SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO–MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Josipa Bogović

KRIPTOGRAFIJA U NASTAVI MATEMATIKE

Diplomski rad

Voditelj rada:
izv. prof. dr. sc. Zrinka Franušić

Zagreb, srpanj, 2021.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Diplomski rad napravljen je u sklopu aktivnosti Projekta KK.01.1.1.01.0004 - Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.

Sadržaj

Uvod

Danas kriptosustavi igraju presudnu ulogu u modernoj tehnologiji. Tehnologije koje uključuju komunikaciju, kao što su mobiteli, internet, digitalna televizija, bankomati, oslanjaju se na šifre kako bi si osigurale sigurnost i privatnost. Nedavni filmovi kao što su *Da Vincijev kôd* i *Nacionalno blago: Knjiga tajni* imaju radnje usredotočene na kriptografiju i šifre, donoseći ove koncepte široj javnosti.

Iako kriptografija nije uvrštena u obaveznu nastavu matematiku, lako je primjenjiva u nastavi, doprinosi razvijanju logičkog načina razmišljanja te povezivanju matematike s drugim nastavnim predmetima i sadržajima.

U prvom dijelu rada predstavljena je matematička teorija i klasifikacija klasične kriptografije. Prikladne supstitucijske i transpozicijke šifre, te kriptosustavi s javnim ključem za osnovnoškolsku i srednjoškolsku nastavu. To je podloga koju nastavnik mora imati kako bi mogao kako bi mogao osmisliti i provesti razne aktivnosti. Drugi dio rada sastoji se od aktivnosti za učenike i ideja za nastavu baziranim na kriptosustavima koje smo opisali u prvom poglavlju.

Poglavlje 1

Klasična kriptografija

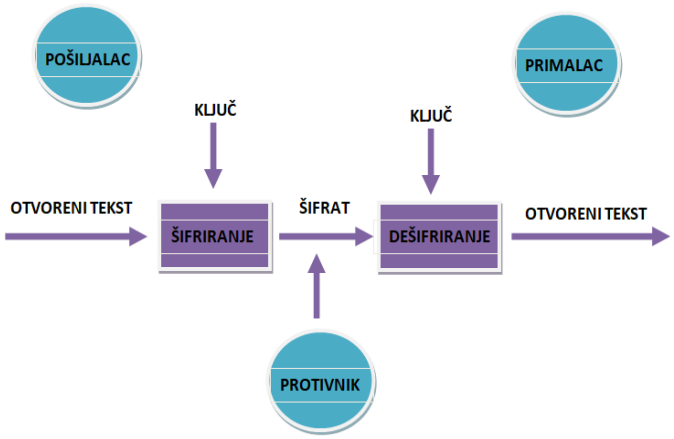
1.1 Osnovni pojmovi

Osnovni zadatak kriptografije je omogućiti dvjema osobama, sudionicima komunikacije, nesmetanu i sigurnu komunikaciju kroz nesiguran komunikacijski kanal kao što su na primjer računalna mreža i telefonska linija. Pod nesmetanom i sigurnom komunikacijom podrazumijevamo da će poruka biti isporučena nepromijenjena te da ju neće moći "pročitati" oni za koje nije namijenjena.

Osobu koja šalje poruku, nazvat ćemo *pošiljatelj*, dok će *primatelj* biti osoba kojoj je poruka namijenjena. U kriptografskoj literaturi uobičajeno ih je zvati imenima *Alice* i *Bob*. Poruka ne bi smjela "doći u ruke" protivnika koji se još naziva Eva ili Oscar. No, za pretpostaviti je da protivnik nadzire komunikacijski kanal pa sudionici razmjenjuju poruke koje protivnik ne može razumjeti. Poruku koju pošiljalac želi poslati primatelju zvat ćemo *otvoreni tekst*. Kako bi pošiljatelj sakrio otvoreni tekst on ga transformira koristeći unaprijed dogovoreni ključ. Taj postupak naziva se *šifriranje*, a dobiveni rezultat *šifrat*. Pošiljalac šalje šifrat preko komunikacijskog kanala, a protivnik prisluškujući komunikacijski kanal može doznati sadržaj šifrata, ali ne može odrediti otvoreni tekst bez poznavanja ključa. Primalac može vrlo jednostavno dešifrirati poruku budući da ima ključ kojim je šifrirana poruka.

Osim samog dešifriranja, postoji i znanstvena disciplina koja proučava postupke za čitanje skrivenih poruka bez poznavanja pravila šifriranja i ključa nazivamo ju *kriptoanaliza* ili *dekriptiranje*. Zajedno s kriptografijom, kriptoanaliza čini znanstvenu granu *kriptologiju*.

Kriptografski algoritam ili *šifra* je matematička funkcija koja se koristi za šifriranje i dešifriranje. Radi se o dvije funkcije, jednoj za šifriranje, a drugoj za dešifriranje. Ove funkcije biramo iz određene familije funkcija, ovisno o ključu koji je odabran te one preslikavaju elemente otvorenog teksta u elemente šifrata i obrnuto. *Prostorom*



Slika 1.1: Ilustracija kriptosustava

ključeva nazivamo skup svih mogućih vrijednosti ključeva. Dakle, *kriptosustav* sastoji se od kriptografskog algoritma, svih mogućih otvorenih tekstova i šifrata, te prostora ključeva.

Definicija 1.1.1. *Kriptosustav je uređena petorka* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *za koju vrijedi:*

1. $\mathcal{P}$ *je konačan skup svih mogućih osnovnih elementa otvorenog teksta,*
2. $\mathcal{C}$ *je konačan skup svih mogućih osnovnih elementa šifrata,*
3. $\mathcal{K}$ *je prostor ključeva, tj. konačan skup svih mogućih ključeva,*
4. *Za svaki* $K \in \mathcal{K}$ *postoji funkcija šifriranja* $e_K \in \mathcal{E}$ *i odgovarajuća funkcija dešifriranja* $d_K \in \mathcal{D}$. *Pritom* $e_K : \mathcal{P} \to \mathcal{C}$ *i* $d_K : \mathcal{C} \to \mathcal{P}$ *funkcije sa svojstvom da je* $d_K(e_K(x)) = x$ *za svaki otvoreni tekst* $x \in \mathcal{P}$.

Napomenimo da je funkcija šifriranja e_K injekcija za svaki $K \in \mathcal{K}$ jer bi u suprotnom poruka bila dvosmislena.

Pretpostavimo da pošiljatelj želi poslati poruku koja se sastoji od više osnovnih elemenata otvorenog teksta

$$x = (x_1, x_2, \ldots, x_n) \in \mathcal{P}^n,$$

za neki prirodan broj n, tada je pripadni šifrat dan s

$$y = (e_K(x_1), e_K(x_2), \ldots, e_K(x_n)) \in \mathcal{C}^n,$$

pri čemu je $K \in \mathcal{K}$.

1.2 Klasifikacija kriptosustava

Kriptosustavi se mogu dijeliti prema:

1. tipu operacije koje se koriste pri šifriranju,
2. načinu na koji se obrađuje otvoreni tekst,
3. tajnosti i javnosti ključa.

Tip operacija koje se koriste pri šifriranju

Imamo podjelu na *supstitucijske šifre*, u kojima se svaki element otvorenog teksta zamjenjuje s nekim drugim elementom prema unaprijed utvrđenoj transformaciji, te *transpozicijske šifre* u kojima se elementi otvorenog teksta permutiraju tj. premještaju. Primjerice, ako riječ KLAUN šifriramo u PQFZS, načinili smo supstituciju, a ako je šifriramo u LANUK, načinili smo transpoziciju.

Način obrade otvorenog teksta

Ovdje imamo podjelu na *blokovne šifre* koje obrađuju jedan po jedan blok elemenata otvorenog teksta koristeći jedan te isti ključ, te *protočne šifre* kod kojih se elementi otvorenog teksta obrađuju jedan po jedan koristeći pritom paralelno generirani niz ključeva.

Tajnost i javnost ključa

Ovdje je osnovna podjela na sustave s *tajnim* i sustave s *javnim* ključem. Kod sustava s tajnim ključem, ključ za dešifriranje se može izračunati poznavanjem ključa za šifriranje i obratno. Ovi su ključevi najčešće identični, pa sigurnost ovih kriptosustava leži u tajnosti ključa.

Kod sustava s javnim ključem, ključ za dešifriranje ne može se izračunati iz ključa za šifriranje. Sigurnost leži u tome da bilo koja osoba može šifrirati poruku poznatim ključem, ali samo osoba koja ima odgovarajući ključ za dešifriranje (privatni ili tajni ključ) može dešifrirati tu poruku.

Poglavlje 2

Supstitucijske šifre

U ovom dijelu opisat ćemo jednostavne simetrične kriptosustave koji mogu poslužiti da se učenicima, čak i nižih razreda osnovne škole, predstavi kreativna i zanimljiva matematika.

Koristit ćemo se engleskim alfabetom od 26 slova, a slova Č, Ć, Đ, Dž, Lj, Nj, Š, Ž, zamijenit ćemo redom slovima C, C, DJ, DZ, LJ, NJ, S, Z. Nadalje, svakom slovu abecede ćemo jednoznačno pridružiti njegov redni broj počevši od nule, prema korespondenciji:

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

Umjesto slova u poruci često ćemo koristiti njihove numeričke ekvivalente dane gornjom tablicom te označavamo skup

$$\mathbb{Z}_{26} = \{0, 1, \ldots, 25\}.$$

Uz operacije zbrajanja i množenja modulo 26 skup $\mathbb{Z}_{26}$ je komutativan prsten s jedinicom. Zbroj i umnožak modulo 26 elemenata $a, b \in \mathbb{Z}_{26}$ zapisivat ćemo kao

$$(a + b) \mod 26, \quad a \cdot b \mod 26.$$

Iako ove operacije nisu dio obrazovnog sadržaja matematike niti u osnovnoj niti u srednjoj školi, učenici ne bi trebali imati poteškoća za njihove usvajanje. Naime, rezultat zbrajanja i množenja modulo m je jedinstveni ostatak pri djeljenju brojem m iz skupa $\{0, 1, \ldots, m\}$. S druge strane, učenicima se *modularna aritmetika* može predstaviti kao *aritmetika sata*. Na primjer, ako sat pokazuje 10:00, onda će nakon 5

sati pokazivati 3:00. Taj 12-satni period kojim mjerimo vrijeme možemo zamijeniti s bilo kojim prirodnim brojem m - modulom. U slučaju supstitucijskih šifri taj modul će uglavnom biti jednak 26, to jest jednak broju slova abecede koju šifriramo.

2.1 Cezarova šifra

Cezarova šifra jedna je od najranije poznatih i najjednostavnijih šifri. Sastoji se u tome da se svako slovo poruke zamijeni slovom koje se nalazi n mjesta dalje u alfabetu. Metoda je dobila naziv po Juliju Cezaru koji ju je koristio za komunikaciju sa svojim generalima, a za komunikaciju je najčešće koristio $n = 3$. Tako bi se otvoreni tekst

V I R U S

pomakom za 3 mjesta u desno šifrirao u

Y L U X V,

pri čemu nakon zadnjeg slova Z, ponovo dolaze slova A, B, C, to jest abeceda se ciklički nastavlja.

Ako prijeđemo na numeričke ekvivalente abecede onda Cezarovu šifru opisujemo kao kriptosustav u kojem su prostor ovorenog teksta, prostor šifrata i prostor ključeva jednaki skupu $\mathbb{Z}_{26}$, a opisani sustav možemo zamijeniti matematičkim modelom.

10 warnings

Matematički model Cezarove šifre

$$\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$$

Funkcije šifriranja i dešifriranja su

$$e_n : \mathbb{Z}_{26} \to \mathbb{Z}_{26}, \quad e_n(x) = (x + n) \mod 26,$$

$$d_n : \mathbb{Z}_{26} \to \mathbb{Z}_{26}, \quad d_n(y) = (y - n) \mod 26,$$

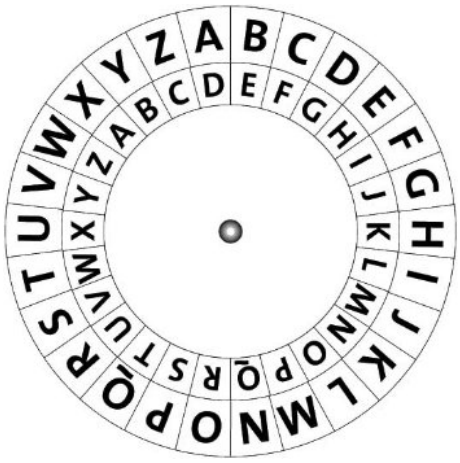
pri čemu je $0 \leq n \leq 25$ ključ ove šifre.

Cezarova šifra ne nudi komunikacijsku sigurnost te ju je vrlo lako razbiti. Jedna od metoda dekriptiranja jest ispitivanje redom svih mogućih ključeva dok ne dobijemo neki smisleni tekst, a to je moguće budući da je broj ključeva mali. Odnosno, broj ključeva je upravo onoliki koliko je i slova - 26. Na primjer, za šifrat SHKSZSVRSWX ispitujući redom ključeve dobivamo:

S	H	K	S	Z	S	V	R	S	W	X	za	$n = 0$,
R	G	J	R	Y	R	U	Q	R	V	W	za	$n = 1$,
Q	F	I	Q	X	Q	T	P	Q	U	V	za	$n = 2$,
P	E	H	P	W	P	S	O	P	T	U	za	$n = 3$,
O	D	G	O	V	O	R	N	O	S	T	za	$n = 4$.

Cezarova šifra primjerena je za učenike osnovne škole i mogli bi ju naučiti učenici petog razreda, a vrlo je zanimljivo to što korelira s nastavnim sadržajem Povijesti - Rimsko carstvo. (Vidjeti Aktivnost 1).

Za sam postupak šifriranja praktično je koristiti tzv. *Cezarov krug* (Slika 2.1) kojeg učenici mogu sami izraditi. (Vidjeti Aktivnost 2)



Slika 2.1: Cezarov krug - šifrarnik

Iako je Cezarovu šifru lako razbiti tzv. *grubom silom*, to jest ispitujući redom sve ključeve, ona je pogodna da na njoj ilustriramo i metodu dekriptiranja koja koristi *frekvencijsku analizu slova*. Naime, u svakom jeziku neka se slova češće pojavljuju od drugih i ti su podatci dobro poznati. Naravno, da bismo mogli primijeniti ovu metodu korisno je znati kojim je jezikom tekst pisan. Na Slici 2.2 prikazane su frekvencije slova u hrvatskom, engleskom i njemačkom jeziku.

U sedmom razredu osnovne škole obrađuje se nastavna jedinica Prikazivanje i analiza podataka u sklopu koje se može uklopiti aktivnost koja bi analizirala frekvenciju

[0]Slika 2.1 preuzeta s `https://www.researchgate.net/publication/332368903_Review_on_DNA_Cryptography/figures?lo=1`

Slika 2.2: Učestalost slova po jezicima

slova danog šifrata pri čemu uzorci šifrata mogu poticati od poruka na različitim stranim jezicima. Rezultati se mogu prikazati supčastim, odnosno kružnim dijagramom. (Vidjeti Aktivnost 3).

2.2 Afina šifra

Afina šifra može se predstaviti učenicima sedmog razreda nakon što se učenici upoznaju s pojmom afine funkcije, $x \mapsto ax + b$, po kojoj je šifra dobila ime.

Općenito, funkcija šifriranja je oblika $e_k(x) = (ax + b) \mod 26$, gdje a i b poprimaju nenegativne cjelobrojne vrijednosti ne veće od 26. Uređeni par (a, b) predstavlja ključ ove šifre. Za $a = 1$ dobivamo Cezarovu funkciju šifriranja, dakle ova šifra je sigurnija od Cezarove budući da je broj ključeva veći.

Da bi šifriranje bilo nedvosmisleno, funkcija šifriranja mora biti injekcija, odnosno mora imati inverz na skupu $\mathbb{Z}_{26}$. Budući da broj 26 nije prost nemaju svi elementi iz $\mathbb{Z}_{26}\backslash\{0\}$ multiplikativni inverz. Upravo zbog toga parametar a nije "sasvim" proizvoljan, nego mora biti relativno prost s modulom 26. Odnosno, mora vrijediti da je najveći zajednički djelitelj od a i 26 jednak 1, što zapisujemo kao $\text{nzd}(a, 26) = 1$.

[0]Slika 2.2 preuzeta s `https://hr2.wiki/wiki/Letter_frequency`

Matematički model afine šifre

$$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26},$$
$$\mathcal{K} = \{(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \text{nzd}(a, 26) = 1\}$$

Za $K = (a, b) \in \mathcal{K}$ funkcije šifriranja i dešifriranja dane su s

$$e_K(x) = (ax + b) \mod 26,$$
$$d_k(x) = a^{-1}(y - b) \mod 26,$$

pri čemu a^{-1} označava multiplikativni inverz broja a u prstenu $\mathbb{Z}_{26}$.

Pretpostavimo da afinom šifrom s ključem $(5, 6)$ želimo šifrati riječ RIJEKA. Najprije otvoreni tekst zamijenimo numeričkim ekvivalentima $(17, 8, 9, 4, 10, 10)$. Množenjem svake koordinate s 5 i dodavanjem 6 u $\mathbb{Z}_{26}$ dobivamo:

$$(17, 8, 9, 4, 10, 10) \mapsto (91, 46, 51, 26, 56, 6) \mapsto (13, 20, 25, 0, 4, 6),$$

što odgovara šifratu NUZAEG. Ključ za dešifriranje je općenito dan s $(a^{-1}, -a^{-1}b)$, a za ovaj primjer je to $(21, 4)$ jer je $5 \cdot 21 \mod 26 = 1$, tj. multiplikativni inverz od 5 u Z_{26} je 21, te $-21 \cdot 6 \mod 26 = 4$. Zaista, množenjem svake koordinate šifrata s 21 i dodavanjem 4 u $\mathbb{Z}_{26}$ dobit ćemo početni otvoreni tekst:

$$(13, 20, 25, 0, 4, 6) \mapsto (277, 424, 529, 4, 88, 130) \mapsto (17, 8, 9, 4, 10, 0).$$

Ako se afinom šifrom šifrira dulja poruka, najbolje je naprije šifrirati svako slovo abecede. Za ključ $(5, 6)$ tako dobivamo

	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

U prethodnoj tablici je $y = 5x +_{26} 6$.

U sljedećoj tablici nabrojani su svi invertiblni elementi iz $\mathbb{Z}_{26}$ s njihovim multiplikativnim inverzima:

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Aktivnost 4 koja je namijenjena učenicima sedmih razreda osmišljena je tako da se učenici sami uvjere da "loš" odabir broja a (tj. onaj za koji je $\text{nzd}(a, 26) > 1$) iz ključa afine dovodi do toga da funkcija šifriranja nije injekcija, odnosno da u tom slučaju postoje različita slova otvorenog teksta koja se preslikaju u isto slovo šifrata.

2.3 Vigenerèova šifra

Ovu je šifru prvi put opisao Giovan Battista Bellaso sredinom 16. stoljeća, no u 19. stoljeću zasluge su pogrešno pripisane Blaiseu de Vigenèreu, francuskom diplomatu i kriptografu, Bellasovom istovremeniku. Tri stoljeća se vjerovalo da je ovu šifru nemoguće razbiti, no sredinom 19. stoljeća godine Friedrich Kasiski prvi je objavio opću metodu dešifriranja Vigenerèove šifre.

Način šifriranja vrlo je sličan Cezarovom. Razlika je što u ovom slučaju ključ je sačinjen od bloka slova, odnosno kraće riječi. Zato je Vigenerèova šifra primjer blokovne šifre. Uzmemo li za ključ riječ PAUK koja se sastoji od 15., 0., 20. i 10. slova u alfabetu, onda ćemo prvo slovo otvorenog teksta pomaknuti za 15 mjesta unaprijed (odnosno ciklički u desno), drugo za 0 mjesta, treće za 20 mjesta, četvrto za 10 mjesta, peto za 15 mjesta itd. Kada bismo šifrirali ASTRONAUT zadanim ključem dobili bismo PSOBDNUEI.

A	S	T	R	O	N	A	U	T
P	A	U	K	P	A	U	K	P
P	S	O	B	D	N	U	E	I

Dešifriranje je analogno šifriranju samo se pomičemo unazad (tj. ciklički u lijevo).

Matematički model Vigenerèove šifre

Neka je $m \in \mathbb{N}$ duljina ključne riječi. Tada je

$$\mathcal{P} = \mathcal{K} = \mathcal{C} = (\mathbb{Z}_{26})^m,$$

tj. prostor ovorenog teksta, prostor ključeva i prostor šifrata jednak je skupu svih uređenih m-torki elemenata iz $\mathbb{Z}_{26}$. Funkcije šifriranja i dešifriranja za ključ $K = (k_1, \ldots, k_m) \in (\mathbb{Z}_{26})^3$ dane su s

$$e_K(x) = (x_1 + k_1, \ldots, x_m + k_m) \mod 26,$$

$$d_K(y) = (y_1 - k_1, \ldots, y_m - k_m) \mod 26,$$

gdje su $x = (x_1, \ldots, x_m), y = (y_1, \ldots, y_m) \in (\mathbb{Z}_{26})^m$.

Rabeći numeričke ekvivalente u prethodnom primjeru imamo:

	0	18	19	17	14	13	0	20	19
$+_{26}$	15	0	20	10	15	0	20	10	15
	15	18	14	1	3	13	20	4	19

Šifriranje je puno jednostavnije uz korištenje Vigenèreovog kvadrata. Šifrirano slovo se nalazi u presjeku stupca koji počinje sa slovom iz otvorenog teksta i retka koji počinje sa slovom ključne riječi, a za dešifriranje se koristi potpuno 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 2.3: Vigenèreov kvadrat

Ako nam nije poznat ključ koriste se statističke metode kako bi se pronašla duljina ključa, a zatim nam frekvencijska analiza omogućuje pronalazak ključa. Kako bi šifriranje bilo što sigurnije ključna riječ bi trebala biti što dulja. Potpuno siguran sustav je onaj s "beskonačno" dugačkim ključem. Također, sustav je sigurniji ako se cijeli ključ sastoji od slučajnih znakova, no to nije baš praktično.

2.4 Beaufortova šifra

Beaufortova šifra vrlo je slična Vigenèreovoj, a potječe od irskog časnika u Britanskoj kraljevskoj mornarici Sir Francisa Beauforta (19. stoljeće). Pretpostavimo da želimo šifrirati riječ MATEMATIKA pri čemu je ključ, odnosno ključna riječ LAV. Šifrat dobivamo na način da prvo slovo ključa (slovo L) pomičemo za dvanaest mjesta ulijevo te dobivamo slovo Z, drugo slovo ključa (slovo A) pomičemo za nula mjesta ulijevo, odnosno ne pomičemo. Treće slovo ključa (slovo V) pomičemo za devetnaest mjesta ulijevo te dobivamo slovo C. Ponovno pomičemo prvo slovo ključa (slovo L) četiri mjesta ulijevo te dobivamo slovo H, itd. Postupak nastavljamo i dobivamo:

L	A	V	L	A	V	L	A	V	L
M	A	T	E	M	A	T	I	K	A
Z	A	C	H	O	V	S	S	L	L

Šifriranje je puno jednostavnije uz korištenje Beaufortovog kvadrata (Slika 2.4). Šifrirano slovo se nalazi na presjeku retka koji počinje sa slovom ključne riječi i stupca koji počinje sa slovom iz otvorenog teksta.

Matematički model Beaufortove šifre

Neka je $m \in \mathbb{N}$ duljina ključne riječi. Tada je

$$\mathcal{P} = \mathcal{K} = \mathcal{C} = (\mathbb{Z}_{26})^m.$$

tj. prostor ovorenog teksta, prostor ključeva i prostor šifrata jednak je skupu svih uređenih m-torki elemenata iz $\mathbb{Z}_{26}$. Funkcije šifriranja i dešifriranja za ključ $K = (k_1, \ldots, k_m) \in (\mathbb{Z}_{26})^m$ su jednake:

$$e_K(x) = (k_1 - x_1, \ldots, k_m - x_m) \mod 26,$$

$$d_K(y) = (k_1 - y_1, \ldots, k_m - y_m) \mod 26,$$

gdje su $x = (x_1, \ldots, x_m), y = (y_1, \ldots, y_m) \in (\mathbb{Z}_{26})^m$.

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

Slika 2.4: Beaufortov kvadrat

Uočimo da su funkcije šifriranja i dešifriranja jednake jer iz $y_i = k_i - x_i \mod 26$ slijedi $x_i = k_i - y_i \mod 26$, za sve $i = 1, \ldots, m$.

Rabeći numeričke ekvivalente u prethodnom primjeru imamo:

	11	0	21	11	0	21	11	0	21	11
$-_{26}$	12	0	19	4	12	0	19	9	10	0
	25	0	2	7	14	21	18	18	11	11

2.5 Jednokratna bilježnica

Ovaj način šifriranja vrlo je sličan Vigenerèovoj šifri s vrlo dugačkim ključem, poput isječka iz knjige. Na primjer, pretpostavimo da želimo šifrirati poruku "Savršen kriptosustav je onaj u u kojem šifrat ne daje nikakvu informaciju o otvorenom tekstu." Ključ koji ćemo koristiti je iz romana Vjekoslava Majera, *Dnevnik malog Perice*.

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

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

Budući da se ključ ne ponavlja, ova je šifra vrlo sigurna, ali komplicirana za praktičnu realizaciju. Kripotosustav koji se zasniva na ovoj ideji naziva se *jednokratna bilježnica*. Njega su konkretno realizirali Gilbert Vernam i Joseph Mauborgne 1917. godine, no ne na šifriranju slova već na šifriranju binarnih podataka, to jest 0 i 1.

Matematički model jednokratne bilježnice

Za neki $n \in \mathbb{N}$ su

$$\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_2)^n = (\{0,1\})^n,$$

a funkcije šifriranja i dešifriranja su

$$e_n : (\mathbb{Z}_2)^n \to (\mathbb{Z}_2)^n,\ e_n(x_1, \ldots, x_n) = (x_1 +_2 k_1, \ldots, x_n +_2 k_n),$$

$$d_n : (\mathbb{Z}_2)^n \to (\mathbb{Z}_2)^n,\ d_n(y_1, \ldots, y_n) = (y_1 +_2 k_1, \ldots, y_n +_2 k_n),$$

pri čemu je $(k_1, \ldots, k_n) \in (\mathbb{Z}_2)^n$ ključ.

Uočimo da su zbrajanje i oduzimanje u $\mathbb{Z}_2$ iste operacije pa je zbog toga postupak šifriranja jednak postupku dešifriranja. No, to je i slaba točka ovog sustava pa njegova sigurnost leži u tome da se ključ uvijek koristi samo jednom. Ovaj se sustav lako može implementirati u računala jer se šifriranje vrši na bitovima. U informatici se zbrajanje modulo 2 naziva operacijom *ekskluzivno ili* i označava kao $\oplus$ (ili XOR).

	x	0	1	1	1	0	1	0	1
$\oplus$	k	0	0	1	1	0	1	1	0
	y	0	1	0	0	0	0	1	1

	y	0	1	0	0	0	0	1	1
$\oplus$	k	0	0	1	1	0	1	1	0
	x	0	1	1	1	0	1	0	1

2.6 Bifid šifra

Bifid šifra potječe od Francuskog kriptografa Felixa Dellastele koji ju je predstavio 1895. godine u francuskom Revue du Genie civil.

Za Bifid šifru potrebna nam je kvadratna mreža 5×5 koju popunjavamo slovima na način na koji mi to želimo. Dakle, ključ za šifru Bifid sastoji se od 25 slova. Budući da abeceda koju rabimo ima 26 slova, dogovor je slovo J "spojiti" slovom I. Pretpostavimo da je zadana sljedeća tablica - ključ:

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

Na primjeru otvorenog teksta SUNCE i gornje tablice opisat ćemo kako funkcionira Bifidova šifra. Šifriranje se prvo sastoji od dijeljenja slova u blokove veličine N. Neka je $N = 3$. Dijeljenje teksta u blokove nije obvezno, ali pojednostavljuje šifriranje dugih tekstova. Poruke koje nisu višekratnik od N nadopunimo nekim slovima koja neće promijeniti smisao poruke npr. X.

Korak 1: Rastavimo otvoreni tekst u blokove duljine 3. Ako poruka nije višekratnik od 3 nadopunimo je

SUN CEX

Korak 2: Svako slovo zamijenimo s uređenim parom koordinata. Prva koordinata je koordinata retka u kojem se nalazi slovo u danoj tablici, a druga je koordinata stupca. Radi preglednosti zapišimo ovaj korak u tablice:

		4	4
SUN	$\rightarrow$	5	3
		2	5

		4	2
CEX	$\rightarrow$	2	1
		3	4

Korak 3: "Pročitamo" stupce odozgo prema dolje iz tablica i grupiramo ih u parove.

$$(4,5,2),(4,3,5) \ \rightarrow \ (4,5),(2,4),(3,5)$$
$$(4,2,3),(2,1,4) \ \rightarrow \ (4,2),(3,2),(1,4)$$

Korak 4: Zamijenimo koordinate odgovarajućim slovima iz tablice:

$$(4,5),(2,4),(3,5),(4,2),(3,2),(1,4) \ \rightarrow \ \text{ZLK CFG}$$

Za dešifriranje koordinate šifrata najprije grupiramo u trojke:

$$\text{ZLK} \ \rightarrow \ (4,5),(2,4),(3,5) \ \rightarrow \ (4,5,2),(4,3,5)$$

$$\text{CFG} \ \rightarrow \ (4,2),(3,2),(1,4) \ \rightarrow \ (4,2,3),(2,1,4)$$

Zatim trojke napišemo u retke i pročitamo po stupcima:

$$\begin{matrix} 4 & 5 & 2 \\ 4 & 3 & 5 \end{matrix} \ \rightarrow \ (4,4),(5,3),(2,5) \ \rightarrow \ \text{SUN}$$

$$\begin{matrix} 4 & 2 & 3 \\ 2 & 1 & 4 \end{matrix} \ \rightarrow \ (4,2),(2,1),(3,4) \ \rightarrow \ \text{CEX}$$

Za formiranje tablice - ključa za Bifidovu šifri obično se koristi ključna riječ koju zapišemo u redak (ili stupac), a ostatak tablice popunimo redom preostalim slovima abecede. Iz ključne riječi se moraju izbaciti slova koja se pojavljuju više od jedanput. Sljedeća tablica nastala je iz ključne riječi ZAGREB.

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

Poglavlje 3

Transpozicijske šifre

Za razliku od supstitucijskih šifri kod transpozicijskih šifri elementi otvorenog teksta ostaju nepromjenjivi, ali se mijenja njihov međusobni položaj.

Matematički model transpozicijske šifre

Neka je m fiksan prirodan broj. Neka je

$$\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m,$$

te neka se $\mathcal{K}$ sastoji od svih permutacija skupa $\{1, 2, \ldots, m\}$. Za $\pi \in \mathcal{K}$ definiramo funkcije šifriranja i dešifriranja kao

$$e_\pi(x_1, ..., x_m) = (x_{\pi(1)}, ..., x_{\pi(m)}),$$

$$d_\pi(y_1, ..., y_m) = (y_{\pi^{-1}(1)}, ..., y_{\pi^{-1}(m)}).$$

Prostor svih ključeva je simetrična grupa stupnja m čiji je kardinalitet $m!$. Kod vrlo kratkih poruka koje se recimo sastoje od jedne riječi ova je metoda vrlo nesigurna zato što se malen broj slova može ispremještati na malen broj načina. Ako se poruka sastoji od više slova, broj mogućih kombinacija raste te dešifriranje takvih poruka nije moguće bez poznavanja samog procesa miješanja.

Dakle, da bi transpozicija imala smisla premještanje slova mora se odvijati u skladu s nekim pravilom, koje je unaprijed dogovoreno s primateljem, a nepoznato je neprijatelju. Na primjer za $m = 5$ i ključ - permutaciju

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 1 & 5 \end{pmatrix},$$

otvoreni tekst MORE JE PLAVE BOJE možemo šifrirati tako da tekst najprije zapišemo po redcima

1	2	3	4	5
M	O	R	E	J
E	P	L	A	V
E	B	O	J	E

a zatim stupce permutiramo prema zadanom ključu π

3	4	2	1	5
R	E	O	M	J
L	A	P	E	V
O	J	B	E	E

i šifrat dobivamo čitanjem po redcima prethodne tablice: REOMJLAPEVOJBEE. Ključ za dešifriranje ovakve šifre je inverzna permutacija

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix}.$$

3.1 Stupčana transpozicija

Stupčana transpozicija je varijanta transpozicijske šifre koja se najviše koristila u praksi. Kod nje se otvoreni tekst upisuje u pravokutnik po redcima, a šifrat se dobije čitanjem po stupcima prema zadanoj permutaciji. Konkretno za otvoreni tekst MORE JE PLAVE BOJE i permutaciju $\pi = (3\,4\,2\,1\,5)$ naprije zapišemo

3	4	2	1	5
M	O	R	E	J
E	P	L	A	V
E	B	O	J	E

i čitajući po stupcima, naprije stupac označen s 1, zatim 2, itd. dobivamo šifrat EAJRLOMEEOPBJVE. Za postupak dešifriranja zapišemo tekst po stupcima

1	2	3	4	5
E	R	M	O	J
A	L	E	P	V
J	O	E	B	E

i nakon što ga posložimo po stupcima prema redoslijedu iz ključa dobivamo početnu tablicu.

Pretpostavimo sada da trebamo dekriptirati šifrat:

MSAOOLEUZMGIUOLGBERTIAZJNNIHODAEBDBNKCUOMASSLUIE

Najprije trebamo odrediti dimenziju tablice, odnosno broj stupaca koji je djelitelj duljine šifrata. Pretpostavit ćemo da je broj stupaca između 5 i 10. Budući da je duljina šifrata 48, moguće dimenzije tablice su 6×8 ili 8×6. Točnu dimenziju možemo otkriti promatrajući odnos samoglasnika i suglasnika u svakom retku koji u hrvatskom jeziku iznosi u hrvatskom 43% : 57%.

1	2	3	4	5	6	7	8	
M	E	U	R	N	A	K	S	3:5
S	U	O	T	N	E	C	S	3:5
A	Z	L	I	I	B	U	L	4:4
O	M	G	A	H	D	O	U	4:4
O	G	B	Z	O	B	M	I	3:5
L	I	E	J	D	N	A	E	4:4

1	2	3	4	5	6	
M	Z	B	N	B	M	0:6
S	M	E	N	D	A	2:4
A	G	R	I	B	S	2:4
O	I	T	H	N	S	2:4
O	U	I	O	K	L	4:2
L	O	A	D	C	U	3:3
E	L	Z	A	U	I	4:2
U	G	J	E	O	E	4:2

Prva tablica ima bolji omjer samoglasnika i suglasnika u svakom retku pa možemo zaključiti da se za šifriranje koristilo 8 stupaca. Sada stupce pravokutnika možemo izrezati i premještati dok ne dobijemo smisleni sadržaj u redcima. Možemo koristiti i podatke o frekvencijama bigrama jer je za očekivati da stupci koji imaju najviše frekventnih bigrama stoje jedan pored drugog. Nakon malo "anagramiranja" pokazuje se da permutacija $\pi = (4\,3\,1\,2\,5\,7\,6\,8)$ daje smisleni tekst: RUMENKASTO SUNCE SILAZI U BLAGOM HODU: ZBOGOM, BIJELI DANE!

4	3	1	2	5	7	6	8
R	U	M	E	N	K	A	S
T	O	S	U	N	C	E	S
I	L	A	Z	I	U	B	L
A	G	O	M	H	O	D	U
Z	B	O	G	O	M	B	I
J	E	L	I	D	A	N	E

Permutacijska šifra primjerena je za učenike srednje škole i mogli bi ju naučiti učenici trećeg razreda (Aktivnost 6).

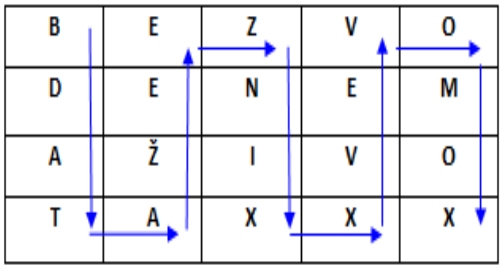
3.2 Šifra s uzorkom

Kod šifre s uzorkom otvoreni tekst zapisujemo u pravokutnu mrežu. Ako želimo šifrirati poruku BEZ VODE NEMA ŽIVOTA, otvoreni tekst zapisujemo u pravokutnu mrežu dimenzije 4×5. Budući da otvoreni tekst ima 17 slova dodajemo tri znaka X kako bismo dobili višekratnik broja 4. Otvoreni tekst zapisujemo u tablicu po redcima:

B	E	Z	V	O
D	E	N	E	M
A	Ž	I	V	O
T	A	X	X	X

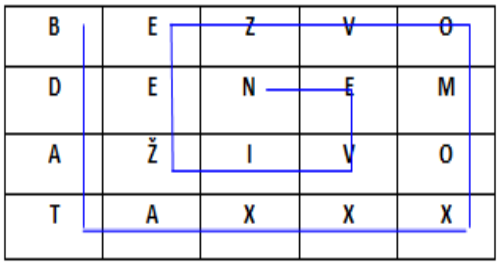
Slika 3.1: Pravokutna mreža dimenzije 4×5

Kako bismo dobili šifrat na pravokutnoj mreži pratimo određeni put čiji je oblik unaprijed dogovoren s onim osobama koje će koristiti taj otvoreni tekst. Najpoznatiji putovi su *plovni* i *spiralni*.



Slika 3.2: Šifriranje *plovnim putom*

Šifriranjem plovnim putom kao na Slici 3.2 dobili smo šifrat BDA TEEŽ AZNI XVEV XOMOX, a spiralnim kao na Slici 3.2 šifrat NEVIŽE EZVO MOXX XATADB.



Slika 3.3: Šifriranje *spiralnim putom*

Oba puta imaju više varijanti s obzirom na to da se može započeti iz bilo kojeg vrha i onda vrtjeti prema unutra ili van, u smjeru kazaljke na satu ili obratno, itd.

Šifriranje i dešifriranje spiralnim putem mogu naučiti učenici drugog razreda srednje škole. Kada se obrađuje logaritamska funkcija učenike upoznajemo s logaritamskom spiralom ili spiralom mirabilis. Kroz Aktivnost 7 učenike možemo upoznati i s Arhimedovom spiralom.

Poglavlje 4

Kriptosustavi s javnim ključem

Začetnici kriptografije javnog ključa smatraju se Whitfield Diffie i Martin Hellman. Ideja javnog ključa sastoji se u konstrukciji kriptosustava kod kojih bi u nekom razumnom vremenu bilo praktički nemoguće iz poznavanja funkcije šifriranja e_K izračunati funkciju dešifriranja d_K te bi u tom slučaju funkcija šifriranja e_K mogla biti javna.

Glavnu ulogu u kreiranju kriptosustava s javnim ključem imaju tzv. *jednosmjerne funkcije*. Za funkciju f kažemo da je jednosmjerna ako je f lako, a f^{-1} teško izračunati. Ako je pritom f^{-1} lako izračunati ukoliko nam je poznat neki dodatni podatak, onda f nazivamo *osobna jednosmjerna funkcija*.

Formalno kriptosustav s javnim ključem definiramo:
Kriptosustav s javnim ključem sastoji se od familija funkcija za šifriranje e_K i dešifriranje d_K sa svojstvima:

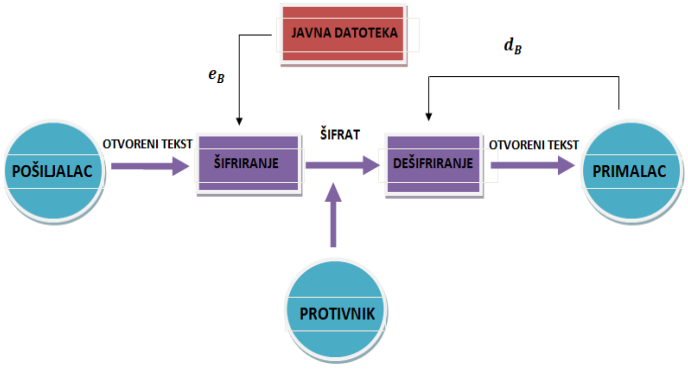
1. Za svaki ključ K je d_K inverz od e_K;
2. Za svaki ključ K je e_K javan, ali je d_K poznat samo osobi K;
3. Za svaki ključ K je e_K osobna jednosmjerna funkcija.

Tada funkciju e_K nazivamo *javnim ključem*, a d_K *tajnim* ili *osobnim ključem*.

Proces slanja poruke x između pošiljatelja A i primatelja B odvija se na sljedeći način: prvo osoba B šalje osobi A svoj javni ključ e_B pomoću kojeg osoba A šifrira svoju poruku. Zatim osoba A šalje osobi B šifrat $y = e_B(x)$ kojeg osoba B dešifrira koristeći svoj tajni ključ d_B te dobiva

$$d_B(y) = d_B(e_B(x)) = x.$$

Ukoliko u komunikaciji sudjeluje više ljudi tada svi korisnici svoje javne ključeve stavljaju u neku datoteku koja je dostupna svima. U tom slučaju osoba B ne šalje svoj javni ključ osobi A već ga osoba A pročita iz datoteke.



Slika 4.1: Ilustracija kriptosustava s javnim ključem

Budući da svatko može pristupiti funkciji e_B, svatko se može predstaviti kao osoba A. Upravo zbog toga dolazi do pitanja vjerodostojnosti ili autentičnosti poruke. Ovaj se problem može riješiti na sljedeći način:

1. Osoba A doda svojoj poruci slučajan broj a od recimo 10 znamenaka:
2. Osoba B generira svoj slučajan $10-$znamenkasti broj b i pošalje osobi A poruku $e_A(a+b)$;
3. Formulom $b = d_A(e_A(a+b)) - a$ pošiljatelj A izračuna b, zatim šalje početnu poruku kojoj doda b.

Učenike možemo upoznati s kriptosustavom s javnim ključem kroz primjer telefonskog imenika. S obzirom na telefonski imenik (javni ključ) možemo šifrirati slovo tako da nasumce izaberemo ime koje započinje tim slovom, a zatim umjesto slova pošaljemo odgovarajući telefonski broj. Jasno je da je lako pronaći ime počevši od zadanog slova, međutim teško je pronaći ime koje pripada zadanom telefonskom broju. Ako primatelj ima specijalni telefonski imenik (privatni ključ) koji je sortiran prema telefonskim brojevima tada je u mogućnosti efikasno dešifrirati poruku. Također, na temelju metafore brave učenicima možemo pojasniti da je javni ključ lokot, a odgovarajući privatni ključ je ključ koji ga otvara. Zgodan i vrlo jednostavan protokol kojim se čuva tajnost podataka dan u Aktivnosti 8.

U sljedećem odjeljku navest ćemo primjer kriptosustava s javnim ključem koji je primjeren za učenike srednjih škola.

4.1 Savršeni kôd

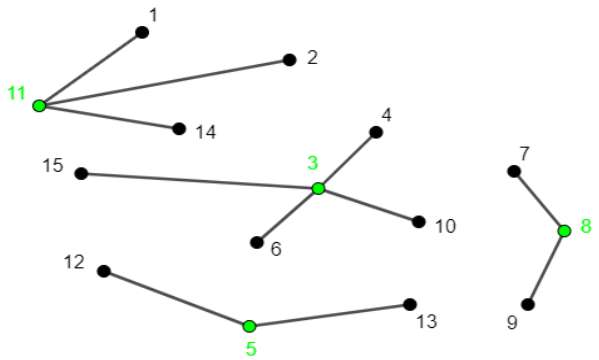
Na samome početku učenike upoznajemo s osnovnim pojmovima iz teorije grafova. *Graf* G je uređena trojka $G = (V(G), E(G), \psi(G))$ koja se sastoji od nepraznog skupa $V(G)$ čiji su elementi vrhovi grafa G, skupa $E(G)$ disjunktnog sa $V(G)$ čiji su elementi bridovi od G i funkcije incidencije koja svakom bridu od G pridružuje neuređeni par (ne nužno različitih) vrhova od G. *Susjedstvo* danog vrha sastoji se od samog tog vrha, te svih vrhova koji su s njim povezani bridom. *Savršeni kôd* u grafu je podskup skupa vrhova sa svojstvom da je svaki vrh grafa u susjedstvu jednog i samo jednog vrha iz tog podskupa.

Konstrukcija tajnog i javnog ključa

Tajni i javni ključ su grafovi, pri čemu je tajni ključ savršen kôd. Njihovu konstrukciju možemo opisati u sljedećih nekoliko koraka.

1. Nacrtati ćemo proizvoljan skup vrhova (u našem slučaju petnaest) te ih numerirati radi lakšeg snalaženja.

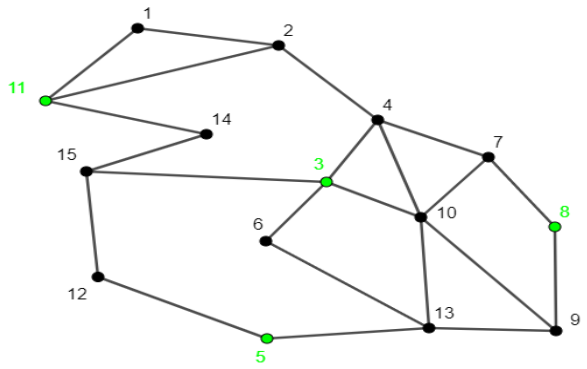
2. Odaberemo tajni ključ C, odnosno odaberemo neke od vrhova npr. $C = \{3, 5, 11, 8\}$. Skup C predstavljati će naš tajni ključ. Radi preglednosti vrhove iz skupa C obojiti ćemo zelenom bojom.



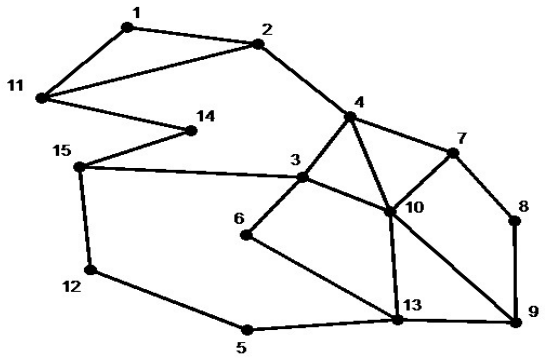
Slika 4.2: Tajni ključ $C = \{3, 5, 11, 8\}$ i "zvjezdasti graf "

3. Od vrhova iz C povlačimo bridove k ostalim vrhovima tako da nam je svaki vrh povezan s točno jednim vrhom iz C. (Slika 4.2)

4. Povlačimo po volji mnogo bridova između "vanjskih bridova" kao na Slici 4.3. Ne smijemo vući nove bridove iz vrhova koji pripadaju skupu C kako ne bismo pokvarili savršeni kôd. Ovako dobiveni graf predstavlja javni ključ (Slika 4.4). Uočili smo da je gotovo nemoguće uočiti tajni ključ, odnosno savršeni kôd ako smo načinili dobro "prikrivanje".



Slika 4.3: "Prikrivanje zvijezda "



Slika 4.4: Javni ključ

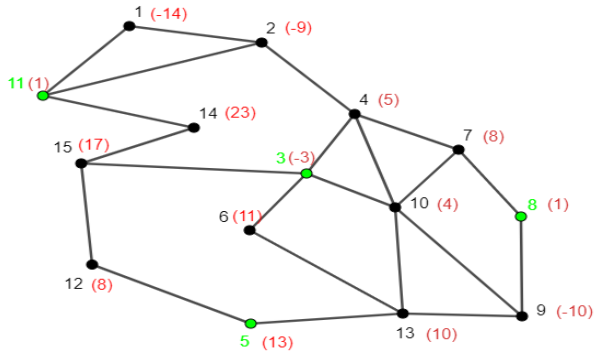
Šifriranje poruke

Pretpostavit ćemo da je naš otvoreni tekst neki cijeli broj m između 50 i 100, na primjer $m = 65$ te da koristimo javni ključ sa Slike 4.4.

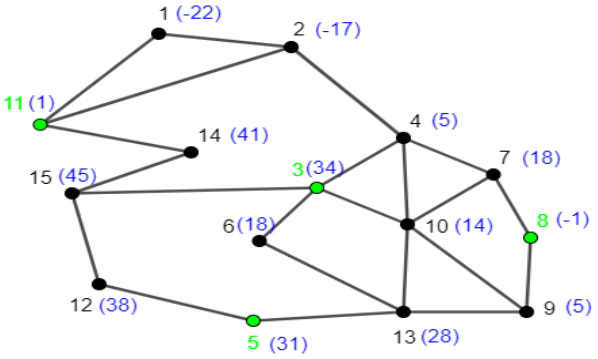
(i) Uz svaki vrh grafa upišimo cijeli broj (može i negativan) x_i tako da je $\sum x_i = m$. U našem slučaju odabrali smo

$$(x_1, x_2, \ldots, x_{15}) = (-14, -9, -3, 5, 13, 11, 8, 1, -10, 4, 1, 8, 10, 23, 17).$$

Zbog preglednosti novoupisane cijele brojeve napisali smo crvenom bojom (Slika 4.5).



Slika 4.5: "crveni brojevi"



Slika 4.6: "plavi brojevi"-šifrat

(ii) Zbrojimo sve crvene brojeve u susjedstvu svakog vrha (uključujući i taj vrh). Zbog preglednosti upisali smo dobivene vrijednosti plavom bojom (Slika 4.6). Naša poruka je šifrirana te otvorenim kanalom šaljemo graf na kojem su upisani samo plavi brojevi.

Dešifriranje poruke

Poruka se dešifrira tako da se zbroje svi plavi brojevi uz vrhove iz savršenog kôda koji su na Slici 4.6 označeni zelenom bojom $C = (3, 5, 8, 11)$:

$$34 + 31 - 1 + 1 = 65.$$

Dekriptiranje šifrata

Sigurnost ovog kriptosustava ne leži samo u prikrivanju savršenog kôda, već i u nedovoljnom znanju linearne algebre učenika. Naime, elemente niza (x_i) možemo izračunati pomoću sustava linearnih jednadžbi. U slučaju šifrata sa Slike 4.6 dobivamo sljedeći sustav:

$$\begin{aligned} x_1 + x_2 + x_{11} &= -22 \quad \text{(iz vrha 1)} \\ x_1 + x_2 + x_4 + x_{11} &= -17 \quad \text{(iz vrha 2)} \\ x_3 + x_4 + x_6 + x_{10} + x_{15} &= 34 \quad \text{(iz vrha 2)} \\ &\vdots \\ x_3 + x_{12} + x_{14} + x_{15} &= 45 \quad \text{(iz vrha 15)} \end{aligned}$$

Nakon što učenicima ukratko objasnimo kako šifrirati i dešifrirati otvoreni tekst Savršenim kodom možemo provesti sljedeću aktivnost u razredu (Aktivnost 9).

Poglavlje 5

Aktivnosti

Aktivnost 1 (Cezarova šifra)**.** ↑

Razred: 5. (OŠ)

Cilj aktivnosti: učenici će otkriti kako šifrirati i dešifrirati poruke Cezarovom šifrom

Korelacija s matematikom i drugim predmetima: računanje s prirodnim brojevima, povijest (Rimsko carstvo), engleski jezik (abeceda)

Oblik rada: suradnički rad u paru

Materijali: nastavni listić

Tijek aktivnosti: Učenicima ukratko objasniti kako se šifriraju, dešifriraju te razbijaju poruke pomoću Cezarove šifre koju je koristio Gaj Julije Cezar (1. st. pr. Kr.) za komunikaciju sa svojim generalima i prijateljima. Nastavni listić rješava se u paru.

Nastavni listić - Cezarova šifra

1. Dani otvoreni tekst (poruku) šifriraj pomakom za jedno mjesto dalje u abecedi:

   R O K O V O L I M A T E M A T I K U

   _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

   Dešifriraj poruku:

   _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

   N B S U B W P M J G J A J L V

2. Originalna Cezarova šifra je dobivena pomakom za tri mjesta dalje u abecedi. U tom slučaju kažemo da ključ $n = 3$.
   Ispod svakog slova abecede napiši šifrirano slovo dobiveno Cezarovom šifrom za $n = 3$.

   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

   _

   Šifriraj poruku pomoću Cezarove šifre za $n = 3$:

   U N A P A D!

   _ _ _ _ _ _!

3. Dana je šifrirana poruka na latinskom jeziku. Ako je poznato da se slova I, E i A najčešće pojavljuju u latinskom, pokušaj odgonetnuti poruku. Koji je ključ korišten za šifriranje?

   _ _ _ _, _ _ _ _, _ _ _ _!

   K T C X, K X S X, K X R X!

Rješenje nastavnog listića

1. Šifrat glasi:

R O K O V O L I M A T E M A T I K U

S P L P W P M J N B U F N B U J L V

Otvoreni tekst glasi:

M A R K O V O L I F I Z I K U

N B S U B W P M J G J A J L V

2. Šifrirana 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
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

U N A P A D!

X Q D S D G!

3. U uz pretpostavku da se slovo I šifriralo u X, odnosno pomakom za 15 mjesta u desno dobiva se:

V E N I, **V I D I**, **V I C I**!

K T C X, K X S X, K X R X!

Aktivnost 2 (Cezarov krug)**.** ↑

Razred: 5. (OŠ)

Cilj aktivnosti: učenici će šifrirati i dekriptirati Cezarovu šifru pomoću šifrarnika

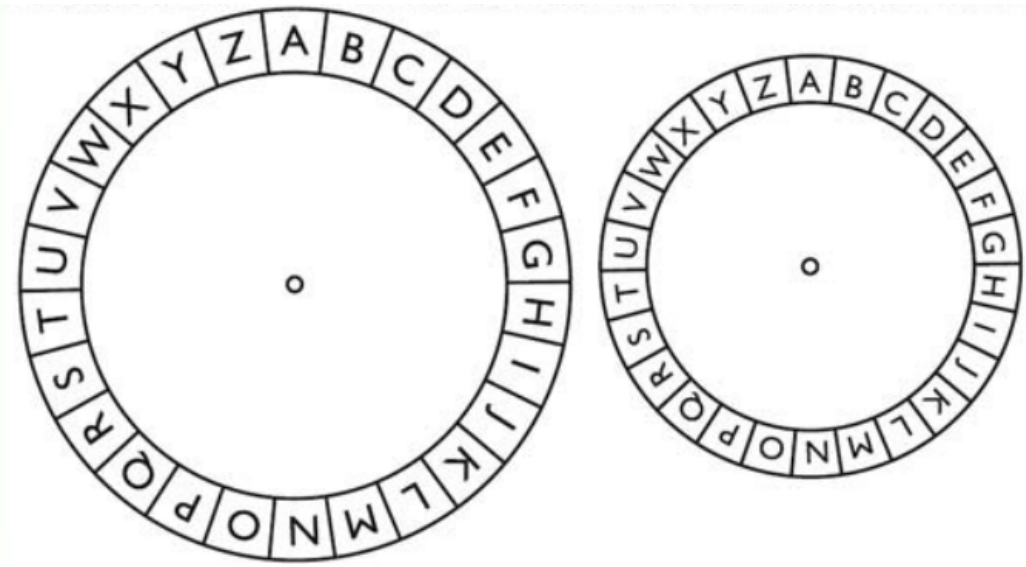
Korelacija s matematikom i drugim predmetima: zakretanje (rotacija) u pozivnom i negativnom smjeru, koncentrične kružnice, tehnički odgoj, engleski jezik (abeceda), povijest (Rimsko carstvo)

Oblik rada: suradnički rad u paru

Materijali: nastavni listić, škare, spajalica

Tijek aktivnosti: Učenici izrađuju šifrarnik Cezarov krug pomoću kojeg šifriraju poruke. Svaki par ima svoj protivnički par koji međusobno razmjenjuju šifrate i pokušavaju ih razbiti. Pobjednički par je onaj koji prvi dekriptira poruku. Poruke se sastoje od najviše 15 slova (pri čemu se zanemaruju razmaci i interpunkcijski znakovi).

Nastavni listić - Cezarov krug



Otvoreni tekst (poruka): _____
Šifrat za protivnički tim: _____

Šifrat od protivničkog tima: _____
Dekodirana poruka protivničkog tima: _____

Napomena: Poruke ne smiju biti dulje od 15 slova. Razmaci između riječi i interpunkcijski znakovi se zanemaruju ("brišu'").

Primjer:

Otvoreni tekst (poruka):	RIMSKI VLADAR
Šifrat za protivnički tim:	YPTZRPCSHKHY ($k = 7$)
Šifrat od protivničkog tima:	KVOKSKMDKOCD ($k = 10$)
Dekodirana poruka protivničkog tima:	ALEA IACTA EST

[0]Nacrt za šifrarnik je preuzet s `http://gimnazija-metkovic.skole.hr/upload/gimnazija-metkovic/images/static3/1266/attachment/(De)sifriranje.pdf`

Aktivnost 3 (Dekriptiranje Cezarove šifre pomoću frekvencije analize slova)**.** ↑

Razred: 7. (OŠ)

Cilj aktivnosti: učenici će primjenom frekvencijske analize dešifrirati zadani šifrat

Korelacija s matematikom i drugim predmetima: obrada podataka (frekvencije, relativne frekvencije, stupčasti dijagram, kružni dijagram), hrvatski jezik (književnost)

Oblik rada: grupni rad (5-6 učenika)

Materijali: nastavni listić

Tijek aktivnosti: Svaki od učenika dobiva šifriranu poruku pri čemu svaka grupa ima svoju poruku. Svaki učenik unutar grupe treba naći frekvenciju 5-6 slova. Zatim svaka grupa načini supčasti dijagram i kružni dijagram za 5 slova koja se u šifratu pojavljuju s najvećom frekvencijom. Ako je poznato da se u hrvatskom jeziku najčešće pojavljuju slova A,I,O,E,N, učenici pokušavaju dekriptirati poruku uz pretpostavku da je najfrekventnije slovo šifrata jedno od navedenih.

Nastavni listić - Frekvencijska analiza šifrata

Zadan je šifrirani tekst koji je zbog preglednosti grupiran po 5 slova. Razmaci i interpunksijski znakovi su izbačeni iz otvorenog teksta (poruke) koja je šifrirana.

XOUKW OCSVK CXKJX YZYFE UVKSJ DSTOV KZYQV ONKYC KWZBO

WKQYB OSCZK JSYZY JXKDS VSUUY TSWSC OYCWT ORSFK YVODS

YCKWW EECEC BODDK WYWOM OUKYC DKBSL STOVK MUSWX EYWST

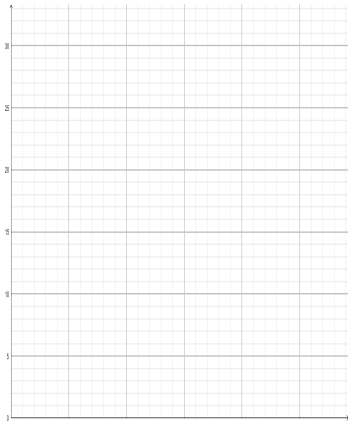
OEJXK UNYLB YNYCV SMOSZ BEJSY ZBOUB KCXKU BSVKU KUFKT

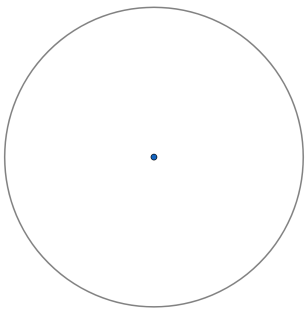
OSCKW SWKY

1. Ispuni tablicu za 5 najfrekventnijih slova šifrata:

slovo	frekvencija	relativna frekvencija

2. Nacrtaj stupčasti i kružni dijagram prema podatcima iz tablice.





3. Ako je poznato da je šifrat dobiven Cezarovom šifrom i da se u hrvatskom jeziku najčešće pojavljuju slova A,I,O,E,N, pokušaj pronaći otvoreni tekst. Pomakom za koliko slova je dobivena šifrirana abeceda? Napiši ju:

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:

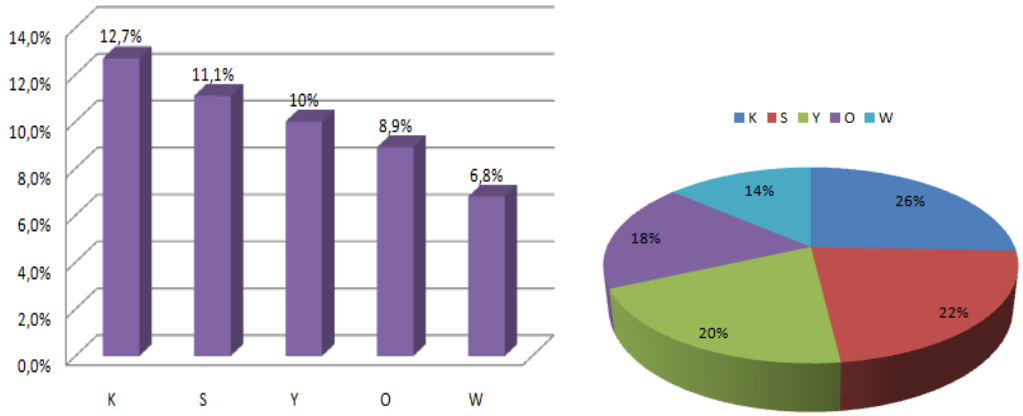
Prepoznaješ li iz kojeg je djela uzet tekst?

Rješenje nastavnog listića

1. Pet najfrekventnijih slova šifrata su K,S,Y,O i W.

slovo	frekvencija	relativna frekvencija
K	24	$0,127$
S	21	$0,111$
Y	19	$0,100$
O	17	$0,089$
W	13	$0,068$

2. Stupčasti i kružni dijagram prema podatcima iz tablice:



3. Uz pretpostavku da se slovo A šifriralo u K, tj. da se šifrirana abeceda dobila pomakom za 10 mjesta u desno imamo:

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
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**

Otvoreni tekst glasi:

Neka me sila snažno povukla iz tijela. Pogledao sam prema gore i spazio poznati lik koji mi se osmjehivao. Letio sam mu ususret. Tamo me čekao stari Bijelac. Kimnuo mi je u znak dobrodošlice i pružio prekrasna krila kakva je i sam imao.

Navedeni tekst je iz djela: **Božidar Prosenjak, Divlji konj.**

Aktivnost 4 (Afina šifra)**.** ↑

Razred: 7. (OŠ)

Cilj aktivnosti: učenici će pomoću linearne (afine) funkcije šifrirati i dešifrirati

Korelacija s matematikom i drugim predmetima: linearna (afina) funkcija, osnovne računske operacije s cijelim brojevima, najveći zajednički djelitelj

Oblik rada: suradnički rad u grupi

Materijali: nastavni listić

Tijek aktivnosti: Učenike dijelimo u skupine. Svaki učenik dobiva svoj radni listić te međusobno u skupinama uspoređuju i provjeravaju svoja rješenja. Svaka skupina bira svoga predstavnika koji pred razredom izlaže rješenja i postupak rješavanja pojedinog zadatka.

Nastavni listić - Afina šifra

1. Zadana je funkcija $f(x) = 3x + 5 \mod 26$. Šifrirajte abecedu pomoću ove funkcije:

	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
$f(x)$	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_
	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_

2. Zadana je funkcija $g(x) = 2x + 3 \mod 26$. Šifrirajte abecedu pomoću ove funkcije:

	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
$g(x)$	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_
	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_

3. Koja od dvije funkcije, f i g može poslužiti za šifriranje? Što misliš koji je razlog tome? Imaš li ideju koje bi afine funkcije bille *pogodne* za korištenje u šifriranju?
(*Uputa*: Izračunaj nzd$(3, 26)$ i nzd$(2, 26)$.)

4. Zadana je funkcija šifriranja $f_e(x) = 9x+2 \mod 26$. Pokušaj odrediti funkciju dešifriranja koja je analognog oblika, $f_d(y) = ay + b \mod 26$. Točnost svoje funkcije deširiranja provjeri na šifratu GCRMGCRWOC.

(*Uputa*: Pronađi koeficijente $a, b \in \{0, 1, 2, \ldots, 25\}$ za koje vrijedi $a(9x + 2) + b \mod 26 = x$, odnosno $9a \mod 26 = 1$ i $2a + b \mod 26 = 0$.)

Funkcija dešifriranja: $f_d(y) =$_ $y+$ _ $\mod 26$

	G	C	R	M	G	C	R	W	O	C
y	_	_	_	_	_	_	_	_	_	_
$f_d(y)$	_	_	_	_	_	_	_	_	_	_
	_	_	_	_	_	_	_	_	_	_

Rješenje nastavnog listića

1. $f(x) = 3x + 5 \mod 26$.

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

2. $g(x) = 2x + 3 \mod 26$

	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
$g(x)$	**3**	**5**	**7**	**9**	**11**	**13**	**15**	**17**	**19**	**21**	**23**	**25**	**1**	**3**	**5**	**7**	**9**	**11**	**13**	**15**	**17**	**19**	**21**	**23**	**25**	**1**
	D	**F**	**H**	**J**	**L**	**N**	**P**	**R**	**T**	**V**	**X**	**Z**	**B**	**D**	**F**	**H**	**J**	**L**	**N**	**P**	**R**	**T**	**V**	**X**	**Z**	**B**

3. Funkcija g ne šifrira sva slova jednoznačno, npr. F i S se šifriraju u N, G i T u P, itd. pa ona nije pogodna za šifriranje. Uočimo da je $\text{nzd}(3, 26) = 1$, dok je $\text{nzd}(2, 26) = 2$. Općenito, za šifriranje mogu poslužiti samo one funkcije $x \mapsto ax + b \mod 26$ za koje su a i 26 relativno prosti brojevi.

4. Treba pronaći $a, b \in \{0, 1, 2, \ldots, 25\}$ za koje vrijedi $a(9x + 2) + b \mod 26 = x$, odnosno $9a \mod 26 = 1$ i $2a + b \mod 26 = 0$. Najprije određujemo broj $a \in \{1, 2, \ldots, 25\}$ koji pomnožen s 9 pri dijeljenju s 26 daje ostatak 1. Ispitujući redom za $a = 1, 2, \ldots$, zaključujemo da je $a = 3$. Sada tražimo $b \in \{0, 1, 2, \ldots, 25\}$ za koji je $2a + b = 6 + b$ djeljivo sa 6. Očito $b = 20$. Dakle, funkcija dešifriranjaje

$$f_d(y) = \mathbf{3}y + \mathbf{20} \mod 26.$$

	G	C	R	M	G	C	R	W	O	C
y	**6**	**2**	**17**	**12**	**6**	**2**	**17**	**22**	**14**	**2**
$f_d(y)$	**12**	**0**	**19**	**4**	**12**	**0**	**19**	**8**	**10**	**0**
	M	**A**	**T**	**E**	**M**	**A**	**T**	**I**	**K**	**A**

Aktivnost 5 (Vigenèreova šifra)**.** ↑

Razred: 7. (OŠ)

Cilj aktivnosti: učenici će dešifrirati pomoću Vigenèreovog kvadrata

Korelacija s matematikom i drugim predmetima: pravokutni koordinatni sustav

Oblik rada: suradnički rad u grupi

Materijali: nastavni listić, list s Vigenèreovim kvadratom

Tijek aktivnosti:
Učenike podijelimo u skupine, svaka skupina ima šest članova. Svaki učenik dobiva list na kojem se nalazi Vigenèreov kvadrat, te svaka skupina dobiva listić sa zadacima. Svaki učenik unutar skupine dešifrira jednu šifru. Nakon što su svi učenici dešifrirali svoje šifre provodimo razrednu diskusiju te zapisujemo zaključak.

Nastavni listić - Vigenèreova šifra

Na odjelu za matematiku dogodilo se ubojstvo.Vaš je posao dešifrirati tragove za pronalaženje:

1. identitet ubojice,
2. oružje kojim je počinjeno ubojstvo,
3. prostorija u kojoj se dogodilo ubojstvo.

Sedam osumnjičenih su: **gosp. Francuz**, **gđa. Rukavina**, **gđa. Merkić**, **gosp. Štop**, **gosp. Bjelić**, **gosp. Bebić**, **gđa. Navić**.

Moguća oružja kojim je počinjeno ubojstvo su: **škare**, **ravnalo**, **klamerica**, **nož**, **stolica**.

Soba u kojoj je počinjeno ubojstvo mogla bi biti: **16**, **23**, **24**, **25**, **28**, **29**, **računalni praktikum**.
Kad završite, morate biti spremni opravdati svoje odluke pred razredom.

Šifra 1. NXFC ETTJ VFWV NOMH FVFL IXVZ FAEN
Ključ: HEJ

Šifra 2. HNLS FVSW LUKA LPMH JVFW FLPR KIVM WCGE UBK
Ključ: HEJ

Šifra 3. YNVF IVTJ GACE ILCW XPUE AVVH BPPN Y
Ključ: DETEKTIV

Šifra 4. MNLV YTWZ YKQE SLJJ ZEJA LHEN WGVF UQWE BISF U
Ključ: DETEKTIV

Šifra 5. RXVF IANT GABY YUBJ KKZL HLVR BPVI DHCT GATQ SLFN ZEZF UKW
Ključ: DETEKTIV

Šifra 6. YNVF IVTJ GABI DVRF HLYR YOUJ QEYE FYAW LZUE XIJT GACW
Ključ: DETEKTIV

Rješenje nastavnog listića

Šifra 1.
"Ubojica nema slovo *e* u svojem prezimenu."

Šifra 2.
"Oružje kojim je počinjeno ubojstvo nema oštar metalni dio."

Šifra 3.
"Broj sobe je višekratnik broja četiri."

Šifra 4.
"Prezime ubojice reći će vam iz koje je zemlje."

Šifra 5.
"Ubojstvo je učinjeno s predmetom na kojem učenici sjede."

Šifra 6.
"Broj sobe je umnožak prvih četiri prirodnih brojeva."

Aktivnost 6 (Permutacijska šifra)**.** ↑

Razred: 3. (SŠ)

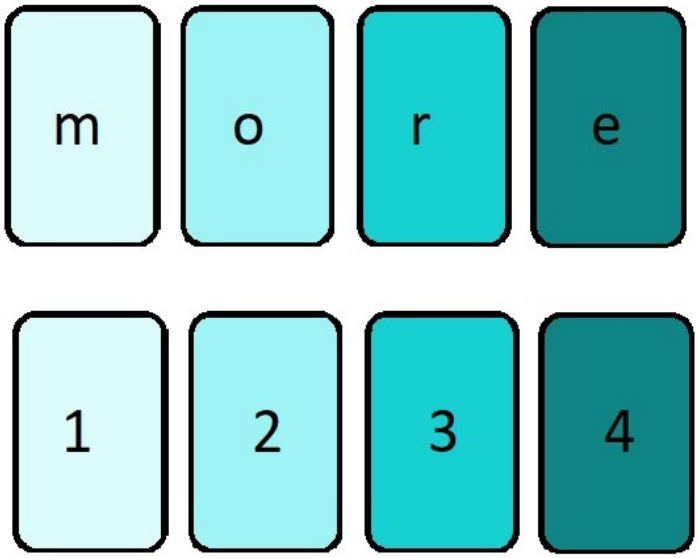
Cilj aktivnosti: učenici će šifrirati permutacijskom šifrom

Korelacija s matematikom i drugim predmetima: kombinatorika (permutacije)

Oblik rada: suradnički rad u grupi

Materijali: nastavni listić

Tijek aktivnosti: Učenike podijelimo u skupine. Svaka skupina dobiva kartice na kojima se s jedne strane nalaze slova M, O, R, E, a s druge strane kartica nalaze se redom brojevi 1, 2, 3, 4. Učenici u skupinama rješavaju nastavni listić.



Nastavni listić - Permutacijska šifra

1. Ispišite sve riječi (bez obzira na smisao) koje možete složiti od danih kartica?

   Postoji li jednostavniji način kojim možemo prebrojati sve riječi?

2. Okrenite kartice te ih složite zadanim redom:

   1. 2. 3. 4.

   – – – –

   Koju riječ ste dobili? Šifrirajte zadanu riječ s ključem $k = (4, 1, 3, 2)$.

3. Šifrirajte sljedeću rečenicu "Najviši vrh na jadranskim otocima je Vidova gora na Braču" s ključem $k = (5, 3, 4, 7, 6, 1, 2, 8)$.

5	3	4	7	6	1	2	8

1	2	3	4	5	6	7	8

Šifrat: _____

Rješenje nastavnog listića

1. Sve riječi u alfabetskom poretku su:

   emor, emro, eomr, eorm, ermo, erom,
   meor, mero, moer, more, mreo, mroe,
   oemr, oerm, omer, omre, orem, orme,
   remo, reom, rmeo, rmoe, roem, rome

   Broj riječi jednak je broju permutacija 4-članog skupa: $P_4 = 4! = 24$.

2.

   1. 2. 3. 4.

   M O R E

   Šifrat glasi: EMRO.

3.

5	3	4	7	6	1	2	8
N	A	J	V	I	Š	I	V
R	H	N	A	J	A	D	R
A	N	S	K	I	M	O	T
O	C	I	M	A	J	E	V
I	D	O	V	A	G	O	R
A	N	A	B	R	A	Č	U

1	2	3	4	5	6	7	8
Š	I	A	J	N	I	V	V
A	D	H	N	R	J	A	R
M	O	N	S	A	I	K	T
J	E	C	I	O	A	M	V
G	O	D	O	I	A	V	R
A	Č	N	A	A	R	B	U

   Šifrat: ŠAMIGAIDOEOČAHNCDNJNSIOANRAOIAIJIAARVAK-MVBVRTVRU

Aktivnost 7 (Šifra s uzorkom)**.** ↑

Razred: 3. (SŠ)

Cilj aktivnosti: učenici će pomoću šifre s uzorkom otkriti otvoreni tekst

Korelacija s matematikom i drugim predmetima: graf funkcije, eksponencijalna funkcija, trigonometrijske funkcije, biologija

Oblik rada: suradnički rad u paru

Materijali i nastavna pomagala: nastavni listić, tablet (ili mobitel), računalo

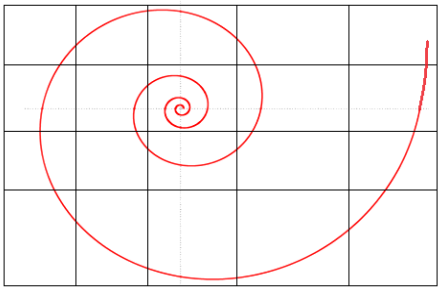
Tijek aktivnosti: U prirodi se mogu naći različiti spiralni uzorci. Najčešće se pojavljuju logaritamska spirala i Arhimedova spirala. Ovdje će spirale poslužiti kao ključ za šifriranje. Učenici će naučiti da se iza tih spirala kriju neke njima poznate elementarne matematičke funkcije. Odgovore na neka pitanja naći će pretraživanjem interneta. Korištenjem Geogebre može se pokazati kako se navedene spirale mogu dobiti kao grafovi parametarski zadanih funkcija.

Nastavni listić - Šifra s uzorkom

1. Dešifriraj šifru ATSEALOMSJNZAKIORAZV.

   Uputa: šifrat upiši u pravokutnu mrežu s lijeva na desno i od gore prema dolje.

   Ključ šifre: spirala od unutra prema van u suprotnom smjeru kretanja kazaljke na satu.

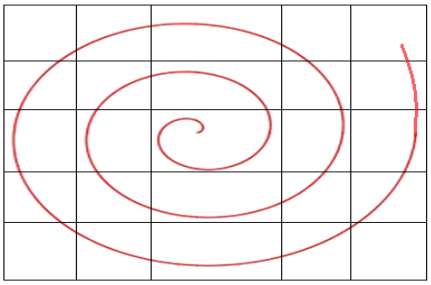


   Otvoreni tekst: _____

2. Dešifriraj šifru ESTSXNJAOXAMNKULANJAHAZIUU.

   Uputa: šifrat upiši u pravokutnu mrežu s lijeva na desno i od gore prema dolje.

   Ključ šifre: spirala od unutra prema van u suprotnom smjeru kretanja kazaljke na satu.



   Otvoreni tekst: _____

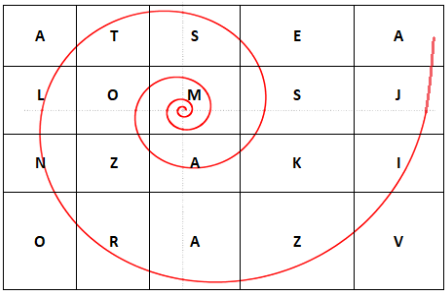
3. Koje su razlike između nacrtanih spirala? Pokušaj otkriti njihove nazive. Pronađi u stvarnom svijetu primjere nacrtanih spirala.

4. Mogu li nacrtane spirale biti graf neke funkcije u Kartezijevom koordinatnom sustavu?

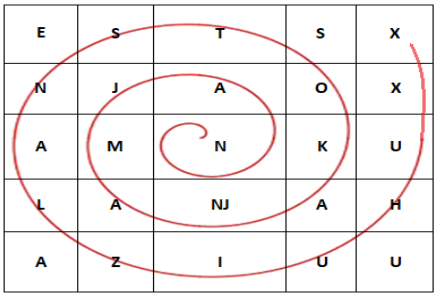
5. Što misliš s kojim elementarnim funkcijama su povezane nacrtane spirale?

Rješenje nastavnog listića

1. Otvoreni tekst: **MOZAK SE STALNO RAZVIJA.**



2. Otvoreni tekst: **NAJMANJA KOST SE NALAZI U UHU.**



3. Spirala iz prvog zadatka se naziva **logaritamska spirala** ili **Spira mirabilis** (čudesna spirala) i razlikuje se od spirale iz drugog zadatka tzv. **Arhimedove spirale** po tome što joj razmak između zavoja raste, dok je kod Arhimedove stalan.
   Logaritamska spirala u prirodi: kućica puža, indijska lađica, suncokret, galaksija, kaktus, uragan Katrina, ...
   Arhimedova spirala u prirodi je rjeđe prisutna. Može se naći kod mladica paprati. Model Arhimedove spirale je namotano uže.

4. Spirale nisu graf neke funkcije jer paralela s osi y siječe spirale u više (štoviše beskonačno) točaka.

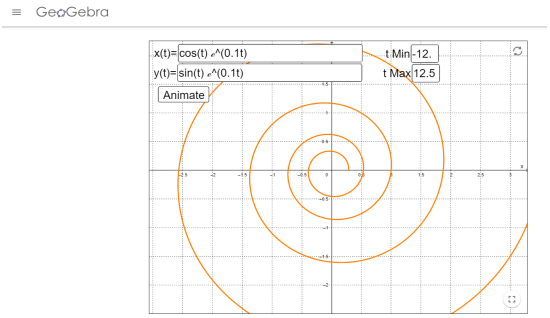
5. Ove spirale su povezane s eksponencijalnom funkcijom, te trigonometrijskim funkcijama. Svaka točka logaritamske spirale može se opisati kao uređeni par dviju funkcija $x(t)$ i $y(t)$:

$$(x(t), y(t)) = (ae^{bt}\cos t, ae^{bt}\sin t), t \in \mathbb{R},$$

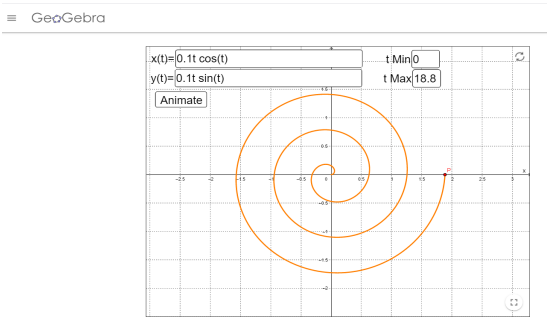
gdje su a i b neke konstante.
Arhimedova spirala povezana je s trigonometrijskim funkcijama, a svaka točka je uređeni par sljedećih funkcija:

$$(x(t), y(t)) = (at\cos t, at\sin t), t \in \mathbb{R}, t \geq 0$$

gdje je a konstanta. Za navedene funkcije kažemo da su zadane parametarski.



Slika 5.1: Graf logaritamske spirala $(e^{0.1t}\cos t, e^{0.1t}\sin t)$ za $t \in [-4\pi, 4\pi]$



Slika 5.2: Graf Arhimedove spirala $(0.1t\cos t, 0.1t\sin t)$ za $t \in [0, 6\pi]$

Aktivnost 8 (Tajni protokol)**.** ↑

Razred: 7. (OŠ)

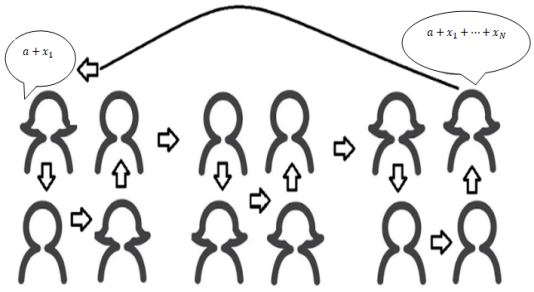
Cilj aktivnosti: učenici će šifrirati i dešifrirati Savršenim kodom

Korelacija s matematikom i drugim predmetima: aritmetička sredina, problem iz života - zaštita osobnih podataka

Oblik rada: suradnički rad

Tijek aktivnosti: Učenicima predstavimo sljedeći problem: Željeli bi imati podatak koliki je prosječni tjedni džeparac učenika u razredu. To je aritmetička sredina iznosa džeparca svih učenika u razredu koji bi izračunali kao kvocijent zbroja džeparaca i broja učenika, $(x_1 + \ldots + x_N)/N$. No, ne bismo željeli da svaki učenik javno kaže koliko tjedno prima novca jer to smatramo *osobnim podatkom*. Možemo li nekako prikupiti podatke tako da nam bude poznat zbroj svih iznosa džeparaca, ali ne i svaki od pojedinačnih iznosa? Za to možemo koristiti tzv. *tajni protokol* koji se sastoji u tome da prvi učenik izabere proizvoljan cijeli broj a i njemu pribroji iznos svog džeparca, $a + x_1$, te ga prišapne drugom učeniku. Drugi učenik ne može znati koji džeparac prima prvi učenik jer ga je on "maskirao" s nepoznatim brojem a. Drugi učenik broju $a + x_1$ pribroji iznos svog džeparca i dalje trećem učeniku šapne broj $a + x_1 + x_2$. Postupak se nastavlja dalje i u zadnjem koraku posljednji učenik iz razreda prvom šapne broj koji sada iznosi $a + x_1 + x_2 + \cdots + x_N$. Prvi učenik sada može izračunati srednju vrijednost:

$$\bar{x} = \frac{(a + x_1 + x_2 + \cdots + x_N) - a}{N}.$$



Aktivnost 9 (Savršeni kôd)**.** ↑

Razred: 1., 2., 3., 4. (SŠ)

Cilj aktivnosti: učenici će šifrirati i dešifrirati Savršenim kôdom

Korelacija s matematikom i drugim predmetima: sustav linearnih jednadžbi

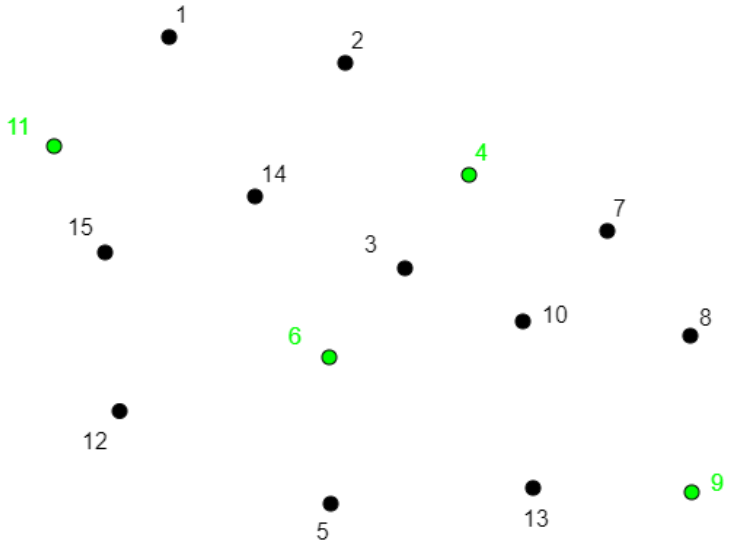
Oblik rada: suradnički rad u grupi

Materijali: nastavni listić, list papira

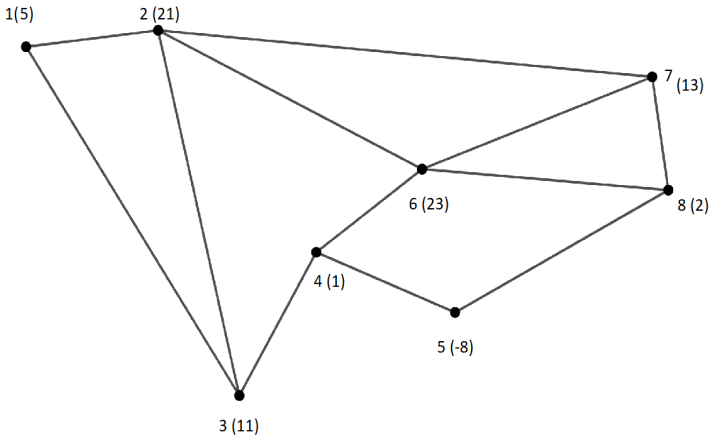
Tijek aktivnosti: Učenike podijelimo u dvije skupine. Svaka skupina dobiva dva lista papira. Na jednom listu papira nacrtan je proizvoljan skup vrhova te su označeni vrhovi (zelena boja) koji predstavljaju tajni ključ. Zadan je otvoreni tekst (skupine ne dobivaju isti otvoreni tekst) te učenici dobivaju zadatak da ga šifriraju. Rješenje zapisuju na drugom listu papira. Kada su obje skupine gotove, skupine međusobno zamjenjuju list na kojem su zapisana rješenja te je njihov zadatak da dešifriraju poruku.

Primjer nastavnog listića - Savršen kôd

1. Pomoću prikazanog grafa šifriraj otvoreni tekst 57. Vrhovi koji pripadaju tajnom ključu označeni su zelenom bojom.

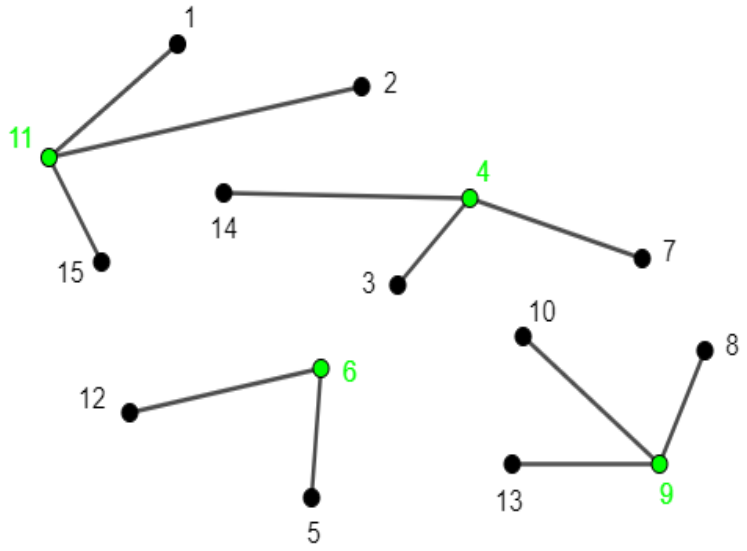


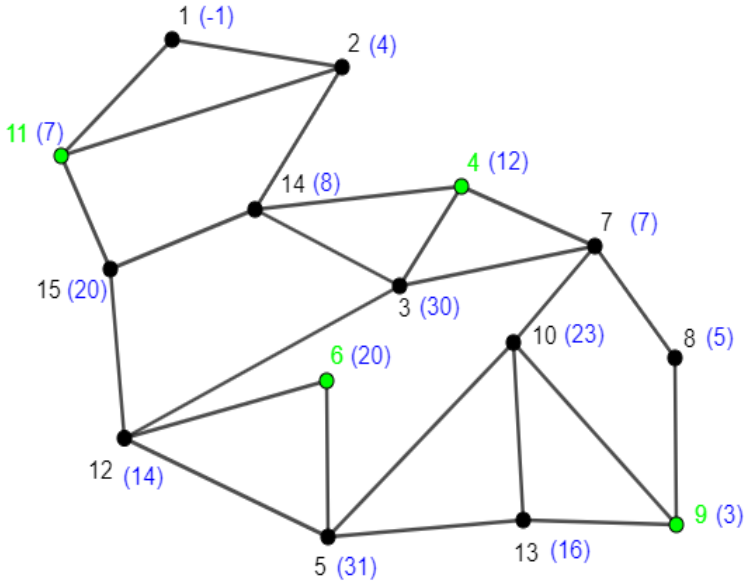
2. Pokušajte otkriti otvoreni tekst ako je šifrat zadan sljedećim kôdom:



Rješenje nastavnog listića

1. Primjer dobrog javnog i tajnog ključa





2. Rješavanjem sustava (supstitucijom)

$x_1+x_2+x_3 = 5, x_1+x_2+x_3+x_6+x_7 = 21, x_1+x_2+x_3+x_4 = 11, x_4+x_5+x_6 = 1,$

$x_4+x_5+x_8 = -8, x_2+x_4+x_6+x_7 = 23, x_2+x_6+x_7+x_8 = 13, x_5+x_6+x_7+x_8 = 2,$

dobiva se

$$(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) = (x_1, 1, 4 - x_1, 6, -10, 5, 11, -4), x_1 \in \mathbb{Z}.$$

Otvoreni tekst je

$$\sum_{i=1}^{8} = x_1 = 13$$

Bibliografija

[1] M. Barun, A. Dujella, Z. Franušić, *Kriptografija u školi*, Poučak, 33 (2008), str. 40-52.

[2] M. Crnogaća, *Kriptografija: tajanstveno komuniciranje*, Drvo znanja - enciklopedijski časopis za mladež, 8 (2004), 78, str. 60-65.

[3] A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.

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

[5] N. Koblitz, *Cryptograpy as a teaching tool*, Cryptologia 21 (1997) 317–326. `http://www.math.washington.edu/~koblitz/crlogia.html`

[6] M. R. Fellows, N. Koblitz, *Combinatorially based cryptography for children (and adults)*, Congr. Numerantium 99 (1994), 9–41. `http://citeseer.ist.psu.edu/95924.html`

[7] D. Komm, L. Keller, A. Sprock, G. Serafini, *Teaching Public-Key Cryptography in School*, str. 122

[8] S. Singh, *Šifre : Kratka povijest kriptografije*, Mozaik knjiga, Zagreb, 2003.

[9] M.T. Sakalli, E. Buluş, F. Büyüksaraçoğlu, *Cryptography Education for Students*, `https://www.researchgate.net/publication/4105618_Cryptography_education_for_students`

[10] Practical Cryptography, `http://practicalcryptography.com/`

Sažetak

Kriptografija kao znanstvena disciplina izaziva zanimanje većine učenika svih dobnih skupina. Iako nije dio redovne nastave matematike u osnovnoj i srednjoj školi, lako je primjenjiva u nastavi.

U ovom diplomskom radu nakon potrebne teorijske podloge, izložene su aktivnosti koje bi se mogle provesti na fakultativnoj nastavi matematike u osnovnoj i srednjoj školi.

Summary

Cryptography as a science arouses the interest of most students of all ages. Although it is not part of the regular math curriculum in elementary and high school, it is easily applicable in teaching.

In this diploma thesis, after the necessary theoretical background, the activities that could be carried out in optional teaching of mathematics in elementary and high school are presented.

Životopis

Rođena sam u Rijeci 1996. godine. Odrasla sam u Portu na otoku Krku gdje sam provela svoje djetinjstvo i ranu mladost. Završila sam osnovnu školu Fran Krsto Frankopan u Malinskoj. Srednju školu pohađala sam u Pazinu, i to Pazinski Kolegij-Klasičnu gimnaziju. U posljednjem trenutku odlučujem se za matematiku te upisujem Preddiplomski Sveučilišni studij Matematika u Rijeci te stičem status prvostupnice matematike. Slijedeći svoju želju za nastavkom studija u tom pravcu, upisujem diplomski studij na Prirodoslovno Matematičkom Fakultetu u Zagrebu, nastavniči smjer.