Sveučilište Josipa Jurja Strossmayera u Osijeku

Odjel za matematiku

Jelena Macanić

Kriptografija u školi

Diplomski rad

Osijek, 2012.

Sveučilište Josipa Jurja Strossmayera u Osijeku

Odjel za matematiku

Jelena Macanić

Kriptografija u školi

Diplomski rad

Mentor: doc. dr. sc. Ivan Matić

Osijek, 2012.

Sadržaj

Uvod

Kriptografija ima veliki potencijal kojim može obogatiti nastavu matematike. Može joj dati uzbudljivost, dramatičnost, dinamičnost, a kod učenika pobuditi znatiželju i kreativnost. Upravo to tako često nedostaje nastavi matematike u kojoj se sve servira "zdravo za gotovo". Stoga, učenici nerijetko dobivaju dojam da se u matematici više ništa novoga ne može otkriti (za razliku od nekih drugih predmeta npr. geografija, povijest, itd. gdje im znatiželju pobuđuju otvorena pitanja poput onog "Koliko je velik svemir?" ili "Zašto su izumrli dinosauri?")
Mnogi primjeri iz kriptografije mogu nam poslužiti da odagnamo uvriježene ukorijenjene stereotipe kao npr. onaj da je svaki matematički problem rješiv pomoću prave formule ili dobrog računala. Naime, sigurnost kriptosustava leži upravo u našoj nemogućnosti da brzo i efikasno riješimo odgovarajući problem iz područja algebre, teorije brojeva ili kombinatorike.

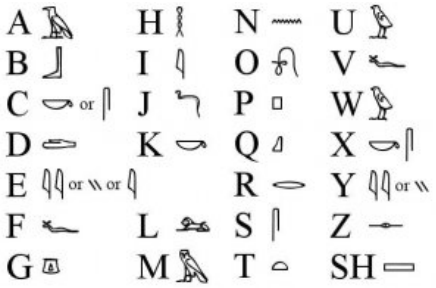
U ovom radu bit će predstavljene osnovne i zanimljive metode za šifriranje i dešifriranje određenih poruka. Metode su prilagođene mogućnostima učenika da shvate postupke šifriranja i dešifriranja i samostalno ih primjene na konkretnim primjerima. To bi moglo omogućiti učenicima da osjete snagu i ljepotu matematike.

Važno je spomenuti da se danas smatra da je informacija najvrijednije dobro. Upravo zbog toga je šifriranje i razbijanje šifri postalo najvažniji izvor tajnih obavještajnih službi na svijetu. No, razbijanje i stvaranje šifri postoji od davnina, pa u povijesti kriptografije razlikujemo dva velika razdoblja. Današnje razdoblje kriptografije naziva se *moderna kriptografija*, dok se razdoblje do pojave interneta naziva *klasična kriptografija*. Upravo je klasična kriptografija odlučivala o ishodima brojnih života i ratova do polovice prošlog stoljeća.

Poglavlje 1

Kratka povijest klasične kriptografije

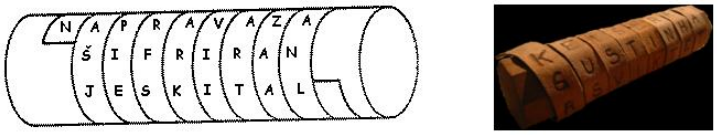
Počeci kriptografije datiraju još iz davne 2000. godine prije Krista. Tada su se pojavili hijeroglifi kojima su stari Egipćani ukrašavali grobnice. Hijeroglifi su male sličice koje obilježavaju stvari ili pojave. Zbog toga, ovaj sustav zamjene nije bio sustav tajnog pisma u današnjem smislu riječi, nego je to bio neusavršen kôd za zamjenu znakova.



Slika 1.1. *Hijeroglifi*

Početkom ratova javlja se sve veća potreba za skrivanjem poruka. Najraniji zapisi sežu iz doba Herodota koji daje kroniku sukoba Grčke i Perzije u 5. stoljeću prije Krista. U kronici je zabilježena upotreba drvenih pločica na koje se napisala poruka i koje su se potom prekrile voskom. Taj je događaj obilježio početak *steganografije, grč. steganos - pokriven, graphein - pisati* tj. proces tajnog komuniciranja pri kojem se skriva i samo postojanje poruke.
Kroz povijest, ljudi su bili prilično domišljati u skrivanju poruka. Tako su neki vojskovođe znali obrijati glasniku glavu i na nju napisati poruku, te su nakon toga pričekali da kosa naraste i poslali glasnika na odredište. Nadalje, Kinezi su poruke pisali na tankoj svili, koju bi zgužvali u kuglicu i natopili voskom, te progutali. Još jedan od načina skrivanja poruke je upotreba nevidljive tinte iz raznih biljaka ili organskih tekućina ("mlijeko" biljke mlječike), koje promjene svoju boju pri njegovom zagrijavanju (posmeđe). Slično se ponašaju i mnoge druge organske tekućine, i to zato što su bogate ugljikom pa lako

izlučuju čađu. Sve ove metode bile su jako opasne jer ih se moglo lako otkriti. Zbog toga se, uz steganografiju počinje razvijati i *kriptografija, grč. kryptos - skriven, graphein - pisati.* Cilj kriptografije nije zatajiti postojanje poruke, već prikriti njezino značenje, i to pomoću procesa zvanog *enkripcija*, odnosno *šifriranje ili kodiranje.* Da bi poruka postala nerazumljiva, slova se u njoj ispremeću po nekom određenom pravilu, unaprijed dogovorenom između pošiljatelja i primatelja. Tako primatelj može to pravilo preokrenuti, pa mu poruka postaje razumljiva.
Prednost je kriptografije što neprijatelj ne može razabrati sadržaj čak ni uhvaćene poruke. Bez poznavanja tog pravila miješanja, neprijatelj će teško ili nikako iz šifriranog teksta moći izvući poruku.
Prva upotreba kriptografije zabilježena je 400. godine prije Krista kod Spartanaca. Oni su upotrebljavali drveni štap na kojeg su namotali traku od pergamenta, te na nju okomito napisali poruku. Kada bi se traka odmotala, poruka na njoj postala bi nečitljiv skup znakova, a pročitati bi je mogao samo onaj koji je posjedovao štap odgovarajućeg promjera. Nakon odmotavanja, na vrpci se nalazio anagram otvorene poruke. Prva naprava za šifriranje koja koristi transpoziciju naziva se *skytale - skital.*



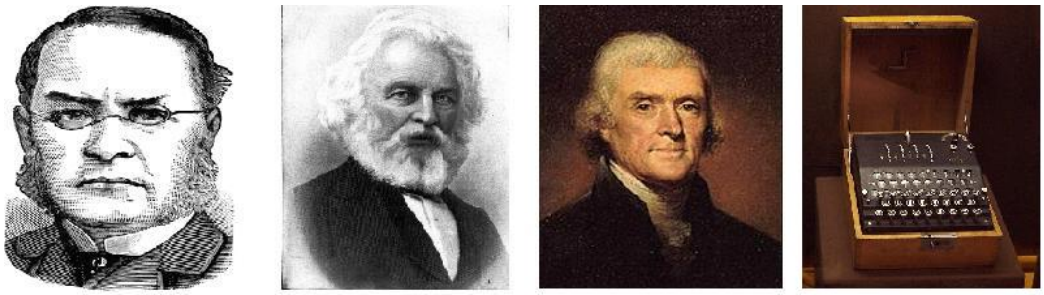
Slika 1.2. *Skital*

Supstitucija se prvi puta pojavljuje kod Hebrejaca, koji mijenjaju slova otvorenog teksta nekim drugim slovima. Najvažnija metoda supstitucije je *Cezarova šifra* koju je koristio sam Cezar u Galskom ratu. Ove šifre su monoalfabetske supstitucijske šifre jer se prilikom kriptiranja koristi samo jedna šifrirana abeceda. Mnogi su stari učenjaci smatrali da se supstitucijska šifra ne može razbiti zbog velikog broja mogućih ključeva. No, počinje razvoj kriptoanalize na istoku zahvaljujući velikom procvatu znanosti, naročito matematike, gramatike, lingvistike i statistike. Arapi su bili prvi koji su opisali tehniku kriptoanalize kojom se mogla razbiti svaka monoalfabetska supstitucijska šifra.
Razbijanjem monoalfabetskih šifri, dolazi do razvoja kriptografije na zapadu. Počinju se primjenjivati monoalfabetske šifre s praznim znakovima i kodiranje. Time se otežao posao kriptoanalitičarima, ali je ponovno postojala opasnost jer je prije komuniciranja bilo potrebno drugoj strani poslati *nomenklator.*
Nomenklator je enkripcijski sustav sastavljen od šifrirane abecede kojom se prenosi većina poruke, te ograničenog broja kodnih riječi. Zato se javlja potreba za boljim šiframa, pa nastaju polialfabetske supstitucijske šifre. Četiri su čovjeka obilježila ovo razdoblje kriptografije.
Prvi je bio *Alberti* koji je predložio da se prilikom kriptiranja koriste dvije šifrirane abecede. Na njegovo se razmišljanje nastavio *Trithemius* koji je po prvi puta uveo

tablicu koja je postala osnovni oblik polialfabetske supstitucije. Treći važan korak napravio je *Belaso* koji je prvi preporučio upotrebu nekog ključa, koji bi se lako pamtio. Služio je za određivanje koju abecedu treba koristiti. Problem je nastao jer je u ovom slučaju ključ trajan kroz cijelu poruku pa ju je također dosta lako razbiti. Zato je *Vigenère* uveo autoključ, ključ koji je ovisio o samoj poruci. Vigenèrova šifra bila je u širokoj upotrebi tijekom američkog rata za nezavisnost, a korištena je i u Američkom građanskom ratu.
Služila je gotovo dva i pol stoljeća. Prvi ju je razbio *Babbage* 1854. godine. No, njegovo otkriće ostalo je nezapaženo. *Kasiski* 1863. godine objavljuje svoju metodu za razbijanje navedene šifre, poznatu kao *Kasiskijeva metoda*, a 1920. godine *Friedman* iznosi drugu metodu za razbijanje ove šifre koja koristi tzv. *indeks koincidencije*.

Slika 1.2. *Alberti, Trithemius, Vigenère, Babbage*

Druga ideja za poboljšanje monoalfabetske supstitucije je uvođenje blokova slova kao osnovnih elemenata otvorenog teksta. Najpoznatija šifra koja se zasniva na tom načelu je *Playfairova šifra*. Ovu šifru osmislio je *Wheatstone* 1854. godine, a ime je dobila po njegovom prijatelju *Playfairu* koji ju je popularizirao. Korištena je u britanskoj vojsci za vrijeme 1. svjetskog rata i u američkoj vojsci za vrijeme 2. svjetskog rata. U međuvremenu, započinje razvoj kriptografskih strojeva. Prvi značajan stroj za šifriranje konstruirao je *Jefferson* 1795. godine. Važno je spomenuti, da je jedan od najmoćnijih kriptografskih strojeva bila Enigma.



Slika 1.3. *Playfair, Wadsworth, Jefferson, Enigma*

Poglavlje 2

Pojmovi iz kriptografije

Kriptologija je znanost koja obuhvaća kriptografiju i kriptoanalizu. Ona koristi znanja matematike, statistike i lingvistike za kriptiranje i dekriptiranje poruka. Postoje dvije vrste poruka (tekstova): *otvoreni, izvorni, čisti* tekst i *šifrirani* tekst.
Izvorna, nešifrirana poruka, pisana je otvorenom abecedom i naziva se *otvoreni tekst*. Poruka koja nastaje nakon šifriranja, pisana je šifriranom abecedom i naziva se *šifrirani tekst*. U pravilu se otvorena abeceda i otvoreni tekst pišu malim slovima, dok se šifrirani tekst i abeceda pišu velikim tiskanim slovima. Primjer jednog takvog zapisa možemo pogledati na sljedećoj slici. (Slika 2.1.)

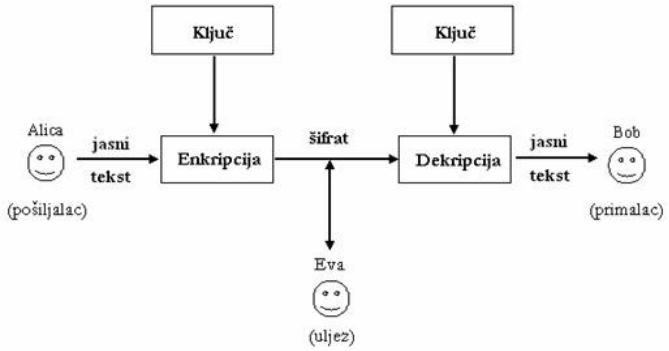
Otvorena abeceda:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Šifrirana abeceda:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Slika 2.1. *Otvorena i šifrirana abeceda*

2.1. Kriptografija

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u oblicima čitljivim samo onima kojima su i namijenjene. Sama riječ kriptografija je grčkog podrijetla i mogla bi se doslovno prevesti kao *tajnopis*.
Cilj kriptografije je omogućiti nesmetano komuniciranje osobe A (pošiljalac) i osobe B (primalac) preko nesigurnog komunikacijskog kanala tako da treća osoba C (protivnik) ne može razumijeti njihove poruke. (U kriptografskoj literaturi su za pošiljaoca i primaoca rezervirana imena Alice i Bob, dok se protivnik najčešće zove Eva ili Oskar).
Poruku koju osoba A želi poslati osobi B nazivamo *otvoreni tekst, engl. plaintext*. Osoba A, najprije transformira, tj. šifrira otvoreni tekst koristeći se unaprijed dogovorenim *ključem* i tako dobiva *šifrat ili kriptogram*. Zatim ga šalje nesigurnim komunikacijskim kanalom (računalne mreže, telefonske linije). U tom je trenutku šifrirana poruka - šifrat

dostupna osobi C, no ona je ne može dešifrirati jer ne posjeduje ključ. Konačno, šifrat stiže osobi B koja ga pomoću ključa dešifrira i dobiva otvoreni tekst.
Model komunikacije između pošiljatelja i primatelja prikazan je sljedećom slikom.



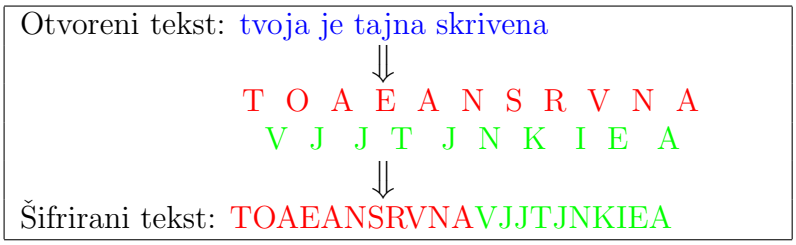
Slika 2.2. *Shema klasične kriptografije*

Kriptografski algoritam ili šifra je matematička funkcija koja se koristi za šifriranje i dešifriranje. Općenito, radi se o dvije funkcije, jednoj za šifriranje, a drugoj za dešifriranje. Te funkcije preslikavaju osnovne elemente otvorenog teksta (najčešće su to slova, bitovi, grupe slova ili bitova) u osnovne elemente šifrata i obratno. Funkcije se biraju iz određene familije funkcija u ovisnosti o ključu. Skup svih mogućih vrijednosti ključeva nazivamo *prostor ključeva*.

2.1.1. Enkripcija

Enkripcija je postupak koji se primjenjuje na strani pošiljatelja. Njome se otvoreni tekst pretvara u šifrirani ili kodirani tekst pomoću odgovarajućeg ključa. Zbog toga se enkripcija dijeli na *šifriranje* i *kodiranje*.
Kod *šifriranja*, bazična jedinica je jedno slovo, par slova (bigram), a ponekad i više slova (poligram), a kod *kodiranja*, bazična jedinica je riječ ili skup riječi.
Zbog toga, ne postoji neka oštra teorijska granica između kodova i šifri. Zašto? Povećanjem šifarskih sustava, oni vrlo lako prijeđu u kodne sustave.
Šifriranje je postupak koji se dijeli na *transpoziciju* i *supstituciju*.

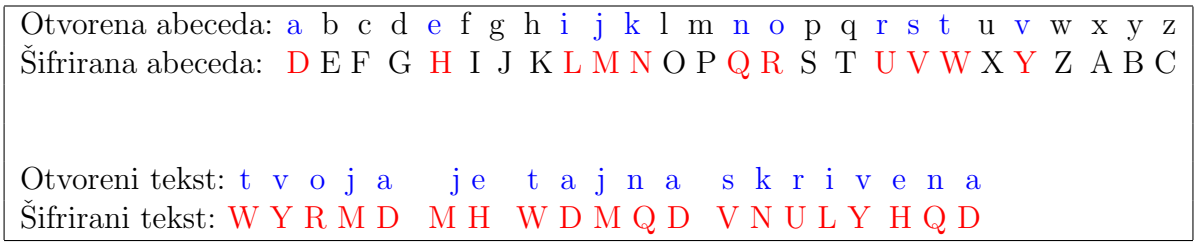
Transpozicija je premještanje slova otvorenog teksta tako da svako slovo zadržava svoj identitet, ali mijenja mjesto. Ovim postupkom dobiva se anagram. Složenost anagrama ovisi o samoj duljini izvorne poruke. Ako je poruka prekratka, onda je moguće doći do izvorne poruke isprobavanjem svih mogućih kombinacija rasporeda slova u šifriranoj poruci. Ako je poruka preduga, anagrami postaju složeniji zbog broja mogućih kombinacija rasporeda slova u poruci. Pokažimo na sljedećem primjeru kako funkcionira transpozicija.



Slika 2.3. *Transpozicija*

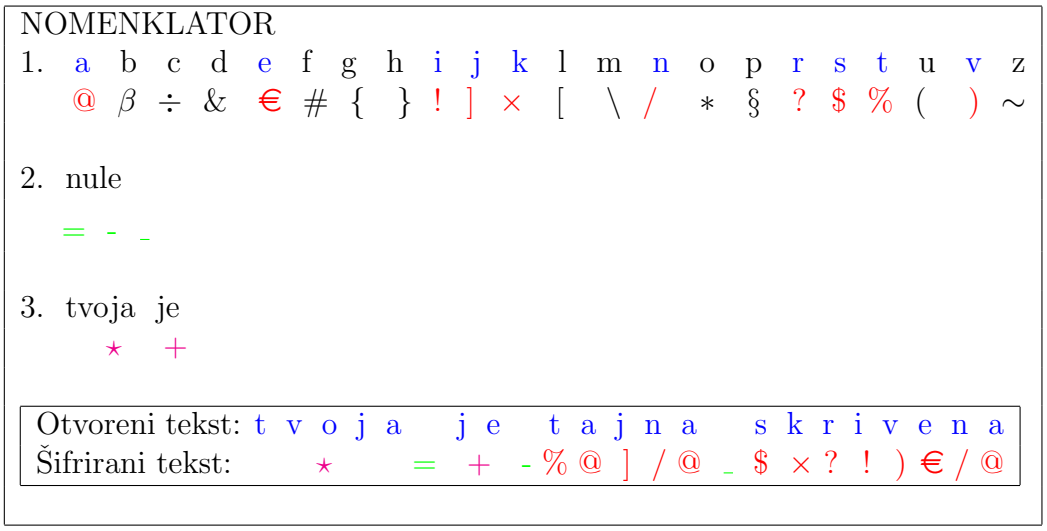
Supstitucija je postupak zamjene slova otvorenog teksta na način da svako slovo zadržava svoje mjesto, ali mijenja svoj identitet. U ovom se postupku, slovo iz poruke prvo pronađe u otvorenoj abecedi te se zamijeni s njemu ekvivalentnim slovom u šifriranoj abecedi. Također, često se upotrebljavaju i znakovi koji ne zamijenjuju niti jedno slovo otvorenog teksta. Pošiljatelj i primatelj će znati da te znakove trebaju preskočiti, dok će trećoj osobi ti znakovi predstavljati problem. Takvi znakovi, koji služe za zavaravanje protivnika i ne znače ništa, nazivaju se nule.

Sustavi koji koriste samo jednu šifriranu abecedu nazivaju se *monoalfabetski sustavi*. Postoje i *polialfabetski sustavi* koji koriste više šifriranih abeceda i oni su znatno kompliciraniji od do sada spomenutih sustava. Sljedeća slika prikazuje primjer jednog postupka supstitucije. Kako bi učenicima što jasnije predočili sve što smo do sada naveli, koristit ćemo se raznim bojama kako bi postupak bio što jednostavniji. Primjer sadrži jednu otvorenu i jednu šifriranu abecedu. Potrebno je zadani otvoreni tekst postupkom supstitucije prevesti u šifrirani tekst.



Slika 2.4. *Supstitucija*

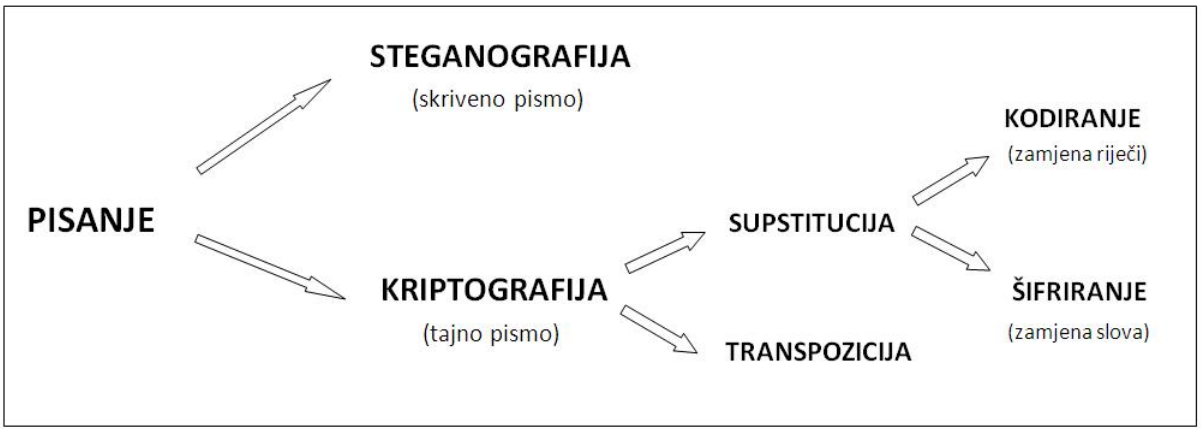
Kodiranje je supstitucija lingvističkih cjelina nekim znakom ili skupom znakova. Ovakav način pretvorbe otvorenog teksta u šifrirani tekst zahtjeva popis svih upotrebljenih zamjena u nekom tekstu. Taj popis svih mogućih zamjena naziva se *kodna lista* ili *nomenklator*. Sljedeća slika prikazuje jedan način kodiranja pomoću nomenklatora. Također, korištene su razne boje kako bi se učenicima zornije prikazao opisani postupak. Primjer sadrži otvoreni tekst kojeg je potrebno kodirati uz pomoć nomenklatora.



Slika 2.5. *Kodiranje*

2.1.2. Dekripcija

Dekripcija je postupak kojim se šifrirani ili kodirani tekst pretvara u otvoreni tekst pomoću unaprijed poznatog ključa i algoritma. Primjenjuje se na strani primatelja poruke. Dakle, ovaj postupak je legalan, jer primatelj komunicira sa pošiljateljem. Samim postupkom nastaje *dekriptat*.
Dekriptat se dijeli na *dešifrat* i *dekodat*, ovisno o tome dekriptira li se šifrirani ili kodirani tekst.
Konačno, sve do sada navedene podjele prikazane su sljedećom slikom.



Slika 2.6. *Glavne podjele*

2.2. Kriptoanaliza

Kriptoanaliza je znanost koja koristi matematiku, statistiku i lingvistiku za dekriptiranje podataka bez unaprijed poznatog ključa. Ona omogućuje nekoj trećoj osobi razbijanje nepoznate poruke, pa je samim time nelegalna.
Ovisno o tome s čime raspolaže treća osoba, razlikujemo četiri osnovna nivoa kriptoanalitičkih napada.

1. **Napad s poznatim šifriranim tekstom**
   Kriptoanalitičar može posjedovati samo šifrirani tekst od nekoliko poruka enkriptiranih pomoću istog algoritma. U ovom slučaju, njegov je zadatak otkriti otvoreni tekst od više poruka ili u najboljem slučaju otkriti ključ kojim se vršila enkripcija.

2. **Napad s poznatim otvorenim tekstom**
   Kriptoanalitičar može posjedovati šifrirani tekst neke poruke, ali i njemu odgovarajući otvoreni tekst. U ovom slučaju, njegov je zadatak otkriti ključ ili neki algoritam kojim je pošiljatelj napravio enkripciju, odnosno primatelj dekripciju.

3. **Napad s odabranim kriptiranim tekstom**
   Kriptoanalitičar može odabrati tekst koji će biti enkriptiran i tako dobiti šifrirani tekst. Ovaj napad je jači od prethodnog napada, ali je manje realističan.

4. **Napad s odabranim otvorenim tekstom**
   Kriptoanalitičar može imati pristup alatu za dekripciju pa može odabrati neki šifrirani tekst i dobiti odgovarajući otvoreni tekst. U ovom slučaju, njegov je zadatak otkriti ključ kojim se vrši enkripcija, odnosno dekripcija.

2.3. Kriptosustav

Kriptosustav se sastoji od kriptografskog algoritma ili šifre, te svih mogućih otvorenih tekstova, šifrata i ključeva. Formalna definicija kriptosustava glasi:

Definicija 2.1 *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, 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 su $e_k \colon \mathcal{P} \to \mathcal{C}$ i $d_k \colon \mathcal{C} \to \mathcal{P}$ funkcije sa svojstvom da je $d_k(e_k(x)) = x$ za svaki otvoreni tekst $x \in \mathcal{P}$.*

Kriptosustave obično klasificiramo obzirom na sljedeća tri kriterija:

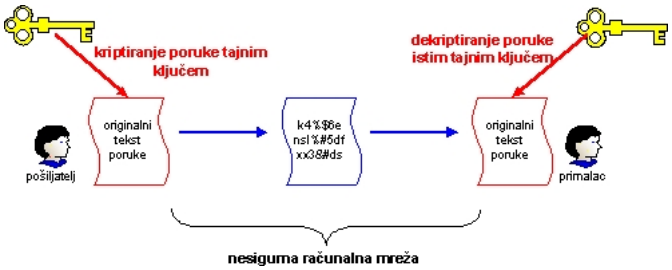
1. **Tip operacija koji se koristi pri šifriranju**
   Imamo podjelu na:
   a) *supstitucijske šifre*
   b) *transpozicijske šifre* (opisane na početku)

2. **Način na koji se obrađuje otvoreni tekst**
   Imamo podjelu na:
   a) *blokovne šifre* - obrađuje se jedan po jedan blok elemenata otvorenog teksta koristeći jedan te isti ključ
   b) *protočne šifre* - elementi otvorenog teksta obrađuju se jedan po jedan koristeći pri tome niz ključeva *engl. keystream* koji se paralelno generira

3. **Tajnost i javnost ključeva**
   Osnovna podjela je na:
   a) *kriptosustave s tajnim ključem*
   b) *kriptosustave s javnim ključem*

Kriptosustavi s tajnim ključem

Kod *simetričnih, konvencionalnih kriptosustava* tj. kriptosustava s tajnim ključem, pošiljatelj i primatelj trajno izabiru ključ K pomoću kojeg generiraju funkcije e_K za šifriranje i d_K za dešifriranje. U ovom slučaju je d_K isti kao i e_K ili se iz njega može jednostavno izračunati. Iz tog razloga, sigurnost simetričnih kriptosustava leži u tajnosti ključa, što i predstavlja veliki nedostatak, jer pošiljatelj i primatelj prije šifriranja moraju biti u mogućnosti da razmjene tajni ključ preko nekog sigurnog komunikacijskog kanala, pomoću kurira ili se osobno sresti. To je nekada teško izvedivo, naročito ako su oni na velikoj udaljenosti i ako su komunikacijski kanali koji su im na raspolaganju prilično nesigurni. Pored toga, tajni ključ se mora često mijenjati, jer šifriranje više puta istim ključem smanjuje sigurnost.



Slika 2.7. *Kriptosustav s tajnim ključem*

Najpoznatije kriptosustave s tajnim ključem koje ću obraditi u ovom radu su:

- Cezarova šifra
- Vigenèrova šifra
- Playfairova šifra

Kriptosustavi s javnim ključem

Kod kriptosustava s javnim ključem, odnosno *asimetričnih kriptosustava* je nemoguće, u nekom razumnom vremenu, odrediti ključ za dešifriranje (usprkos tome što je ključ za šifriranje poznat) ključ za šifriranje je *javni ključ*. Naime, bilo tko može šifrirati poruku pomoću njega, ali samo osoba koja ima odgovarajući ključ za dešifriranje (privatni ili tajni ključ) može dešifrirati tu poruku. Ideju jednog takvog kriptosustava iznijeli su Whitfield Diffie i Martin Hellman, kada su dali prijedlog rješenja problema razmjenjivanja ključeva za simetrične kriptosustave putem nesigurnih komunikacijskih kanala.
U svrhu realizacije ideje kriptosustava s javnim ključem, koriste se *osobne jednosmjerne funkcije.*

Definicija 2.2 *Za funkciju $f: X \to Y$ kažemo da je jednosmjerna funkcija (engl.one - way function), ako je $f(x)$ lako izračunati za svaki $x \in X$, ali je f^{-1} jako teško izračunati. Ako je f^{-1} lako izračunati ukoliko nam je poznat neki dodatni podatak (engl. trapdoor - tajni ulaz), onda za funkciju f kažemo da je osobna jednosmjerna funkcija.*

Kako učenicima predočiti pojam jednosmjerne funkcije?
Navela sam neke primjere iz svakodnevnog života, kako bih učenicima približila pojam jednosmjernih funkcija.

1. miješanjem žute i plave boje dobijemo zelenu boju služeći se jednosmjernom funkcijom iz čega slijedi da je boje lako miješati, ali ih je nemoguće razdvojiti

2. razbijanje jaja - jaja je lako razbiti, ali nemoguće ih je vratiti u početno stanje.

Formalna definicija kriptosustava s javnim ključem glasi:

Definicija 2.3 *Kriptosustav s javnim ključem sastoji se od dva skupa funkcija. Funkcija za šifriranje e_K i funkcija za dešifriranje d_K, gdje K prolazi skupom svih mogućih korisnika sa svojstvom:*

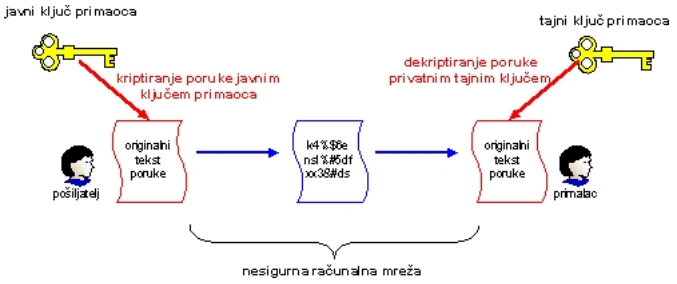
1. *Za svaki K je d_k inverz od e_K*
2. *Za svaki K je e_K javan, ali je d_K poznat samo osobi K*
3. *Za svaki K je e_K osobna jednosmjerna funkcija.*

Ključ e_K zove se javni ključ, a d_K se zove tajni ili vlastiti ključ.

Kako bih učenicima što jednostavnije ilustrirala procese šifriranja i dešifriranja kod kriptosustava s javnim ključem, koristit ću tri zamišljena lika (Alice, Bob i Eve) koji su postali standard u svim kriptografskim raspravama.

Ako Alice (A) želi poslati poruku x Bobu (B), onda Bob prvo pošalje potpuno otvoreno Alice svoj javni ključ e_B. Pomoću e_B, Alice šifrira svoju poruku i Bobu šalje šifrat $y = e_B(x)$. Na kraju, Bob dešifrira šifrat pomoću svog tajnog ključa d_B i dobije otvoreni tekst $x = d_B(y) = d_B(e_B(x))$.

Napomena 2.1 *Redoslijed enkriptiranja i dekriptiranja je neobično važan i moramo se držati pravila "zadnji došao, prvi otišao". Drugim riječima, posljednji stupanj enkripcije mora se prvi dešifrirati.*



Slika 2.8. *Kriptosustav s javnim ključem*

Najpoznatiji kriptosustav s javnim ključem kojeg ću obraditi u radu je RSA kriptosustav.

Prednosti i nedostatci u usporedbi sa simetričnim kriptosustavima

- nema potrebe za sigurnim komunikacijskim kanalom
- kriptografija javnog ključa ne koristi se za šifriranje poruka, već za šifriranje ključeva jer su algoritmi s javnim ključem puno sporiji (oko 1000 puta) od modernih simetričnih algoritama
- kriptosustavi s javnim ključem slabi su na napad "odabrani otvoreni tekst"

Poglavlje 3

Metode šifriranja i dešifriranja

U ovom poglavlju opisani su neki jednostavni kriptosustavi sa tajnim i javnim ključem koji mogu poslužiti za popularizaciju matematike u školama i drugdje. Oni su namijenjeni i razumljivi i onima koji nemaju visoku matematičku naobrazbu, prvenstveno učenicima osnovnih i srednjih škola, ali i odraslima. Grana kriptografije koja razvija takve sustave naziva se *Kid Krypto*.

3.1. Cezarova šifra

Cezarova šifra dobila je ime po tvorcu Gaju Juliju Cezaru. Osnova ove šifre je supstitucija jednog slova otvorenog teksta nekim drugim slovom. Kako postoji samo jedna šifrirana abeceda, ovaj sustav je *monoalfabetski*.
U radu će biti prikazano nekoliko tipova Cezarovih šifri, koji su prilagođeni učenicima. Njihove osnovne značajke prikazane su na konkretnim primjerima. Također, dana je i formalna definicija Cezarove šifre koju ćemo koristiti u daljnjem radu.

Definicija 3.1 *Neka je* $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26} = \{0, 1, \ldots, 25\}$. *Za* $0 \leqslant K \leqslant 25$ *definiramo*

$$e_K(x) = x + K \bmod 26, \quad d_K(y) = y - K \bmod 26 \tag{3.1}$$

Sa $a \bmod 26$ označavamo ostatak pri dijeljenju broja a sa 26.
Prvo ćemo predstaviti originalnu Cezarovu šifru i njezine glavne karakteristike, kako teorijski tako i na konkretnim primjerima. Važno je za napomenuti, da su svi primjeri prilagođeni učenicima. Radi lakšeg razumijevanja, prilikom rješavanja primjera korištene su razne boje i opisana je njihova uloga.

3.1.1. Originalna Cezarova šifra

Originalnu Cezarovu šifru koristio je sam Cezar u svojim ratovima i u komunikaciji sa svojim prijateljima. Kod ove šifre, slova otvorenog teksta, zamijenjivala su se slovima koja su se nalazila tri mjesta dalje od njih u alfabetu ($A \to D$, $B \to E$, itd). Pretpostavljamo da se alfabet ciklički nastavlja tj. da nakon zadnjeg slova Z, ponovno dolaze slova A, B, C, ...
U daljnjem radu, 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 i Z.

Otvorena abeceda:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Šifrirana abeceda:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Slika 3.1. *Originalna Cezarova šifra*

Primjer 3.1 *Originalnom Cezarovom šifrom, šifrirajmo sljedeću poznatu izreku: VENI VIDI VICI.*

Rješenje:

Otvorena abeceda:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Šifrirana abeceda:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Otvoreni tekst:	v	e	n	i		v	i	d	i		v	i	c	i
Šifrirani tekst:	Y	H	Q	L		Y	L	G	L		Y	L	F	L

zelena boja - označava originalnu Cezarovu šifru
crvena i plava - zamjena slova otvorene i šifrirane abecede

3.1.2. Cezarova šifra sa proizvoljnim pomakom

Analogna prethodno opisanoj šifri, jedina razlika je u tome da se svako slovo poruke, odnosno otvorenog teksta može zamijeniti sa slovom koje se nalazi n mjesta dalje u alfabetu. Označimo sa n pomak. Također ćemo se koristiti engleskim alfabetom od 26 slova. Kako funkcionira ova šifra, pokazat ćemo na sljedećem primjeru:

Primjer 3.2 *Uz pomak $n = 5$, šifrirajmo sljedeću poznatu izreku: VENI VIDI VICI.*

Rješenje

Otvorena abeceda: a b c d e f g h i j k l m n o p q r s t u v w x y z
Šifrirana abeceda: F G H I J K L M N O P Q R S T U V W X Y Z A B C D E

Otvoreni tekst: v e n i v i d i v i c i
Šifrirani tekst: A J S N A N I N A N H N

zelena - označava pomak ($n = 5$) u šifriranoj abecedi
crvena i plava - zamjena slova otvorene i šifrirane abecede obzirom na pomak

Općenito, koristeći se definicijom (3.1) uz oznaku da je $n = K$, šifriranje i dešifriranje Cezarove šifre s pomakom može se opisati sljedećim funkcijama:

$$e_n \colon \mathbb{Z}_{26} \to \mathbb{Z}_{26}, \quad e_n(x) = (x + n) \bmod 26 \tag{3.2}$$

$$d_n \colon \mathbb{Z}_{26} \to \mathbb{Z}_{26}, \quad d_n(y) = (y - n) \bmod 26 \tag{3.3}$$

pri čemu je $0 \leqslant n \leqslant 25$, a svakom slovu abecede jednoznačno smo pridružili njegov redni broj počevši od 0, prema korespodenciji:

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

Primjenjujući (3.2) i (3.3) na naš primjer ($n = 5$) dobivamo sljedeće funkcije šifriranja odnosno dešifriranja:

$$e_5 \colon \mathbb{Z}_{26} \to \mathbb{Z}_{26}, \quad e_5(x) = (x + 5) \bmod 26 \tag{3.4}$$

$$d_5 \colon \mathbb{Z}_{26} \to \mathbb{Z}_{26}, \quad d_5(y) = (y - 5) \bmod 26 \tag{3.5}$$

Skup $\{0, 1, 2, 3, \ldots, 25\}$ označavat ćemo sa $\mathbb{Z}_{26}$ i pretpostavljat ćemo da su na njemu definirane operacije zbrajanja, oduzimanja i množenja na isti način kao u skupu cijelih brojeva, ali tako da se rezultat (ukoliko nije iz skupa $\{0, 1, 2, 3, \ldots, 25\}$) na kraju zamijeni s njegovim ostatkom pri dijeljenju s 26. Skup $\mathbb{Z}_{26}$ uz operacije $+_{26}$ i $\cdot_{26}$ čini *prsten*.

Kako učenicima olakšati korištenje Cezarove šifre s proizvoljnim pomakom?

Umjesto zbrajanja u prstenu $\mathbb{Z}_{26}$, učenici mogu koristiti krug ("kolo") načinjeno npr.

od kartona pri čijem su rubu ispisana redom sva slova abecede. Neka se krug ("kolo") sastoji od dva kružna dijela. Ako zamislimo da je vanjski dio fiksiran i da unutarnji dio možemo okretati u krug, dobivamo svih 25 mogućih kombinacija otvorene i šifrirane abecede.

Slika 3.2. *"Kolo"*

3.1.3. Cezarova šifra s permutiranom abecedom

Originalnu Cezarovu šifru moguće je transformirati tako da se svako slovo otvorenog teksta zamijeni s proizvoljnim slovom abecede. Dakle, šifrirana abeceda može sadržavati bilo koju permutaciju slova A, B, ..., Z. Ovim postupkom nastaje 26! mogućih kombinacija šifrirane abecede, pa je ova metoda znatno složenija od prethodnih. Kada se danas nešto kriptira Cezarovom šifrom misli se na ovaj oblik Cezarove šifre. Ključ kod ove šifre predstavlja čitava šifrirana abeceda, pa sveukupno postoji $26! \approx 4 \cdot 10^{26}$ ključeva.

Ovaj način kriptiranja za učenike je puno složeniji od prethodno navedenih. Potrebno predznanje učenika, pa i odraslih, je poznavanje permutacija i prethodno navedenih pojmova koji su nužni za primjenu ove šifre na konkretnim primjerima.

3.1.4. Cezarova šifra s ključnom riječi

Kod prethodnog oblika Cezarove šifre, vidljivo je da obje strane moraju kao ključ pamtiti cijelu šifriranu abecedu koja nastaje nasumičnim odabirom slova, što ponekad zna biti neefikasno. Kako bi se to riješilo, moguće je izraditi šifriranu abecedu tako da se pošiljatelj i primatelj dogovore za jednu ključnu riječ ili frazu koja će predstavljati ključ. Šifrirana abeceda nastaje tako da se na njen početak stavi ključ bez praznina i slova koja se ponavljaju više puta, a ostatak se popuni slovima koja se ne nalaze u ključu i to redom od početka abecede. Prednost ovog oblika slaganja šifrirane abecede

je ta što se ključ lako pamti. Opisanu Cezarovu šifru pokazat ćemo na sljedećem primjeru.

Primjer 3.3 *Uz ključnu riječ TAJNA, Cezarovom šifrom šifrirajmo sljedeću izreku: TVOJA JE TAJNA SKRIVENA.*

Rješenje

Ključ: TAJNA → TAJN

Otvorena abeceda: a b c d e f g h i j k l m n o p q r s t u v w x y z
Šifrirana abeceda: T A J N B C D E F G H I K L M O P Q R S U V W X Y Z

Otvoreni tekst: t v o j a j e t a j n a s k r i v e n a
Šifrirani tekst: S V M G T G B S T G L T R H Q F V B L T

zelena - označava ključnu riječ tj. ključ koji se sastoji od slova koja se pojavljuju samo jedanput, uvijek se stavlja na početak šifirane abecede
crvena i plava - zamjena slova otvorene i šifrirane abecede obzirom na ključnu riječ

3.1.5. Razbijanje Cezarove šifre

Postoje dvije metode pomoću kojih možemo razbiti Cezarovu šifru. U radu će biti ukratko objašnjene na način primjeren učenicima.

Metoda "grube sile"

Metoda "grube sile" temelji se na ispitivanju svih mogućih ključeva redom, sve dok ne dobijemo neki smisleni tekst. Ova je metoda opravdana jer je broj ključeva mali (tj. upravo onoliki koliko je i slova - 26).
Opisanu metodu pokazat ćemo na dva jednostavna primjera. Neka je $K = n$.

Primjer 3.4 *Dekriptirajmo šifrat XENRSTMW dobiven Cezarovom šifrom.*

Rješenje

X	E	N	R	S	T	M	W	za $n = 0$
W	D	M	Q	R	S	L	V	za $n = 1$
V	C	L	P	Q	R	K	U	za $n = 2$
U	B	K	O	P	Q	J	T	za $n = 3$
T	A	J	N	O	P	I	S	za $n = 4$

Ključ je $n = 4$, a otvoreni tekst je TAJNOPIS.

Primjer 3.5 *Dekriptirajmo šifrat PWNUYTLWFKNOF dobiven Cezarovom šifrom.*

Rješenje

P	W	N	U	Y	T	L	W	F	K	N	O	F	za $n = 0$
O	V	M	T	X	S	K	V	E	J	M	N	E	za $n = 1$
N	U	L	S	W	R	J	U	D	I	L	M	D	za $n = 2$
M	T	K	R	V	Q	I	T	C	H	K	L	C	za $n = 3$
L	S	J	Q	U	P	H	S	B	G	J	K	B	za $n = 4$
K	R	I	P	T	O	G	R	A	F	I	J	A	za $n = 5$

Ključ je $n = 5$, a otvoreni tekst je KRIPTOGRAFIJA.

Frekvencijska analiza slova

Kriptoanaliza se razvija na istoku zahvaljujući razvoju znanosti, posebno matematike, gramatike, lingvistike i statistike. Sam postupak kriptoanalize zasniva se na učestalosti pojedinih slova abecede u određenom jeziku. Učestalost pojedinog slova dobiva se pretraživanjem pojavljivanja traženog slova u nekom drugom otvorenom tekstu slične duljine. Vrijednost pojavljivanja slova abecede zapisuje se u tablicu. Ovaj postupak se uglavnom preskače ukoliko je trećoj strani unaprijed poznat jezik na kojem primatelj i pošiljatelj razgovaraju, tj. ukoliko posjeduje unaprijed gotovu tablicu učestalosti slova na tom jeziku.

Frekvencija slova u hrvatskom jeziku (u promilima)

A	I	O	E	N	S	R	J	T	U	D	K	V	L	M	P	C	Z	G	B	H	F
115	98	90	84	66	56	54	51	48	43	37	36	35	33	31	29	28	23	16	15	8	3

Frekvencija slova u engleskom jeziku (u promilima)

E	T	A	O	I	N	S	H	R	D	L	C	U	M	W	F	G	Y	P	B	V	K	J	Q	X	Z
127	91	82	75	70	67	63	61	60	43	40	28	28	24	23	22	20	20	19	15	10	8	2	1	1	1

Frekvencija slova u njemačkom jeziku (u promilima)

E	N	I	R	S	A	T	D	H	U	L	G	O	C	M	B	F	W	K	Z	P	V	J	Y	X	Q
175	98	77	75	68	65	61	48	42	42	35	31	30	27	26	19	17	15	15	11	10	9	3	1	0	0

Slika 3.2. *Učestalost slova po jezicima*

Nakon ustanovljavanja učestalosti pojavljivanja slova u nekom jeziku, potrebno je jednaku analizu napraviti i nad šifriranim tekstom. Time nastaje još jedna tablica učestalosti pojavljivanja slova. Obje tablice se sortiraju i vrši se zamjena tako da se slovo iz šifrirane tablice zamijeni sa slovom iz otvorene tablice ukoliko je učestalost pojavljivanja slova približno jednaka.

Primjena u školi

Otkrivanje frekvencije slova može biti i jedna zanimljiva nastavna aktivnost. Analiziranjem manjih tekstualnih odlomaka na različitim jezicima, učenici se mogu osobno uvjeriti da su najfrekventnija slova hrvatskog jezika redom A, I, O, E, N, engleskog jezika E, T, A, O, I, njemačkog E, N, I, R, S, itd.
Na primjer, ako šifrat glasi

"REYJREYNPEOJPWEQONHENXQZLE" ,

onda pronađemo najfrekventnije slovo u šifratu. To je slovo E jer se ono pojavljuje najveći broj puta, 6 puta. Ukoliko pretpostavimo da je to slovo A, dobit ćemo sljedeći otvoreni tekst (s umetnutim razmacima)

MATEMATIKA JE KRALJICA I SLUGA.

Postupak frekvencijske analize djelotvoran je samo idejno. Prvi nedostatak je nepodudaranje učestalosti slova. Zbog toga se primjenjuju različite lingvističke metode da bi se došlo do ispravnih rješenja. Šifrirana poruka može biti prekratka pa će ova metoda dati krivi rezultat. Također, moguće je da strane prilikom komuniciranja namjerno ispuštaju neka od najučestalijih slova ili ih uopće ne koriste.
Postoji jedna zanimljivost. Naime, francuski književnik Perec napisao je *La Disparation (Odlazak)*, roman od dvjesto stranica bez ijedne riječi sa slovom e.

3.2. Vigenèrova šifra

Vigenèrova šifra je metoda šifriranja abecednog teksta korištenjem serije Cezarovih šifri, zasnovanih na slovima ključa. Osnova ove šifre je da se svako slovo otvorenog teksta može preslikati u jedno od m mogućih slova (gdje je m duljina ključa), u ovisnosti o svom položaju unutar otvorenog teksta. Kako postoji više šifriranih abeceda, ovaj sustav je *polialfabetski*.
Vigenèrova šifra je otkrivana više puta. Ime je dobila po Blaiseu de Vigenèru. Šifra je dobro poznata, a iako je lako razumljiva (učenicima i početnicima) izgleda kao neprobojna odnosno nerazmrsiva. Zbog toga je dobila epitet *le chiffre indèchiffrable* što bi u prijevodu značilo *"neprobojna šifra"*.

Prilikom uvođenja pojma Vigenèrove šifre učenicima, najbolje je krenuti od najjednostavnije metode šifriranja, Albertijeve šifre na koju se nadovezuje Belasova šifra od koje se konačno razvila Vigenèrova šifra.

3.2.1. Albertijeva šifra

Albertijeva šifra temelji se na upotrebi dvije šifrirane abecede. Sva slova na neparnim mjestima zamijenjuju se pomoću prve šifrirane abecede, a slova na parnim mjestima pomoću druge šifrirane abecede.

Zapažanja kod učenika

Učenici mogu primjetiti da su obje šifrirane abecede jednake Cezarovim šifriranim abecedama i da mogu nastati kombinacijom ranije navedenih metoda o kojima će ovisiti ključ što možemo vidjeti na sljedećem primjeru.

Primjer 3.6 *Uz ključnu riječ TAJNA, Albertijevom šifrom šifrirajmo sljedeću izreku: TVOJA JE TAJNA SKRIVENA.*

Rješenje

1. šifrirana abeceda → ključ: TAJNA → TAJN
2. šifrirana abeceda → ključ: 5

U daljnjem navodimo otvorenu, te prvu i drugu šifriranu abecedu.

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

Otvoreni tekst: t v o j a j e t a j n a s k r i v e n a
Šifrirani tekst: S Z M N T N B X T N L E R O Q M V I L E

zelena - označava ključnu riječ, tj. ključ koji se sastoji od slova koja se pojavljuju samo jedanput, uvijek se stavlja na početak šifirane abecede
plava - označava slova na neparnim mjestima koja se zamjenjuju pomoću prve šifrirane abecede
crvena - označava slova na parnim mjestima koja se zamjenjuju pomoću druge šifrirane abecede

Pitanja koja možemo uputiti učenicima

1. Što možete primjetiti, kako nastaje prva šifrirana abeceda?
(*Odgovor: Na početak prve šifrirane abecede stavi se ključ bez praznina i slova koja se ponavljaju više puta, ostatak se popuni slovima koja se ne nalaze u ključu i to redom od početka abecede.*)

2. Koju poznatu šifru primjenjujemo prilikom korištenja Albertijeve šifre?
(*Odgovor: Koristimo Cezarovu šifru s ključnom riječi.*)

3. Kako nastaje druga šifrirana abeceda?
(*Odgovor: Druga šifrirana abeceda nastaje pomakom, u našem primjeru za 5 mjesta, u odnosu na otvorenu abecedu. To je zapravo Cezarova šifra s proizvoljnim pomakom.*)

4. Što možete na temelju primjera primjetiti, koja je prednost, a koji nedostatak Albertijeve šifre?
(*Odgovor: Ključna je prednost Albertijeve šifre da se ista slova u otvorenom tekstu ne pojavljuju nužno kao ista slova u šifriranom tekstu. Glavni nedostatak je upotreba premalog broja šifriranih abeceda.*)

3.2.2. Vigenèrova šifra s ključnom riječi

Prvo ćemo navesti formalnu definiciju Vigenèrove šifre.

Definicija 3.2 *Neka je m fiksan prirodan broj. Definiramo $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^m$. Za ključ $K = (k_1, ..., k_m)$ definiramo:*

$$e_K(x_1, ..., x_m) = (x_1 +_{26} k_1, x_2 +_{26} k_2, ..., x_m +_{26} k_m) \tag{3.6}$$

$$d_K(y_1, ..., y_m) = (y_1 -_{26} k_1, y_2 -_{26} k_2, ..., y_m -_{26} k_m) \tag{3.7}$$

Sa $+_{26}$ i $-_{26}$ označili smo zbrajanje i oduzimanje modulo 26. Slova otvorenog teksta pomičemo za k_1, ... , ili k_m mjesta.
O čemu ovisi pomak?
Pomak ovisi o ostatku koji dobijemo kada poziciju slova podijelimo sa duljinom ključa m. Osnovni elementi otvorenog teksta i šifrata su "blokovi" od po m slova. Šifriranje se provodi "slovo po slovo", pa nije nužno nadopuniti zadnji blok ako broj slova u otvorenom tekstu nije djeljiv s m.

Ovaj način šifriranja je možda malo složeniji učenicima od prethodno navedenih, ali postupak je vrlo jednostavan. Pokazat ću postupak na sljedećem primjeru.

Primjer 3.7 *Neka je $m = 4$ i ključna riječ BROJ. Njezin numerički ekvivalent je ključ $K = (1, 17, 14, 9)$. Šifrirajmo otvoreni tekst KRIPTOLOGIJA.*

Rješenje

Ključ: BROJ, K = (1, 17, 14, 9)
Otvoreni tekst: KRIPTOLOGIJA, K = (10, 17, 8, 15, 19, 14, 11, 14, 6, 8, 9, 0)

Otvoreni tekst podijelimo na blokove od po četiri slova jer je duljina ključa $m = 4$.

K	R	I	P	T	O	L	O	G	I	J	A
B	R	O	J	B	R	O	J	B	R	O	J

Numerički:

10	17	8	15	19	14	11	14	6	8	9	0
1	17	14	9	1	17	14	9	1	17	14	9 $+_{26}$
11	34	22	24	20	31	25	23	7	25	23	9
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
11	8	22	24	20	5	25	23	7	25	23	9
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
L	I	W	Y	U	F	Z	X	H	Z	X	J $\rightarrow$ Šifrat

Brojeve označene crnom bojom pretvaramo u slova na sljedeći način.
Računamo:

$34 \bmod 26 = 8 = \text{I}$
$31 \bmod 26 = 5 = \text{F}$

U ovom primjeru vidljivo je da se ključ ponavlja u nedogled, pa prema podjeli šifara s obzirom na način na koji se obrađuje otvoreni tekst, ova šifra je primjer *blokovne šifre*.

Pitanje učenicima

1. Što mislite, koji je glavni nedostatak ove šifre?
(*Odgovor: Glavni nedostatak je stalan ključ što može predstavljati problem zbog sigurnosnih razloga.*)

3.2.3. Originalna Vigenèrova šifra

- **Uvođenje autoključa (engl. autokey)**
  Otvoreni tekst generira ključ. Originalni ključ koristi se samo za šifriranje prvog bloka od m slova, dok se za šifriranje daljnjih blokova koristi prethodni blok otvorenog teksta. Ta varijanta spada u *protočne šifre*.

- **Vigenèrov kvadrat (lat. tabula recta)**
  Sastoji se od alfabeta napisanog 26 puta u novom redu. Svaki red je rotiran ulijevo u odnosu na prethodni, odgovarajući svim mogućim kombinacijama Cezarove šifre. U pojedinoj točki postupka šifriranja, šifra koristi drugi alfabet iz jednog od redova. Koji će se red koristiti zavisi od ponavljajućeg ključa. Vigenèrov kvadrat koristi se i za šifriranje i za dešifriranje.

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

Slika 3.3. *Vigenèrov kvadrat*

Primjer 3.8 *Enkriptirajmo poruku DIVERT TROOPS TO EAST RIDGE pomoću ključne riječi WHITE koristeći Vigenèrov kvadrat.*

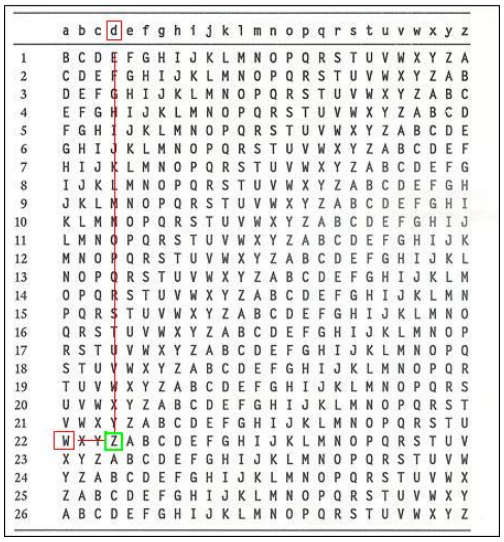
Rješenje

Ključna riječ, otvoreni tekst i šifrirani tekst:

W	H	I	T	E	W	H	I	T	E	W	H	I	T	E
d	i	v	e	r	t	t	r	o	o	p	s	t	o	e
Z	P	D	X	V	P	A	Z	H	S	L	Z	B	H	I

W	H	I	T	E	W	H	I
a	s	t	r	i	d	g	e
W	Z	B	K	M	Z	N	M

Ključna riječ ispisuje se iznad poruke mnogo puta zaredom, tako da je svako slovo poruke povezano sa slovom ključne riječi.
Kako dobivamo šifrirani tekst?
Koristimo Vigenèrov kvadrat na sljedeći način:
Da bismo enkriptirali prvo slovo d, najprije odredimo ključno slovo iznad njega, a to je W. d određuje stupac, a W redak kojim ćemo se služiti u Vigenèrovom kvadratu. Presjekom stupca koji počinje sa d i retka koji počinje sa W dobivamo šifrat Z. Postupak ponavljamo analogno za sva ostala slova.



Slika 3.3. *Primjer 3.8*

Vigenèrov kvadrat kod učenika

Ovakvim načinom šifriranja, učenici mogu na vrlo brz način šifrirati određene dijelove teksta koji im se zadaju. Time učenici razvijaju sposobnost brzog i jednostavnog snalaženja u Vigenèrovom kvadratu. Učenicima možemo podijeliti tablice koje sadrže

opisani kvadrat, objasnimo im postupak enkripcije na jednostavnom primjeru i učenici samostalno pristupaju enkripciji danog teksta.

Za što nam služi *autoključ*, pokazat će nam sljedeći primjer.

Primjer 3.9 *Analogno prethodnom primjeru, enkriptirajmo navedenu poruku koristeći autoključ.*

Rješenje
Također koristimo Vigenèrov kvadrat na opisan način.

Ključna riječ, otvoreni tekst i šifrirani tekst:

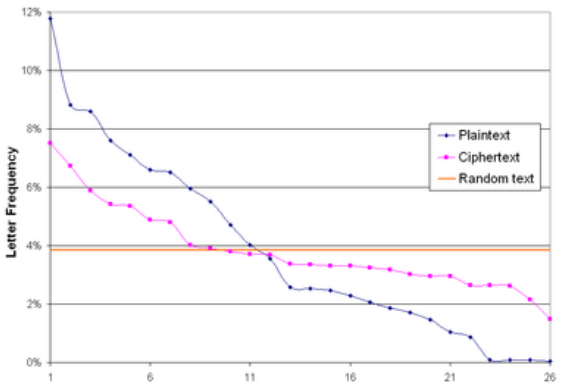
W	H	I	T	E	D	I	V	E	R	T	T	R	O	O
d	i	v	e	r	t	t	r	o	o	p	s	t	o	e
Z	P	D	X	V	W	B	M	S	F	I	L	K	C	S

P	S	T	O	E	A	S	T
a	s	t	r	i	d	g	e
P	K	M	F	M	A	Y	X

Prednosti i nedostaci Vigenèrove šifre

Snaga Vigenèrove šifre, kao i svih polialfabetskih šifara je njena sposobnost otežavanja frekvencijske analize. Frekvencijska analiza je vještina dekriptiranja poruke brojanjem frekvencije slova šifrata i uspoređivanje s frekvencijom slova normalnog teksta.

Osnovna slabost Vigenèrove šifre je njen relativno kratak i ponavljajući ključ. Ako kriptoanalitičar otkrije dužinu ključa, onda se šifrat može smatrati serijom Cezarovih šifri, koje se zatim pojedinačno jednostavno razbijaju.



Slika 3.3. *Prednosti i nedostaci*

3.2.4. Razbijanje Vigenèrove šifre

Ovdje ću samo ukratko spomenuti na čemu se postupak razbijanja Vigenèrove šifre temelji i koje metode pri tome koristimo.

Postupak se temelji na određivanju duljine ključne riječi. Postoje dvije metode kojima se ta duljina može otkriti: *Kasiskijev test* i *test pomoću indeksa koincidencije*.

Pitanja koja možemo uputiti učenicima

1. Što se događa ukoliko je pretpostavka o duljini ključne riječi bila pogrešna?

2. Koliko bi šifrat trebao biti dug da bi ga imalo smisla analizirati?

3. Koliko bi trebala biti dugačka ključna riječ pa da šifriranje bude sigurnije?

3.3. Playfairova šifra

Playfairova šifra je bigramska šifra jer se šifriraju parovi slova i to tako da rezultat ovisi i o jednom i o drugom slovu. Algoritam se bazira na 5×5 matrici koja sadrži slova abecede. Ovisno o nastanku ove matrice, postoje dvije vrste Playfairove šifre, bez upotrebe ključa i sa upotrebom ključa.

3.3.1. Playfairova šifra bez ključa

Matrica slova nastaje popunjavanjem slovima abecede po redovima. Zato ne postoji ključ. Kako matrica ima samo 25 slovnih mjesta, a abeceda se sastoji od 26 slova, po dogovoru se poistovjećuju slova I i J. U slučaju da je otvoreni tekst na hrvatskom jeziku, poistovjećujemo V i W da bismo izbjegli moguće nesporazume kod dešifriranja.

Šifriranje se sada vrši na sljedeći način:
Otvoreni tekst podijelimo na bigrame, odnosno na blokove koji se sastoje od samo dva slova. Pri tome se ne smije dogoditi da jedan blok sadrži dva jednaka slova, te da je duljina teksta parna. Zato se između jednakih slova umeće novo slovo X, koje se najrjeđe koristi u svim jezicima. Zadnji blok mora sadržavati dva slova što se osigurava dodavanjem slova X na kraj bigrama.
Nakon podijele otvorenog teksta na bigrame, pošiljatelj poruke uzima prvi bigram i traži položaj unutar matrice riječi.

Ovisno o tom položaju, moguće je postupiti na tri različita načina:

1. Ukoliko se slova nalaze u istom retku, mijenjaju se sa slovima koja su ciklički pomaknuta za jedno mjesto udesno.

2. Ukoliko se slova nalaze u istom stupcu, mijenjaju se sa slovima koja su ciklički pomaknuta za jedno mjesto ispod njih.

3. Ukoliko se slova nalaze u nekom drugom položaju, promatra se pravokutnik koji određuje ta dva slova. Slova se mijenjaju s preostala dva vrha tog pravokutnika. Redoslijed poretka ta dva vrha ovisi o bigramu i to tako da najprije dođe ono slovo koje se nalazi u istom retku kao prvo slovo u početnom bigramu.

Primjer 3.10 *Playfairovom šifrom bez ključa šifrirajmo sljedeću izreku: TVOJA JE TAJNA SKRIVENA.*

Rješenje

Matrica riječi:

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

Otvoreni tekst: t v o j a j e t a j n a s k r i v e n a

Niz bigrama: TV OJ AJ ET AJ NA SK RI VE NA

Šifrirani tekst: QY TO DF DU DF LC UH TG ZA LC

Primjena u školi

Kako učenicima objasniti pojam matrice?
Učenici matricu mogu shvatiti kao tablicu koja se sastoji od 5 stupaca i 5 redaka. To im je dovoljno znati.
Kod ovog načina šifriranja bez ključa, matrica slova uvijek je ista ovisno o abecedi pomoću koje šifriramo. Kako bismo učenicima olakšali navedeni način šifriranja, a time ga i učinili što zanimljivijim, učenici si mogu napraviti male tablice dimenzije

5×5 unutar kojih će napraviti 25 kvadratića, a u svaki kvadratić unijet će slova zadane abecede (engleske ili hrvatske).
Ukoliko pak, učenici posjeduju magnetiće, mogu slagati slova abecede na ploču, pa prema navedenim pravilima provesti postupak šifriranja.
Ovaj način šifriranja određenog otvorenog teksta je vrlo jednostavan, pa je i samim time vrlo zanimljiv učenicima.

Pitanje za učenike
1. Koji je glavni nedostatak ove metode šifriranja?
(*Odgovor: Nedostatak ove metode je konstantna matrica riječi, pa se slova otvorenog teksta šifriraju svaki puta na isti način.*)

3.3.2. Playfairova šifra s ključem

Kod ove šifre matrica slova je ovisna o ključu, koji može biti bilo koja riječ ili fraza. Matrica se popunjava po redovima tako da se na početku unese ključ iz kojeg se izbace slova koja se ponavljaju i praznine, a nakon toga se redom unose preostala slova, krenuvši od početka abecede.
Postupak enkripcije je identičan kao i kod Playfairove šifre s ključem.

Primjer 3.11 *Uz ključnu riječ TAJNA, Playfairovom šifrom s ključem, šifrirajmo sljedeću izreku: TVOJA JE TAJNA SKRIVENA.*

Rješenje

Matrica riječi:

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

Otvoreni tekst: t v o j a j e t a j n a s k r i v e n a

Niz bigrama: TV OJ AJ ET AJ NA SK RI VE NA

Šifrirani tekst: CT LB JN CJ JN BJ QM XE XC BJ

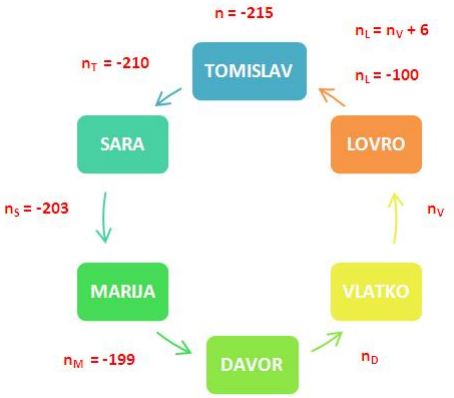
Prednosti koje učenici mogu uočiti u odnosu na supstitucijske šifre

- šifra je bigramska
- u šifriranom se tekstu gube riječi od jednog slova (npr. "a") koje dosta utječu na frekvenciju
- bigramsko šifriranje smanjuje na polovicu broj elemenata dostupnih analizi frekvencije
- broj bigrama je puno veći od broja individualnih slova (26 slova $\rightarrow 26^2 = 676$ bigrama), ta činjenica znatno otežava kriptoanalizu.

3.4. Tajni protokol

Ova aktivnost može se provesti i kod učenika nižih razreda, no i svugdje gdje je potrebno brzo i diskretno provesti neku "numeričku" anketu.

Kako ova metoda funkcionira?
Zamislimo da nastavnik želi saznati prosječan broj sati koje učenik troši na učenje i pisanje zadaće svakog tjedna. Postoji opravdana bojazan da učenici ne bi bili potpuno iskreni ukoliko taj podatak trebaju iznijeti javno. Zašto? Jer, bolji učenici bi svoju "brojku" mogli umanjiti, a oni lošiji uvećati. Stoga, nastavnik može primijeniti sljedeću proceduru koja će sačuvati pravo na privatnost svakog učenika.
Protokol započinje Tomislav koji izabire "tajni" cijeli broj n. Neka je $n = -215$. "Tajni" broj n Tomislav uveća za broj sati koji provodi u učenju, npr. 5. Numerički, to prikazujemo kao: $n_T = n + 5 = -215 + 5 = -210$. Tomislav šapne n_T sljedećoj učenici Sari. Sara za svoje školske obaveze utroši tjedno 7 sati, odnosno $n_S = n_T + 7 = -210 + 7 = -203$. Svoj broj n_S, Sara došapne Mariji. Marija uveća n_S za "svoj" broj 4, tj. $n_M = n_S + 4 = -203 + 4 = -199$, te ga prošaputa Davoru. Protokol se nastavlja redom do posljednjeg učenika Lovre kojemu je prišapnut broj n_V njegovog prethodnika Vlatka. Numerički prikaz nakon uvećanja broja n_V je $n_L = n_V + 6$. Lovro tu informaciju prosljeđuje Tomislavu, prvom učeniku od kojeg je započet protokol. Tomislav od konačnog broja n_L odbija "tajni" broj n.
Pretpostavimo da je $n_L = -100$. Sada Tomislav svima može priopćiti da je ukupan broj sati koji njegov razred utroši na izvršavanje školskih obaveza jednak $n_L - n = -100 - (-215) = 115$. Budući da razred broji 22 učenika, potrebno je izračunati koliko iznosi prosječna vrijednost utrošenih sati koja je jednaka količniku ukupnog broja sati utrošenih na učenje i ukupnog broja učenika u razredu. Prosječna vrijednost iznosi 5.2 sata.



Slika 3.4. *Tajni protokol*

Pitanje učenicima

1. Kako "razbiti" tajnost ovog protokola?
(*Odgovor: Razbijanje protokola je moguće ukoliko npr. Marija i Tomislav surađuju. Njih dvoje tada zajedno mogu otkriti koliko se zadaćama tjedno bavi njihova kolegica Sara. Znači, Mariji je zaista poznat broj n_S, pa uz Tomislavovu pomoć može odrediti da je to broj $n_S - n_T = -203 - (-210) = 7$.*)

3.5. RSA

RSA kriptosustav je prvi kriptosustav sa javnim ključem. Osmislili su ga Ron **R**ivest, Adi **S**hamir i Len **A**dleman 1977. godine i do danas je jedan od najrasprostranjenijih kriptosustava s javnim ključem. Njegova sigurnost zasnovana je na činjenici da je faktorizacija velikih prirodnih brojeva na produkt dva prosta broja izuzetno teška.
Navest ću preciznu definiciju RSA kriptosustava.

Definicija 3.3 *Neka je n=p·q, gdje su p i q prosti brojevi. Neka je $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$ i neka je*

$$\mathcal{K} = \{(n, p, q, d, e) : n = p{\cdot}q,\ p,q \text{ prosti}, de \equiv 1 \pmod{\varphi(n)}\}$$

gdje je $\varphi(n)$ Eulerova funkcija, koja prirodnom broju n pridružuje broj prirodnih brojeva manjih od n, koji su relativno prosti sa n. ($\varphi(n) = \varphi(p \cdot q) = \varphi(p) \cdot \varphi(q)$)
Za $\mathbf{K} = (n, p, q, d, e) \in \mathcal{K}$ definiramo

$$e_K(x) = x^e \mod n \quad d_K(y) = y^d \mod n\ , \quad \text{gdje su } x, y \in \mathbb{Z}_n.$$

Vrijednosti n i e su javne, dok su vrijednosti p, q i d tajne.

Definicija 3.4 *Prirodan broj $p > 1$ se zove prost ako p nema niti jednog djelitelja d takvog da je $1 < d < p$. Ako prirodan broj $a > 1$ nije prost, onda kažemo da je složen.*

Pitanje učenicima
1. Što je u ovom slučaju jednosmjerna, a što osobna jednosmjerna funkcija?
(*Odgovor: Jednosmjerna* $\rightarrow x^e \bmod n$, *osobna jednosmjerna funkcija* $\rightarrow$ *poznavanje faktorizacije* $n = p \cdot q$.)

Definicija 3.5 *S* $(a_1, a_2, \ldots, a_n)$ *označavamo najveći zajednički djelitelj brojeva* $a_1, a_2, \ldots, a_n$. *Reći ćemo da su cijeli brojevi a i b i relativno prosti ako je (a, b) = 1. Za cijele brojeve* $a_1, a_2, ..., a_n$ *reći ćemo da su relativno prosti ako je* $(a_1, a_2, ..., a_n) = 1$, *a da su u parovima relativno prosti ako je* $(a_i, a_j) = 1$ *za sve* $1 \leq i, j \leq n$, $i \neq j$.

Funkcije e_K i d_K su jedna drugoj inverzne. Da bismo to dokazali, potrebno nam je iskazati Eulerov teorem.

Teorem 3.1 *(Eulerov teorem). Ako je (a, m) = 1, onda je* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Pokažimo da su funkcije e_K i d_K jedna drugoj inverzne.

$$d_K(e_K(x)) \equiv (e_K(x))^d \equiv (x^e)^d \equiv x^{de} \pmod{n}$$

Kako je $de \equiv 1 \pmod{n}$, to znači da postoji prirodan broj t takav da je $de = t \cdot \varphi(n) + 1$, pa imamo:

$$x^{de} = x^{t \cdot \varphi(n)+1} = x^{t \cdot \varphi(n)} \cdot x = \left[x^{\varphi(n)}\right]^t \cdot x$$

U zavisnosti od n i x imamo 2 slučaja:

1. $(x, n) = 1$
   Kako je tada, prema Eulerovom teoremu, $x^{\varphi(n)} \equiv 1 \pmod{n}$, to je
   $$x^{de} = 1^t \cdot x \equiv x \pmod{n}$$
2. $(x, n) \neq 1$.
   Ako je $(x, n) = n$ tada je $x = 0$, pa je kongruencija trivijalno zadovoljena.
   Neka je $(x, n) = p$ ili $(x, n) = q$.
   Bez smanjenja općenitosti, uzmimo da je $(x, n) = p$ pa je $x^{de} \equiv 0 \equiv x \pmod{p}$.
   Kako je $(x, p \cdot q) = p$, gdje su p i q prosti, to je $(x, q) = 1$ pa je prema Eulerovom teoremu
   $$x^{\varphi(q)} \equiv 1 \pmod{q} \Longrightarrow x^{q-1} \equiv 1 \pmod{q}$$
   $$x^{de} = (x^{q-1})^{(p-1) \cdot t} \cdot x \equiv x \pmod{q}$$
   Konačno je
   $$x^{de} \equiv x \pmod{pq}, \text{ tj. } x^{de} \equiv x \pmod{n}$$

□

Napomena 3.1 *Funkciji e_K je vrlo teško odrediti inverz ukoliko nam nije poznata faktorizacija broja $n = p \cdot q$, pa se klasičan napad na ovaj kriptosustav sastoji upravo od traženja faktorizacije broja n. Inače, do sad nije poznato je li određivanje poruke x iz poznavanja šifrata $x^e \bmod n$ ekvivalentno faktorizaciji od n.*

Opišimo sada kako se primjenjuje *RSA*. Odabir parametara za ovaj sustav vrši se u sljedećih nekoliko koraka:

1. Izabiremo tajno dva velika (barem 100 znamenaka) prosta broja p i q slične veličine, no ne preblizu jedan drugome. Odabir se vrši tako da se, pomoću nekog generatora slučajnih brojeva, generira dovoljno velik prirodan broj k, a zatim se korištenjem nekog testa za testiranje prostosti traži prvi prost broj koji je veći ili jednak k.

2. Računamo $n = p \cdot q$ i $\varphi(n) = (p-1)(q-1)$.

3. Odabiremo broj e koji je relativno prost s brojem $(p-1)(q-1)$ tj. $e < \varphi(n)$ i $M(\varphi(n), e) = 1$. Često se ovaj broj bira slučajnim odabirom i potom se provjeri zadani uvjet.

4. Pomoću Euklidovog algoritma izračuna se broj d takav da je
   $de \equiv 1 \pmod{(p-1)(q-1)} \Leftrightarrow de \equiv 1 \pmod{\varphi(n)}$, tj. $d \equiv e^{-1} \pmod{\varphi(n)}$

Teorem 3.2 *(Teorem o dijeljenju s ostatkom). Za proizvoljan prirodan broj a i cijeli broj b postoje jedinstveni cijeli brojevi q i r takvi da je $b = q \cdot a + r$, $0 \leq r < a$.*

Teorem 3.3 *(Euklidov algoritam). Neka su b i $c > 0$ cijeli brojevi. Pretpostavimo da je uzastopnom primjenom Teorema 3.2 dobiven niz jednakosti*

$$\begin{aligned} b &= cq_1 + r_1, 0 < r_1 < c; \\ c &= r_1q_2 + r_2, 0 < r_2 < r_1; \\ r_1 &= r_2q_3 + r_3, 0 < r_3 < r_2; \\ &\dots \\ r_{j-2} &= r_{j-1}q_j + rj, 0 < r_j < r_{j-1}; \\ r_{j-1} &= r_jq_j + 1. \end{aligned}$$

Tada je (b, c) jednak r_j , posljednjem ostatku različitom od nule. Vrijednosti od x_0 i y_0 u izrazu $(b, c) = bx_0 + cy_0$ mogu se dobiti izražavanjem svakog ostatka r_i kao linearne kombinacije od b i c.

Primjer 3.12 *Ilustrirat ćemo šifriranje i dešifriranje u RSA kriptosustavu na malim parametrima, $p = 3$ i $q = 11$.*

Rješenje

1. Neka su dani prosti brojevi $p = 3$, $q = 11$. (Uzeli smo male brojeve kako bi učenike jednostavnije proveli kroz primjenu RSA).

2. Računamo $n = p{\cdot}q = 3{\cdot}11 = 33$ i $\varphi(n) = \varphi(pq) = (p-1)(q-1) = (3-1)(11-1) = 2 \cdot 10 = 20$.

3. Odabiremo broj e koji je relativno prost sa $\varphi(n)$ tj. $(\varphi(n), e) = 1$, $e < \varphi(n)$, tj. $e < 20$.
   Neka je $e = 7 \Rightarrow (20, 7) = 1$, $7 < 20$.

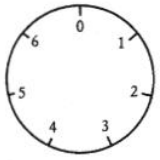
4. Euklidovim algoritmom računamo d.
   $de \equiv 1 \pmod{\varphi(n)}$
   $7d \equiv 1 \pmod{20} \Rightarrow d = 3$.

$(n, e) = (33, 7)$ je javni ključ. Pretpostavimo da netko želi poslati poruku $x = 17$. To znači da treba izračunati $e_K(x) = x^e \ mod \ n$ tj. $e_K(x) = 17^7 \ mod \ 33$.
$17^7 = 17 \cdot 17^2 \cdot 17^4 \equiv 17 \cdot 25 \cdot (-2) \equiv -25 \equiv 8 \pmod{33}$
Šifrat je $y = e_K(x) = 8$.

Kad primimo ovaj šifrat. dešifrirat ćemo ga pomoću tajnog ključa d.
$x = d_K(y) = d_K(8) \equiv 8^3 \equiv 8 \cdot 8^2 \equiv 8 \cdot (-2) \equiv 17 \pmod{33} \Rightarrow x = 17$.

3.6. "Dječji" RSA

U ovom dijelu opisat ću pojednostavljeni ("dječji") RSA kriptosustav koji je primjeren učenicima srednjih škola. Preduvjet je da su učenici upoznati s osnovama teorije kongruencija, te da znaju prikazati prirodan broj u različitim bazama.
Kako bismo učenicima približili osnovne pojmove i postupke teorije kongruencija, možemo koristiti *modularnu aritmetiku* koju u nekim školama nazivaju *"satnom aritmetikom"*. To je matematička disciplina bogata jednosmjernim funkcijama. Ona radi s konačnim skupom brojeva poredanih u petlju, baš kao što su, primjerice, poredani brojevi na brojčaniku sata.



Slika 3.5. *"Brojčanik sata"*

Na slici je prikazan sat sa modularom (modom) 7, što znači da on ima sedam brojeva: od 0 do 6.

Ilustrativni primjer učenicima
1. Izračunajmo koliko je 2+3. Krećemo od 2 i pomaknemo se za tri mjesta, tako stignemo do broja 5, a time i do rješenja koje je jednako onom u normalnoj aritmetici. To zapisujemo kao: $2 + 3 = 5 \pmod 7$.

2. Izračunajmo koliko je 2+6. Ponovno krećemo od 2, ovaj put se pomičemo za šest mjesta i stižemo do 1. To već nije rezultat koji nam daje normalna aritmetika. To zapisujemo kao: $2 + 6 = 1 \pmod 7$.

Zapišimo to matematički proučavajući sljedeći primjer.

Primjer 3.13 *Riješimo sljedeću zadaću:* $11 \cdot 9 \pmod{13}$.

Rješenje
$11 \cdot 9 = 99$
$99 : 13 = 7$ cijelih i ostaje nam 8.
Naše rješenje glasi: $11 \cdot 9 = 8 \pmod{13}$.

Nakon što smo učenicima objasnili način rješavanja modularne aritmetike, promatrat ćemo sljedeći primjer.

Neka Alice izabire cijele brojeve a, b, a', b' i postavlja sljedeće vrijednosti:

$M = ab - 1$
$e = a'M + a$
$d = b'M + b$
$n = \frac{ed-1}{M} = \frac{((a'M+a)(b'M+b)-1)}{M} = \frac{a'b'M^2+a'bM+ab'M+ab-1}{M} = \frac{a'b'M^2}{M} + \frac{a'bM}{M} + \frac{ab'M}{M} + \frac{ab-1}{M} \Rightarrow$
$n = a'b'M + a'b + ab' + 1$

Alicein javni ključ je (n, e), a tajni ključ je d.
Definirajmo sljedeće funkcije:

$$e_{ALICE}(x) = ex \pmod n$$
$$d_{ALICE}(y) = dy \pmod n$$

gdje je x prirodan broj koji predstavlja poruku, tj. otvoreni tekst. Funkcije e_{ALICE} i d_{ALICE} međusobno su inverzne. (Pokazali smo ranije!) Zaista, neka je $0 \leq x < n$. Tada je

$$\begin{aligned} d_{ALICE}(e_{ALICE}(x)) \equiv dex &\equiv (b'M+b)(a'M+a)x \\ &\equiv (a'b'M^2+ab'M+a'bM+ab)x \\ &\equiv (M(a'b'M+ab'+a'b+1-1)+ab)x \\ &\equiv (M(n-1)+ab)x \equiv (Mn-M+ab)x \\ &\equiv (Mn-ab+1+ab)x \equiv (Mn-1)x \equiv x \pmod{n} = x \end{aligned}$$

Nadalje, Bob odabire cijele brojeve a_1, b_1, a_1', b_1', te na isti način kao i Alice generira brojeve:

$M_1 = a_1b_1 - 1$
$e_1 = a_1'M_1 + a_1$
$d_1 = b_1'M_1 + b_1$
$n_1 = a_1'b_1'M_1 + a_1'b_1 + a_1b_1' + 1$

Analogno su definirane funkcije:

$$\begin{aligned} e_{BOB}(x) &= e_1x \pmod{n_1} \\ d_{BOB}(y) &= d_1y \pmod{n_1} \end{aligned}$$

Bobov javni ključ: (n_1, e_1), a tajni d_1.

Pretpostavimo da Alice želi Bobu poslati poruku x. *Šifriranje* Alice vrši tako što redom računa vrijednosti

$$\begin{aligned} y &= d_{ALICE}(x) \\ z &= e_{BOB}(y) \end{aligned}$$

te Bobu šalje poruku y. Primivši ju, Bob ju dešifrira na sljedeći način:

$$e_{ALICE}(d_{BOB}(z)) = e_{ALICE}(d_{BOB}(e_{BOB}(y))) = e_{ALICE}(y) = x$$

Konkretno, pretpostavimo da Alice želi poslati Bobu poruku "ALICE". Najprije ovu poruku treba pretvoriti u numeričku vrijednost. Kako ne bismo dobili velike brojeve, pretvaranje ćemo vršiti po blokovima veličine 3 slova. Ukoliko poruka nije višekratnik broja 3, onda je nadopunimo s jednim ili dva prazna mjesta. pretvaranje vršimo u bazi 27: slovu A pridružujemo broj 1, slovu B broj 2,..., slovu Z broj 26. Praznom mjestu pridružujemo vrijednost 0. U našem slučaju šifriramo najprije poruku "ALI", a zatim "CE".

$$x = (ALI)_{27} = (1 \cdot 27^2 + 12 \cdot 27 + 9)_{10} = (1062)_{10}$$

Pretpostavimo da je Alice odabrala sljedeće vrijednosti: $a = 15$, $b = 12$, $a' = 10$, $b' = 11$, te dobila da je
$M = ab - 1 = 15 \cdot 12 - 1 = 180 - 1 = 179$
$e = a'M + a = 10 \cdot 179 + 15 = 1790 + 15 = 1805$
$d = b'M + b = 11 \cdot 179 + 12 = 1969 + 12 = 1981$
$n = a'b'M + ab' + a'b + 1 = 10 \cdot 11 \cdot 179 + 15 \cdot 11 + 10 \cdot 12 + 1 = 19690 + 165 + 120 + 1 = 19976.$

U javni direktorij Alice je stavila $(19976, 1805)$.
Na isti način, Bob je odabrao brojeve $a_1 = 10$, $b_1 = 8$, $a_1' = 15$, $b_1' = 13$, te na analogan način izračunao da je njegov javni ključ $(15656, 1195)$, a tajni 1035. (Pripaziti da je $x < n$ i $x < n'$!, Koji je najmanji takav n?) Sada Alice najprije koristi svoj tajni ključ 1981 i računa

$$y = 1981x \bmod 19976 = 6342,$$

a zatim, iskoristivši Bobov javni ključ, dobiva

$$z = 1195y \bmod 15656 = 1186.$$

Bob prima šifrat 1186, te ga dešifrira tako da što prije iskoristi svoj tajni ključ, a onda uporabi Alicein javni ključ, odnosno računa

$$1035 \cdot 1186 \bmod 15656 = 6342 = y$$
$$1805 \cdot 6342 \bmod 19976 = 1062 = x$$

Analogno ponovimo postupak za poruku "CE".

$$x_1 = (CE)_{27} = (3 \cdot 27^2 + 5 \cdot 27 + 0)_{10} = (2322)_{10},\ 2322 < 19976 \text{ i } 2322 < 15656$$

Alice koristi svoj tajni ključ 1981 i računa

$$y_1 = 1981x_1 \bmod 19976 = 1981 \cdot 2322 \bmod 19976 = 4599882 \bmod 19976 = 5402.$$

Alice koristi Bobov javni ključ 1195 i dobiva

$$z_1 = 1195y_1 \bmod 15656 = 1195 \cdot 5402 \bmod 15656 = 6455390 \bmod 15656 = 5118.$$

Bob prima šifrat $z_1 = 5118$ i koristi svoj tajni ključ $d_1 = 1035$, a onda Alicein javni ključ.

$$1035z_1 \bmod 15656 = 1035 \cdot\ 5118 \bmod 15656 = 5297130 \bmod 15656 = 5402 = y_1$$
$$1805y_1 \bmod 19976 = 1805 \cdot\ 5402 \bmod 19976 = 9750610 \bmod 19976 = 2322 = x_1$$

Ovaj kriptosustav može se razbiti pronalaženjem prirodnog broja d takvog da je $de \equiv 1 \pmod{n}$ (čak ne nužno onog d koje Alice koristi kao svoj tajni ključ). To je moguće efikasno napraviti pomoću Euklidovog algoritma, no taj algoritam vjerojatno nije poznat onima kojima je ovaj sustav namijenjen. Otvoreno je pitanje može li se ovaj sustav razbiti bez primjene neke verzije Euklidovog algoritma. Ovaj primjer možda može poslužiti kao dodatna motivacija za uvođenje Euklidovog algoritma u nastavu matematike ili informatike.

Pokažimo kako se pomoću Euklidovog algoritma može pronaći tajni ključ d. Primijenimo Euklidov algoritam na brojeve $n = 19976$ i $e = 1805$ (koji su javni):

$$\begin{aligned} 19976 &= 1805 \cdot 11 + 121 \\ 1805 &= 121 \cdot 14 + 111 \\ 121 &= 111 \cdot 1 + 10 \\ 111 &= 10 \cdot 11 + 1 \\ 10 &= 1 \cdot 10 \end{aligned}$$

Krenuvši od pretposljednjeg retka prema gore redom imamo:

$$\begin{aligned} 1 = 111 - 10 \cdot 11 &= 111 - (121 - 111 \cdot 1) \cdot 11 = 111 \cdot 12 - 121 \cdot 11 \\ &= (1805 - 121 \cdot 14) \cdot 12 - 121 \cdot 11 = 1805 \cdot 12 - 121 \cdot 179 \\ &= 1805 \cdot 12 - (19976 - 1805 \cdot 11) \cdot 179 = 1805 \cdot 1981 - 19976 \cdot 179, \end{aligned}$$

pri čemu smo u svakom drugom koraku izvršili sređivanje izraza. Vidimo da $d = 1981$ zadovoljava uvjet $de \equiv 1 \pmod{n} \Rightarrow 1981 \cdot 1805 = 3575705 \equiv 1 \pmod{19976}$.

3.7. Savršen kôd

Kriptosustav koji ću ovdje opisati spada u kriptosustave s javnim ključem, a primjeren je učenicima srednjih škola. Za početak, navest ću neke osnovne pojmove iz teorije grafova.

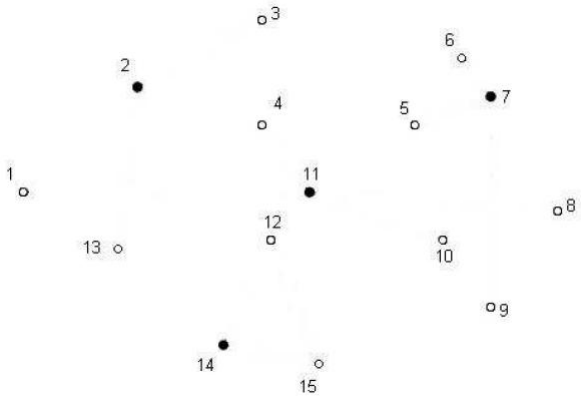
Definicija 3.6 *Graf je skup točaka koje nazivamo vrhovi, od kojih su neki povezani crtama koje zovemo bridovi. Susjedstvo danog vrha sastoji se od samog tog vrha, te svih vrhova koji su s njime povezani bridom.*

Definicija 3.7 *Savršen kôd u grafu je podskup skupa vrhova sa svojstvom da je svaki vrh grafa u susjedstvu jednog i samo jednog vrha iz tog podskupa. Graf ne mora nužno posjedovati savršen kôd, no grafovi o kojima će ovdje biti riječ imat će jedan ili više savršenih kôdova.*

Ilustrativni primjer učenicima
Zamislimo graf kocke koji se sastoji od 8 vrhova i 12 bridova. Upitamo učenike, što misle, što sve predstavlja savršen kôd kocke?
(*Odgovor: Svaki par nasuprotnih bridova prestavlja savršen kôd, npr. vrhovi s koordinatama (0,0,0) i (1,1,1)*).

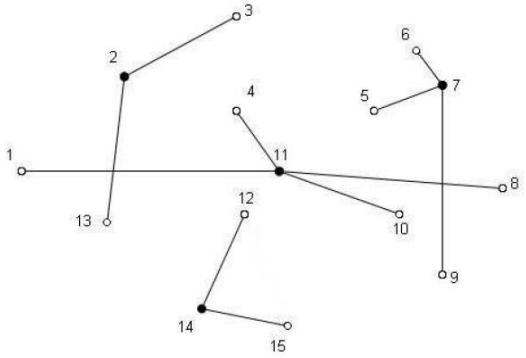
Konstruirati graf sa savršenim kodom je jednostavno, za razliku od pronalaženja istog u danom grafu, što može biti vrlo težak problem. U sljedećih nekoliko koraka opisat ću konstrukciju grafa sa savršenim kodom:

- Nacrtamo proizvoljan skup vrhova (najbolje između 15 i 25), te ih numeriramo zbog lakšeg snalaženja.
- Odaberemo savršen kôd **C**, odnosno neke od vrhova, te ih zapišemo. Ovi vrhovi predstavljaju naš *tajni ključ*.



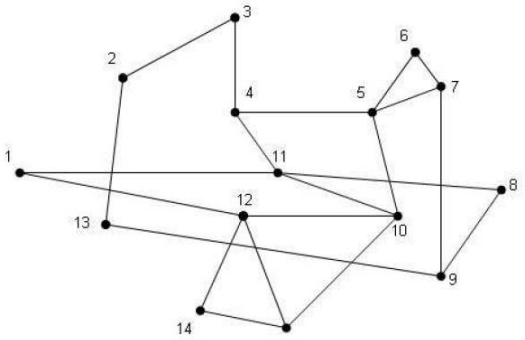
Slika 3.6. *Savršen kôd* $\boldsymbol{C}$= {*2, 7, 11, 14*}

- Povlačimo bridove od vrhova iz **C** ka ostalim vrhovima tako da je svaki vrh povezan s točno jednim vrhom iz **C**. Na taj način dobit ćemo "zvijezde" čija su središta točke iz **C**, a ostali vrhovi predstavljaju "vanjske točke". Na Slici 3.7. prikazana je samo jedna od mogućnosti kako to možemo napraviti.



Slika 3.7. *"Zvijezde" sa središtima iz* $\boldsymbol{C}$

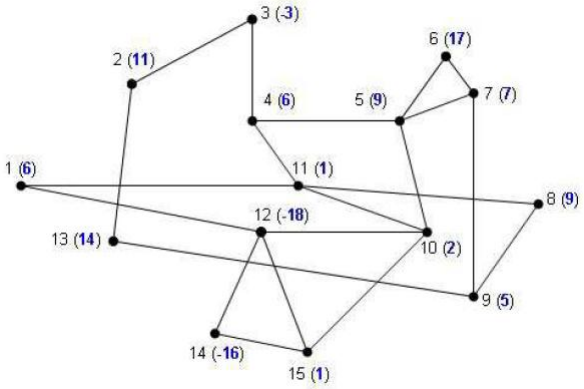
- Prikrivamo formu "zvijezda" tako što povlačimo po volji mnogo bridova između "vanjskih" vrhova. Nipošto ne smijemo vući bridove iz središta "zvijezda", jer bi tako pokvarili savršen kôd. Naša konstrukcija je gotova kada se središta "zvijezda" mogu teško uočiti. Ovako dobiveni graf predstavlja *javni ključ*.



Slika 3.8. *Prikrivanje "zvijezda"*

Pretpostavit ćemo da je naš otvoreni tekst neki cijeli broj m između 0 i 100. *Šifriranje* poruke provodi se u dva koraka, koje ćemo nazvati *plavi* i *zeleni*.

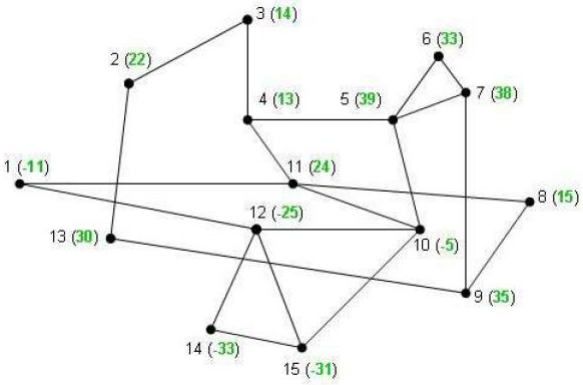
plavi Uz svaki vrh grafa upišimo cijeli broj (može i negativan) x_i tako da je $\sum x_i = m$. Dobro je ove brojeve napisati u nekoj drugoj boji od one kojom su označeni vrhovi, npr. u plavoj, te za njih koristiti naziv *plavi brojevi*. Potrebno je napomenuti, da plavi brojevi ne bi trebali biti preveliki (po apsolutnoj vrijednosti) zbog lakšeg računanja sljedećeg koraka.



Slika 3.9. *"Plavi" brojevi (u zagradama); otvoreni tekst je : 6+11-3+6+9+17+7+9+5+2+1-18+14-16+1=51*

zeleni Zbrojimo sve plave brojeve u susjedstvu svakog vrha (uključujući i sam taj vrh), te dobivene vrijednosti upišimo zelenom bojom. Tako smo dobili tzv. *zelene brojeve* i naša je poruka šifrirana! Otvorenim kanalom šaljemo graf na kojem su

upisani samo zeleni brojevi i numeracija vrhova, odnosno graf bez plavih brojeva. U praksi vrhovi nisu numerirani, odnosno šalje se graf samo sa zelenim brojevima.



Slika 4. *"Zeleni" brojevi (u zagradama)*

Poruka se *dešifrira* tako što se zbroje svi zeleni brojevi uz vrhove iz savršenog koda. Zaista, svaki zeleni broj je zbroj plavih brojeva iz njegovog susjedstva. U zbroju zelenih brojeva iz savršenog koda pojavit će se svi plavi brojevi točno jednom, jer svaki vrh grafa leži u susjedstvu jednog i samo jednog vrha iz savršenog koda. Sigurnost ovog kriptosustava, leži u dobrom kamufliranju savršenog koda, a također i u nedovoljnom poznavanju linearne algebre (od strane protivnika). Naime, jasno je da izvornu poruku možemo odrediti ukoliko su nam poznati plavi brojevi. Njih možemo izračunati pomoću sljedećeg linearnog sustava:

$$\sigma_{1i}x_1 + \sigma_{2i}x_2 + \ldots + \sigma_{ni}x_n = z_i,\ i = 1, \ldots, n$$

gdje su $x_1, x_2, \ldots, x_n$ plavi brojevi (odnosno nepoznanice), z_i je zeleni broj pri i-tom vrhu, a koeficijenti σ_{1i}, σ_{2i}, $\ldots$, σ_{ni} su jednaki 0 ili 1. Ako se j - ti vrh nalazi u susjedstvu i - tog vrha, onda je $\sigma_{ji} = 1$, a inače je $\sigma_{ji} = 0$. Sustav se sastoji od n jednadžbi, odnosno onoliko koliko je i vrhova. Za primjer navodim nekoliko jednadžbi vezanih uz graf sa Slike 4.:

$$\begin{gathered}
x_1 + x_{11} + x_{12} = -11 \text{ (iz vrha 1)}, \\
x_2 + x_3 + x_{13} = 22 \text{ (iz vrha 2)}, \\
\vdots \\
x_1 + x_{10} + x_{12} + x_{14} + x_{15} = -25 \text{ (iz vrha 12)}, \\
\vdots \\
x_{10} + x_{12} + x_{14} + x_{15} = -31 \text{ (iz vrha 15)}.
\end{gathered}$$

Čak i ako se ovakav sustav postavi, teško je očekivati da će ga učenici moći riješiti (barem u nekom razumnom vremenu), budući da je n barem 15. Ovaj primjer će možda motivirati ambicioznije učenike da saznaju nešto više o rješavanju takvih sustava ili da se upoznaju s programskim paketima pomoću kojih se oni mogu riješiti.

Poglavlje 4

Primjena u nastavi

U ovom poglavlju bit će prikazana sinteza prethodno navedenih metoda kriptografije u nastavi matematike, informatike, hrvatskog jezika, engleskog jezika, a dijelom i povijesti.
Kao budući nastavnik matematike i informatike, iznijet ću neka svoja stajališta o primjeni kriptografije u nastavi.

Uspješno podučavati matematiku, ili bilo koji drugi predmet, nije ni najmanje jednostavan niti lak posao. Potrebno je dobro poznavanje osnovnih načela metodike u nastavi. Uz primjerenost, vlastitu aktivnost, individualizaciju, postupnost, jedno od jednako važnih načela u metodici nastave matematike je i zornost. Zornost predstavlja transformaciju apstraktnih sadržaja u empirijske. Jedan od oblika nastave pogodne za to je grupni rad i projektna nastava. Projektna nastava je pogodna za povezivanje s drugim predmetima, ona kombinira osnovno stručno znanje s eksperimentima. Unutar nje, postiže se cjelovito učenje s jakim samostalnim elementom, veza sa životnom praksom i društvom, komunikacija, interdisciplinarni rad.
Jedna od nedjeljivih veza je ona matematike i informatike. Kao stanovnik računalnog svijeta, pojedinac vrlo brzo shvati da sigurnost igra veliku ulogu kada su u pitanju poslovne transakcije, osobne poruke i ostali prijenosi podataka putem malih i velikih mreža, kao npr. internetom. No, kako u tome predočiti važnost matematike? Kako primjeniti naučenu teoriju u praksi i uočiti svrhovitost? Odgovor nam zapravo daje ovaj cjelokupni diplomski rad u kojem su opisane osnove kriptografije i temeljne metode šifriranja i dešifriranja.

Matematika

Dobri učenici počinju shvaćati da se učenje matematike ne sastoji samo u učenju definicija i tehnika, dok slabi učenici mogu otkriti razumljive primjene. Konkretno, svatko se od nas, barem jednom u životu zapitao: "A što će mi ovo?" Upravo slabi učenici u

pravilu ne vide da matematika ima primjene u stvarnom životu.

Problemi

Dva su čimbenika ključna za zornost u nastavi matematike: primjena i analiza. Najveći problem na koji možemo naići kao nastavnik odnosno profesor predavajući matematiku jest činjenica da učenici slabo povezuju i prenose podatke iz jedne školske godine u drugu, ali i iz jedne nastavne cjeline u drugu. Većina profesora radi toga je sklona kritiziranju učenika, ali mislim da dio krivice leži i u nama samima (načini na koje očekujemo od učenika da uče). Kada pojedinac pamti informaciju koja nije povezana s ostalim do tada poznatim informacijama, ta se informacija rijetko kada pohranjuje u dugotrajno pamćenje. Zato je ovdje vrlo bitna korelacija nastave matematike s drugim predmetima. Povezivajući predmete jedan s drugim, učenicima se nudi više mogućnosti da nove informacije povežu sa već postojećim znanjem.

Učenici često matematiku vide kao dosadan, mučan i zamoran predmet. Srednjoškolska matematika postaje kompleksnija, a učenje matematike svodi se na niz naučenih formula i vještina koje se primjenjuju na smišljene problemske situacije. Te situacije imaju svoju primjenu u znanosti i realnom svijetu, ali nažalost, učenici svoj negativan stav prema matematici razvijaju u ranoj dobi jer nisu u stanju povezati matematiku sa drugim disciplinama. Gotovo svi učenici imaju iskustva sa zagonetkama i igrama u kojima je potrebno otkrivati dijelove koji posloženi na pravi način daju rješenje problema. Jedna takva jedinica, kao što je kriptografija, uključuje šifre i špijuniranje i kao takva sama po sebi privlači pozornost učenika, čak i onih slabijih (ne znajući da je u pozadini svega toga zapravo matematika).

Djeca od najranijeg djetinjstva uče kroz igru, te kroz nju poimaju stvarnost. One im pomažu da odrastu, da stvarnost prihvate postupno, ali i u cjelini. Kao odgojno - obrazovno sredstvo, igra je djelotvorna na svim odgojnim područjima, u tjelesnom odgoju, intelektualnom, moralnom, estetskom i radnom. Igra potiče na slobodan stvaralački rad i kreativnost, što je od velike važnosti za estetski odgoj. O njihovoj primjeni u pojedinim predmetima, te o njihovoj učestalosti i zanimljivosti odlučuju sami profesori i njihova kreativnost.
Matematika je znanost u kojoj je korištenje igre moguće u najvećoj mogućoj mjeri. To jesu igre i trebaju biti one koje pozivaju na ispitivanje i istraživanje, igre koje postavljaju zagonetke, ali ih uspješno rješavaju. Učenik bi trebao u njoj naći ono što će ga zaokupiti, zaintrigirati i što bi želio naučiti. Potrebno je spoznati kojim se vrijednim i zanimljivim poslovima bavi matematika, potaknuti da se učenici samostalno počnu baviti matematičkim problemima i da samostalno razvijaju vlastite zamisli. Obilje slika i zornih prikaza kroz igru trebali bi pridonijeti tome da se cilj postigne.

Rješenje problema

Kako u životu ne postoje strogo odvojeni predmeti i sve je isprepleteno, tako bi trebalo biti i u obrazovanju. Teško je i nemoguće svim učenicima prikazati važnost matematike, no trebali bi se potruditi povezati materijalno sa iskustvom što je često nemoguće. Primarni cilj obrazovanja trebao bi biti osposobljavanje svakog učenika da voli učiti i želi nastaviti učiti kroz svoj život. To bi bio uspjeh svakog učitelja!

Matematika unutar kriptografije može biti vrlo složena, pa tako i vrlo lako premašiti sposobnosti većine srednjoškolskih učenika. No, gotovo svi učenici, pa i oni najslabiji, trebali bi biti u mogućnosti shvatiti osnove kriptografije, predstavljene u ovom radu.

Cezarova šifra

Cezarova šifra primjerena je za osnovne škole, učenicima od petog do osmog razreda. Preciznije, Cezarovu šifru, mogli bismo koristiti već u petom razredu. Potrebno predznanje učenika su osnovne računske operacije koje su učenici učili u nižim razredima.

Cezarovu šifru možemo koristiti i u sedmom razredu kada učenike upoznajemo s pojmom funkcije, domenom i kodomenom funkcije. Učenici u sedmom razredu susreću pojam linearne funkcije oblika $f(x) = ax + b$, a u šestom razredu rješavaju linearne jednadžbe s jednom nepoznanicom. Ako to sve povežemo u jedan primjer, možemo učenicima pokazati dešifriranje zadane poruke danom linearnom funkcijom, koristeći Cezarovu šifru.

Primjer 4.1 *Dana je linearna funkcija $f(x) = x + 3$. Cezarovom šifrom dešifrirajmo sljedeću poruku UXELFRQ SRPSHB.*

Rješenje

$f(x) = x + 3 \rightarrow y = x + 3 \rightarrow x = y - 3$

UXELFRQ SRPSHB $\rightarrow$ RUBICON POMPEY

Domena je skup cijelih brojeva, a kodomena također. Sa skupom cijelih brojeva učenici se susreću u šestom razredu. Postupak dešifriranja dane poruke svodimo na rješavanje linearnih jednadžbi s jednom nepoznanicom (šesti razred).
Kako je slovu U pridružen broj 20, slijedi da je x, odnosno traženo slovo 20 - 3 = 17, a to je slovo R. Na analogan način dobijemo ostala slova zadane poruke.

$x = 20 - 3 = 17 \rightarrow \mathbf{R}$
$x = 23 - 3 = 20 \rightarrow \mathbf{U}$
$x = 4 - 3 = 1 \rightarrow \mathbf{B}$
$x = 11 - 3 = 18 \rightarrow \mathbf{I}$
$x = 5 - 3 = 2 \rightarrow \mathbf{C}$
$x = 17 - 3 = 14 \rightarrow \mathbf{O}$
$x = 16 - 3 = 16 \rightarrow \mathbf{N}$
$x = 18 - 3 = 15 \rightarrow \mathbf{P}$
$x = 17 - 3 = 14 \rightarrow \mathbf{O}$
$x = 15 - 3 = 12 \rightarrow \mathbf{M}$
$x = 18 - 3 = 15 \rightarrow \mathbf{P}$
$x = 7 - 3 = 4 \rightarrow \mathbf{E}$
$x = 1 - 3 = -2 \rightarrow \mathbf{Y}$

Ovakav način učenicima može biti zanimljiv kod rješavanja linearnih jednadžbi s jednom nepoznanicom. Ukoliko ovaj način nije ostvariv u redovnoj nastavi, preporuča se da se pokaže u dodatnoj nastavi.
Ovaj primjer zapravo možemo poistovjetiti i sa traženjem inverza dane linearne funkcije. Inverzne funkcije vezane su za gradivo četvrtog razreda srednjih škola (gimnazija i strukovnih škola).

Primjena u nastavi hrvatskog jezika

Otkrivanje frekvencije slova može biti jedna zanimljiva nastavna aktivnost. Vjerojatno su učenici na nastavi hrvatskog jezika upoznati sa informacijom da su najfrekventnija slova hrvatskog jezika redom A, I, O, E, N. Stoga, u nastavi hrvatskog jezika možemo učenicima zadati da analiziraju manje tekstualne odlomke na različitim jezicima i uvjere se koja su slova hrvatskog jezika najfrekventnija (analogno u nastavi engleskog jezika).

Primjena u nastavi povijesti

U sedmom razredu osnovne škole u nastavi povijesti učenici upoznaju lik Gaja Julija Cezara, rimskog vojskovođu, političara i pisca. U tom dijelu, učenicima se može spomenuti i poznata Cezarova šifra koju je koristio sam Cezar u Galskom ratu.

Vigenèrova šifra

Može se primjeniti već u osnovnim školama. Ukoliko učenici dobiju gotove tablice sa Vigenèrovim kvadratom, neko osnovno predznanje učenika i nije potrebno. Također se navedena šifra može primjeniti u nastavi hrvatskog i engleskog jezika.

Playfairova šifra

Može se primjeniti u osnovnim školama, svojim sadržajem je pogodna i za srednje škole (gimnazije) kod traženja inverzne funkcije (četvrti razredi). Za osnovnu školu, učenici trebaju poznavati kvadrat. To se uči u šestom razredu, cjelina: Četverokuti.

RSA kriptosustav

RSA kriptosustav pogodan je za matematičke gimnazije, posebice za dodatnu nastavu. Učenici se upoznaju s pojmom prostog broja već u osnovnoj školi (peti razred), dok se s pojmom relativno prostih brojeva ne susreću u redovnoj nastavi, pa se preporuča da se time bavi dodatna nastava. Euklidovim algoritmom i teorijom kongruencija učenici se također ne susreću u redovnoj nastavi, pa ih uključujemo u dodatnu nastavu. Dodatna nastava uključivala bi učenike četvrtih razreda srednjih škola (gimnazija).

Savršen kôd

Savršen kôd je primjeren učenicima srednjih škola (gimnazija) u nastavi dodatne matematike. Osnovni pojmovi teorije grafova su potrebno predznanje učenika. Ovaj kriptosustav je možda primjeren i za strukovne škole. Cilj je ambicioznije učenike motivirati da saznaju nešto više o rješavanju sustava od n jednadžbi s n nepoznanica (sustave dviju linearnih jednadžbi s dvjema nepoznanicama učenici upoznaju u sedmom razredu).

Informatika

Nastava informatike je sama po sebi učenicima vrlo zanimljiva. Većina učenika je danas vrlo dobro upoznata sa nekim osnovama informatike, korištenjem interneta, MS Officea, itd. No sve ovo navedeno nije sva informatika koja se u školama uči.
Važno je naglasiti da se učenici u srednjim školama (četvrti razredi - gimnazije, ekonomske škole) prvi puta susreću sa programiranjem u Pascalu i C++. Nekima je to izuzetno zanimljivo, a s druge strane, nekima je to noćna mora. Najjednostavniji programski jezik u kojem učenici programiraju je C ili C++.
Kako bismo motivirali ambicioznije učenike, navedene metode šifriranja i dešifriranja u ovom diplomskom radu, učenici mogu programirati u C++. Za neke učenike to bi moglo biti vrlo zanimljivo i izazovno.

Sažetak

Ovim radom opisana je kriptografija kao znanstvena disciplina koja može obogatiti nastavu u školama. Npr. nastavu matematike može obogatiti na način da joj da uzbudljivost i dramatičnost, a kod učenika pobudi kreativnost i znatiželju.
Na samom početku rada dan je kratki povijesni pregled kriptografije. Zatim su opisani osnovni pojmovi kriptografije kao i jednostavne i zanimljive metode šifriranja i dešifriranja određenih poruka (Cezarova šifra, Vigenèrova šifra, Playfairova šifra, RSA kriptosustav, Savršen kôd samo su neke od njih). Navedene metode prilagođene su mogućnostima učenika da shvate postupke šifriranja i dešifriranja i samostalno ih primjene na konkretnim primjerima.
Na samom kraju ovog rada, opisana je primjena kriptografije u nastavi, kako u nastavi matematike tako i u nastavi informatike, engleskog jezika, njemačkog jezika, pa donekle i u nastavi povijesti.

Ključne riječi: kriptografija u školi, kriptosustavi s tajnim i javnim ključem

Abstract

This graduate work describes cryptography as a scientific discipline which can enrich the teaching process in school. For example, it can enrich mathematics classes by providing them with exciting and dramatic features, and it can also encourage pupils to be more creative and curious.
At the beginning of the work, a brief historic overview is introduced. Furthermore, main cryptography terms are described, as well as simple and interesting coding and decoding methods (Caesar cipher, Vigenère cipher, Playfair cipher, the RSA cryptosystem, Perfect code is just some of them). These methods are adjusted to the capabilities of pupils in order to understand the process of coding and decoding, as well as their application in specific situations.
At the end of this work, the application of cryptography is described in mathematics classes , and also in informatics, German, English classes, and to some degree in history classes.

Key words : cryptography in school, cryptosystems with secret and public key

Literatura

[1] M. Barun, A. Dujella, Z. Franušić *Kriptografija u školi*, Poučak 33 (2008), 40-52, PMF - Matematički odjel, Zagreb.
http://web.math.pmf.unizg.hr/∼fran/clanci/kripto-poucak4.pdf

[2] M. Čeri, *Radno okruženje za klasične kriptografske algoritme*, završni rad, FER, Zagreb, lipanj 2008.
http://os2.zemris.fer.hr/algoritmi/2008_ceri/ispis/zavrsni.pdf

[3] A. Dujella, *Kriptografija*, skripta, PMF - Matematički odjel, Zagreb.
http://web.math.hr/∼duje/kript/kriptografija.html

[4] A. Dujella, *Diskretna matematika*, skripta, PMF - Matematički odjel, Zagreb.
http://web.math.pmf.unizg.hr/∼duje/diskretna/diskretna.pdf

[5] A. Dujella, *Uvod u teoriju brojeva*, skripta, PMF - Matematički odjel, Zagreb.
http://web.math.hr/∼duje/utb/utblink.pdf

[6] B. Ibrahimpašić, *RSA kriptosustav*, Osječki matematički list 5 (2005), 101 - 112

[7] N. Koblitz, *Cryptography as a teaching tool*, Cryptologia 21 (1997) 317 - 326
http://www.math.washington.edu/∼koblitz/crlogia.html

[8] S. Singh, *Šifre - kratka povijest kriptografije*, Tisak GZH, Zagreb, 2003.

[9] Wikipedia,
http://hr.wikipedia.org/wiki/Kriptografija

Životopis

Zovem se Jelena Macanić. Rođena sam 12. srpnja 1988. godine u Virovitici. Živim u Orahovici. Godine 1995. upisujem prvi razred u Osnovnoj školi Ivane Brlić - Mažuranić u Orahovici. Svoje osnovnoškolsko obrazovanje završavam 2003. godine. Iste godine upisujem Opću gimnaziju Stjepan Ivšić u Orahovici koju uspješno završavam 2007. godine. Daljnje obrazovanje nastavljam upisom, 2007. godine, Sveučilišnog nastavničkog studija matematike i informatike na Odjelu za matematiku u Osijeku.

Trenutno sam zaposlena u Osnovnoj školi Ivane Brlić - Mažuranić u Orahovici.