Radionice klasične kriptografije u osnovnoškolskoj matematici

Bajac, Ana

Sveučilište u Rijeci - Odjel za matematiku

Diplomski sveučilišni studij Matematika i informatika - smjer nastavnički

Ana Bajac

Radionice klasične kriptografije u osnovnoškolskoj matematici

Diplomski rad

Rijeka, rujan 2020.

Sveučilište u Rijeci - Odjel za matematiku

Diplomski sveučilišni studij Matematika i informatika - smjer nastavnički

Ana Bajac

Radionice klasične kriptografije u osnovnoškolskoj matematici

Mentor: doc. dr. sc. Marija Maksimović

Diplomski rad

Rijeka, rujan 2020.

Sadržaj

1 Sažetak

U ovom radu bavit ćemo se klasičnom kriptografijom i njenom primjenom u osnovnoškolskoj matematici. Ideja ovog diplomskog rada je prikazati neke od mogućih radionica u kojima bi na zanimljiv način učenicima približili kriptografiju tajnog ključa. U sklopu ovog diplomskog rada također smo izradili jednu online igricu koja se može pogledati na [6].
Šifre koje smo koristili su: skital, Pigpen, Polybiusov kvadrat, Cezarova šifra, Albertijev disk i Vigenèrova šifra.
Dane metode šifriranja prilagođene su učenicima osnovne škole, te ih je moguće provesti u redovnoj nastavi, dodatnoj nastavi matematike ili kao izvannastavnu aktivnost.

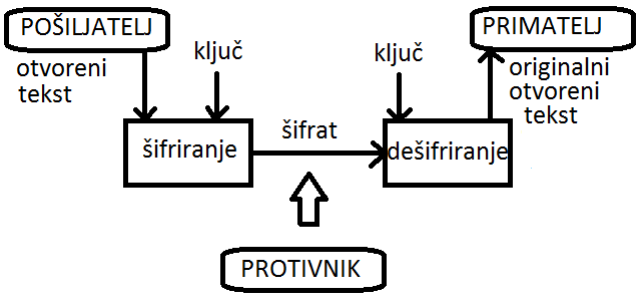
Ključne riječi: kriptografija, šifre, radionice, nastava, matematika

2 Uvod

Kako od davnina tako i danas postoji potreba za pisanje tajnih poruka između dvije strane. Međutim pri prijenosu poruke dolazi do opasnosti presretanja iste od treće strane. Upravo zato došlo je do razvoja kriptografije.
Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u obliku da ih može pročitati samo onaj kome su namijenjene.
U kriptografiji postoje dva razvoja kriptografije: klasično (do pojave interneta) i moderno (od pojave interneta).
Klasična kriptografija kojom ćemo se baviti u radu je bila ta koja je odlučivala o ishodima ratova i brojnih života do polovice prošlog stoljeća kada ju je zamijenila moderna kriptografija na računalima i sustavima.
U ovom radu bavimo se klasičnom kriptografijom i njenom primjenom u osnovnoškolskoj matematici. Naglasak će biti na šiframa: skital, Pigpen, Polybiusov kvadrat, Cezarova, Albertijeva i Vigenèreova šifra.
Danas u vrijeme digitalizacije kada se informacija smatra vrijednom šifriranje i dešifriranje se koriste svakodnevno. Potrebna nam je šifra kojom bismo zaštitili sebe i svoje podatke. Naučimo li učenike koristiti kriptosustave i šifrirati poruke nekom od opisanih šifri, zasigurno će naučeno primijeniti u životu.

3 Osnovno o kriptografiji

Kriptografija je proces prevođenja (kriptiranja, šifriranja) razgovijetnog teksta (jasan, otvoren tekst) u nerazgovijetan tekst (kriptiran tekst, šifrat) kako bi ga jedino osoba koja posjeduje unaprijed određen ključ mogla odgonetnuti (dekriptirati, dešifrirati). Sama riječ kriptografija grčkog je podrijetla i može se prevesti kao tajnopis.
Kriptoanaliza (dekriptiranje) je znanstvena disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa.
Kriptologija je grana znanosti koja obuhvaća i kriptografiju i kriptoanalizu. Dolazi od grčke riječi cryptos što znači tajan (potajan, skriven) i riječi logos što znači smisao (znanost). To je znanost o tajnom sporazumijevanju, odnosno znanost koja se bavi načinima i sredstvima prikrivanja poruka (podataka).
Osobu koja šalje poruke nazvat ćemo **pošiljatelj**, a osobu koja prima poruke **primatelj**, te **protivnik** osobu koja želi otkriti sadržaj njihovih poruka. U Engleskoj literaturi to su redom Alice (pošiljatelj), Bob (primatelj) i Oskar (protivnik).
Poruka koju pošiljatelj želi poslati primatelju nazvat ćemo **otvoren tekst**. Pošiljatelj tu poruku na unaprijed dogovoreni način pomoću određenog ključa šifrira u nerazgovijetan tekst koji nazivamo **šifrat**. Protivnik prisluškujući komunikacijski kanal između pošiljatelja i primatelja može otkriti samo sadržaj šifrata, ali ne i sadržaj otvorenog teksta. Nakon što primatelj dobije šifrat, pomoću određenog ključa dešifrira poruku te ju čita kao otvoren (početni) tekst koji je pošiljatelj uputio primatelju.



Slika 1: Shema kriptosustava

Ako želimo matematički opisati kriptosustav to ćemo učiniti na sljedeći način:

Definicija 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 elemenata otvorenog teksta;*
2. $\mathcal{C}$ *je konačan skup svih mogućih osnovnih elemenata šifrata;*
3. $\mathcal{K}$ *je prostor 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 su* $e_K : \mathcal{P} \to \mathcal{C}$ *i* $d_K : \mathcal{C} \to \mathcal{P}$ *funkcije sa svojstvom da je* $d_K(e_K(x)) = x$ *za svaki otvoreni tekst* $x \in \mathcal{P}$.

Svojstvo $d_K(e_K(x)) = x$ nam kaže da funkcije e_K moraju biti injekcije, te je stoga ono najbitnije jer ako bi za dva različita otvorena teksta x_1 i x_2 vrijedilo:

$$e_K(x_1) = e_K(x_2) = y$$

primalac ne bi mogao odrediti treba li on y dešifrirati u x_1 ili u x_2, odnosno $d_K(y)$ ne bi bio definiran.

3.1 Klasifikacija kriptosustava

Kriptosustave klasificiramo s obzirom na sljedeća tri kriterija:

1. **Tipu operacija koje se koriste pri šifriranju** – supstitucijske šifre i transpozicijske šifre.

   (a) **Supstitucijske šifre** svaki element otvorenog teksta zamijene s nekim drugim elementom. Dijele se na monoalfabetske i polialfabetske.

      i. Kod **monoalfabetskih šifri** svako slovo otvorenog teksta odgovara jedinstvenom slovu šifrata. Tu spada Cezarova šifra.

      ii. **Polialfabetske šifre** su naprednije od monoalfabetskih jer se svako slovo otvorenog teksta može šifrirati u nekoliko različitih slova šifrata. Tu spadaju Albertijeva šifra i Vigenèrova šifra.

   (b) **Transpozicijske šifre** elemente (slova/brojeve) otvorenog teksta ostave nepromijenjenim, samo promjene njihov međusobni položaj u tekstu. Od transpozicijskih šifri najviše se koristi stupčana transpozicija.

2. **Načinu na koji se obrađuje otvoreni tekst** – blokovne šifre i protočne šifre.

3. **Tajnosti i javnosti ključa** – simetrični (konvencionalni) kriptosustavi u kojima se ključ za dešifriranje može izračunati poznavajući ključ za šifriranje i obrnuto (često su ta dva ključa identična) i kriptosustavi s javnim ključem (asimetrični kriptosustavi) u kojima se ključ za dešifriranje ne može izračunati iz ključa za šifriranje. U kriptosustavu s javnim ključem sam naziv kaže da je ključ javan, odnosno

bilo tko može šifrirati poruku pomoću njega, ali samo osoba koja ima odgovarajući ključ za dešifriranje može ju dešifrirati.

U ovom radu bavit ćemo se simetričnim kriptosustavima, odnosno kriptosustavima s tajnim ključem i upoznat ćemo se s nekim transpozicijskim i supstitucijskim šiframa.

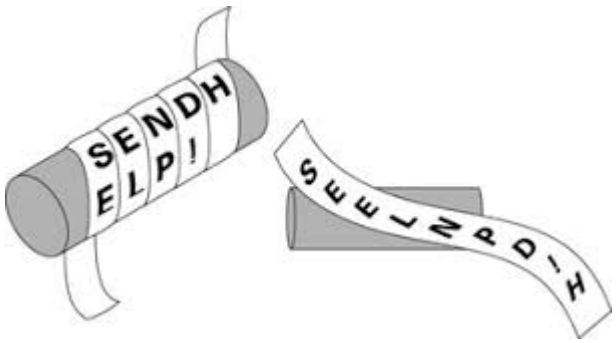
4 Neki kriptosustavi s tajnim ključem

4.1 Transpozicijske šifre

4.1.1 Skital

U petom stoljeću prije Krista kod starih Grka zabilježena je prva upotreba kriptografije u svrhu komuniciranja. Upotrebljavali su napravu za šifriranje zvanu skital. To je drveni štap oko kojeg bi se namotala tanka vrpca od kože ili pergamenta, na koju bi se zatim okomito pisala slova. Kada bi se vrpca odmotala sa štapa, poruka napisana na vrpci bi postala nečitljiva (šifrat). Pročitati bi ju mogla samo ona osoba koja je imala štap istog promjera. Vidimo da je skital primjer transpozicijske šifre.

Primjer 1. *Šifriranje poruke pomoću skitala* (*Slika 2 [8]*).



Slika 2: Skital

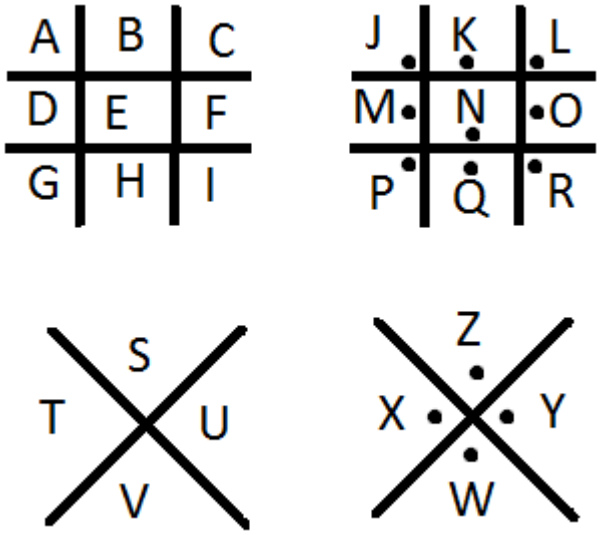
Rješenje: Nakon što smo namotali vrpcu oko štapa na nju pišemo otvoren tekst SEND HELP!. Odmotavajući vrpcu sa štapa dobivamo šifrat SEELNPD!H. Ključ s kojim šifriramo, odnosno dešifriramo poruku je promjer štapa.

4.2 Supstitucijske šifre

Za sve šifre koje ćemo koristiti u nastavku ćemo koristiti engleski alfabet od 26 slova. Ukoliko želimo šifrirati poruku napisanu pomoću hrvatskog alfabeta onda ćemo prvo slova Č, Ć, Đ, DŽ, LJ, NJ Š i Ž zamijeniti redom s C, C, DJ, DZ, LJ, NJ, S i Z i na taj način dobiti poruku napisanu pomoću engleskog alfabeta koju ćemo onda šifrirati.

4.2.1 Pigpen

Pigpen je geometrijska monoalfabetska supstitucijska šifra koja je ime dobila po načinu na koja se slova odvajaju linijama kao svinje u svinjcu. Koristila se od 1500-ih godina, a slobodni zidari koristili su Pigpen u zidarskoj dokumentaciji na masonskim medaljama, potvrdama i nadgrobnim spomenicima, te je stoga poznata i pod nazivom Masonska šifra. Zbog svoje jednostavnosti za šifriranje i dešifriranje Pigpen je bila često korištena.
Da bi šifrirali poruku Pigpen šifrom koristit ćemo se Pigpen tablicom. Tablica se sastoji od rešetka i slova. Svako slovo otvorenog teksta šifriramo tako da slovo zamijenimo crtežom rešetke u kojem se slovo nalazi.
Dešifriramo tako da se u Pigpen tablici pronađe znak u šifratu, te mu se pridruži odgovarajuće slovo.

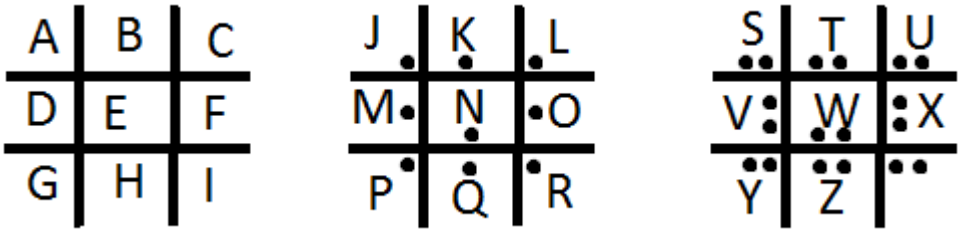


Slika 3: Pigpen tablica

Primjer 2. *Šifrirajmo riječ MATEMATIKA Pigpen šifrom.*
Rješenje: Potražimo u rešetkama slovo M i pogledajmo crtež rešetke u kojem se ono nalazi, vidimo da se slova M preslika u ⊐. *Na isti način je slovu A pridružen znak* ⌟, *a slovu T znak* >. *Ponovimo postupak sa svakim slovom i dobijemo šifrat:*

⊐⌟>□⊐⌟>⌜⊔⌟

Osim prikazanog Pigpena sa 4 rešetke, koristi se i Pigpen sa 3 rešetke koji je prikazan na Slici 4.



Slika 4: Pigpen2 tablica

Primjer 3. *Dešifrirajmo šifrat:*

dobiven pomoću Pigpen2 tablice (Slika 4).

Rješenje: U Pigpen2 tablici pronađemo znak koji dešifriramo. Ako imamo samo jednu točku, promatramo rešetku u sredini ispunjenu slovima J, K, L, M, N, O, P, Q, R. Ako imamo rešetku s dvije točke, pogledati ćemo zadnju (treću) rešetku ispunjenu slovima S, T, U, V, W, X, Y, Z, a ako nema točke, onda u prvu rešetku.
Primjenjujući navedeno vidimo da prvi znak ima jednu točku, pa se nalazi u drugoj rešetki, gledajući obrise zaključujemo da se radi o slovu M. Drugi znak nema točke te se stoga nalazi u prvoj rešetki. Gledajući obrise zaključujemo da se radi o slovu A. Treći znak ima dvije točke te se nalazi u trećoj rešetki, prema obrisima vidimo da se radi o slovu T. Nastavljajući postupak dobivamo riječ MATEMATIKA.

4.2.2 Polybiusov kvadrat

Polybiusov kvadrat je naprava koju su izmislili stari Grci, a proslavio ju je povjesničar i znanstvenk Polybius. To je kvadrat dimenzije 5×5 unutar kojeg su zapisana slova abecede. Budući da mi koristimo slova engleske abecede to znači da će nam jedna ćelija sadržavati dva slova (recimo da su to slova I i J). Redove i stupce označimo brojevima od 1 do 5 te dobijemo sljedeći kvadrat:

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

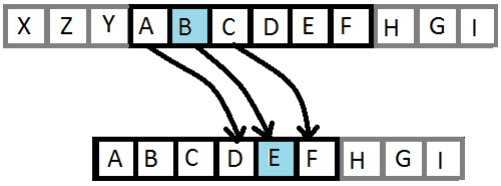
Tablica 1: Polybiusov kvadrat

Šifrira se tako da se slovo koje se nalazi u r-tom retku i s-tom stupcu zamijeni brojem $r \cdot 10 + s$. Npr. slovo B šifriramo s 12, slovo R s 43, itd. Poruke dešifriramo tako da svakom broju $r \cdot 10 + s$ pridružimo slovo koje se nalazi u r-tom retku i s-tom stupcu Polybiusova kvadrata.

Primjer 4. *Šifriraj otvoren tekst MATEMATIKA Polybiusovim kvadratom prikazanim u Tablici 1.*
Rješenje: Slovo M se nalazi u trećem redu i trećem stupcu te ga šifriramo kao 32.
Slovo A se nalazi u prvom redu i prvom stupcu te ga šifriramo kao 11.
Slovo T se nalazi u četvrtom redu i petom stupcu te ga šifriramo kao 44.
Slovo E se nalazi u prvom redu i petom stupcu te ga šifriramo kao 15.
Slovo I se nalazi u drugom redu i četvrtom stupcu te ga šifriramo kao 24.
Slovo K se nalazi u trećem redu i prvom stupcu te ga šifriramo kao 25.
Dobiveni šifrat je: 32 11 44 15 32 11 44 24 25 11.

U Polybiusovom kvadratu ne moramo slova stavljati u abecednom redoslijedu nego ih možemo posložiti nasumično. Isto tako ne moramo šifrirati na način kao što smo prikazali, odnosno da prvo zapisujemo broj retka, a potom broj stupca već možemo prvo zapisati broj stupca, a potom broj retka u kojem se slovo nalazi. Koji god način odabrali, Alice i Bob se moraju usuglasiti kako bi mogli šifrirati, odnosno dešifrirati poruke koje si šalju.

4.2.3 Cezarova šifra



Slika 5: Cezarova šifra

Cezarova šifra dobila je ime po znamenitom rimskom vojskovođi Gaju Juliju Cezaru. U komunikaciji sa svojim prijateljima koristio se šifrom u kojoj je slovo otvorenog teksta zamjenio slovom koje je za tri mjesta udesno dalje od njega u alfabetu (A $\rightarrow$ D, B$\rightarrow$ E, C$\rightarrow$ F, itd.). Da bi svako slovo abecede mogli zamijeniti slovom koje je za tri mjesta udaljeno od njega (pomak za 3) moramo pretpostaviti da se alfabet ciklički nastavlja, odnosno nakon slova Z, ponovno idu slova A, B, C. To nam omogućava preslikavanje slova X, Y i Z u slova A, B i C, itd.
Općenito se Cezarovom šifrom smatra svaka šifra istog oblika za bilo koji pomak, a ako je pomak tri onda se radi o originalnoj Cezarovoj šifri.

Prije nego što matematički opišemo Cezarovu šifru uvest ćemo podudarnost između slova engleskog alfabeta i brojeva iz skupa $\{0, 1, 2, \cdots, 25\}$.
To radimo na način prikazan u Tablici 2.

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

Tablica 2: Numerički ekvivalenti slova engleskog jezika

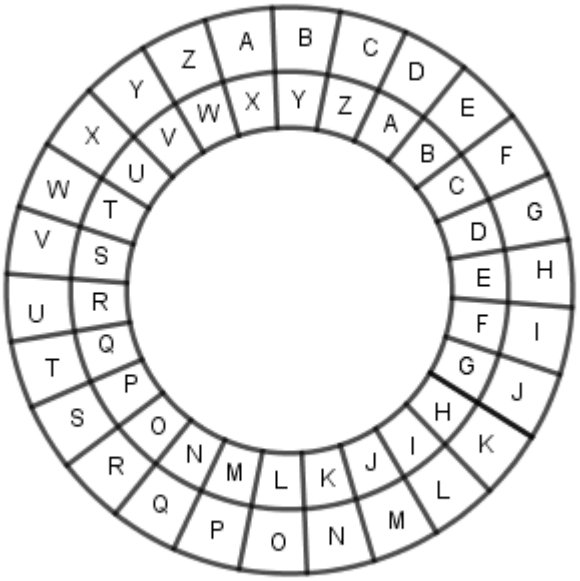
Definiramo skup $\mathbb{Z}_{26} = \{0, 1, 2, \cdots, 25\}$ te pretpostavimo da su na tom skupu definirane operacije zbrajanja, oduzimanja i množenja na isti način kao i na skupu cijelih brojeva. Ako broj koji je rezultat operacije nije iz navedenog skupa $\{0, 1, 2, \cdots, 25\}$, broj se zamijeni s njegovim ostatkom pri dijeljenju s 26.
Oznaka koju ćemo koristiti za zbrajanje je $a +_{26} b$ ili $(a + b) \bmod 26$. Analogno će biti oznake za oduzimanje i množenje.
Skup $\mathbb{Z}_{26}$ s navedenim operacijama $+_{26}$, i $\cdot_{26}$ čini prsten.
Na potpuno analogan način možemo definirati skup $\mathbb{Z}_r$ i operacije na njemu za neki prirodan broj r.
Sada, Cezarovu šifru možemo definirati pomoću matematičkih formula na sljedeći način.

Definicija 2. *Neka je* $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$. *Za* $0 \leq K \leq 25$ *definiramo funkciju šifriranja* $e_K(x) = (x + K) \bmod 26$ *i dešifriranja* $d_K(y) = (y - K) \bmod 26$.

Ukoliko bismo koristili hrvatsku abecedu, kriptosustav bismo definirali na skupu $\mathbb{Z}_{30}$.
Umjesto korištenja matematičkih formula za šifriranje i dešifriranje Cezarovom šifrom možemo koristiti Cezarov disk.

4.2.4 Cezarov disk

Radi jednostavnosti šifriranja i dešifriranja koristio se Cezarov disk (Slika 6). Cezarov disk se sastoji od dva kruga, vanjskog i unutarnjeg na kojima su ispisana slova iste abecede. Vanjski krug je onaj na kojem tražimo elemente otvorenog teksta, a unutarnji onaj na kojem tražimo elemente šifrata.



Slika 6: Cezarov disk

Šifriranje pomoću Cezarovog diska za pomak K se radi u sljedećim koracima:

1. Namjestimo krugove tako da se slova na unutarnjem i vanjskom krugu podudaraju.
2. Vanjski krug pomaknemo za K mjesta udesno, gdje je K odgovarajući ključ.
3. Pronađemo slovo otvorenog teksta u vanjskom krugu, te ga zamijenimo slovom koje se nalazi ispod njega u unutarnjem krugu.

Ako pak poruku želimo dešifrirati to možemo učiniti na sljedeći način:

1. Namjestimo krugove tako da se slova na unutarnjem i vanjskom krugu podudaraju.
2. Vanjski krug pomaknemo za K mjesta udesno, gdje je K odgovarajući ključ.
3. Pronađemo slovo šifrata u unutarnjem krugu, te ga zamijenimo slovom koje se nalazi iznad njega u vanjskom krugu.

Možemo pogledati kako šifriranje otvorenog teksta originalnom Cezarovom šifrom izgleda na primjeru.

Primjer 5. *Šifrirajmo otvorent tekst MATEMATIKA originalnom Cezarovom šifrom.*
Rješenje: I. način
Budući da se koristi originalna Cezarova šifra u kojoj je ključ K jednak 3 prilikom šifriranja otvorenog teksta koristit će se formula $e_3(x) = (x+3) \ mod\ 26$.
Pogledamo li u Tablicu 2, numerički ekvivalenti slova riječi MATEMATIKA su

$$12\ 0\ 19\ 4\ 12\ 0\ 19\ 8\ 10\ 0.$$

Koristeći funkciju e_K šifriramo odabrano slovo uzimajući u obzir da je ključ $K = 3$.
Dobivamo:

$$\begin{aligned}
e_3(12) &= (12+3)\ mod\ 26 = 15\ mod\ 26;\\
e_3(0) &= (0+3)\ mod\ 26 = 3\ mod\ 26;\\
e_3(19) &= (19+3)\ mod\ 26 = 22\ mod\ 26;\\
e_3(4) &= (4+3) mod\ 26 = 7\ mod\ 26;\\
e_3(0) &= (0+3) mod\ 26 = 3\ mod\ 26;\\
e_3(12) &= (12+3)\ mod\ 26 = 15\ mod\ 26;\\
e_3(19) &= (19+3)\ mod\ 26 = 22\ mod\ 26;\\
e_3(8) &= (8+3)\ mod\ 26 = 11\ mod\ 26;\\
e_3(10) &= (10+3)\ mod\ 26 = 13\ mod\ 26;\\
e_3(0) &= (0+3)\ mod\ 26 = 3\ mod\ 26.
\end{aligned}$$

Dakle, dobili smo da su numerički ekvivalenti slova šifrata 15 3 22 7 15 3 22 11 13 3, *odnosno pomoću Tablice 2 vidimo da je šifrat PDWHPDWLND.*

II. način
Zadatak smo mogli riješiti pomoću Cezarovog diska. Namjestimo

Cezarov disk tako da se slovo A vanjskog kruga nalazi iznad slova X unutarnjeg kruga (Slika 6). Potražimo slovo M na vanjskom krugu i zamijenimo ga slovom unutarnjeg kruga, tj. sa slovom P. Postupak se nastavlja do kraja i dobije se šifrat PDWHP-DWLND.

Nakon što Bob dobije poruku šifriranu Cezarovom šifrom s ključem K, on mora dešifrirati poruku koristeći Cezarovu šifru s pomakom $-K$.

Sljedeći primjer će pokazati kako će Bob dešifrirati primljeni šifrat.

Primjer 6. *Dešifrirajmo šifrat TVEZEG ako znamo da je šifriran Cezarovom šifrom s ključem $K = 4$.*
Rješenje: Prvo potražimo numeričke ekvivalente slova šifrata u Tablici 2. Dobivamo 19 21 4 25 4 6.
Budući da moramo dešifrirati poruku koristit ćemo funkciju $d_K(y) = (y - K) \ mod\ 26$.
U ovom primjeru tekst je šifriran Cezarovom šifrom s ključem 4. Uvrštavajući numeričke ekvivalente u danu formulu dobivamo:

$$\begin{aligned} d_3(19) &= (19-4) \ mod\ 26 = 15 \ mod\ 26; \\ d_3(21) &= (21-4) \ mod\ 26 = 17 \ mod\ 26; \\ d_3(4) &= (4-4) \ mod\ 26 = 0 \ mod\ 26; \\ d_3(25) &= (25-4) \ mod\ 26 = 21 \ mod\ 26; \\ d_3(4) &= (4-4) \ mod\ 26 = 0 \ mod\ 26; \\ d_3(6) &= (6-4) \ mod\ 26 = 2 \ mod\ 26. \end{aligned}$$

Pogledamo li ostatke pri dijeljenju s brojem 26*, dobivamo* 15 17 0 21 0 2*, odnosno koristeći Tablicu 2, vidimo da se radi o otvorenom tekstu PRAVAC.*

4.2.5 Kriptoanaliza supstitucijskih šifara

U ovom poglavlju ćemo opisati dvije metode kojima možemo razbiti supstitucijsku šifru. To su metoda grube sile i metoda analize frekvencije slova.

4.2.6 Metoda grube sile

Ova metoda temelji se na ispitivanju svih mogućih ključeva dok se ne dobije neki smisleni otvoreni tekst.
Budući da je mali broj ključeva ova metoda razbijanja Cezarove šifre je opravdana. Ako Oskar ne zna ključ, a zna da se poruka šifrirala Cezarovom šifrom, probat će svaki od preostalih 25 ključeva ($K \in \{1, 2, \cdots, 25\}$) i naposljetku dobiti originalnu poruku.

Primjer 7. *Dešifrirajmo šifrat PDWHPDWLND dobiven Cezarovom šifrom pomoću metode grube sile.*
Rješenje: Svako slovo šifrata zamijenit ćemo slovom koje se nalazi za jedno mjesto ulijevo od njega. Postupak nastavljamo sve dok ne dobijemo neki smisleni tekst.

0	P	D	W	H	P	D	W	L	N	D
1	O	C	V	G	O	C	V	K	M	C
2	N	B	U	F	N	B	U	J	L	B
3	M	A	T	E	M	A	T	I	K	A

Primjenjujući navedeni postupak nakon treće iteracije dobili smo smisleni tekst MATEMATIKA iz čega slijedi da je ključ 3.

4.2.7 Metoda analize frekvencije slova

Umjesto da smo šifrirali Cezarovom šifrom s pomakom K kao funkciju šifriranja mogli smo odabrati bilo koju permutaciju slova.
Tada bi imali 26! mogućih ključeva pa bi napad ispitivanja svih mogućih ključeva "grubom silom" bio teško izvediv.
Koristeći statistička svojstva jezika pomoću kojeg je pisan otvoren tekst moguće je dešifrirati supstitucijske šifre.
Ta metoda naziva se metoda analize frekvencije slova.
Metoda analize frekvencije slova mjeri pojavljivanje svakog slova u šifratu, a zatim se distribucija slova u šifrata uspoređuje s poznatim podacima o distribuciji slova u jeziku kojim je pisan otvoren tekst. U tom slučaju će vjerojatno najfrekventnija slova šifrata odgovarati najfrekventnijim slovima jezika kojim je pisan otvoren tekst. Vjerojatnost će biti veća što je šifrat dulji.

Hrvatski		Engleski	
A	115	E	127
I	98	T	91
O	90	A	82
E	84	O	75
N	66	I	70
S	56	N	67
R	54	S	63
J	51	H	61
T	48	R	60
U	43	D	43
D	37	L	40
K	36	C	28
V	35	U	28
L	33	M	24
M	31	W	23
P	29	F	22
C	28	G	20
Z	23	Y	20
G	16	P	19
B	15	B	15
H	8	V	10
F	3	K	8
		J	2
		Q	1
		X	1
		Z	1

Tablica 3: Najfrekventnija slova hrvatskog i engleskog jezika (u promilima)

Primjer 8. *Dešifrirajmo šifrat PDWHPDWLND dobiven Cezarovom šifrom pomoću metode analize frekvencije slova.*
Rješenje: Pogledajmo koje se slovo najviše puta pojavljuje u šifratu i pretpostavimo da je to slovo slika slova koje se najviše pojavljuje u hrvatskom jeziku, slova A. Vidimo da je to slovo D. Zaključujemo da se slovo A preslikalo u slovo D, odnosno da je traženi ključ $K = 3$. *Primijenimo li ga u funkciji za dešifriranje dobit ćemo otvoren tekst MATEMATIKA.*

4.2.8 Albertijev disk

Slika 7: Albertijev disk

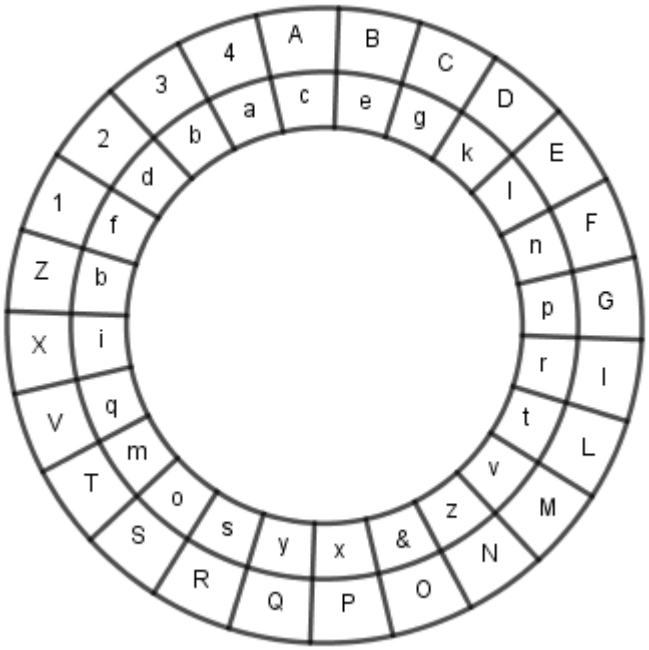
Leone Battista Alberti (1404. – 1472.) je zbog svog doprinosa u kriptografiji, dobio titulu "oca zapadne kriptografije". Izumio je šifru koju je nazvao "dostojna kraljeva" za koju je govorio da se ne može probiti. To je šifrirajući disk koji je danas poznat kao Albertijev disk (Slika 7 [4]).
Albertijev disk se sastojao od dva bakrena kruga, jednog vanjskog statičnog i drugog manjeg (unutarnjeg) pomičnog. Prednje strane diskova podijeljene su na 24 jednaka dijela (polja). Na gornjem su napisana slova engleske abecede bez H, J, K, U, W, Y te su još zapisani brojevi 1,2,3,4, a na unutarnjem disku ispisana su 24 slova latinske abecede.

Budući da otvoreni tekst pišemo slovima engleske abecede u dogovoru ćemo slova koja nedostaju pisati na sljedeći način:

Slovo koje nedostaje	H	J	K	U	W	Y
Zapis slova koje nedostaje	FF	II	QQ	VV	XX	ZZ

Tablica 4: Supstitucija slova koja nedostaju u Albertijevu disku

Da bi Alice i Bob mogli komunicirati trebali bi imati iste Albertijeve diskove, te dogovoreno indeksno slovo u pomičnom krugu s kojim će šifrirati odnosno dešifrirati poruke. Alice određuje kojim će slovom ili brojem velikog kruga upariti dogovoreno indeksno slovo. Nakon toga Alice potraži slova otvorenog teksta na vanjskom krugu te ih zamijeni malim slovima koja se nalaze ispod njih u unutarnjem krugu. Alice tijekom šifriranja može mijenjati slovo ili broj vanjskog kruga koje upari s indeksnim. To može učiniti na proizvoljnim mjestima.
Pogledat ćemo to na primjeru.



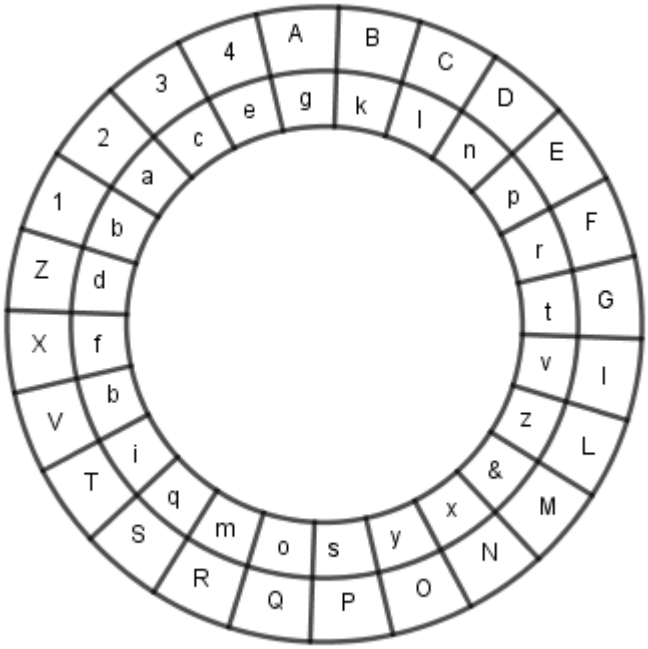
Slika 8: Albertijev disk

Primjer 9. *Šifrirajmo otvoreni tekst MATEMATIKA JE ZAKON primjenom Albertijevog diska.*
Rješenje:

1. *KORAK: Slova J, K se ne nalaze na gornjem disku. Potrebno ih je zamijeniti slovima kao što piše u tablici 4. Slovo J zamijenjujemo slovima II, a slovo K slovima QQ.*
   Otvoreni tekst sada glasi: MATEMATIQQA IIE ZAQQON.

2. *KORAK: Neka nam je dogovoreno da je c indeksno slovo. Slovo A vanjskog kruga namjestimo iznad indeksnog slova c koje se nalazi u unutarnjem krugu (Slika 8).*
   Prva riječ otvorenog teksta se tada šifrira na sljedeći način: prvo zapišemo veliko slovo (A) koje se preslikava u indeksno, a potom slova otvorenog teksta potražimo na vanjskom

krugu i zamijenimo ih slovima koja se nalaze ispod njih u unutarnjem krugu.
Vidimo da se slovo M iz vanjskog kruga preslika u slovo s unutarnjeg kruga, slovo T u slovo d, odnosno dobijemo da se otvoreni tekst MATEMATIKA šifrira u Avcmlvcmryyc.



Slika 9: Albertijev disk

3. KORAK: Indeksno slovo c ćemo upariti s brojem 3. Nakon što ispod broja 3 vanjskog kruga namjestimo slovo c iz unutarnjeg kruga šifrirat ćemo riječ IIEZAQQON na analogan način kao što smo riječ MATEMATIKA. Šifriranjem otvorenog teksta (Slika 9) dobivamo da se IIEZAQQON šifrira u 3vvpdgooyx.
Konačno, dobivena šifra je : Avcmlvcmryyc3vvpdgooyx.

Obrnuto, želimo li dešifrirati šifrat dobiven pomoću Albertijevog diska uparit ćemo odgovarajuće indeksno slovo sa odgovarajućim znakom koji se nalazi u šifratu i potom potražiti mala slova na unutarnjem disku i zamijeniti ih slovima iznad njih u vanjskom disku.

4.2.9 Vigenèrova šifra

Vigenèreova šifra je za razliku od Cezarove šifre primjer polialfabetske supstitucijske šifre. To je jedna od najpoznatijih šifri u povijesti te je ime dobila po francuskom diplomatu Blaise-u de Vigenère-u koji je 1586. godine objavio knjigu "Traicte de Chiffres". Knjiga je sadržavala sve što se do tada znalo o kriptografiji, ali gotovo ništa o kriptoanalizi, te je unutar nje opisano više originalnih polialfabetskih sustava.
Vigenèreovu šifru definiramo na sljedeći način:

Definicija 3. *Neka je m fiksan prirodan broj. Definiramo $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^m$. Za ključ $K = (k_1, k_2, \cdots, k_m)$, definiramo*

$$e_k(x_1, x_2, \cdots, x_m) = (x_1 +_{26} k_1, x_2 +_{26} k_2, \cdots, x_m +_{26} k_m),$$
$$d_k(y_1, y_2, \cdots, y_m) = (y_1 -_{26} k_1, y_2 -_{26} k_2, \cdots, y_m -_{26} k_m).$$

Definicija 3 nam kaže da slova otvorenog teksta pomičemo za k_1, k_2, $\cdots$ ili k_m mjesta ovisno o tome gdje se ona u otvorenom tekstu nalaze. Šifriranje otvorenog teksta provodimo slovo po slovo stoga nije nužno nadopuniti zadnji blok ukoliko broj slova u otvorenom tekstu nije djeljiv s duljinom ključa.

Primjer 10. *Neka je $m = 5$ i ključna riječ $K = (S, L, O, V, A)$. Vigenèrovom šifrom šifrirajmo otvoren tekst MATEMATIKA.*

Rješenje: Šifriranje se provodi na sljedeći način:

1. *Podijelimo slova otvorenog teksta u blokove u ovisnosti o ključu.*
2. *Pronađimo numeričke ekvivalente od slova ključne riječi i slova pripadnog otvorenog teksta.*
3. *Zbrojimo modulo 26.*
4. *Pronađemo šifrat.*

1.	Ključ	S	L	O	V	A	S	L	O	V	A
	Otvoreni tekst	M	A	T	E	M	A	T	I	K	A
2.	Ključ	18	11	14	21	0	18	11	14	21	0
	Otvoren tekst	12	0	19	4	12	0	19	8	10	0
3.	$+_{26}$	4	11	7	25	12	18	4	22	5	0
4.	Šifrat	E	L	H	Z	M	S	E	W	F	A

Šifrat je ELHZMSEWFA.

4.2.10 Vigenèrov kvadrat

Za jednostavniju primjenu možemo koristiti Vigenèrov kvadrat (Slika 10 [9]). Vigenèrov kvadrat ili Vigenèrova tablica sastoji se od 26 redova i stupaca. U svakom redu je napisan alfabet, s tim da u svakom novom redu se početno slovo rotira ulijevo u odnosu na prethodno početno slovo alfabeta.
Prvo se ispiše otvoren tekst i ključ ispod njega tako da svako slovo otvorenog teksta ima odgovarajuće slovo ključa. Slova otvorenog teksta pronalazimo u prvom stupcu tablice, a slova ključne riječi u prvom redu tablice (Slika 11). Slovo šifrata pronalazimo u presjeku stupca slova otvorenog teksta i reda njemu pripadnog slova ključne riječi.

	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 10: Vigenèrov kvadrat

Primjer 11. *Šifriraj otvoreni tekst MATEMATIKA Vigenèreovim kvadratom s ključnom riječi SLOVA.*
Rješenje:

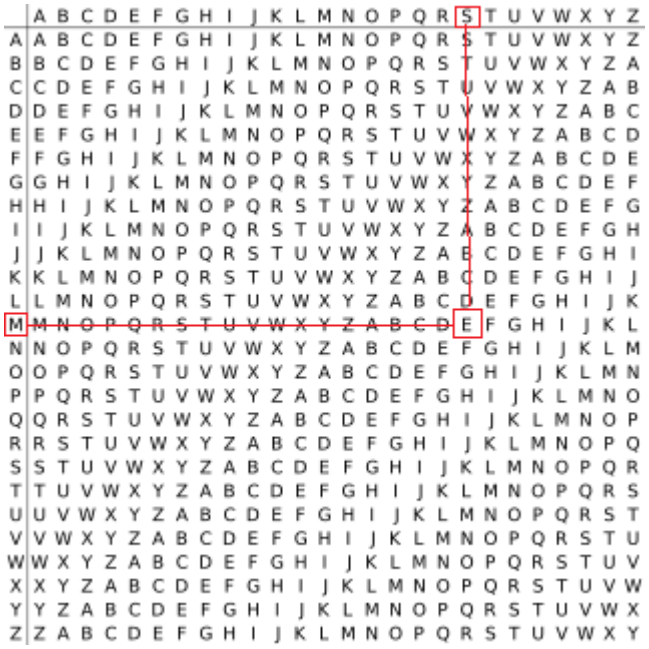
1. *Kao što je bilo opisano svakom slovu otvorenog teksta pridružimo određeno slovo ključa.*

Otvoren tekst	M	A	T	E	M	A	T	I	K	A
Ključ	S	L	O	V	A	S	L	O	V	A

2. *U prvom stupcu potražimo slovo otvorenog teksta, a u prvom retku slovo ključne riječi kojim ga šifriramo, potom u presjeku odabranog stupca i retka pronađemo slovo šifrata.*

Konkretno, slovo M otvorenog teksta pronađemo u prvom stupcu, a slovo S u prvom retku. Vidimo da se u presjeku odabranog retka i stupca nalazi slovo E. Ono je šifrat slova M (Slika 11).

3. *Nastavljajući postupak dobivamo šifrat ELHZMSEWFA.*



Slika 11: Vigenèrov kvadrat

4.2.11 Playfairova šifra

Playfairova šifra je polialfabetska šifra koju je dizajnirao britanski znanstvenik Charles Wheatsone 1854 godine. Ime Playfair dobila je po britanskom barunu Playfairu koji ju je popularizirao.
To je bigramska šifra, odnosno njome se šifriraju parovi slova. Tekst dijelimo u bigrame (parove slova), a u slučaju da se u

bigramu pojave dva identična slova odvojimo ih drugim slovom (najčešće slovom X ili Z), a ako otvoren tekst ima neparan broj slova na kraj dodamo slovo X ili Z.

Tekst šifriramo pomoću matrice koju konstruiramo na sljedeći način:

1. Ukoliko Alice i Bob nemaju unaprijed dogovorenu ključnu riječ koriste 5×5 matricu sljedećeg izgleda:

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

Tablica 5: Playfairova šifra bez ključne riječi

2. Ukoliko Alice i Bob imaju unaprijed dogovorenu ključnu riječ u 5×5 matricu upisuju redom slova ključne riječi bez ponavljanja i nakon toga preostala slova abecede.
   Na primjer, ako je ključna riječ RAVNALO matrica će biti oblika:

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

Tablica 6: Playfairova šifra s ključnom riječi MATEMATIKA

Otvoren tekst šifriramo tako da ga prvo podijelimo u parove slova pazeći da se niti jedan blok ne sastoji od dva jednaka slova.

Prilikom šifriranja bloka bigrama mogu se dogoditi sljedeća tri slučaja:

1. Slova se nalaze u istom redu − zamjenjujemo ih slovima koja se nalaze za jedno mjesto udesno. To radimo ciklički, odnosno najdesnije slovo ćemo zamijeniti najlijevijim slovom toga retka.

2. Slova se nalaze u istom stupcu − zamijenimo ih slovima koja se nalaze za jedno mjesto ispod u stupcu. Najdonje slovo u stupcu zamijenit ćemo s prvim slovom iz tog stupca.

3. Ukoliko slova nisu iz istog retka ili stupca pogledati ćemo pravokutnik koji određuju, te ih zamijeniti s preostala dva vrha tog pravokutnika tako da prvo dođe slovo koje se nalazi u istom retku kao i prvo slovo u bigramu koji šifriramo.

Primjer 12. *Šifrirajmo otvoreni tekst MATEMATIKA Playfairovom šifrom bez ključa (Tablica 5).*
Rješenje: Prvo otvoreni tekst rastavimo na bigrame i dobijemo:

MA TE MA TI KA

Bigram MA sastavljen je od slova M i slova A koja se ne nalaze u istom retku, niti istom stupcu već tvore pravokutnik. Slovo M se preslikava u slovo L, a slovo A u slovo B. Bigrame TE i KA šifriramo na isti način kao i bigram MA. Bigram TI se sastoji od slova T i I koja se nalaze u istom stupcu pa se ona preslikaju u prvo slovo ispod njega, odnosno u bigram YO.

Nastavljajući postupak dobivamo da je šifrat riječi MATEMATIKA Playfairovom šifrom bez ključa LBUDLBYOFE.

Primjer 13. *Šifrirajmo otvoreni tekst MATEMATIKA Playfairovom šifrom s ključem CIKLUS.*

Rješenje: Prvo je potrebno napraviti matricu pomoću kojeg ćemo šifrirati dani otvoren tekst. Prvo ispisujemo slova ključne riječi, a zatim preostala slova alfabeta. Matrica će izgledati ovako:

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

Tablica 7: Playfairova šifra s ključnom riječi CIKLUS

Zatim slova otvorenog teksta podijelimo u bigrame:

MA TE MA TI KA

Promotrimo prvi bigram MA i primijetimo da slova M i A tvore pravokutnik s vrhovima A, D, M, G. Slovo G se nalazi u istom retku kao slovo M pa bigram MA zamijenimo GD. Slova bigrama TE nalaze se u istom stupcu pa njih zamjenjujemo slovima koja se nalaze ispod njih u tom stupcu odnosno bigramom ZN.

Nastavljajući postupak dobivamo bigrame šifrata:

GD ZN GD PU IB

Odnosno šifrat je GDZNGDPUIB.

Ova šifra u odnosu na supstitucijsku je sigurnija iz razloga što bigramsko šifriranje smanjuje broj elemenata dostupnih za analizu frekvencije. Osim tih razloga je i broj bigrama veći od broja individualnih slova. Playfairova šifra je upravo zbog tih razloga dugo smatrana sigurnom.

Dešifriranje Playfairovom šifrom provodi se obrnutim postupkom.

1. Slova koja se nalaze u istom retku zamijenit će se slovima koja se nalaze za jedno mjesto ulijevo pri čemu uzimamo u obzir da se slova u redcima ciklički ponavljaju.
2. Slova koja se nalaze u istom stupcu zamijenit će se slovima koja se nalaze za jedno mjesto iznad pri čemu uzimamo u obzir da se slova u stupcima ciklički ponavljaju.
3. Inače pogledamo pravokutnik koja ta dva slova sačinjavaju te ih zamijenimo s preostala dva vrha tog pravokutnika pri čemu prvo dodamo slovo koje se nalazi u retku kao i polazno slovo bigrama koje dešifriramo.

5 Kriptografija u školi

Iako nije implementirana u nastavi matematike u školama, kriptografiju možemo predstaviti djeci u obliku radionica na otvorenom danu škole, danu kruha i ostalim danima koji su predviđeni za radionice i predah od klasične nastave. Osim toga možemo na zanimljiv način obraditi sate ponavljanja za pisane provjere.
Možemo ju predstaviti kroz igru istražitelja ili špijuna, potrage za blagom ili izgubljenog broda. Prikazat ćemo neke od mogućih radionica. One će se sastojati od nekih zadataka primjerenih danom uzrastu. Naravno nije nužno radionicu koristiti u razredu za koji je pripremljena, ali tada će se morati konstruirati novi set pitanja ovisno o gradivu koji se želi pokriti.

5.1 Radionica: Potraga za blagom

Trajanje: 70 minuta

Razred: 5. razred

Potrebno predznanje: djeljivost prirodnih brojeva (djelitelji, višekratnici)

Predmetna korelacija: matematika, engleski

Ključni pojmovi: kriptografija, Cezarova šifra, Cezarov disk, Pigpen, Playfairova šifra

Učenici će moći:

- Razvijati svoje komunikacijske i socijalne vještine
- Unaprijediti vještinu rada u grupi
- Usvojiti vještine dešifriranja Cezarovim diskom i Pigpenom

Potreban materijal: Prilog 7.1, Cezarov disk, olovka, brisalo

Tijek aktivnosti:
Na stolu se nalaze radni listići, Cezarov disk, olovka i brisalo. Oko svakog stola nalazi se 5 stolica kako bi se već na samom početku formirale grupe do 5 učenika.
Učenike se na početku upozna s osnovnim pojmovima: Kriptografija, otvoren tekst, šifrat, šifriranje i dešifriranje. Zatim im se pokaže šifriranje i dešifriranje pomoću Cezarovog diska i PigPen

tablice.
Nakon što su se upoznali s potrebnim kriptosustavima učenici uzimaju radni listić 7.1 i krenu ga rješavati.
Nakon što jedna od grupa riješi ispravno radni listić igra je gotova.
Napomena: Rješenje radnog listića nalazi se u Prilogu 7.2.

5.2 Radionica: Tajni dokument

Trajanje: 60 min

Razred: 7. Razred

Potrebno predznanje: Mnogokuti (dijagonale mnogokuta, kutovi mnogokuta)

Predmetna korelacija: matematika, engleski

Ključni pojmovi: kriptografija, Cezarova šifra, skital, Vigenèrova šifra, Polybiusov kvadrat

Učenici će moći:

- Razvijati svoje komunikacijske i socijalne vještine
- Unaprijediti vještinu rada u grupi
- Usvojiti vještine dešifriranja i šifriranja različitim napravama

Potrebni materijal: Prilog 7.3, Cezarov disk, Vigenèreov kvadrat, Polybiusov kvadrat, štapovi, olovka, brisalo

Tijek aktivnosti:
Učenici se podijele u grupe od 4 člana. Na stolu se nalaze radni listić Tajni dokument, Vigenèreov kvadrat, Polybiusov kvadrat, drveni štap.
Učenike se na početku upozna s osnovnim pojmovima: Kriptografija, otvoren tekst, šifrat, šifriranje i dešifriranje. Zatim im se pokaže šifriranje i dešifriranje pomoću skitala, Cezarovog diska

te Vigenèrovog i Polybiusovog kvadrata.
Nakon što se učenicima objasni primjena pripadnih naprava za šifriranje, počinju s rješavanjem radnog listića.
Nakon što jedna od grupa riješi ispravno radni listić igra je gotova.
Napomena: Rješenje radnog listića nalazi se u Prilogu 7.4.

5.3 Radionica: Zumići

Trajanje: 45 min

Razred: 5. Razred

Potrebno predznanje: Pravokutnik i kvadrat

Predmetna korelacija: matematika

Ključni pojmovi: kriptografija, Polybiusov kvadrat, Playfairova šifra

Učenici će moći:

- Razvijati svoje komunikacijske i socijalne vještine
- Usvojiti vještine dešifriranja i šifriranja različitim napravama

Potreban materijal: Prilog 7.5, žetoni cvijeta

Tijek aktivnosti:

Učenike se na početku upozna s osnovnim pojmovima: Kriptografija, otvoren tekst, šifrat, šifriranje i dešifriranje. Zatim im se pokaže šifriranje i dešifriranje pomoću Playfairove šifre i Polybiusovog kvadrata te ih se podijeli u grupe od 4 člana.
Nakon što su učenici podijeljeni u grupe podijele im se nastavni listić sa pitanjima. Svakim točnim odgovorom pojedina grupa dobiva po jedan žeton cvijeta.
Pobjednička grupa je ona s najviše žetona.
Napomena: Rješenje radnog listića nalazi se u Prilogu 7.6.

5.4 Escape Room

Trajanje: 90 min

Razred: 8. Razred

Potrebno predznanje: Geometrijska tijela

Predmetna korelacija: matematika, informatika

Ključni pojmovi: kriptografija, Cezarova šifra, Pigpen, Vigenèrova šifra, Polybiusov kvadrat

Učenici će moći:

- Razvijati svoje komunikacijske i socijalne vještine
- Unaprijediti vještinu rada na računalu
- Usvojiti vještine dešifriranja i šifriranja različitim napravama

Potreban materijal: Računalo

Tijek aktivnosti:

Danas je sve više popularan EscapeRoom s različitim tematikama i za različite uzraste.
Program koji sam odabrala za izradu EscapeRoom-a je dinamički programski jezik za djecu Scratch!.
U igrici [6] je potrebno šifrirati i dešifrati zagonetke kako bi pomogli vitezu spasiti princezu Katarinu koja je zatočena u kuli kralja Goblina.
Učenike je potrebno upoznati s pravilima igranja te upoznati sa

kriptosustavima koji se koriste u igrici: Cezarova šifra, Pigpen, Polybiusov kvadrat, Vigenèreov kvadrat.
Napomena: Rješenje i objašnjenje igrice nalazi se u Prilogu 7.7.

6 Zaključak

U ovom radu bavili smo se klasičnom kriptografijom, odnosno supstitucijskim i transpozicijskim šiframa i njihovom primjenom u osnovnoškolskoj matematici kroz radionice. Radionice nastale kao sati ponavljanja za nastavne jedinice "Višekratnici", "Konstrukcija kutova" ili kao ponavljanje nastavne cjeline "Mnogokuti" za pisanu provjeru znanja samo su neki od prikaza mogućih radionica.

Dane radionice mogu se koristiti i u drugim razredima jedino je potrebno osmisliti druga pitanja ovisno o nastavnoj jedinici koju se želi pokriti.

Dali smo i primjer online igrice o kriptografiji za djecu osnovnoškolskog uzrasta. Ekonomična je jer ne iziskuje stalno printanje materijala, lagana je za pohranu i može se jednostavno koristiti.

Popis tablica

Popis slika

Literatura

[1] *Alberti Cipher Disk*, Venetian Cryptography, Dostupno na: https://vcrypto.tonyo.info/venetian_crypto/website/index.php/alberti, Zadnji pristup 30.09.2020.

[2] Barun, M., Dujella, A., Franušić, Z., *Kriptografija u školi*, Dostupno na: https://web.math.pmf.unizg.hr/~fran/clanci/kripto-poucak4.pdf. Zadnji pristup 30.09.2020.

[3] *Cipherwheel*, Inventwithpython. Dostupno na: http://inventwithpython.com/cipherwheel/. Zadnji pristup 30.09.2020.

[4] *Alberti cipher disk powerful encryption from 15th century*, Creative Crafthouse. Dostupno na: https://www.creativecrafthouse.com/alberti-cipher-disk-powerful-encryption-from-15th-century.html. Zadnji pristup 30.09.2020.

[5] Dujella, A.: *Kriptografija*, online skripta kolegija Kriptografija. Dostupno na: https://web.math.pmf.unizg.hr/~duje/kript.html. Zadnji pristup 30.09.2020.

[6] *Escaperoom igrica*, Scratch program, Dostupno na: https://scratch.mit.edu/projects/421150182/fullscreen/. Zadnji pristup 30.09.2020.

[7] *Pigpen*, Boxentriq, Dostupno na: https://www.boxentriq.com/code-breaking/pigpen-cipher. Zadnji pristup 30.09.2020.

[8] *Skytale*, Prairie Creek Makers. Dostupno na: https://prairiecreek.typepad.com/makers/2019/03/skytale.html. Zadnji pristup 30.09.2020.

[9] *Vigenère Square*, Commons Wikimedia. Dostupno na: https://commons.wikimedia.org/wiki/File:Vigen%C3%A8re_square_shading.svg. Zadnji pristup 30.09.2020.

7 Prilog

7.1 Prilog 1

Radni listić 1

Potraga za blagom

U vašoj učionici nalazi se skriveno blago. Da biste otkrili gdje se nalazi riješite ovaj radni listić.

Ime grupe: _____

1. Dešifriraj šifrat YLVHNUDWQLNRGRVDP dobiven originalno Cezarovom šifrom.

Rješenje:

---

2. Dešifriraj šifrat QBZQ dobiven Cezarovom šifrom s pomakom 8.

Rješenje:

---

3. Dešifriraj šifrat VIRUIVRQHIRMLVQKSQ dobiven Cezarovom šifrom s pomakom 8.
Rješenje:

---

4. Spoji odgovore redom dobivene u zadacima 3, 1 i 2.
Rješenje:

---

5. Riješi zadatak postavljen u rješenju prethodnog zadatka.
Rješenje:

---

6. Dešifriraj šifrat: 
dobiven standardnom PigPen šifrom.
Rješenje:

---

7. Riješi zadatak postavljen u rješenju prethodnog zadatka:
Rješenje:

---

8. Dešifriraj šifrat PQNESNUWJYNSFHPTONOJXFXYFASNINVWFISTLXYTQF dobiven Cezarovom šifrom s pomakom 5.
Rješenje:

---

9. Riješi zadatak postavljen u rješenju prethodnog zadatka.
Rješenje:

---

10. Dešifriraj šifrat XIZIVJZWRQHUMLRCBZQQXMB dobiven Cezarovom šifrom s pomakom 8.
Rješenje:

---

11. Riješi zadatak postavljen u rješenju prethodnog zadatka:
Rješenje:

---

12. Dešifriraj šifrat SRJOHGDMSURCRU dobiven originalnom Cezarovom šifrom.
Rješenje:

---

13. Dešifriraj šifrat QDMYHFLCDMHGQLFNLGMHOL WHOM dobiven originalnom Cezarovom šifrom.
Rješenje:

---

14. Spoji odgovore redom dobivene u zadacima 13, 11 i 5.
Rješenje:

---

15. Riješi zadatak postavljen u rješenju prethodnog zadatka.
Rješenje:

---

16. Blago se nalazi u (spoji odgovore redom dobivene u zadacima 12, 15, 9 i 7).
Rješenje:

---

17. Konačno rješenje:

7.2 Prilog 2

Rješenje radnog listića 1:

1. VISEKRATNIK OD OSAM

2. I TRI

3. NAJMANJI ZAJEDNICKI

4. NAJMANJI ZAJEDNICKI VISEKRATNIK OD OSAM

I TRI

5. 24

6. NIJE LIIJEVO NEGO

7. DESNO

8. KLIZNI PRETINAC KOJI JE SASTAVNI DIO

RADNOG STOLA

9. LADICA

10. PARAN BROJ IZMEDJU TRI I PET

11. ČETIRI

12. POGLEDAJ PROZOR

13. NAJVECI ZAJEDNICKI DJELITELJ

14. NAJVECI ZAJEDNICKI DJELITELJ OD CETIRI I

DVADESET I CETIRI

15. 4

16. POGLEDAJ PROZOR CETVRTA LADICA DESNO

17. BLAGO SE NALAZI U ČETVRTOJ LADICI DESNO PORED PROZORA

7.3 Prilog 3

Radni listić 2

Tajni dokument
Pomozite agentici Riti da riješi tajne zadatake.

Ime grupe:_____

1. Dešifrirajte šifrat 4525453511331242342414242411223433113111145111331115434415423425454411 dobiven standardnim Polybiusovim kvadratom.
Rješenje:

---

2. Riješi zadatak postavljen u rješenju prethodnog zadatka.
Rješenje:

---

3. Dešifriraj šifrat EOSNIFVSNHMNEKSREPEMDNIHRSKZVLEWIHEQOSNMNIXSQRSKSOYX dobiven Cezarovom šifrom s pomakom 4.
Rješenje:

---

4. Riješi zadatak postavljen u rješenju prethodnog zadatka.
Rješenje:

---

5. Koliki je zbroj unutarnjih kutova dvanaesterokuta? *Rješenje:*

---

6. Šifriraj rješenje prethodnog zadatka Vigenèrovom šifrom s ključnom riječi LIST.
Rješenje:

---

7. Skitalom pošaljite Riti poruku o rješenjima.

7.4 Prilog 4

Rješenja zadataka s radnog listića 2:

1. UKUPAN BROJ DIJAGONALA DVANAESTEROKUTA

2. 54

3. AKO JE BROJ DIJAGONALA IZ JEDNOG VRHA

SEDAM KOJI JE TO MNOGOKUT

4. DESETEROKUT

5. TISUCU OSAMSTO

6. EQKNNC GLLUKMZ

7.5 Prilog 5

Radni listić 3.

1. Dešifriraj šifrat 34354315223542115134254544332425 11 dobiven Polybiusovim kvadratom.
Rješenje:

---

2. Dešifriraj šifrat 11241535154433111543441224 15444224 dobiven Polybiusovim kvadratom.
Rješenje:

---

3. Spoji rješenja dobivena u 1. i . zadatku.
Rješenje:

---

4. Riješi zadatak postavljen u rješenju prethodnog zadatka.
Rješenje:

---

5. Šifriraj rješenje prethodnog zadatka Playfairovom šifrom s ključnom riječi MATEMATIKA.
Rješenje:

---

6. Dešifriraj šifrat 3534514243243311255111144211441 1 dobiven Polybiusovim kvadratom.
Rješenje:

---

7. Dešifriraj šifrat 1445312424331543444211332413114442241 4154315442434431132 dobiven Polybiusovim kvadratom.
Rješenje:

---

8. Spoji rješenja dobivena u 6. i 7. zadatku.
Rješenje:

---

9. Riješi zadatak postavljen u rješenju prethodnog zadatka.
Rješenje:

---

10. Šifriraj rješenje 9. zadatka Playfairovom šifrom s ključnom riječi MATEMATIKA.
Rješenje:

7.6 Prilog 6

Rješenja zadataka s radnog listića no.3:

1. OPSEG PRAVOKUTNIKA

2. A JE PETNAEST B JE TRI

3. OPSEG PRAVOKUTNIKA A JE PETNAEST B JE TRI

4. TRIDESER I SEST

5. CX EF DY IE EU DY CT

6. POVRSINA KVADRATA

7. DULJINE STRANICA TRIDESET I OSAM

8. POVRSINA KVADRATA DULJINE STRANICA TRIDESET I OSAM

9. TISUCU CETRISTO CETRDESET I CETIRI

10. EM UP FR DT CX EU IL DT CX ND YD EM DT EM UT

7.7 Prilog 7

Rješenja Escape rooma:

Soba broj 1 i broj 2 daju upute za igru.

SOBA BROJ 3

Nakon što kliknemo na Sliku 1 postavljenu u hodniku postavlja se pitanje "Tko je lik na slici?".
Odgovor je GAJ JULIJE CEZAR.
U sobi se nalaze i bubnjevi. Nakon što kliknemo na njih prikaže se šifrirana poruka "YLVLQD SHWQDHVW; SROXPMHU WULQDHVW".
Pauci koji se kreću po sobi simboliziraju ključ kojim su se šifrirale poruke.
Nakon što dešifriramo šifrat dobiven originalnom Cezarovom šifrom prikazuje se poruka:

"VISINA PETNAEST, POLUMJER TRINAEST".

Kliknemo li na strelicu pojaviti će se poruka: "RGUHGL REXMDP EXEQMD", dešifriranjem dobivamo *"ODREDI OBUJAM BUBNJA".*
Obujam bubnja je jednak 2535π. U uvodu je rečeno da se rezultat piše bez znaka π, odnosno upisuje se broj 2535. Nakon što ga upišemo prelazimo u sljedeću sobu.

SOBA BROJ 4

U knjižnici vidimo razne predmete. Jedan od njih su naočale. Nakon što ih kliknemo dobivamo poruku "Vigenère je bio sjajan kriptograf!".

Poruka nas upućuje da se ovdje raditi o Vigenèrovoj šifri.

Kliknemo li na olovku pojavit će se poruka: "ŠIFRIRAJ ME OBLIM GEOMETRIJSKIM TIJELOM IZ STAKLENKE".

U staklenci se nalaze geometrijska tijela. Oblo geometrijsko tijelo u staklenci je kugla.

Dakle, riječ KUGLA će biti ključna riječ kojom ćemo šifrirati otvoreni tekst OLOVKA.

Dobit ćemo šifrat:

YFUHKK.

Nakon što šifrat upišemo na odgovarajuće mjesto prelazimo u sljedeću sobu.

SOBA BROJ 5

Na monitoru računala je prikazan Polybiusov kvadrat s kojim šifriramo i dešifriramo poruke.

Poruka na papiru je:

41422422551144124224225511322324154255111311544114343211414225425511

i dešifriranjem dobivamo:

V JEDNAKO JEDNA TRECINA BAZA PUTA VISINA

Kliknemo li na prozor pojavljuje se druga poruka: 2542312311321253122233124112234212441242245332424224513425242311224 2?

Dešifriramo li ju dobivamo tekst:

SIFRATOM ODGOVORI O KOJEM TIJELU SE RADI?

Odgovor je STOZCU, te nakon što ga šifriramo Polybiusovim kvadratom dobijemo šifrat:

253212541534.

Upišemo li dobiveni šifrat na predviđeno mjesto, ulazimo u sljedeću sobu.

SOBA BROJ 6
Prikazana je farma svinja te ona simbolizira da se radi o Pigpen šifri.
Nakon što kliknemo na stog sijena pojavi se poruka:

napisana PigPen šifrom. Dešifriramo li ju dobivamo tekst:

ODREDI OBUJAM STOGA SIJENA

Štap u stogu ima oznaku 4, odnosno visina stoga je 4. Vodoravni štap ispred stoga ima oznaku 3, odnosno ima duljinu 3 pa imamo sve potrebne elemente za odrediti obujam stožca (stoga).

$$h = 4$$
$$r = \frac{3}{2}$$
$$V = \frac{1}{3} \cdot r^2\pi \cdot h$$

$$V = \frac{1}{3} \cdot \frac{9}{4} \cdot \pi \cdot 4$$
$$V = 3\pi$$

Uvrštavajući poznate vrijednosti u formula za obujam stošca dobivamo 3π, odnosno na predviđeno mjesto upisujemo 3. Nakon što to upišemo prelazimo u sobu u kojoj je zatočena princeza, odnosno dolazimo do kraja igrice.