Elementi kriptografije u nastavi

Gradištanac, Kristina

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

FAKULTET ZA ODGOJNE I OBRAZOVNE ZNANOSTI

Kristina Gradištanac

ELEMENTI KRIPTOGRAFIJE U NASTAVI

DIPLOMSKI RAD

Osijek, 2018.

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

FAKULTET ZA ODGOJNE I OBRAZOVNE ZNANOSTI

Integrirani preddiplomski i diplomski sveučilišni učiteljski studij

Kristina Gradištanac

ELEMENTI KRIPTOGRAFIJE U NASTAVI

DIPLOMSKI RAD

Predmet: Matematika

Mentorica: izv. prof. dr. sc. Ružica Kolar-Šuper

Komentorica: prof. dr. sc. Zdenka Kolar-Begović

Studentica: Kristina Gradištanac

Matični broj: 2715

Modul: B

Osijek

rujan, 2018.

SAŽETAK

Kriptografija je znanstvena disciplina koja proučava metode slanja poruka u obliku u kojemu ih može pročitati samo osoba kojoj su namijenjene. U ovom su radu navedeni elementi povijesti kriptografije te predstavljene zanimljive metode šifriranja i dešifriranja. Neke od tih metoda prilagođene su učenicima osnovnih škola, a moguće ih je provesti u redovnoj ili dodatnoj nastavi matematike. Uključivanje elemenata kriptografije može obogatiti nastavu, dati joj dinamičnost i uzbudljivost, ali i potaknuti kreativnost, znatiželju i motiviranost kod učenika. Ideja rada prikazati je kako na zanimljiv način približiti učenicima kriptografiju, što je i provedeno s učenicima razredne i predmetne nastave. Radionica je provedena i sa studentima Fakulteta za odgojne i obrazovne znanosti u Osijeku, budućim učiteljima, s ciljem upoznavanja s mogućnostima uvođenja kriptografskih sadržaja u redovnu ili dodatnu nastavu matematike.

Ključne riječi: *kriptografija, nastava, matematika, kriptoanaliza, povijest, šifra*

SUMMARY

Cryptography is a scientific discipline that studies the methods of sending messages in a form that can only be read by the person they are intended for. In this paper elements of cryptographic history are presented as well as interesting methods of encryption and decryption. Some of the methods are adjusted for primary school students and can be implemented in both regular and additional (advanced) mathematics class. The use of cryptographic elements may enrich teaching and contribute to its dynamics and excitement, but also stimulate creativity, curiosity and motivation among students. The idea of the paper is to present cryptography in an interesting way in classes, which was tested among primary school students. The workshop was also conducted with students of the Faculty of Education in Osijek, i.e. future teachers, with the aim to learn about different possibilites of including a cryptographic content into regular or additional (advanced) mathematics classes.

Keywords: *cryptography, teaching, math, cryptoanalysis, history, cipher*

SADRŽAJ

1. UVOD

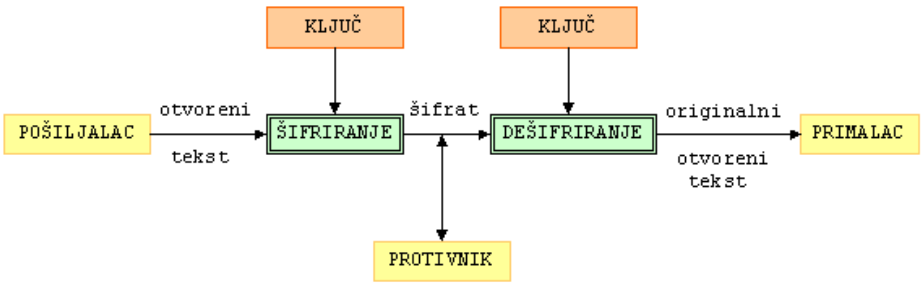
Tajno pisanje postoji otkako postoji i pismo. Poriv za otkrivanjem tajni duboko je utkan u ljudsku narav zbog čega se većina ljudi zadovoljava rješavanjem zagonetki smišljenih za razbibrigu te čitanjem kriminalističkih romana. Djeca su također opčinjena intrigom i avanturom, a igrajući motivirajuće i sofisticirane logičke igre, razvijaju svoju kreativnost i logičko mišljenje. S obzirom na to da većina učenika ima iskustva sa zagonetkama i igrama, kriptografija, koja uključuje šifre i špijuniranje, svakako može privući pozornost učenika, zainteresirati ih, zabaviti, a oni pritom neće ni biti svjesni da je u pozadini svega toga zapravo matematika. Igre su vrlo važne za stvaranje okruženja u kojem će učenici biti željni novih znanja. Matematika je pogodna za primjenu raznih igara koje učenike potiču na samostalno rješavanje matematičkim problemima.

Čovječanstvo je privlačila kriptografija još od antičkih vremena. Kraljevi, kraljice i vojskovođe, pri upravljanju svojim zemljama i vođenju svojih vojski, stoljećima su ovisili o djelotvornoj komunikaciji. Istodobno, bili su svjesni posljedica ako bi njihove poruke došle u krive ruke i tako suparničkim stranama razotkrile dragocjene tajne te odale ključne podatke. Ta opasnost potaknula je razvoj kriptografije, odnosno šifri koje su poslužile kao sredstvo koje je omogućavalo da poruku pročita samo onaj kojem je ona namijenjena. Kriptografija je često odlučivala o ishodima bitaka te sudbinama špijuna i urotnika. Povijest kriptografije priča je o stoljetnoj borbi između tvoraca šifri (kriptografa) i njihovih razbijača (kriptoanalitičara), intelektualna trka u naoružavanju koja je dramatično utjecala na puteve povijesti. Svaka nova šifra bila je razbijena, što je motiviralo kriptografe cijelog svijeta na stvaranje neke nove, jače i neslomljive šifre, a navedeni ciklus ponavlja se sve do danas. Informacije, naime, postaju sve vrjednijim dobrom, pa kako komunikacijska revolucija sve više mijenja društvo, tako će i proces šifriranja poruka igrati sve veću ulogu u svakodnevnom životu.

2. OSNOVNI POJMOVI U KRIPTOGRAFIJI

Razvoju kriptografije prethodila je uporaba *steganografije*, odnosno tajnog komuniciranja pri kojem se skriva i samo postojanje poruke, a kojoj je ime izvedeno iz grčkih riječi *steganos* („*pokriven*") i *graphein* („*pisati*"), a znači *skriveno pismo* (Singh, 2003). *Kriptografija* je pak znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih može pročitati samo onaj komu su namijenjene. Sama riječ kriptografija izvedenica je iz grčkog pridjeva κρυπτός *kriptós* (što znači *tajan, skriven*) i glagola γράφω *gráfo* (što znači *pisati*)[1] te bi se mogla doslovno prevesti kao *tajnopis* (Dujella, Maretić, 2007).

Osnovni je zadatak kriptografije omogućiti dvjema osobama (pošiljatelju i primatelju) komuniciranje preko nesigurnog komunikacijskog kanala (telefonska linija, računalna mreža, ...) na način da treća osoba (protivnik) ne može razumjeti njihove poruke. Pošiljatelj se poruke u literaturi najčešće naziva Alice, primatelj Bob, a treća osoba Eva ili Oskar. Poruka koju pošiljatelj želi poslati primatelju naziva se *otvoreni tekst* (engl. *plaintext*). Pošiljatelj transformira otvoreni tekst koristeći se unaprijed dogovorenim *ključem* (engl. *key*) postupkom koji se naziva *šifriranje* ili *enkripcija* u *šifrirani tekst* ili *šifrat* (engl. *ciphertext*). Sama riječ *šifra* potječe od hebrejske riječi *saphar* što znači *davanje brojeva*. Nakon toga pošiljatelj šalje šifrat preko komunikacijskog kanala pri čemu protivnik prisluškujući može doznati sadržaj šifrata, ali ne može odrediti otvoreni tekst. Primatelj, koji zna ključ kojim je šifrirana poruka, tada može *dešifrirati* šifrat, tj. odrediti otvoreni tekst (vidi sliku 1.) (Aydin i sur., 2011; Dujella, Maretić, 2007).



Slika 1. Komunikacija preko nesigurnog komunikacijskog kanala uz pomoć šifriranja i dešifriranja (izvor: https://web.math.pmf.unizg.hr/~duje/kript/osnovni.html)

[1] *Računalna kriptografija u nastavi*. Pribavljeno 15.5.2018., sa https://www.academia.edu/7816725/Ra%C4%8Dunalna_kriptografija_u_nastavi

Konvencija je u kriptografiji da se izvorna poruka ili otvoreni tekst piše malim, a enkriptirana poruka ili šifrirani tekst velikim slovima (Singh, 2003). *Kriptografski algoritam* ili *šifra* matematička je funkcija koja se koristi za šifriranje i dešifriranje. Funkcije za šifriranje i dešifriranje preslikavaju osnovne elemente otvorenog teksta u osnovne elemente šifrata i obratno. Skup svih mogućih vrijednosti ključeva naziva se *prostor ključeva*. *Kriptosustav* se sastoji od kriptografskog algoritma te svih mogućih otvorenih tekstova, šifrata i ključeva. Prema Dujelli i Maretiću (2007) moguće je uspostaviti definiciju:

Definicija 1. Kriptosustav je uređena petorka ($P, C, K, \mathcal{E}, D$) za koju vrijedi:

1) P je konačan skup svih mogućih osnovnih elementa otvorenog teksta;
2) C je konačan skup svih mogućih osnovnih elemenata šifrata;
3) K je prostor ključeva, tj. konačan skup svih mogućih ključeva;
4) $\mathcal{E}$ je skup svih funkcija šifriranja;
5) D je skup svih funkcija dešifriranja.

Za svaki $K \in K$ postoji funkcija šifriranja $e_K \in \mathcal{E}$ i odgovarajuća funkcija dešifriranja $d_K \in D$. Pritom su $e_K : P \rightarrow C$ i $d_K : C \rightarrow P$ funkcije sa svojstvom da je $d_K(e_K(x)) = x$ za svaki otvoreni tekst $x \in P$. Iz svojstva $d_K(e_K(x)) = x$ slijedi da funkcije e_K moraju biti injekcije, odnosno ako bi vrijedilo da je $e_K(x_1) = e_K(x_2) = y$, za dva različita otvorena teksta x_1 i x_2, onda $d_K(y)$ ne bi bilo definirano, tj. primatelj ne bi mogao odrediti treba li y dešifrirati u x_1 ili x_2. Također, ako je $P = C$, onda su funkcije e_K permutacije.

Kriptosustavi se klasificiraju prema tipu operacija koje se koriste pri šifriranju, načinu na koji se obrađuje otvoreni tekst te tajnosti i javnosti ključeva. S obzirom na tip operacija koje se koriste pri šifriranju, kriptosustavi se dijele na *supstitucijske šifre* (zamjene) i *transpozicijske šifre* (premještanje). Također, postoje i kriptosustavi koji kombiniraju te dvije metode. Supstitucijska (zamjenska) šifra šifra je u kojoj je svako slovo otvorenog teksta zamijenjeno nekim drugim slovom (šifriranje) ili, pak, simbolom ili riječima (*kodiranje*) kako bi se dobila šifrirana poruka. Kod transpozicijske šifre svako slovo zadržava svoj identitet, ali mijenja mjesto, dok kod supstitucije slova mijenjaju identitet, ali zadržavaju položaj. Također postoji i vrsta šifriranja pomoću *nomenklatora* koji se sastoji od supstitucijske šifre i ograničenog broja kodnih riječi (Dujella, Maretić, 2007; Singh, 2003). Nadalje, s obzirom na način na koji se obrađuje otvoreni tekst, kriptosustavi se dijele na *blokovne šifre*, kod kojih se obrađuje jedan po jedan blok elemenata otvorenog teksta koristeći se jednim te istim ključem, te *protočne šifre* (engl. *stream cipher*) kod

kojih se elementi otvorenog teksta obrađuju jedan po jedan koristeći se pritom paralelno generiranim nizom ključeva (engl. *keystream*). S obzirom na tajnost i javnost ključeva kriptosustavi se dijele na *simetrične kriptosustave* i *kriptosustave s javnim ključem*. Kada je riječ o simetričnim kriptosustavima, ključ se za dešifriranje može izračunati poznavajući ključ za šifriranje i obratno. Sigurnost kriptosustava leži u tajnosti ključa, pa se zbog toga i zovu kriptosustavi s tajnim ključem. Kod kriptosustava s javnim ključem ili asimetričnih kriptosustava, ključ se za dešifriranje ne može tako lako izračunati iz ključa za šifriranje jer se primjenjuju „jednosmjerne" funkcije koje se računaju lako, ali njihov inverz vrlo teško, rabe se „teški" matematički problemi, koji uglavnom potječu iz algoritamske teorije brojeva, poput faktorizacije velikih prirodnih brojeva ili logaritmiranja. Ideju javnog ključa prvi su javno iznijeli Whitfield Diffie i Martin Hellman 1976. godine (Dujella, 2016; Dujella, Maretić, 2007).

Za razliku od dešifriranja, *kriptoanaliza* ili *dekriptiranje* znanstvena je disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa. *Kriptologija* je pak grana znanosti koja obuhvaća kriptografiju i kriptoanalizu. Dok kriptografi razvijaju nove metode tajnog pisanja, kriptoanalitičari se trude u njihovim metodama pronaći pukotine koje će im omogućiti razbijanje tajnih poruka (Dujella, Maretić, 2007; Singh, 2003). Osnovna je pretpostavka kriptoanalize da kriptoanalitičar zna koji se kriptosustav koristi. To se zove *Kerckhoffsovo načelo*, a naziv je dobilo po Nizozemcu Augustu Kerckhoffsu (1835. – 1903.), autoru knjige *La Cryptographie militaire* (*Vojna kriptografija*). Postoje četiri osnovne razine kriptoanalitičkih napada. U prvom napadu kriptoanalitičar posjeduje samo šifrat od nekoliko poruka šifriranih pomoću istog algoritma i njegov je zadatak otkriti otvoreni tekst i ključ. U drugom napadu kriptoanalitičar posjeduje šifrat neke poruke, ali i njemu odgovarajući otvoreni tekst, a njegov je zadatak otkriti ključ ili algoritam za dešifriranje. U trećem napadu on ima mogućnost odabira teksta koji će biti šifriran te može dobiti njegov šifrat dok u četvrtom kriptoanalitičar dobije pristup alatu za dešifriranje pa može odabrati šifrat te dobiti odgovarajući otvoreni tekst. Nije pogrešno ni reći da postoji i peti napad u kojem dolazi do potkupljivanja, ucjene, krađe i sličnoga, ali taj napad zapravo ne pripada kriptoanalizi (Dujella, Maretić, 2007). Smatra se da znanstveno razdoblje kriptografije započinje djelom C. E. Shannona *Komunikacijska teorija tajnih sustava* iz 1949. Tim su djelom utemeljene osnove kriptologije kao znanstvene discipline[2].

[2] *Kriptografija*. Pribavljeno 15.5.2018., sa http://www.enciklopedija.hr/natuknica.aspx?ID=33988#start

3. POVIJEST KRIPTOGRAFIJE

3.1. Steganografija

Neki od najranijih zapisa o tajnom pisanju potječu još od Herodota koji u svojim *Historijama* spominje kako je, u sukobu između Grčke i Perzije u 5. st. pr. Kr., Grke spasilo upravo umijeće tajnog pisanja. Perzijsko je naoružavanje opazio Demarat koji je odlučio upozoriti Grke. On je, naime, skinuo vosak s par drvenih pisaćih tablica, napisao poruku na drvo te ju prekrio rastaljenim voskom. Tu je poruku uspjela pročitati Gorgona koja se sjetila sastrugati vosak, a zahvaljujući tom upozorenju, Grci su se počeli naoružavati i naposljetku su porazili Perzijance. Herodot također spominje i priču o Histajeju koji je Aristagoru Miletskog želio nagovoriti na bunu protiv perzijskoga kralja. Radi sigurnog prenošenja poruke Histajej je glasniku obrijao glavu na koju je napisao poruku te je pričekao da mu kosa ponovno naraste. Na taj je način glasnik mogao nesmetano putovati, a stigavši na cilj, obrijao bi glavu i pokazao poruku primatelju (Singh, 2003).

Steganografija se primjenjivala u različitim oblicima. Stari Kinezi pisali su poruke na tankoj svili koju bi zatim zgužvali u kuglicu i natopili voskom, a potom bi ju glasnik progutao. Steganografiji pripada i pisanje nevidljivom tintom koju je, prema Pliniju Starijem, moguće dobiti iz „mlijeka" biljke mlječike. „Takva je tinta kad se osuši nevidljiva, ali pri laganom zagrijavanju posmeđi. Slično se ponašaju i mnoge druge organske tekućine, i to zato što su bogate ugljikom pa lako izlučuju čađu" (Singh, 2003; 16–17). Moguće je zaključiti da takav način slanja poruke ima nedostatak – hvatanje poruke smjesta razrješava tajnu.

Sofisticiranija metoda steganografije bila je upotreba tzv. *mikrotočaka (microdots)*, odnosno vrlo malih fotografija skrivenih u tekstu ili na razglednicama, a koje su se pregledavale samo mikroskopom[3]. Ta je metoda bila popularna među špijunima tijekom i nakon Drugog svjetskog rata, dok se u suvremenom svijetu upotrebljava u samo nekim slučajevima. Zahvaljujući njoj, moguće je utvrditi koji je pisač korišten za ispis određene stranice. Pisač će dodati sitne točkice u jedinstvenom rasporedu na stranici, što se može vidjeti samo pod povećalom[4].

[3] *Atbash cipher*. Pribavljeno 15.5.2018., sa http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/atbash_cipher.pdf

[4] *Steganography*. Pribavljeno 15.5.2018., sa http://crypto.interactive-maths.com/steganography.html

3.2. Pojava kriptografije

Začetke kriptografije, odnosno šifriranja poruka, moguće je pronaći još kod starih Grka u 5. st. pr. Kr. Spartanci su upotrebljavali Skital (vidi sliku 2.), drveni štap ili palicu na koji bi namotali traku od kože ili pergamenta te na njega okomito napisali poruku. Kada bi se traka odmotala, poruka na njoj postala bi nečitljiv skup znakova koju bi glasnik mogao predati, a pročitati bi je mogao samo onaj koji je posjedovao Skital jednakog promjera (Barun i sur., 2008). Često su glasnici opasali traku poput remena sa slovima s unutrašnje strane kako bi nesmetano putovali (Sigh, 2003). To je bio prvi oblik transpozicijske šifre u kojem je štap uređaj za šifriranje i dešifriranje, a promjer štapa ključ.

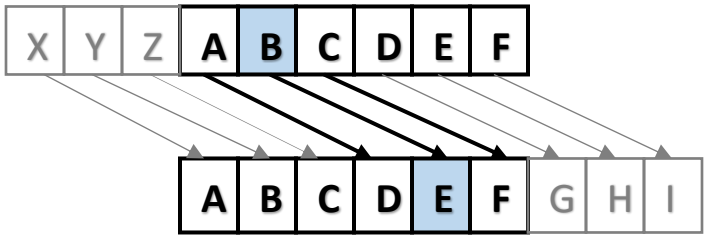
Slika 2. Skital s namotanom vrpcom i porukom (izvor: https://en.wikipedia.org/wiki/Scytale)

3.3. Povijest supstitucijske šifre

„Jedan od prvih opisa supstitucijske šifre nalazimo u Kama sutri, knjizi koju je u 4. st. naše ere napisao bramanski učenjak Vatsjajana, ali na temelju rukopisa koji sežu sve do 4. st. pr. Kr." (Singh, 2003: 19). Kama sutra savjetuje ženama da izuče šezdeset četiri vještine, kao na primjer kuhanje, odijevanje, masažu i pripravu miomirisa, a četrdeset peta na popisu jest *mlecchita-vikalpa,* to jest umijeće tajnog pisanja kojim žene mogu prikriti potankosti svojih ljubavnih veza.

Prvi se zapis o primjeni supstitucijske šifre u vojne svrhe pojavljuje u *Galskom ratu* (*De bello Galico*) znamenitog vojskovođe i državnika Julija Cezara. U njemu Cezar opisuje kako je poslao šifriranu poruku Ciceronu u kojoj su rimska slova bila zamijenjena grčkim zbog čega su neprijatelju postala nerazumljiva. U Svetonijevom *Životu Cezara LVI,* napisanom u 2. st., opisana

je jedna supstitucijska šifra kojom se služio Julije Cezar i koja je i danas poznata kao *Cezarova šifra* (Singh, 2003). Cezar se u komunikaciji sa svojim prijateljima i saveznicima koristio šifrom u kojoj su se slova otvorenog teksta zamjenjivala slovima koja su se nalazila tri mjesta dalje od njih u abecedi (A → D, B → E, vidi sliku 3). Na taj bi način zbunio neprijatelja koji bi presreo poruku (Dujella, 2016). On se koristio ključem za šifriranje i dešifriranje koji je iznosio K = 3 (tri mjesta dalje u abecedi), no u supstitucijskoj šifri ključ K može biti bilo koji prirodan broj iz skupa {1, 2, 3, …, 26}, ukoliko se radi o engleskom alfabetu ili, pak, {1, 2, 3, …, 30} ukoliko se radi o hrvatskoj abecedi. Dakle, Cezarova šifra samo je jedan oblik supstitucijske šifre, a više o njoj bit će riječ u sljedećim poglavljima.



Slika 3. Cezarova šifra

Jednostavnost supstitucijske šifre omogućila joj je da dominira umijećem tajnog pisanja čitavim prvim tisućljećem naše ere. Sav teret pao je na kriptoanalitičare, ljude koji su pokušavali razbiti supstitucijsku šifru. Mnogi su stari učenjaci smatrali da se supstitucijska šifra, zahvaljujući velikom broju mogućih ključeva, uopće i ne može razbiti te se stoljećima činilo da je upravo tako. Ipak, razvio se revolucionarni postupak na istoku, i to zahvaljujući briljantnom spoju lingvistike, statistike i pobožnosti (Singh, 2003).

Tehnika koja je nastala u 9. stoljeću iz pera znanstvenika Abu Jusufa Jakuba ibn Is-hak ibn as-Sabbaha ibn 'omran ibn Ismail al-Kindija, poznatog i kao „arapski filozof", otkrivena je tek 1987. godine u raspravi pod nazivom *Rukopis o dešifriranju kriptografskih poruka*. Opisana je u dva kratka odlomka: „Enkriptiranu poruku na poznatom nam jeziku možemo razriješiti i na sljedeći način. Potražimo neki drugi otvoreni tekst na istom jeziku, dovoljno dug da ispuni list ili dva papira, pa zatim izbrojimo pojedina slova i utvrdimo kako se često ponavljaju. Zatim uzmemo šifrirani tekst koji želimo odgonetnuti pa na isti način poredamo simbole. Tako ćemo naći slovo koje se najčešće ponavlja, pa ga sad zamijenimo „prvim" slovom uzorka, a ono koje se ponavlja odmah iza njega „drugim" slovom, a treći ćemo opet po redu među najučestalijim simbolima zamijeniti „trećim" slovom i tako dalje, dok tako ne poredamo sve simbole kriptograma koji želimo riješiti"

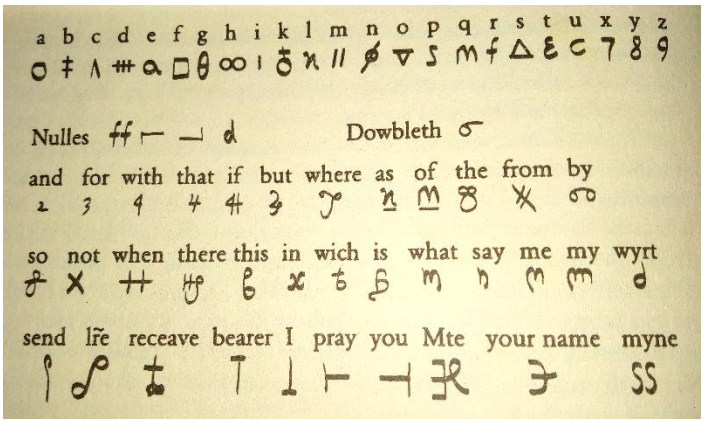
(Singh, 2003: 27). Al-Kindijeva metoda, poznata pod nazivom *frekvencijska analiza* ili *analiza učestalosti*, pokazuje da je zapravo nepotrebno provjeravati sve moguće ključeve. Poruku je moguće razmrsiti i bez toga i to analizom učestalosti pojedinih slova (simbola) u šifriranom tekstu. Al-Kindijev kriptoanalitički postupak ipak nije primjenjiv bezuvjetno. Naime, kod kratkih tekstova dolazi do značajnijeg otklona od standardnih frekvencija, pa ako su kraći od stotinu slova, dešifriranje može biti jako teško. S druge strane, dugi se tekstovi vjernije drže standardnih frekvencija, iako i tu ima iznimaka. Primjerice, roman *La Disparition* francuskog književnika Georgesa Pereca iz 1969. godine sastoji se od 200 stranica teksta bez ijedne riječi koja sadrži slovo „e", odnosno slovo koje je najučestalije u francuskom jeziku (Singh, 2003).

Prvi veliki europski kriptoanalitičar bio je Giovanni Soro kojeg su 1506. godine postavili za mletačkog šifrantskog tajnika. G. Soro bio je poznat diljem Italije pa su prijateljske države uhvaćene poruke slale njemu na kriptoanalizu. U međuvremenu zemlje su, svjesne slabosti jednostavne monoalfabetske supstitucijske šifre, težile k boljem. Jedno od najjednostavnijih poboljšanja svodilo se na uvođenje nula (*nulla*) ili praznih znakova, to jest slova i simbola koji nisu zamjenjivali prava slova, nego su zapravo bili prazna mjesta bez ikakva značenja. Te nule primatelju nisu stvarale teškoće zato što je on znao da ih treba preskočiti. One su, međutim, mogle smesti neprijatelja jer su ga bunile kad je poruku „napadao" frekvencijskom analizom (Singh, 2003). Osim toga, monoalfabetsku su supstitucijsku šifru pokušali pojačati i uvođenjem kodnih riječi. Već u 16. stoljeću kriptografi su uočili urođene slabosti kodova pa su se uglavnom oslanjali na šifre, a samo ponekad i na nomenklatore koje je koristila i škotska kraljica Marija Stuart.

3.4. Babingtonova urota i šifre Marije Stuart

Kraljici Mariji Stuart 15. listopada 1586. godine sudilo se zbog veleizdaje, a bila je optužena za planiranje umorstva kraljice Elizabete radi preotimanja engleske krune. Sir Francis Walsingham, glavni Elizabetin tajnik, dobio je zadatak dokazati Marijinu krivnju. Urotnici, za koje se sumnjalo da im je na čelu bila upravo Marija, bili su mladi katolički plemići, a nakana im je bila maknuti luteranku Elizabetu te je zamijeniti njezinom rođakinjom Marijom, pripadnicom svoje vjere. Marijin položaj, međutim, nije bio beznadan i to zato što se pobrinula da svoja dopisivanja s urotnicima obavlja pomoću šifre koja je njezine riječi pretvorila u besmisleni niz simbola. Pretpostavljala je da nitko ne može odgonetnuti šifru. No, na Marijinu nesreću, Walsingham nije

bio samo glavni tajnik nego i šef engleske špijunaže. On je došao do Marijina pisma i točno je znao tko bi ih mogao dešifrirati - Thomas Phelippes, najbolji stručnjak za razbijanje šifri u državi. Marijin život ovisio je o neslomljivosti šifre.



Slika 4. Nomenklator Marije Stuart sastavljen od šifrirne abecede i kodnih riječi (izvor: Singh, 2003)

Vođa urotnika bio je Anthony Babington. Urotnici su se suglasili da se Babingtonova urota (pod kojim je imenom kasnije postala poznata) ne može ostvariti bez Marijina blagoslova. Babington je zbog toga poslao šifriranu poruku Mariji u kojoj je pojasnio planove urotnika. Pritom se nije poslužio šifrom koja se temeljila tek na pukoj monoalfabetskoj supstituciji, nego na nomenklatoru (vidi sliku 4.) koji je bio sastavljen od 23 simbola koji su zamjenjivali slova alfabeta (s iznimkom j, v i w) te 35 simbola koji su predstavljali pojedine riječi i fraze. Osim toga, sadržavao je i četiri nule te simbol koji govori da se sljedeće slovo piše dvostruko („dowbleth", tj. dublet). Osoba koja je dostavljala pisma Mariji bio je Gilbert Gifford, za kojeg se kasnije ispostavilo da je bio dvostruki agent. Svaki puta kad bi Gifford preuzeo poruku za Mariju, najprije bi ju odnio Walsinghamu koji bi poruku prepisao i naizgled netaknutu vratio Giffordu koji bi ju potom predao Mariji. Kad je Phelippes dešifrirao Babingtonovu poruku Mariji, a u kojoj je jasno predložen atentat na Elizabetu, smjesta je taj optužujući tekst proslijedio Walsinghamu. Preostalo je bilo čekati Marijin odgovor. Marija je naposljetku odgovorila Babingtonu prihvativši plan urotnika i tako u biti potpisala vlastitu smrtnu presudu. Phelippes je također krivotvorio postskriptum Marijine poruke u kojem je zatražio imena ostalih urotnika na koji je Babinghton, ne znajući tko se zapravo krije iza Marijina postskriptuma, rado odgovorio. Urotnici su uhvaćeni i pogubljeni, a Marija je Stuart osuđena i pogubljena 8. veljače 1587. godine (Singh, 2003).

3.5. Povijest Vigenèreove šifre

Nova vrsta šifre pojavila se krajem 16. stoljeća, a njezino se korijenje može slijediti sve do Leona Battiste Albertija, firentinskog polihistora iz 15. stoljeća. On je predložio primjenu dviju ili više šifrirnih abeceda koje bi se izmjenjivale unutar jedne poruke i tako zbunjivale potencijalne kriptoanalitičare. Ključna prednost Albertijeva sustava bila je da se ista slova u otvorenom tekstu ne pojavljuju nužno kao ista slova u šifriranom tekstu.

Francuski diplomat Blaise de Vigenère upoznao se s Albertijevim spisima u Rimu. Razmotrio je njegovu ideju i pretvorio ju u moćnu novu šifru koja je danas poznata pod njegovim imenom. Snaga Vigenèreove šifre bila je u tom da poruku enkriptira pomoću ravno 26 šifrirnih abeceda, bila je neosjetljiva na frekvencijsku analizu te je imala mogućnost velikog broja ključeva. Ključ je, za razliku od supstitucijske šifre, bila riječ, a pošiljatelj i primatelj mogli su se dogovoriti da to bude bilo koja riječ u rječniku, svaka njihova kombinacija, a mogli su čak i izmišljati riječi (Singh, 2003). Godine 1586. Vigenère je svoj izum objavio u *Raspravi o tajnom pisanju* u kojoj se nalazilo sve što se u to vrijeme znalo o kriptografiji. U njoj je opisano više originalnih polialfabetskih sustava kojima pripada i Vigenèreova šifra. Primjena Vigenèreove šifre nastavila se širiti tijekom cijelog 17. i 18. stoljeće te posebno u 19. stoljeću zbog pojave brzojava, a bila je u primjeni tijekom važnih povijesnih događaja, poput Američkoga građanskog rata. Ta se šifra smatrala nerazmrsivom, pa je postala poznata pod nazivom *le chiffre indèchiffrable*[5] (Dujella, 2016; Singh, 2003).

Charles Babbage, britanski genij najpoznatiji po osnovnoj ideji suvremenog računala, još je za života uspio razbiti Vigenèreovu šifru. Stvorio je niz jednostavnih koraka za razbijanje dotad nerazmrsive šifre služeći se ponavljanjima u šifratu koja su ga dovela do određivanja duljine ključne riječi. Babbageovo otkriće prošlo je posve neopaženo, jer ga nije nikada objavio. Na svjetlo je dana izbilo tek u 20. stoljeću kad su znanstvenici pregledali Babbageove iscrpne bilješke. U međuvremenu je tu metodu neovisno otkrio Friedrich Wilhelm Kasiski. Sve od 1863., kad je objavio svoje revolucionarno kriptoanalitičko djelo *Die Geheimschriften und die Dechiffrirkunst* (*Tajna pisma i umijeće dešifriranja*), tu su tehniku zvali Kasiskijevim testom, dok se za Babbageov doprinos uglavnom nije znalo (Singh, 2003).

[5] franc. *nerazrješiva šifra*

3.6. Popularizacija kriptografije

Razvoj telegrafije potaknuo je komercijalno zanimanje za kriptografiju te stvaranje općeg zanimanja za tu disciplinu. Mladim zaljubljenicima iz viktorijanske Engleske često je bilo zabranjeno javno iskazivati osjećaje pa su slali enkriptirane poruke preko privatnih novinskih rubrika. „*Rubrike slomljenih srdaca*" („*Agony columns*"), kako su ih zvali, budile su radoznalost kriptoanalitičara koji su čitali pisma i pokušavali dešifrirati škakljive poruke.

Starogrčki historik Eneja Taktičar predložio je slanje tajnih poruka bušenjem rupica ispod određenih slova na naizgled bezazlenom pismu. Ta slova onda tvore tajnu poruku koju će primatelj lako pročitati. Dvije tisuće godina kasnije Britanci su posegnuli za tim postupkom zbog štednje na prekomjerno visokoj poštarini. Naime, ljudi su bušili rupice na naslovnim stranicama novina te ih slali poštom jer novine su se, za razliku od pisama, slale besplatno.

Sve veće zanimanje i oduševljenje javnosti kriptografskim tehnikama u 19. stoljeću dovela je do pojave kriptografije i u književnosti. U romanu *Put u središte Zemlje* Julesa Vernea junaci moraju dešifrirati pergament ispisan runskim pismom, odnosno supstitucijskom šifrom koja razbijena daje latinsku poruku, no dobiva smisao samo kad se čita naopako. U Britaniji je jedan od najboljih pisaca kriptografske beletristike bio sir Arthur Conan Doyle čiji je lik Sherlock Holmes bio stručnjak za kriptografiju. Najslavnije je Holmesovo razbijanje šifre ispričano u *Pustolovini plesača (The Adventure of the Dancing Men)* u kojoj je šifra sastavljena od shematski nacrtanih ljudi pri čemu svaka poza čovjeka predstavlja drugo slovo. S druge se strane Atlantika za kriptoanalizu zanimao Edgar Allan Poe koji je prevodio monoalfabetske šifre čitatelja filadelfijskog *Alexanderova Weekly Messengera* koji su u novine slali svoje šifrirane tekstove kako bi ih on razriješio. Godine 1843. E. A. Poe napisao je kratku priču o šiframa pod naslovom *Zlatni skarabej (The Gold Bug)*, a koju profesionalni kriptografi smatraju najboljim književnim djelom na tu temu. Iako je *Zlatni skarabej* čista fikcija, u 19. stoljeću se i stvarno dogodila priča s mnogo sličnih elemenata. U slučaju Bealeove šifre nalazi se kauboj s Divljeg zapada koji je stekao golem imetak, zakopano blago vrijedno 20 milijuna dolara i misteriozno enkriptirane listove koji opisuju gdje se ono nalazi. Brošura objavljena 1885. godine sadrži većinu priče te enkriptirane listove. Iako ima samo 23 stranice, ta je brošura ipak zbunjivala generacije kriptoanalitičara i osvajala generacije lovaca na blago. Blago nikada nije pronađeno, a razriješen je samo jedan enkriptirani list (druga Bealeova šifra) od ukupno tri (Singh, 2003).

3.7. Naprave za šifriranje

Prvi najpoznatiji kriptografski stroj bio je *šifrirni disk*, a izumio ga je u 15. stoljeću talijanski graditelj Leon Alberti, jedan od očeva polialfabetske šifre. Stroj se sastojao od dva bakrena diska učvršćenih iglom s alfabetom na obodima pri čemu je jedan bio malo veći od drugog. Takav šifrirni disk mogao je poslužiti za šifriranje poruke Cezarovom šifrom jer su se slova otvorenog teksta nalazila na vanjskom, a odgovarajuće šifrirano slovo na unutarnjem disku. Koristio se i u Američkom građanskom ratu. Alberti je predložio zakretanje diska za vrijeme pisanja poruke čime se zapravo umjesto monoalfabetske dobivala polialfabetska šifra, i to najčešće Vigenèreova (Singh, 2003).

Sljedeću napravu, *Jeffersonov kotač za šifriranje* (vidi sliku 5.), izumio je američki državnik Thomas Jefferson krajem 18. stoljeća. Naprava je bila ispred svog vremena, a američka ju je vojska počela upotrebljavati tek 1922. godine. Naprava se sastojala od drvenog cilindra s rupom u sredini kroz koju je bila provučena željezna os. Cilindar je bio presječen na 26 manjih cilindara (*diskova*) jednakih širina koji su se mogli neovisno okretati oko zajedničke osi. Na vanjštini svakog diska nalazilo se 26 jednakih kvadratića s 26 slova engleskog alfabeta. Da bi šifrirao otvoreni tekst, pošiljatelj je morao podijeliti tekst na blokove od po 26 slova. Blok se šifrirao tako da se rotiranjem diskova u jednom od 26 redaka dobije otvoreni tekst. Tada se za šifrat mogao izabrati bilo koji od preostalih 25 redaka. Osnovna ideja Jeffersonova kotača bila je stvaranje polialfabetskih kriptosustava s ključnom riječi ogromne duljine (obično više od 10^{10}) (Dujella, Maretić, 2007).

Godine 1915. Amerikanac Edward Hugh Hebern izumio je *električni stroj za kodiranje* (vidi sliku 5.) koji se sastojao od dva električna pisaća stroja spojena pomoću 26 žica. Na jednom se stroju tipkao otvoreni tekst, a drugi bi automatski ispisivao šifrat. Budući da je položaj žica ostajao isti tijekom šifriranja, njime se dobila samo monoalfabetska šifra. Dvije godine kasnije E. H. Hebern ugradio je u uređaj 5 rotora kojima je postigao polialfabetsku šifru s periodom $26^5 \approx 10^7$ (Dujella, Maretić, 2007). Iste godine Gilbert Vernam, zaposlenik tvrtke AT & T, izradio je stroj za stvaranje pseudoslučajnih nizova znakova koji bi se koristili kao ključ u šifri nazvanoj *jednokratna bilježnica* (engl. *One-Time Pad*, poznata i kao Vernam šifra). Za tu se vrstu šifre govorilo da jedina jamči apsolutnu sigurnost pa su je često nazivali i „svetim gralom" kriptografije. Ona se koristi

slučajnim ključem iste duljine kao originalan tekst, stoga kriptoanalitičar nema apsolutno nikakvo uporište za razbijanje šifre (Wijesekera, 2011).

3.8. Enigma

Nijemac Artur Scherbius 1918. godine izumio je rotorsku napravu koja je zapravo bila električna verzija Albertijeva šifrirnog diska, a nazvao ju je Enigma (vidi sliku 5.). Razlikovala se od drugih rotorskih naprava po tome što su pomacima rotora upravljali zupčanici, pa se moglo postići da ti pomaci imaju nepravilan slijed (Dujella, Maretić, 2007; Singh, 2003).

Slika 5. Jeffersonov kotač za šifriranje, električni stroj za kodiranje i Enigma

(izvor: https://web.math.pmf.unizg.hr/~duje/kript/naprave.html)

Enigma se sastojala od tipkovnice s 26 tipaka poput pisaćeg stroja, zaslona s 26 žaruljica za prikaz šifriranog izlaza i tri mehanička rotora, a napajala se pomoću ugrađene baterije. Pritiskom na tipku zatvarao se strujni krug i palila odgovarajuća žaruljica koja je prikazivala šifrirano slovo. Rotori su se sastojali od diskova s 26 kontakata kružno smještenih na obodu svake strane. „Izlaz" jednog rotora predstavljao je „ulaz" drugog, a „izlaz" trećeg rotora bio je povezan na reflektor, statični mehanički disk sličan rotoru čija je zadaća bila da električni signal šalje natrag kroz rotore, ali drugim putem (Čavrak, 2004; Dujella, Maretić, 2007).

Ukoliko je neki operater želio poslati tajnu poruku, prije nego što je započeo enkripciju, morao je rotore zaokrenuti u neki početni položaj. Taj početni položaj predstavljao je zapravo ključ šifre i obično ga je diktirala knjiga šifri u kojoj su bili nabrojeni ključevi za svaki pojedini dan, a koja je bila dostupna svima unutar komunikacijske mreže. Da bi mogao dešifrirati poruku, i primatelj je morao imati i Enigmu i primjerak knjige šifri. Utipkavajući šifrirani tekst u Enigmu,

primatelj bi dobio otvoreni tekst jer su šifriranje i dešifriranje bili zrcalni postupci, a za tu je lakoću dešifriranja bio zaslužan baš reflektor. Scherbius je odlučio poboljšati sigurnost svog izuma povećanjem broja početnih položaja, a time i broja mogućih ključeva. Uveo je mogućnost vađenja i zamjene rotora te razvodnu ploču koja je pošiljatelju omogućavala da umetne vodove koji će zamijeniti mjesta pojedinim slovima prije ulaska u rotor. Operater Enigme imao je šest kablova što znači da je šest parova slova moglo zamijeniti mjesta. Raspored rotora te slova kojima treba zamijeniti mjesta također su tvorila ključ šifre (Singh, 2003).

Ukupan broj ključeva koji je omogućavala takva Enigma moguće je izračunati. Položaj rotora omogućavao je $26 \cdot 26 \cdot 26 = 26^3 = 17\,576$ početnih položaja. Redoslijed rotora omogućavao je $3 \cdot 2 \cdot 1 = 6$ puta više početnih položaja (123, 132, 213, 231, 312, 321). Razvodna ploča omogućavala je spajanjem šest parova slova 100 391 791 500 početnih položaja. Ukupno, kada se pomnože dobivena tri broja $17\,576 \cdot 6 \cdot 100\,391\,791\,500$ dobije se više od 10^{16} ključeva. Ne čudi onda da je u Enigminoj reklamnoj brošuri sredinom 1920. godins pisalo: „Ako bi čovjek bio u mogućnosti podesiti novi ključ svake minute, danju i noću, trebalo bi mu 4000 godina da isproba sve mogućnosti jednu za drugom" (Taylor & Francis, Inc., 2001).

Godine 1925. Scherbius je počeo masovno proizvoditi Enigmu, a postojale su različite vojne i komercijalne inačice te naprave. Posebno je bila poznata japanska inačica koju su Amerikanci nazivali Purple. U dva desetljeća njemačka je vojska kupila preko trideset tisuća Enigmi. Činilo se da će Enigma odigrati ključnu ulogu u nacističkoj pobjedi u Drugom svjetskom ratu, ali je umjesto toga postala bitnim elementom Hitlerova pada (Dujella, Maretić, 2007; Singh, 2003).

Akcijom obavještajne službe u kojoj je francuski tajni agent kodnog imena Rex stupio u vezu s Hansom-Thilom Schmidtom, Nijemcem čiji je brat Rudolph odobrio primjenu Enigme u njemačkoj vojsci, započelo je razbijanje Enigme. Dana 8. studenog 1931. godine, uz naknadu od 10 000 njemačkih maraka, Schmidt je dopustio fotografiranje dvaju dokumenata s uputama za upotrebu Enigme (*Gebrauchsanweisung für die Chiffriermaschine Enigma* i *Schlüsselanleitung für die Chiffriermaschine Enigma*). Saveznici su tada mogli stvoriti točnu repliku njemačke vojne Enigme. S druge strane, Nijemci su poduzeli još jednu dodatnu mjeru opreza pa su zahvaljujući dnevnom ključu slali novi ključ poruke, i to za svaku poruku posebno. Taj novi ključ imao je iste

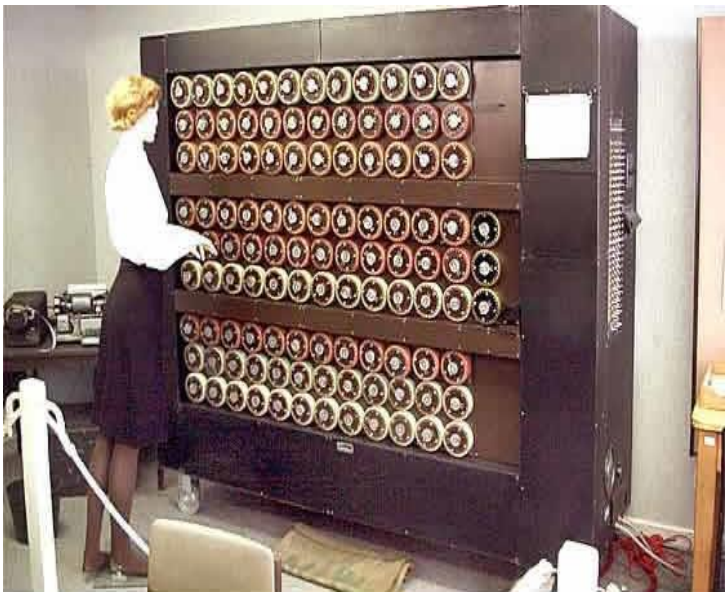
spojeve na razvodnoj kutiji i isti redoslijed rotora, ali različitu orijentaciju svakog rotora (Čavrak, 2004; Singh, 2003).

Budući da su Francuzi i Poljaci po završetku Prvog svjetskog rata potpisali ugovor o vojnoj suradnji, te su informacije završile u rukama poljskog ureda za kriptografiju *Biuro Szyfrów*. Marian Rejewski, dvadesettrogodišnjak koji je završio studij statistike i tečno govorio njemački, bio je jedan od zaposlenika tog ureda. Njegova se strategija napada na Enigmu temeljila na činjenici da je ponavljanje neprijatelj sigurnosti. Najočitije se ponavljanje pojavljivalo kod enkripcije ključa poruke koja se dvaput ponavljala na početku svake poruke radi izbjegavanja pogrešaka izazvanim radiosmetnjama ili operaterovom omaškom. M. Rejewski nije znao odrediti dnevni ključ, ali je mogao sastaviti tablicu odnosa te tražiti obrasce i stvoriti lance slova:

A→F→W→A C→H→G→O→Y→P→C

B→Q→Z→K→V→E→I→B J→M→X→S→T→N→U

Orijentirao se samo na rotore, odnosno na njihov redoslijed i položaj pa je zapravo proučavao samo $6 \cdot 17\,576 = 105\,456$ mogućih konfiguracija rotora i njihovu povezanost s brojem veza u nekom skupu lanaca. Njegova je skupina izradila katalog svih konfiguracija rotora zajedno s lancima koje stvaraju te su tako prilikom presretanja poruke znali o kojoj je konfiguraciji rotora riječ. Potrebno je bilo samo zaključiti koji su parovi slova povezani kablovima, a to je uspio tako da je iz razvodne ploče iskopčao sve kablove, utipkao poruku te logički zaključio na temelju dobivenih riječi koja su slova zamijenjena. Time je imao sve podatke koji su mu otkrivali dnevni ključ pa je mogao dešifrirati sve poruke pristigle tog dana. Osmislio je mehanički uređaj, tzv. bombu, koji je automatski provjeravao svaku od 17 576 mogućih postavki rotora. Paralelno je radilo šest bombi zbog nepoznatog redoslijeda rotora od kojih je svaka predstavljala jednu permutaciju poretka diskova rotora te koje su zajedno tvorile jedinicu visoku oko metar (vidi sliku 6.), a koja je dnevni ključ mogla pronaći za otprilike dva sata (Čavrak, 2004; Singh, 2003).



Slika 6. Muzejski eksponat, voštana figura prikazuje pripadnicu ženske kraljevske mornarice (Wrens) koja upravlja replikom bombe (izvor: http://e.math.hr/old/enigma/index.html)

Shvativši ratnu opasnost, Britanci su, poučeni iskustvom Poljaka, osnovali *Vladin ured za šifre* (*Government Code and Cypher School*) sa sjedištem u Bletchley Parku te su počeli novačiti matematičare i ostale znanstvenike. Alan Turing, koji je često nazivan ocem modernog računarstva, te Gordon Welchman, obojica matematičari sa sveučilišta Cambridge, pridružili su se uredu. Turingova je zadaća bila pronaći alternativni način napada na Enigmu, postupak koji neće ovisiti o ponovljenom ključu poruke. Proučavajući tako stare dešifrirane poruke, uočio je da Nijemci svakodnevno nedugo poslije 6 sati ujutro šalju šifrirane vremenske izvještaje u kojima se uvijek nalazila riječ WETTER[6]. Alan je Turing zbog toga konstruirao stroj za provjeru konfiguracija Enigminih rotora koristeći se načelom pretpostavljenog sadržaja poruke („cribs"), a kojim je dolazio do ključa poruke. Njemački operateri često su kao ključ odabirali tri uzastopna slova s tipkovnice ili su se često koristili istim ključem, a nijedno se slovo nije moglo šifriranjem preslikati u to isto slovo. To su bili nedostaci koji su pomogli kriptoanalitičarima (Čavrak, 2004; Singh, 2003).

„Razbijanje šifre njemačke Enigme bilo je samo dio obavještajne operacije pod kodnim imenom Ultra. Dokumenti Ultre, a među kojima su bile i dešifrirane talijanske i japanske poruke, pribavile su Saveznicima jasnu prednost na svim glavnim bojištima. Pri svemu je tome, međutim,

[6] njem. *vrijeme*

od ključne važnosti bilo i sve te informacije iskoristiti tako da se u njemačkoj vojsci ne probudi sumnja" (Singh, 2003: 137).

Postignuća Bletchleya ostala su strogo čuvanom tajnom i poslije 1945. godine, a tisuće ljudi koje su pripomogle stvaranju Ultre nisu dobile nikakvo priznanje za svoje zasluge. Nakon tri desetljeća šutnje kapetan F. W. Winterbotham, čovjek zadužen za raspodjelu Ultrinih informacija, napisao je knjigu o tajnom uredu Bletchley Park pod nazivom *The Ultra Secret* objavljenu 1974. godine kojom je šifrolomcima iz Bletchleya odano zasluženo priznanje. Nažalost, Alan Turing nije poživio dovoljno dugo da primi javno priznanje. Poslije rata, umjesto da ga proglase herojem, počeli su ga progoniti zbog homoseksualnosti, a britanska mu je država oduzela dozvolu za tajni rad. Bio mu je zabranjen rad na istraživačkim projektima kojima je cilj bio razvoj računala, a na kojima je radio prije rata. Dana 7. lipnja 1954. godine jedan od istinskih genija kriptoanalize završio je svoj život samoubojstvom.

3.9. Kriptografija u Hrvatskoj

Djelo *Cryptographia nova seu Ars cryptographica noviter inventa* (*Nova kriptografija ili nedavno izmišljena kriptografska vještina*) objavljeno je 1732. godine, a napisao ju je hrvatski latinist Ivan Krstitelj Prus. U romanu Julesa Vernea *Mathias Sandorf* iz 1885. godine transpozicijska šifra igra važnu ulogu. U njemu ugarski plemići Mathias Sandorf, Stjepan Bathory i Ladislav Zathmar pripremaju urotu 1867. godine za odcjepljenje Mađarske od Austro--Ugarske. Veliki dijelovi romana odvijaju se u Istri i Dubrovniku, a posebno je detaljan opis pazinskog Kaštela i jame uključujući i ilustracije Leona Benetta prema fotografijama koje je J. Verne dobio od tadašnjeg pazinskog gradonačelnika Giuseppea Cecha (Dujella, 2016; Kapitanović, 2012).

Danas se kriptografija može pronaći kao redovan ili izborni predmet na fakultetima i to na Odjelu za matematiku u Osijeku, na Matematičkom odsjeku PMF-a u Zagrebu, PMF-a u Splitu, FER-a u Zagrebu, FOI-a u Varaždinu te u državnim agencijama za sigurnost. Primjerice, na Odjelu za matematiku u Osijeku kolegij *Kriptografija i sigurnost sustava* izborni je predmet. Ipak, pojavljuje se zainteresiranost za kriptografiju i izvan fakulteta i državnih agencija za sigurnost. Škola kriptografije Enigma započela je s radom 2016. godine u Tehničkom muzeju Nikola Tesla u Zagrebu. Sama ideja o osnivanju škole potekla je od poznatog matematičara Tonija Miluna i

popularizatora znanosti Krešimira Čanića u suradnji sa Tehničkim muzejom Nikola Tesla i udrugom HUM. Sastavni dijelovi radionice Spartanska su šifra (Skital), Cezarova šifra, Masonski kod (Pigpen šifra) te Enigma, a radionice su namijenjene prvenstveno djeci, ali i odraslima. Moguće je preuzeti simulator Enigme na mrežnim stranicama škole te naručiti materijale potrebne za izradu seta za kriptografiju[7]. Krešimiru Čaniću, voditelju Škole kriptografije Enigma, 21. prosinca 2016. godine svečano je uručena Državna nagrada tehničke kulture Faust Vrančić za 2015. godinu.

[7] *Škola kriptografije Enigma*. Pribavljeno 15. 5. 2018., sa http://kriptografija.udruga-hum.hr/index.php?section=about

4. METODE ŠIFRIRANJA I DEŠIFRIRANJA

4.1. Supstitucijska šifra

Monoalfabetska supstitucijska šifra ili šifra jednostavne zamjene supstitucijska je šifra u kojoj se šifrirna abeceda sastoji od slova ili simbola ili njihove kombinacije (Singh, 2003). Kao što je već spomenuto, znameniti rimski vojskovođa Julije Cezar u komunikaciji sa svojim prijateljima koristio se šifrom u kojoj su se slova otvorenog teksta zamjenjivala slovima što su se nalazila tri mjesta dalje od njih u alfabetu (A ↦ D, B ↦ E, C ↦ F itd.). Ukoliko se alfabet ciklički nastavlja, tj. nakon zadnjeg slova Z, ponovo dolaze A, B, C i koristi se engleski (međunarodni) alfabet od 26 slova (hrvatska slova Č, Ć , Đ, DŽ, LJ, NJ, Š, Ž, zamijenjena su redom slovima C, C, DJ, DZ, LJ, NJ, S, Z), tada postoji prirodna podudarnost između slova alfabeta (A - Z) i cijelih brojeva (0 - 25). Skup $\mathbf{Z}_{26} = \{0, 1, 2, ..., 25\}$, uz operacije $+_{26}$ i $\cdot_{26}$, zadovoljava aksiome matematičke strukture koja se naziva *prsten*. To znači da su operacije zbrajanja i množenja zatvorene (rezultat je ponovno iz $\mathbf{Z}_{26}$), komutativne ($a +_{26} b = b +_{26} a$, $a \cdot_{26} b = b \cdot_{26} a$) i asocijativne ($(a +_{26} b) +_{26} c = a +_{26} (b +_{26} c)$, $(a \cdot_{26} b) \cdot_{26} c = a \cdot_{26} (b \cdot_{26} c)$) te vrijedi distributivnost množenja prema zbrajanju ($(a +_{26} b) \cdot_{26} c = (a \cdot_{26} c) +_{26} (b \cdot_{26} c)$). Broj 0 neutralni je element za zbrajanje ($a +_{26} 0 = 0 +_{26} a = a$) te svaki element a ima suprotni element (aditivni inverz) -a (za $a \neq 0$ to je broj 26 - a, jer vrijedi $a +_{26} (26 - a) = (26 - a) +_{26} a = 26 \bmod 26 = 0$). Nadalje, broj 1 neutralni je element za množenje ($a \cdot_{26} 1 = 1 \cdot_{26} a = a$), no samo neki elementi a imaju multiplikativni inverz a^{-1}, tj. element za koji vrijedi $a \cdot_{26} a^{-1} = a^{-1} \cdot_{26} a = 1$. Ako dva cijela broja a i b daju isti ostatak pri dijeljenju s 26, tada vrijedi $a \equiv b \pmod{26}$. Prema Dujella, Maretić (2007) *Cezarova šifra* definirana je na sljedeći način:

Definicija 2. Neka je $P = C = K = \mathbf{Z}_{26}$. Za $0 \leq K \leq 25$ definiramo

$$e_K(x) = (x + K) \bmod 26, \quad d_K(y) = (y - K) \bmod 26.$$

Za K = 3 dobiva se originalna Cezarova šifra u kojoj odnos otvorene i šifrirne abecede izgleda ovako:

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

Šifrirna 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

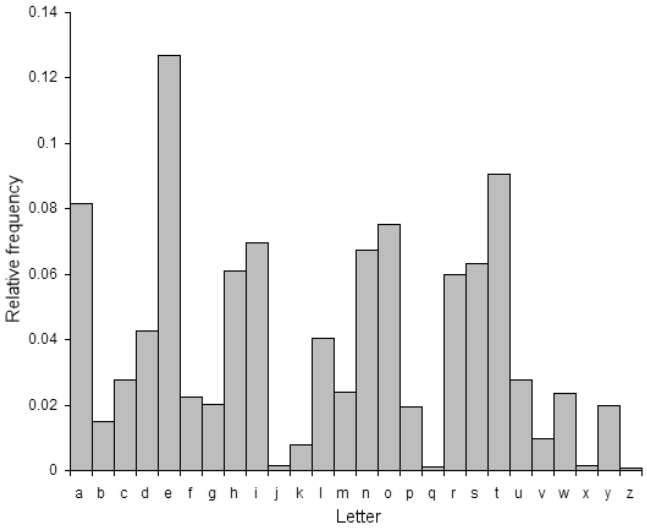
Cezarova je šifra poseban slučaj *supstitucijske šifre* koja je prema Dujella, Maretić (2007) definirana na sljedeći način:

Definicija 3. Neka je $P = C = \mathbf{Z}_{26}$. Prostor ključeva K se sastoji od svih permutacija skupa {0, 1, 2, ... , 25}. Za svaku permutaciju $\pi \in K$ definiramo $e_\pi(x) = \pi(x)$, $d_\pi(y) = \pi^{-1}(y)$, gdje je π^{-1} inverzna permutacija od π.

Jedna od metoda dekriptiranja supstitucijske šifre jest ispitivanje svih mogućih ključeva sve dok se ne dobije neki smisleni tekst. Ta je metoda opravdana jer je broj ključeva mal i iznosi 26. Na primjer, ako šifrat glasi „XENRSTMW", tada za K = 1 otvoreni tekst glasi WDMQRSLV, za K = 2 glasi VCLPQRKV, za K = 3 glasi UBKOPQJT, a za K = 4 glasi TAJNOPIS, odnosno jedina riječ koja ima značenje (Dujella, 2016). Supstitucijsku šifru moguće je dekriptirati koristeći se *frekvencijskom analizom ili analizom frekvencije slova* u kojoj je, kao što je Al-Kindi napomenuo, potrebno prebrojati pojavljivanje svakog slova u šifratu te distribuciju slova u šifratu usporediti s poznatim podatcima o distribuciji slova u jeziku na kojem se pretpostavlja da je napisan otvoreni tekst. Velika je vjerojatnost da će najučestalija slova šifrata odgovarati najučestalijim slovima jezika, a vjerojatnost je veća što je dulji šifrat. Također, korisni mogu biti i podatci o najčešćim bigramima (parovima slova) i trigramima (nizovima od tri slova) u jeziku (Dujella, 2016).

Frekvencije slova (u promilima) za hrvatski jezik (hrvatska slova Č, Ć , Đ, DŽ, LJ, NJ, Š, Ž zamijenjena su redom slovima C, C, DJ, DZ, LJ, NJ, S, Z) iznose: A (115), I (98), O (90), E (84), N (66), S (56), R (54), J (51), T (48), U (43), D (37), K (36), V (35), L (33), M (31), P (29), C (28), Z (23), G (16), B (15), H (8), F (3); za engleski jezik iznose (vidi sliku 7): E (127), T (91), A (82), O (75), I (70), N (67), S (63), H (61), R (60), D (43), L (40), C (28), U (28), M (24), W (23), F (22), G (20), Y (20), P (19), B (15), V (10), K (8), J (2), Q (1), X (1), Z (1); a za njemački jezik iznose: E (175), N (98), I (77), R (75), S (68), A (65), T (61), D (48), H (42), U (42), L (35), G (31), O (30), C (27), M (26), B (19), F (17), W (15), K (15), Z (11), P (10), V (9), J (3), Y (1), X (0), Q (0). Najčešći bigrami u hrvatskom jeziku su: JE (2. 7 %), NA (1. 5 %), RA, ST, AN, NI, KO, OS, TI, IJ, NO, EN i PR, a najčešći su trigrami: IJE (0. 6 %), STA, OST, JED, KOJ, OJE i JEN. U engleskom jeziku najčešći bigrami su: TH (3. 2 %), HE (2. 5 %), AN, IN, ER, RE, ON, ES, TI i AT, a trigrami: THE (3. 5 %), ING (1. 1 %), AND, ION, TIO, ENT, ERE i HER. U njemačkom jeziku najučestaliji bigrami su: ER (4. 1 %), EN (4.0 %), CH, DE, EI, ND, TE, IN, IE i GE, a trigrami: EIN (1. 2 %), ICH (1. 1 %), NDE, DIE, UND, DER, CHE i END[8].

[8] *Frekvencija slova.* Pribavljeno 15.5.2018., sa https://www.mathos.unios.hr/index.php/nastava/matematika-i-racunarstvo/274



Slika 7. Frekvencija slova u engleskom jeziku (izvor http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/letter_frequencies.pdf)

Također, za alfabet šifrata, odnosno šifrirne abecede, može biti izabrana bilo koja permutacija slova A, B, …, Z te je tako svako slovo otvorenog teksta zamijenjeno (supstituirano) sa slovom koje se nalazi u tablici ispod njega. Tada postoji čak 26! $=1 \cdot 2 \cdot 3 \cdot \ldots \cdot 26 \approx 4 \bullet 10^{26}$ mogućih ključeva tako da je napad ispitivanjem svih mogućih ključeva praktički nemoguć, čak i uz pomoć računala. Ljepota je takve šifre u tom što se lako primjenjuje, no ipak nudi visok stupanj sigurnosti. Pošiljatelj može vrlo lako definirati ključ, potrebno je samo poredati 26 slova alfabeta, a neprijatelj ipak ne može provjeriti sve ključeve (Dujella, Maretić, 2007; Singh, 2003).

Postoji, međutim, i još jednostavniji ključ. Umjesto da šifrirna abeceda bude izabrana nasumičnim premetanjem otvorene abecede, potrebno je izabrati *ključnu riječ* ili *frazu,* recimo JULIJE CEZAR. Najprije treba iz nje ukloniti razmake i ponovljena slova, pa tako dobiti JULIECZAR, a onda na zadnje slovo nadovezati ostatak alfabeta bez ponavljanja slova. Tada odnos otvorene i šifrirne abecede izgleda ovako:

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

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

Prednost je takvog slaganja šifrirne abecede u tome što je ključnu riječ ili frazu lako zapamtiti, a potom je vrlo lako generirati čitavu abecedu (Singh, 2003).

Kao što je napomenuto, jedan je oblik supstitucijske šifre i kodiranje u kojem kodovi mogu biti, primjerice: ubij = D, general = Ó, smjesta = 08, ucijeni = P, kralj = ?, danas = 73, zarobi = J,

ministar = ∅, noćas = 28. Pomoću vrlo ograničenog skupa kodnih riječi moguće je pisati jednostavne poruke, primjerice:

Otvorena poruka: noćas ubij kralja

Enkodirana poruka: 28 D ?

Kodovi ipak imaju dva praktična nedostatka, a to su ograničenost riječi i nemogućnost kodiranja više tisuća riječi jer bi tada knjiga kodnih riječi morala imati na stotine stranica pa bi se pretvorila u svojevrstan rječnik. Međutim, ukoliko bi se neprijatelj domogao te knjige, posljedice bi bile katastrofalne. Trebala bi se napisati u potpunosti nova knjiga kodnih riječi i ponovno podijeliti u komunikacijskoj mreži. Za razliku od toga, ako neprijatelj uspije doći do ključa šifre, dovoljno je samo promijeniti ključ koji se lako pamti i lako distribuira. Nomenklator, o kojemu je ranije bilo riječ, nije mnogo sigurniji od jednostavne supstitucijske šifre, i to zato što je glavninu teksta moguće dešifrirati frekvencijskom analizom, a preostale je kodirane riječi moguće naslutiti iz konteksta (Singh, 2003).

4.2. Transpozicijska šifra

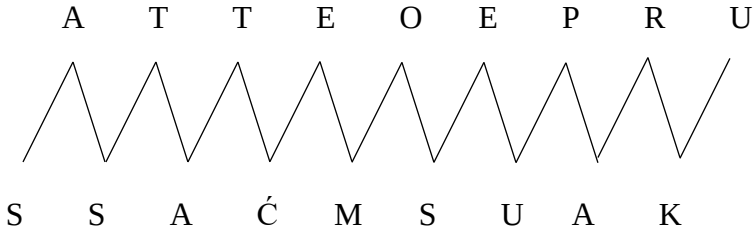
Ideja je transpozicijske šifre da se elementi otvorenog teksta ostave nepromijenjeni, ali da se promijeni njihov međusobni položaj. Često se šifrat nastao transpozicijom naziva *anagram*. Kod vrlo kratkih poruka, kao na primjer onih koje se sastoje od samo jedne riječi, ta je metoda prilično nesigurna zato što se malen broj slova može ispremještati na samo malen broj načina. Tako se, primjerice, tri slova daju ispremještati na samo $3 \cdot 2 \cdot 1 = 6$ načina, na primjer nos, nso, ons, osn, sno, son. Ukoliko postupno povećamo broj slova, broj mogućih kombinacija eksplozivno raste zbog čega povratak na početnu poruku i nije moguć bez točnog poznavanja samog procesa miješanja (Dujella, Maretić, 2007; Singh 2003). Formalna je definicija *transpozicijske šifre* prema Dujella, Maretić (2007) sljedeća:

Definicija 4. Neka je m fiksan prirodan broj. Neka je $P = C = (\mathbf{Z}_{26})^m$, te neka se K sastoji od svih permutacija skupa $\{1, 2, \ldots, m\}$. Za $\pi \in K$ definiramo

$$e_\pi (x_1, x_2, \ldots, x_m) = (x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(m)}), \quad d_\pi(y_1, y_2, \ldots, y_m) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, \ldots, y_{\pi^{-1}(m)}).$$

Da bi transpozicija imala smisla, premještanje slova mora se odvijati u skladu s jasnim pravilom, unaprijed dogovorenim s primateljem, no nepoznatim neprijatelju. Tako je primjerice poruke moguće slati takozvanom *izmjeničnom transpozicijom,* koja često nosi naziv i *Cik-cak šifra,* u kojoj

se slova poruke naizmjence pišu u gornji i donji redak pa se onda oni nadovezuju jedan na drugi (Singh, 2003). Primjerice, poruka: „SASTAT ĆEMO SE U PARKU" nakon transpozicije glasi: „ATTEOEPRU SSAĆMSUAK" (vidi sliku 8.).



Slika 8. Postupak izmjenične transpozicije

4.3. Vigenèreova šifra

Kod supstitucijske šifre svakom slovu otvorenog teksta odgovara jedinstveno slovo šifrata, a takve se šifre zovu monoalfabetske. No, Vigenèreova šifra pripada polialfabetskim kriptosustavima jer 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, a prema Dujella, Maretić (2007) definirana je na sljedeći način:

Definicija 5. Neka je m fiksan prirodan broj. Definiramo $P = C = K = (\mathbf{Z}_{26})^m$.
Za ključ K = $(k_1, k_2, \dots, k_m)$, definiramo

$$e_K(x_1, x_2, \dots, x_m) = (x_1 +_{26} k_1, x_2 +_{26} k_2, \dots, x_m +_{26} k_m),$$
$$d_K(y_1, y_2, \dots, y_m) = (y_1 -_{26} k_1, y_2 -_{26} k_2, \dots, y_m -_{26} k_m).$$

Kod te šifre osnovni elementi otvorenog teksta i šifrata „blokovi" su od po m slova, odnosno za šifriranje potrebna je ključna riječ, a ono se zapravo provodi „slovo po slovo" pa nije nužno nadopuniti zadnji blok ako broj slova u otvorenom tekstu nije djeljiv s m. Ako postoji prirodna podudarnost između slova alfabeta (A − Z) i cijelih brojeva (0 − 25) tada vrijedi:

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

Ukoliko je, na primjer, ključna riječ ZEC, odnosno m = 3, tada se otvoreni tekst MATEMATIKA šifrira Vigenèreovom šifrom na sljedeći način:

	12	0	19	4	12	0	19	11	10	0
$+_{26}$	25	4	2	25	4	2	25	4	2	25
	11	4	21	3	16	2	18	15	12	25

pa šifrat glasi LEVDQCSPMZ. Vidljivo je da se prvo slovo M preslikalo u L, a drugo slovo M u Q. Ključ se ponavlja u nedogled pa prema podjeli šifri, s obzirom na način na koji se obrađuje otvoreni tekst, ta šifra pripada blokovnim šiframa. Pri šifriranju može se koristiti tzv. Vigenèreovim kvadratom u kojem je jednostavno pronaći stupac sa slovom M i redak sa slovom Z te zaključiti da je slovo L šifrat jer se ondje stupac i redak preklapaju (vidi sliku 9.). Ključna riječ trebala bi biti što dulja kako bi šifriranje bilo sigurnije (Dujella, 2016). Vigenèreova šifra jedan je od najpopularnijih kriptosustava u povijesti. Njezina je velika prednost neosjetljivost na frekvencijsku analizu jer određeno slovo šifriranog teksta može predstavljati niz slova otvorenog teksta, a ne samo jedno. Kriptoanalitičar takvu poruku neće moći razbiti traženjem svih mogućih ključeva naprosto zato što je njihov broj prevelik. Frekvencije su slova uravnoteženije, i to zbog ključne riječi koja prebacuje između pojedinih šifrirnih abeceda (Singh, 2003).

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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 9. Vigenèreov kvadrat

Kasiskijev test temelji se na činjenici da će dva identična odsječka otvorenog teksta biti šifrirana na isti način ukoliko se njihove početne pozicije razlikuju za neki višekratnik od m, pri čemu je m duljina ključa. Obrnuto, ako postoje dva identična segmenta u šifratu, duljine barem 3, tada je vrlo vjerojatno da oni odgovaraju identičnim odsječcima otvorenog teksta, tj. potrebno je tražiti parove identičnih odsječaka duljine barem 3 te zabilježiti udaljenosti između njihovih

početnih položaja čime se zapravo određuje duljina ključne riječi m. Šifrirani tekst tada se razdijeli u m dijelova. Svaki od tih dijelova šifriran je monoalfabetskom supstitucijom određenom jednim slovom ključne riječi pa se utvrđuje distribucija frekvencija za pojedino slovo. Primjerice, provjeravaju se distribucije frekvencija za slova na poziciji 1, m + 1, 2m + 1, 3m + 1, … Zatim slijede slova na poziciji 2, m + 2, 2m + 2, 3m + 2, …, a na kraju i slova na poziciji m, 2m, 3m, … Ukoliko je m = 4, to znači da se provjeravaju distribucije frekvencija za 1., 5., 9., 13, … slovo, zatim za 2., 6., 10., 14, … i na kraju za 4., 8., 12., … slovo. Dobivene distribucije ponovno se uspoređuju sa standardnom distribucijom radi određivanja pomaka i ključne riječi, a zatim slijedi dešifriranje cijelog teksta. Druga metoda za određivanje duljine ključa upotrebljava tzv. *indeks koincidencije*. Taj je pojam 1920. godine uveo William Friedman u knjizi *Indeks koincidencije i njegove primjene u kriptografiji* koja se smatra jednom od najvažnijih publikacija u povijesti kriptologije (Dujella, Maretić, 2007; Singh, 2003).

4.4. Jednokratna bilježnica (*One-time pad*)

Pojam savršene sigurnosti uveo je 1949. godine Claude Shannon, utemeljitelj teorije informacija kao znanstvene discipline. Riječ je o kriptosustavu u kojem šifrat ne daje nikakvu informaciju o otvorenom tekstu. Potpuna sigurnost ostvariva je kriptosustavom poznatim pod nazivom *jednokratna bilježnica* (engl. *One-time pad*), a uveli su ga Gilbert Vernam i Joseph Mauborgne 1917. godine. Nedavno je pronađeno da je istu ideju imao već 1882. godine Frank Miller[9]. Njegova je definicija, ukoliko se koriste binarni podaci:

Definicija 6. Neka je n prirodan broj, $P = C = K = (Z_2)^n$. Za $K = (k_1, ..., k_n) \in K$ definiramo

$$e_K(x_1, x_2, ..., x_n) = (x_1 +_2 k_1, x_2 +_2 k_2, ..., x_n +_2 k_n),$$

$$d_K(y_1, y_2, ..., y_n) = (y_1 +_2 k_1, y_2 +_2 k_2, ..., y_n +_2 k_n)$$ (Dujella, Maretić, 2007).

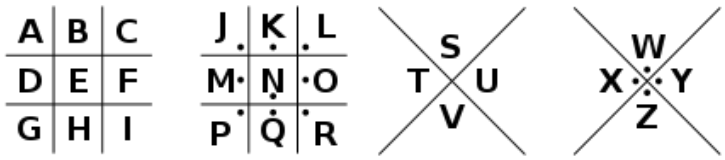
Sigurnost kod ovog kriptosustava može se postići samo ako se svaki ključ koristi samo jednom, a otud i dolazi naziv *jednokratna bilježnica*. Naime, različitim su se varijantama tog kriptosustava koristili obavještajci (špijuni) koji bi za tu svrhu upotrebljavali bilježnicu u kojoj bi se svaki list koristio kao jednokratni ključ. U praktičnoj primjeni velik problem predstavlja činjenica da je ključ, koji mora biti sigurno prenesen, jednako dug kao i sama poruka. Ključevi se

[9] *Jednokratna bilježnica*. Pribavljeno 15. 5. 2018., sa https://web.math.pmf.unizg.hr/~duje/kript/otp.html

moraju redovito fizički razmjenjivati kako bi se izbjegla ponovna upotreba ključa, što je vrlo dugotrajan proces osobito ako su dopisnici zemljopisno udaljeni, a pritom šifrirna abeceda (ukoliko se radi o engleskom alfabetu) može sadržavati slova koja se ponavljaju. Drugim riječima, ako je n duljina ključa tada može biti ukupno 26^n mogućih ključeva poruke (Dujella, Maretić, 2007; Wijesekera, 2011). Na primjer, ako se na svaki papir ispiše jedna mogućnost šifre za riječ duljine n = 5 te slože mogućnosti (papiri) jedna na drugu, nastat će oko 12 milijuna papira koji poslagani čine stup visine jedan kilometar[10]. Dakle, prednosti su te šifre nepostojanje ponavljanja i slijedova u šifratu te ujednačena frekvencijska distribucija koja kriptoanalitičarima ne daje nikakve informacije osim duljine otvorenog teksta.

4.5. Fragmentarna šifra

„Monoalfabetska supstitucijska šifra ili šifra jednostavne zamjene održala se u raznim oblicima stoljećima. Jedna od njih je i *fragmentarna šifra* (*pigpen cipher*) kojom su u 18. stoljeću masoni čuvali tajnost svojih spisa i po kojima ta šifra često nosi naziv *masonska šifra*. Ta šifra ne zamjenjuje jedno slovo drugim, nego na mjesto slova stavlja druge simbole. Slovo se enkriptira tako da se pronađe u rešetki i zatim skicira njemu pripadajući dio" (Singh, 2003: 226). Dakle, slova engleskog alfabeta moguće je zamijeniti simbolima A = ⌟ , B = ⌞⌟ , W = ⋁ i tako dalje (vidi sliku 10.).

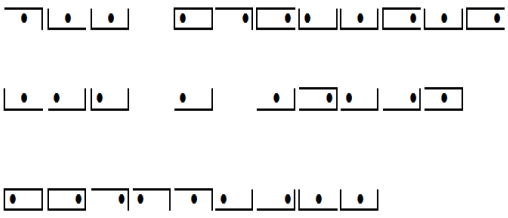


Slika 10. Pigpen šifra (izvor: https://en.wikipedia.org/wiki/Pigpen_cipher)

Ponekad se ta šifra pojavljuje u obliku u kojem ključ nalikuje rasporedu slova na tipkovnici mobitela, a slovo se enkriptira isto tako da se pronađe u rešetki i zatim skicira njemu pripadajući dio. S obzirom na to da svako pojedino polje u rešetci sadrži minimalno dva slova, važna je pozicija slova u polju rešetke koja se označava točkicom pa je slovo A označeno prvom točkicom po redu, slovo B drugom, a slovo C trećom (vidi sliku 11.).

[10] *The one-time pad*. Pribavljeno 15. 5. 2018., sa https://www.khanacademy.org/computing/computer-science/cryptography/crypt/p/perfect-secrecy-exploration

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 11. Inačica Pigpen šifre, u primjeru piše: THE MURDERER HAD A BLACK MOUSTACHE (izvor: https://www.stem.org.uk/resources/elibrary/resource/36022/cryptography-workshop)

4.6. Atbash šifra

Atbash šifra vrlo je stara supstitucijska šifra koja je izvorno razvijena za uporabu u hebrejskoj abecedi. Zapravo, u Knjizi o Jeremiji postoji nekoliko riječi koje su šifrirane koristeći se Atbashovom šifrom. U njoj je Sheshakh šifra za Babel (ili Babilon). Obično se smatra jednom od najlakših šifri za upotrebu jer slijedi vrlo jednostavnu metodu zamjene. Naime, prvo slovo abecede zamijenjeno je posljednjim slovom, drugo slovo zamjenjuje se s drugim od kraja i tako dalje. Na hebrejskom, aleph (prvo slovo) je zamijenjeno sa tav (posljednje slovo), beth (drugo slovo) sa shin (pretposljednje slovo). Iz tih slova vidljivo je kako je šifra dobila svoje ime: prvo slovo je aleph, a slijedi tav, zatim beth i napokon shin. S obzirom na to da je svako slovo uvijek jednako šifrirano, riječ je o vrlo nesigurnoj šifri jer je vrlo laka za razbijanje nekomu tko presretne poruku. Međutim, čini se da to nije bio problem u vrijeme kada se njome koristilo i čini se da je dobro poslužila svojoj svrsi[11]. Ukoliko abeceda otvorenog teksta ima neparan broj slova, slovo koje se nalazi na (n + 1) : 2 mjestu šifrirat će se u isto to slovo, dok u abecedi otvorenog teksta koja ima paran broj slova (engleska, hrvatska), niti jedno slovo neće se šifriranjem preslikati u to isto slovo. Ukoliko treba šifrirati riječ „SUPSTITUCIJA" dobit će se sljedeći šifrat:

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

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

Šifrat: HFKHGRGFXRQZ

[11] *Atbash cipher*. Pribavljeno 15.5.2018., sa http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/atbash_cipher.pdf

4.7. Polibijev kvadrat i Uesugi šifra

Polibijev kvadrat šifra je koju je Polibije prvi puta opisao u svojim *Povijestima* oko 150. godine pr. Kr., a upotrebljavale su ga mnoge kulture tijekom povijesti u različitim veličinama, ovisno o duljini abecede. Korisna je kao oblik enkripcije, no nije osobito jaka te je osjetljiva na frekvencijsku analizu. Iako je riječ o supstitucijskoj šifri, razlikuje se od ostalih jer je svako slovo zamijenjeno dvama brojevima. Polibije je predložio da se šifra upotrebljava signaliziranjem brojeva pomoću dva seta baklji, no postojalo je mnogo različitih načina prijenosa šifrirane poruke poput treperenja svjetiljke, dimnih signala, kuckanja i slično. Vjerojatno najpoznatiji primjer korištenja Polibijeva kvadrata bio je kod američkih ratnih zatvorenika u Vijetnamskom ratu. Zalijepili bi poruku koju su šifrirali na zidove i cijevi kako bi međusobno komunicirali jer su ih držali zarobljene bez ikakvog ljudskog kontakta[12].

Ukoliko treba šifrirati otvoreni tekst „FREKVENCIJSKA ANALIZA" Polibijevim kvadratom koji sadrži slova hrvatskog alfabeta te grčka slova α, β, γ i π, potrebno je provjeriti poziciju svakog slova u tablici (vidi sliku 12.). Slovo F nalazi se u 2. retku i 4. stupcu pa će njegov šifrat biti broj 24. Tako će šifrat otvorenog teksta „FREKVENCIJSKA ANALIZA" glasiti „24 45 23 33 54 23 41 13 31 32 46 33 11 11 41 11 34 31 55 11". Dešifriranje se obavlja obrnutim procesom, odnosno šifrat koji glasi 45 odnosi se na slovo u 4. retku i 5. stupcu, a to je slovo otvorenog teksta R.

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

Slika 12. Polibijev kvadrat koji sadrži slova hrvatskog alfabeta te grčka slova α, β, γ i π

[12] *Polybius square*. Pribavljeno 15.5.2018., sa http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/polybius_square.pdf

Tijekom 16. stoljeća stvorena je šifra koja je uključivala upotrebu Polibijeva kvadrata u Japanu. Metoda pripreme šifriranih poruka opisana je u knjizi o ratnoj znanosti koju je napisao Sadayuki Usami, a govori o strategu Kenshinu Uesugiju koji je bio vojni rukovoditelj tijekom razdoblja Sengoku (građanskog rata) u Japanu. Uesugi šifra uključivala je uporabu tablice (vidi sliku 13.) koja se sastojala od 48 japanskih slojevitih fonetskih znakova upisanih u tablicu od sedam redaka i sedam stupaca pri čemu svaki lik predstavlja brojeve na vrhu svakog retka i stupca[13].

七	六	五	四	三	二	一	
ゑ	あ	や	ら	よ	ち	い	一
ひ	さ	ま	む	た	り	ろ	二
も	き	け	う	れ	ぬ	は	三
せ	ゆ	ふ	み	そ	る	に	四
す	め	こ	の	つ	を	ほ	五
ん	み	え	お	ね	わ	へ	六
	し	て	く	な	か	と	七

Slika 13. Uesugi šifra (izvor: https://adgrafics.net/docs/thawte/history-cryptography.pdf)

[13] *History of Cryptography: an easy to understand history of cryptography*. Pribavljeno 15.5.2018., sa https://adgrafics.net/docs/thawte/history-cryptography.pdf

5. KRIPTOGRAFIJA U NASTAVI

Učenici koji aktivno sudjeluju u učenju matematike bolje razumiju nastavni predmet, a jedan je od glavnih problema matematičkog obrazovanja pronaći načine motiviranja i uključivanja učenika u razredu (Aydin i sur., 2011). Fellows i Koblitz (2000) u nastavi matematike pronalaze obilježja tradicionalnog školskog kurikuluma, a među ostalima i velik broj kratkih zadataka koji se ponavljaju, a svaki se koristi jednostavnom, niskom razinom misaonog procesa, mnoštvo neposrednih odgovora točno/netočno (kao da postoji pretpostavka da su djeca nesposobna za trajne napore u matematičkom rješavanju problema). Također, smatraju da nema zadataka koji, umjesto jednog pravog odgovora, sadrže dobre i bolje odgovore (kao u nekim problemima optimizacije). Prevladavaju arhaične teme i terminologija (od kojih su neke praktički nepromijenjene od srednjeg vijeka) te dosadni primjeri i primjene. Isto tako, nedovoljno je rasprava o trenutnim granicama znanja o matematici, o aktualnim događajima te vezama sa svijetom žive matematike. Postoji vrlo malo samostalne aktivnosti te nedovoljno matematičkih projekata i domaćih zadaća. Među učenicima prevladava pasivnost jer su osposobljeni da slijede kratki predvidljivi put do točnog odgovora i ne pridonose razvoju procesa rješavanja (postavljanje novih modela matematičkih situacija i formuliranje vlastitih pitanja). S druge strane, među učiteljima prisutna je nemilosrdna usredotočenost na ono što djeca „trebaju" znati u raznim prilikama, a poučavanje je usmjereno na poboljšanje njihove uspješnosti u standardiziranim ispitima s kratkim odgovorima.

Kriptografija ima ogroman potencijal obogatiti nastavu matematike jer je njome moguće stvoriti dramatično okruženje. U njoj su važni elementi drame, kazališta, neizvjesnosti. Na šarmantan način može uvesti teme tradicionalne ili manje tradicionalne matematike, algebre, modularne aritmetike, računalne lingvistike, kombinatorike, algoritama i statističkih procjena. Također, vrlo je važno sredstvo za predstavljanje temeljnih matematičkih pojmova djeci. Može se primijeniti u učionicama u vrlo ranoj fazi, čak i na razini osnovne škole na kojoj djeca spontano formuliraju pretpostavke i razvijaju argumente koji se dokazuju ili opovrgavaju. Djeca su oduševljena intrigom i avanturom, a igrajući motivirajuće i sofisticirane logičke igre, riskira se više od ocjene na testu jer primjerice, ako pogriješite igrajući uloge tajnih agenata, vaš će agent biti izdan. Malo će toga motivirati djecu kao što to čini želja da se porazi „negativac" ili, pak, igranje uloge „negativaca". Također, kriptografija pruža mogućnost da djeca prirodnim načinom samostalno otkriju pojedine ključne matematičke pojmove i tehnike. Ona potiče razvoj vještina za

rješavanje problema i povećava sposobnosti argumentiranja. Prečesto učitelji matematike oduzimaju djeci radost otkrića, no ako, na primjer, nakon mnogo utrošenih sati djeca konačno razviju metodu razbijanja kriptosustava, vjerojatno će više cijeniti moć i ljepotu matematike koju su otkrili (Borelli i sur., 2002; Fellows, Koblitz, 2000; Koblitz, 1997).

Kriptografiju i njezinu sposobnost da zabavi djecu prepoznali su davno oglašivači proizvoda poput Rice Krispies i Crackerjacks. Mnogi su se svađali s braćom i sestrama oko toga tko će dobiti prsten za dekodiranje u kutiji Crackerjacks, a neke kutije Rice Krispiesa imale su na poleđini „tajni algoritam", odnosno igru pogađanja temeljenu na binarnom prikazu cijelih brojeva. Neki jednostavni kriptosustavi mogu poslužiti za popularizaciju matematike u školama i drugdje, a namijenjeni su 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* (Fellows, Koblitz, 2000).

5.1. Dosadašnja istraživanja i radionice

Aydin, Güler i Şükrü Özdemir u svom članku *Effects of Cryptographic Activities on Understanding Modular Arithmetic* (2011) prikazali su učinke kriptografskih aktivnosti na razumijevanje studenata, a koje su se koristile kao pomoć u poučavanju teme modularne aritmetike. Tu su temu predstavili dvjema grupama učenika osmih razreda. U kontrolnoj skupini koristila se tradicionalna metoda poučavanja, a u eksperimentalnoj kriptografske aktivnosti i zagonetke. Analiza podataka pokazala je da su učenici koji su učili predmet provodeći kriptografske aktivnosti bili uspješniji od tradicionalno poučavanih učenika.

U prvom tjednu eksperimentalnoj je skupini predstavljena Cezarova šifra te šifrirni diskovi, a učenici su naučili kako šifrirati i dešifrirati tom metodom. Također, upoznali su i aritmetičku analizu vremena. U drugom tjednu dane su informacije o frekvencijskoj analizi koja omogućuje dešifriranje Cezarove šifre bez poznavanja ključa. Učenici su ispunjavali frekvencijske tablice odabirom tekstova iz knjiga. Zatim je slijedilo upoznavanje učenika s algoritmima te su osmišljene aktivnosti poput pronalaženja točnog dana učenikova rođendana uz pomoć kalendara i pronalaženja vrijednosti cijelih brojeva u danom modulu. U trećem tjednu uvedena je definicija prostog broja, a dani su i primjeri iz svakodnevnog života. Učenici su upoznali Eratostenovo sito i metodu pronalaženja prostih brojeva, a trebali su pronaći i sve proste brojeve do 50 primjenjujući

tu metodu. Nakon toga predstavljena je Morseova abeceda i Pigpen šifra. Neki su učenici imali poteškoća s dešifriranjem, ali većina njih bila je vrlo uspješna i odlučna razbiti kodove. Prema rezultatima istraživanja, u nastavi matematike za učenike osmih razreda postoji statistički značajna razlika u stavovima učenika prema matematici u korist skupine učenika koji su upućeni u šifriranje u odnosu na grupu učenika koja je učila na tradicionalan način. Stavovi učenika prema matematici promijenili su se na pozitivan način kao rezultat uvođenja nastave kriptografije u osmom razredu. Istraživanje također pokazuje da se kriptografske aktivnosti mogu koristiti za motiviranje i učinkovitije poučavanje određenih tema u osmom razredu.

Borelli, Fioretto, Sgarro i Zuccheri u svom radu *Cryptography and statistics: a didactical project* (2002) govore o eksperimentu koji je započeo 1989. godine u školama sjeveroistočne Italije u kojem je sudjelovalo oko 300 učenika u dobi od sedam do deset godina, a eksperiment se provodi i danas zbog pozitivnih reakcija učenika i učitelja. Rad u učionicama sastoji se od izrade i razbijanja šifri, a temelji se na tajnim porukama koje šalju kriptografi i presreću kriptoanalitičari. Alati koji se koriste ograničeni su na tehnologiju nulte razine, tj. na papir i olovku. Nakon kratkog treninga učenici rade na šifriranim tekstovima od oko 300 znakova. Kako bi razbili kriptogram, računaju frekvenciju slova otvorenog teksta od približno 1000 riječi i stvaraju histograme. Zatim uspoređuju svoje rezultate sa standardnim tablicama frekvencija te stvaraju vlastite uređaje za enkripciju, šifrirne diskove i klizna ravnala, koje izrađuju od kartonskog papira.

Ukieova Digital School House[14] udružila se s Odjelom za obrazovanje u Bletchley Parku kako bi stvorila radionicu koja upoznaje učenike s kriptografijom i postupcima korištenja naprednih funkcionalnosti proračunskih tablica. Radionicu je pokrenuo PlayStation, pod pokroviteljstvom SEGA-e i Warwickshireova županijskog vijeća, a upotrebljava metodu učenja temeljeno na igrama kako bi pripremilo sljedeće generacije za digitalno doba. Skup aktivnosti uvodi djecu u kriptografske tehnike, pokazujući kako se korištenjem računala može šifriranje učiniti bržim i učinkovitijim. Učenici započinju nastavnu jedinicu upoznavanjem poviješću šifriranja te načinom na koji se računarstvo uklapa u suvremenu komunikaciju. Igrajući uloge, djeca se upoznaju s brojnim tehnikama šifriranja kao što su transpozicijska, supstitucijska i fragmentarna šifra. Djeca se pritom koriste Excelovim tablicama koje im pomažu pri dešifriranju

[14] *Cryptography Workshop*. Pribavljeno 15. 5. 2018., sa https://www.stem.org.uk/resources/elibrary/resource/36022/cryptography-workshop

pojedinih poruka, izrađuju šifrirne diskove, a upoznaju i Polibijev kvadrat. Kasnije upoznaju naprednije tehnike dešifriranja poput traženja visokofrekventnih slova u supstitucijskim šiframa (frekvencijska analiza). Radionica je namijenjena djeci u dobi od pet do jedanaest godina.

Neki od ishoda učenja te radionice jesu: razumjeti važnost kriptografije i razvoj računala tijekom povijesti, što se podrazumijeva pod pojmovima kriptografija i šifriranje, razumjeti način na koji funkcionira šifriranje, razumjeti strukturu proračunske tablice te naučiti primjenjivati jednostavne formule unutar proračunske tablice, ali i šifrirati i dešifrirati poruke jednostavnim tehnikama, izraditi i manipulirati postojećim proračunskim tablicama za šifriranje i dešifriranje podataka, upotrijebiti jednostavne tehnike frekvencijske analize, naučiti sigurno, pošteno i odgovorno koristiti se tehnologijom, prepoznati prihvatljivo i neprihvatljivo ponašanje te razumjeti važnost šifriranja u suvremenoj tehnologiji.

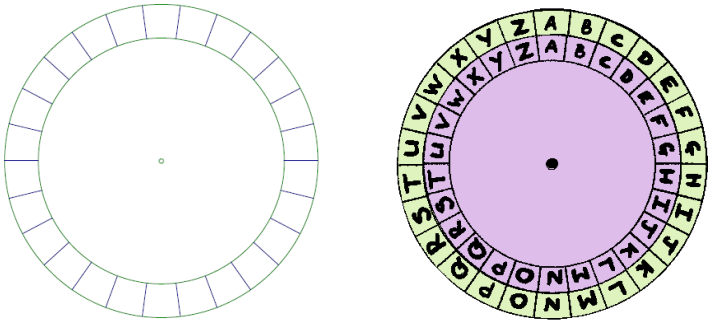
5.2. Savjeti u radu s učenicima

Kako bi si djeca predočila kriptografiju, postoje određene ideje aktivnosti koje je korisno prvo provesti među njima. Na primjer, postoji mnogo zabavnih načina za uvođenje pojma algoritma i računalne složenosti. Zanimljiva aktivnost kojom se brzo i diskretno provodi „numerička" anketa, a moguće ju je provesti kod učenika nižih razreda, naziva se „Tajni protokol". Primjerice, ukoliko učitelj želi saznati prosječan džeparac koji učenik ima, a postoji mogućnost da učenici neće biti potpuno iskreni u javnom iznošenju tog podatka, učitelj može primijeniti „Tajni protokol" koji će sačuvati pravo na privatnost svakog učenika. Protokol započinje prvi učenik koji izabire „tajni" broj n. Neka je n = 21. „Tajni" broj n prvi učenik uvećava za iznos svog džeparca, npr. za 50, $n_1 = n + 50 = 71$. Zatim, prvi učenik šapne broj n_1 drugom učeniku. Drugi učenik, primjerice, primi mjesečno 100 kn džeparca, pa je $n_2 = n_1 + 100 = 171$. Broj n_2 drugi učenik došapne trećem učeniku. Protokol se nastavlja redom do posljednjeg učenika kojem je prišapnut broj n_{12} njegovog prethodnika, odnosno dvanaestog učenika. Nakon uvećavanja broja n_{12}, $n_{13} = n_{12} + 30$, posljednji učenik tu informaciju prosljeđuje prvom učeniku. Prvi učenik od konačnog zbroja n_{13} oduzima „tajni" broj n. Neka je $n_{13} = 931$. Sada prvi učenik može svima priopćiti da je ukupan džeparac koji njegov razred prima jednak $n_{13} - n = 931 - 21 = 910$ kn. Budući da taj razred broji 13 učenika, prosječna vrijednost iznosi 70 kn. Pitanje koje se može postaviti učenicima jest kako „razbiti" tajnost tog protokola, što je moguće ukoliko npr. prvi i treći učenik surađuju. Naime,

njihovom suradnjom tada mogu otkriti koliki džeparac prima drugi učenik. Trećem je učeniku poznat broj n_2 te uz pomoć prvog učenika može odrediti da je to broj $n_2 - n_1 = 171 - 71 = 100$ (Barun i sur., 2008; Fellows, Koblitz, 2000).

Postoje brojne ideje kako provesti kriptografske aktivnosti u nastavi. Najpoznatije su svakako igre uloga istražitelja, svjedoka i zločinca te kriptografa i kriptoanalitičara (špijuna), ali i razni oblici potraga za skrivenim blagom. Pri upoznavanju učenika sa steganografijom moguće je prirediti eksperiment koji uključuje pisanje nevidljivom tintom, a za to su potrebni samo papir, kist, neka organska tekućina bogata ugljikom i svijeća, a koji će u učenicima probuditi tajnog agenta. Kada se raspravlja o uporabi skitala, bilo bi vrlo korisno imati model pripremljen prije nastavne jedinice. Sve što je zapravo potrebno je cilindar bilo koje veličine (ili poželjno 2 identična cilindra i nekoliko cilindara različitih promjera) te duga traka papira koju treba omotati oko cilindra. Radi prikazivanja uporabe u razredu, potrebno je napisati kratku poruku na papir dok je omotana oko cilindra, a zatim ju odmotati. Učenici mogu omotati traku oko različitih oblika cilindara kako bi provjerili izvornu poruku. Kao praktična aktivnost, moguća je izrada vlastitog skitala[15]. U nedostatku cilindara postupak se može primijeniti i na olovkama raznih veličina.

Pri upoznavanju učenika sa supstitucijskim šiframa šifrirni diskovi pružaju živopisan način ilustracije te jednostavne, ali važne ideje (Koblitz, 1997). Svakom učeniku potrebno je podijeliti nacrt šifrirnog diska (vidi sliku 14.) koji je potrebno izrezati, zalijepiti na karton, obojiti, ispisati slova abecede te spojiti dva diska spajalicom zajedno.



Slika 14. Nacrt šifrirnog diska i konačna verzija (izvor: http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/shift.pdf)

[15] *Atbash cipher*. Pribavljeno 15. 5. 2018., sa http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/atbash_cipher.pdf

Moguće je slova otvorenog teksta ispisati crno, a šifrirana slova crveno kako bi učenici razlikovali otvoreni tekst od šifrata. Disk djeluje podudaranjem slova „a" na unutarnjem kotaču s odgovarajućim slovom na vanjskom kotaču. Za ključ 3, slovo „a" poravnamo sa slovom „D". Za ovu šifru postoji 26 različitih ključeva: „a"→ „A" (ključ 0), „a" → „B" (ključ 1), „a" → „C" (ključ 2) itd. Također, treba napomenuti učenicima da je pomak od 26 isti kao pomak od 0, čime ih se uvodi u modularnu aritmetiku[16]. Ukoliko se radi o učenicima nižih razreda osnovne škole, moguće je prilagoditi šifrirni disk povezivanjem dvaju diskova spajalicom, ali pritom izrezati dva otvora na manjem disku koja će prikazivati jedno slovo otvorenog teksta i pripadajući šifrat (koji može biti primjerice neki broj) (vidi sliku 15.). Također, moguće je izraditi napravu od kartonske role toaletnog papira ili ubrusa te na njoj pričvrstiti dvije tablice identičnog sadržaja koje sadrže slova abecede. Tablice ne treba zalijepiti na karton, već samo pričvrstiti krajeve kako bi se mogle pomicati za rad sa supstitucijskom šifrom (vidi sliku 15.)

Slika 15. Šifrirni disk prilagođen učenicima nižih razreda te uređaj za supstituciju načinjen od kartonske role

Pri obradi supstitucijske šifre moguće je izraditi tablice u Excelu u kojima se nalaze slova abecede te pripadna slova šifrirne abecede koja će se mijenjati ovisno o jednom polju u koji će se unositi ključ šifre. Učenici će pritom upotrebljavati matematičke funkcije samog programa, a mogu izrađivati i dijagrame. Također, jednostavnim Wordovim programom može se odrediti frekvencija pojedinih slova u uzorku od milijuna znakova. Naredba „Replace" neće samo obaviti određenu zamjenu nego i reći koliko je ona puta obavljena. Ukoliko se ponovi za svako slovo posebno, za

[16] *Shift*. Pribavljeno 15. 5. 2018., sa http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/shift.pdf

nekoliko minuta bit će prikazane prilično pouzdane frekvencijske tablice hrvatskoga ili nekog drugog jezika (Singh, 2003). Učenici mogu istražiti koliko dugačak tekst treba biti da bi sa sigurnošću mogli tvrditi koje se slovo najčešće javlja te koje se strategije mogu koristiti za kratki tekst na kojem pretpostavka o učestalosti slova ne vrijedi. Također, mogu provjeriti koja su druga i treća najčešća slova u pojedinim jezicima. Primjeri iz, na primjer, španjolskog jezika mogu se koristiti čak i ako ga većina djece ne poznaje. Bilo bi dobro odabrati izraze koji su poznati iz filmova (poput „hasta la vista") tako da djeca mogu shvatiti značenje nakon dešifriranja (Koblitz, 1997).

Učenicima će biti zanimljiva i izrada nomenkaltora te kodiranje (na papiru) koje može poslužiti kao priprema za rad u nekom računalnom programu poput Terrapin Loga ili Pascala. Raznim igrama moguće je upoznati učenike sa supstitucijskim šiframa s proizvoljnim rasporedom slova šifrirne abecede, supstitucijskim šiframa s ključnom riječi ili frazom, Vigenèreovom šifrom (pomoću Vigenèreova kvadrata ili pak zbrajanja), jednokratnom bilježnicom, raznim oblicima fragmentarne šifre, Polibijevim kvadratom (možda izrada kvadrata za neku drugu abecedu) te Uesugi šifrom. Učenicima se mogu prirediti tekstovi na kojima su izbušene rupice ispod određenih slova te oni potom u skupinama mogu sami na taj način stvarati šifre. Ako je riječ o učenicima nižih razreda, moguće je obraditi pisanje vlastitog tajnog pisma ili nekim njima nepoznatim pismom (glagoljica, ćirilica) te ih upoznati s Atbash šifrom i Cik-cak šifrom koje su vrlo jednostavne.

Neke aktivnosti moguće je uklopiti u jedan nastavni sat (npr. šifriranje Cezarovom šifrom i izrada šifrirnog diska), ali za neke je potrebno puno više vremena (frekvencijska analiza). Najbolje je rješenje za to integrirani dan jer je kriptografija jedna od znanosti koja je zapravo interdisciplinarna, tj. u sebi sadržava i društvene (lingvistika i jezici) i prirodoslovne znanosti (matematika, informatika i tehnika). Moguće je provesti korelaciju s brojnim predmetima poput povijesti, prirode i društva, stranih jezika, informatike itd. Ukoliko se kriptografija primjenjuje u nastavi hrvatskog jezika, otkrivanje frekvencije slova može biti jedna zanimljiva nastavna aktivnost. U nastavi stranih jezika moguće je učenicima zadati da analiziraju manje tekstualne odlomke na različitim jezicima i uvjere se koja su slova tog jezika najčešća. U nastavi povijesti moguće je obraditi sve povijesne činjenice i događaje obrađene u ovom radu. Pritom će brojnim učenicima biti zanimljivo razgovarati o kriptografiji koja se pojavljuje u filmovima i knjigama.

Neki od filmova u kojima se mogu pronaći metode šifriranja i dešifriranja su *The Da Vinci Code*, *Angels & Demons* te *The Imitation Game* o Alanu Turingu i razbijanju Enigme. Također, brojne web stranice[17] nude mogućnost simulacije same Enigme, stoga učenici mogu vidjeti na koji je način radila.

5.3. Radionica „Šifriranje poruka“

Za potrebe ovog diplomskog rada provedena je radionica s učenicima sedmih razreda osnovne škole te prilagođena radionica s učenicima trećih razreda osnovne škole. Obje radionice provedene su i sa studentima treće godine Fakulteta za odgojne i obrazovne znanosti u Osijeku na Danima fakulteta 2018. godine te na Festivalu znanosti 2018. godine s temom *Otkrića*.

U radionici za učenike predmetne nastave, koja je provedena sa sedmim razredima osnovne škole, pojašnjeno je samo značenje riječi kriptografija te opisana uloga kriptografije kao znanstvene discipline. Učenicima su pojašnjeni pojmovi poput originalnog teksta, kriptoteksta ili šifrata, šifriranja, dešifriranja te ključa. Upoznati su s razvojem kriptografije tijekom povijesti od Atbash šifre i Skitala, Julija Cezara i Al-Kindija do Enigme. Nakon toga, slijedilo je upoznavanje s metodama šifriranja i dešifriranja. Prva šifra koju su učenici upoznali bila je Cezarova šifra koja je pojašnjena zbrajanjem (šifriranje) i oduzimanjem (dešifriranje). Prikazana im je tablica (vidi sliku 17.) u kojoj su slovima hrvatske abecede pridruženi brojevi od 0 (A) do 29 (Ž). Slovo A prilikom šifriranja zamjenjuje se slovom Č (0 + 3 = 3), a pri dešifriranju samo se oduzima, primjerice, slovo Š zamjenjuje se slovom P (24 - 3 = 21). Učenici su potom sami šifrirali i dešifrirali pojedine rečenice i riječi. Zatim je predstavljena supstitucijska šifra na sličan način kao i Cezarova šifra te je pojašnjeno da njezin ključ može biti bilo koji prirodan broj. Učenici su potom pokušali šifrirati i dešifrirati Atbash šifrom, a nakon toga i Vigenèreovom šifrom. Vigenèreova je šifra također pojašnjena zbrajanjem na primjeru riječi ŠIFRIRANjE ključem ZEC. Učenici su ispisivali riječ ZEC ispod riječi ŠIFRIRANjE, a potom zbrajali Š + Z = 24 + 28 = 52 = R (vidi sliku 17.) i tako redom dok nisu dobili šifrat. Slijedile su Cik-cak šifra i Polibijev kvadrat, a radionica je završila potragom za blagom (vidi Prilog 3.) koje se nalazilo u jednoj od 30 omotnica označenim brojevima od 1 do 30. Učenici su na kraju popunili evaluacijske listiće o radionici (vidi Prilog 4.).

[17] *Škola kriptografije Enigma*. Pribavljeno 15. 5. 2018., sa http://kriptografija.udruga-hum.hr/index.php?section=about

A	B	C	Č	Ć	D	Dž	Đ	E	F	G	H	I	J	K	L	Lj	M	N	Nj	O	P	R	S	Š	T	U	V	Z	Ž
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
A	B	C	Č	Ć	D	Dž	Đ	E	F	G	H	I	J	K	L	LJ	M	N	NJ	O	P	R	S	Š	T	U	V	Z	Ž
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59

Slika 17. Tablica u kojoj su slovima hrvatske abecede pridruženi brojevi od 0 do 29.

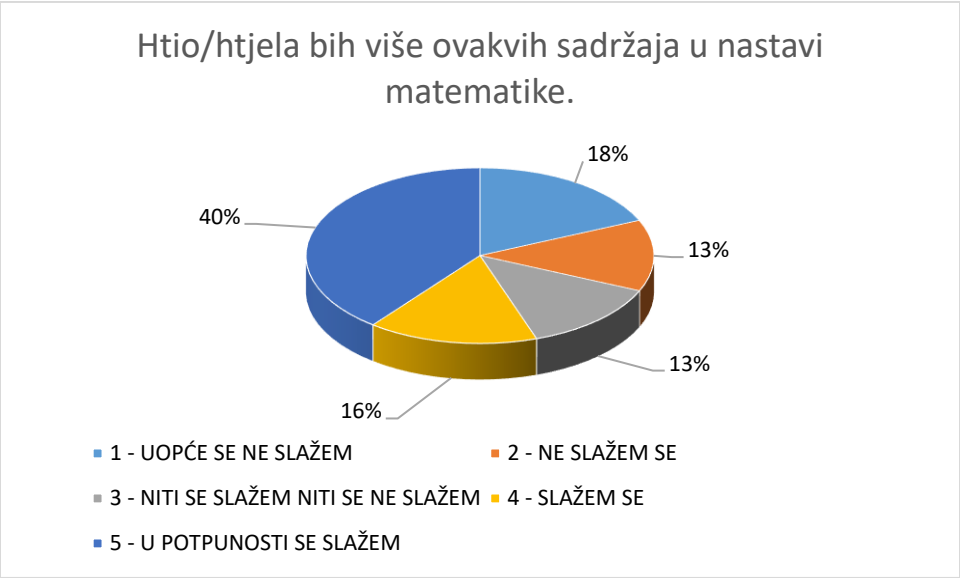
Među učenicima trećih razreda razredne nastave provedena je prilagođena radionica koja je također započela pojašnjenjem riječi kriptografija i njezine uloge kao znanstvene discipline. Povijesni pregled bio je isti kao i kod učenika predmetne nastave, no s većim naglaskom na tajna pisma te supstituciju sa slovima glagoljice ili ćirilice. Cezarova šifra i ostale supstitucijske šifre pojašnjene su na isti način kao i u radionici za učenike predmetne nastave. Na kraju je, također, slijedila potraga za blagom (vidi Prilog 1.) koje se nalazilo u jednoj od 20 omotnica označenim brojevima od 1 do 20. Pri radu su se učenici koristili šifrirnim diskom prilagođenim učenicima nižih razreda (vidi sliku 15.) te uređajem za supstituciju načinjenim od kartonske role. Učenici su na kraju popunili evaluacijske listiće o radionici (vidi Prilog 2.).

Studenti 3. godine Fakulteta za odgojne i obrazovne znanosti u Osijeku prošli su obje radionice s ciljem da provjere svoje znanje, možda nauče nešto novo, ali i dobiju ideje za budući rad s učenicima. Oni su također odgovorili na pitanja s evaluacijskog listića (vidi Prilog 5.).

5.4. Rezultati

Prilikom obrade podataka dobivenih odgovorima 40 učenika trećih razreda koji su prisustvovali radionici namijenjenoj učenicima razredne nastave, utvrđeno je da se radionica svidjela 97 % učenika, 95 % učenika izjavilo je da im je šifriranje i dešifriranje zanimljivo, samo 21 % učenika nije razumjelo radionicu, a 66 % učenika šifrirat će poruke u budućnosti.

Na temelju odgovora 38 učenika sedmih razreda, koji su prisustvovali radionici namijenjenoj učenicima predmetne nastave, utvrđeno je da se radionica svidjela 95 % učenika, dok je ostatak bio neutralan. Ukupno 56 % učenika htjelo bi više takvih sadržaja u nastavi matematike (vidi sliku 18.), a 13 % bilo je neutralno. Za 29 % učenika metode šifriranja i dešifriranja bile su preteške za razumjeti, a 16 % izjasnilo se kao neutralno. Čak 81 % učenik smatra da je šifriranje i dešifriranje zanimljivo. Samo se 31 % učenika već susrelo sa spomenutim metodama, a 44 % učenika izjavilo je da će i u budućnosti nastaviti sa šifriranjem i dešifriranjem.



Slika 18. Rezultati ankete nakon provedene radionice u sedmim razredima osnovne škole

Prilikom obrade podataka dobivenih odgovorima 49 studenata koji su prisustvovali radionici utvrđeno je da se svima svidjela radionica, metode šifriranja i dešifriranja. Čak 96 % studenata ocijenili su radionicu jednostavnom za razumijevanje, a 98 % studenata izjavilo je da im je tema bila zanimljiva. Čak 94 % studenata (vidi sliku 19.) iskoristilo bi pojedine sadržaje u nastavi matematike, a 98 % u dodatnoj nastavi matematike. Samo je 18 % studenata prije upotrebljavalo šifriranje, a 48 % će ga upotrebljavati i u budućnosti.

Slika 19. Rezultati ankete nakon provedenih radionica sa studentima

6. ZAKLJUČAK

Živimo u dobu kada se promjene događaju svakodnevno, stoga je vrlo važno usvajati nova znanja te prilagođavati način poučavanja suvremenoj generaciji učenika. Zahvaljujući modernoj tehnologiji, informacije koje su danas svima brzo i lako dostupne utječu i na način učenja i stjecanja znanja.

U ovom radu navedeni su primjeri kako brojnim metodama šifriranja i dešifriranja uvesti igru, neizvjesnost i zagonetke u nastavu matematike. Prema rezultatima dobivenim nakon provođenja radionice vidljivo je da se učenicima sviđaju kriptografski sadržaji te da žele više takvih sadržaja u nastavi matematike, odnosno sadržaja koji u njima bude natjecateljski duh i želju za učenjem. Gotovo svi učenici, pa čak i oni koji inače nisu aktivni na satu, pomno su pratili metode i prihvatili se šifriranja. Neki su od njih čak i tražili dodatne materijale kako bi se i kod kuće bavili kriptografijom. Današnja su djeca svakodnevno okružena društvenim mrežama i računalnim programima, stoga je važno da od najranije dobi upoznaju šifriranje jer u doba interneta i zaštite podataka, treba shvatiti da sigurnost više nije zadaća samo tajnih službi.

Budući učitelji, koji su također sudjelovali u radionici, opisali su kriptografske sadržaje zanimljivima te naveli da bi takve sadržaje primijenili i u vlastitoj učionici. Oni su time podržali uvođenje novih znanja te načina poučavanja prilagođenih suvremenoj generaciji učenika. Primijetili su brojne mogućnosti koje im kriptografija nudi, ali i načine rada koje mogu iskoristiti ne samo u matematici već i u drugim predmetima.

Važnost se kriptografije svakodnevno povećava, a ona se koristi čak i kada nismo toga svjesni. Ona postaje važnijom zbog razvoja mrežne komunikacije u elektronskim transakcijama (na internetu, e-pošti, mobitelu) koje su danas platforma za osjetljive novčane, poslovne, političke ili, pak, osobne komunikacije. Zaključno, važno je da svatko bude upoznat s osnovnim elementima kriptografije kako bi zaštitio sebe i svoje podatke.

7. LITERATURA

1. Aydin, N.,, Güler, E., Şükrü Özdemir, A. (2011). *Effects of Cryptographic Activities on Understanding Modular Arithmetic. Turkish Journal of Computer and Mathematics Education (Vol. 2, No. 3).* Pribavljeno 15.5.2018., sa https://digital.kenyon.edu/cgi/viewcontent.cgi?article=1004&context=math_pubs
2. Barun, M., Dujella, A., Franušić, Z. (2008). *Kriptografija u školi, Poučak (1332-3008) 33*. Pribavljeno 15.5.2018., sa https://www.researchgate.net/publication/258340051_Kriptografija_u_skoli
3. Borelli, M., Fioretto, A., Sgarro, A., Zuccheri, L. (2002). *Cryptography and statistics: a didactical project. Proceedings of ICTM2.* Pribavljeno 15.5.2018., sa https://www.researchgate.net/publication/228959989_Cryptography_and_Statistics_A_didactical_project
4. Čavrak, H.(2004). *Enigma. Hrvatski matematički elektronski časopis (Broj 3).* Pribavljeno 15.5.2018., sa http://e.math.hr/old/enigma/index.html
5. Dujella, A.(2016). *Teorija brojeva i kriptografija*. *Novigrad nekad i sad*. Pribavljeno 15.5.2018., sa https://www.researchgate.net/publication/316076279_Teorija_brojeva_i_kriptografija
6. Dujella, A., Maretić, M. (2007). *Kriptografija.* Zagreb: Element.
7. Fellows, M. R., Koblitz, N. (2000). *Combinatorially Based Cryptography for Children (and Adults). Congressus Numerantium.* Pribavljeno 15.5.2018., sa https://www.researchgate.net/profile/Michael_Fellows/publication/2327196_Combinatorially_Based_Cryptography_for_Children_and_Adults/links/5419e9250cf2218008bfa37b.pdf
8. Kapitanović, V. (2012). *Povijesna vrela i pomoćne znanosti*. Split: Filozofski fakultet.
9. Koblitz, N. (1997). *Cryptography As a Teaching Tool. Cryptologia (Vol. 21, No. 4.).* Pribavljeno 15.5.2018., sa https://sites.math.washington.edu/~koblitz/crlogia.html
10. Singh, *S.* (2003). *Šifre: kratka povijest kriptografije.* Zagreb: Mozaik knjiga.
11. Taylor & Francis, Inc.(2001). *From The Archives: The Glow-Lamp Ciphering and Deciphering Machine, Cryptologia (Vol. 25, No.3)*. Pribavljeno 15.5.2018., sa

https://www.globalspec.com/reference/62871/203279/the-glow-lamp-ciphering-and-deciphering-machine-enigma-from-the-archives

12. Wijesekera, S. (2011). *Quantum Cryptography for Secure Communication in IEEE 802.11 Wireless Networks. Degree of Doctor of Philosophy.* Pribavljeno 15.5.2018**.,** sa https://pdfs.semanticscholar.org/fe4f/8154a5ba77c632015ea41ca273a7b16ca13f.pdf

PRILOZI

Prilog 1. Radni listić za rad s učenicima razredne nastave s rješenjima.

Potraga za blagom

1. Pokušaj svoje ime i prezime napisati pomoću glagoljice (slova Č i Ć zamijeni sa C, Dž i Đ sa D, Lj napiši kao dva slova L i J, NJ napiši kao dva slova N i J, Š kao S, a Ž kao Z.)

Moje ime je _____

2. Pokušaj osmisliti svoje vlastito tajno pismo i napiši poruku nekome u razredu.

A		B		C		Č		Ć	
D		Dž		Đ		E		F	
G		H		I		J		K	
L		Lj		M		N		Nj	
O		P		R		S		Š	
T		U		V		Z		Ž	

Poruka: _____

3. Pomoću kruga pokušaj brojevima napisati svoje ime.

_____

4. Pomoću kruga pokušaj brojevima napisati:

M A T E M A T I K A 18 1 26 9 18 1 26 13 15 1

5. Od najvećeg neparnog broja iz prošlog zadatka oduzmi najmanji neparan broj. Zapamti taj broj.

15	-	1	=	14

6. Pomoću Cezarove šifre (Slovo A poravnamo sa slovom Č, tj. pomičemo ga za 3 mjesta) šifriraj ovu rečenicu i odgovori:

HMGF NVNjVL ZNjMG GD ŠDBF MC RNjF, V KVLjF GD MC PDOR?

Šifra: KOJI PARAN BROJ JE VEĆI OD TRI, A MANJI JE OD ŠEST?

Odgovor na pitanje: ČETIRI

7. Od rješenja 5. zadatka oduzmi rješenje 6. zadatka i dobit ćeš broj omotnice u kojoj je blago.

14	-	4	=	10

Omotnica u kojoj je blago je pod brojem 10 .

Prilog 2. Evaluacijski listić za učenike trećih razreda.

Zaokruži:

1. Radionica mi se svidjela.	DA	NE
2. Ne razumijem radionicu.	DA	NE
4. Šifriranje i dešifriranje je zanimljivo.	DA	NE
6. Šifrirat ću poruke u budućnosti.	DA	NE

Prilog 3. Radni listić za rad s učenicima predmetne nastave s rješenjima.

Potraga za blagom

1. Pomoću Cezarove šifre (ključ = 3) dešifriraj poruku:

A	B	C	Č	Ć	D	DŽ	Đ	E	F	G	H	I	J	K	L	LJ	M	N	NJ	O	P	R	S	Š	T	U	V	Z	Ž
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

A	B	C	Č	Ć	D	DŽ	Đ	E	F	G	H	I	J	K	L	LJ	M	N	NJ	O	P	R	S	Š	T	U	V	Z	Ž
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59

ĆTSLj SOSZPLDH PH UČETCL BPČOHPMŽ ZTL.

(BROJ OMOTNICE NE SADRŽI ZNAMENKU TRI.)

2. Pomoću supstitucijske šifre kojoj je ključ = 10 dešifriraj poruku:

A	B	C	Č	Ć	D	DŽ	Đ	E	F	G	H	I	J	K	L	LJ	M	N	NJ	O	P	R	S	Š	T	U	V	Z	Ž
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

A	B	C	Č	Ć	D	DŽ	Đ	E	F	G	H	I	J	K	L	LJ	M	N	NJ	O	P	R	S	Š	T	U	V	Z	Ž
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59

HCAS AVADZRIN SN ĐNKR AL LNČND.

(BROJ OMOTNICE JE VEĆI OD DESET.)

3. Pomoću Polibijevog kvadrata dešifriraj poruku:

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

12 45 43 32 43 36 43 52 41 31 13 23 41 31 32 23 16 32 23 35 31 54 46 44 23 52.

(BROJ OMOTNICE NIJE DJELJIV S PET.)

4. Pomoću Vigenèreove šifre dešifriraj poruku, ključ = ZEC

A	B	C	Č	Ć	D	DŽ	Đ	E	F	G	H	I	J	K	L	LJ	M	N	NJ	O	P	R	S	Š	T	U	V	Z	Ž
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

A	B	C	Č	Ć	D	DŽ	Đ	E	F	G	H	I	J	K	L	LJ	M	N	NJ	O	P	R	S	Š	T	U	V	Z	Ž
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59

ŽARH UKHLj ĐHLjNGD T BLjVGAK.

(BROJ NIJE DJELJIV S ČETIRI.)

5. Pomoću ATBASH šifre dešifriraj poruku:

A	B	C	Č	Ć	D	DŽ	Đ	E	F	G	H	I	J	K	L	LJ	M	N	NJ	O	P	R	S	Š	T	U	V	Z	Ž
Ž	Z	V	U	T	Š	S	R	P	O	NJ	N	M	LJ	L	K	J	I	H	G	F	E	Đ	DŽ	D	Ć	Č	C	B	A

ZĐFLj FIFĆHMVP DžŽŠĐAM BHŽIPHLČ ŠCŽ.

(BROJ OMOTNICE SADRŽI ZNAMENKU DVA.)

6. Pomoću Cik-cak šifre dešifriraj poruku:

RJMTIEEJLjVDVT BOOONCJDEISEE.

(BROJ OMOTNICE JE DJELJIV S DEVET.)

Rješenje: Blago je u 27. omotnici ☺

Prilog 4. Evaluacijski listić za učenike sedmih razreda.

Ocijeni ocjenom od 1 do 5 (zaokruži) te izrazi svoje mišljenje o radionici.
1 - UOPĆE SE NE SLAŽEM, 2 - NE SLAŽEM SE, 3 - NITI SE SLAŽEM NITI SE NE SLAŽEM, 4- SLAŽEM SE, 5- U POTPUNOSTI SE SLAŽEM

1. Radionica mi se svidjela.	1	2	3	4	5
2. Metode šifriranja i dešifriranja su bile preteške za razumjeti.	1	2	3	4	5
3. Htio/htjela bih više ovakvih sadržaja u nastavi matematike.	1	2	3	4	5
4. Smatram da je šifriranje i dešifriranje zanimljivo.	1	2	3	4	5
5. Šifriranje poruka sam već upotrebljavao/upotrebljavala prije.	1	2	3	4	5
6. U budućnosti ću upotrebljavati šifriranje poruka.	1	2	3	4	5

Prilog 5. Evaluacijski listić za studente.

Ocijeni ocjenom od 1 do 5 (zaokruži) te izrazi svoje mišljenje o radionici.
1 - UOPĆE SE NE SLAŽEM, 2 - NE SLAŽEM SE, 3 - NITI SE SLAŽEM NITI SE NE SLAŽEM, 4- SLAŽEM SE, 5- U POTPUNOSTI SE SLAŽEM

1. Radionica mi se svidjela.	1	2	3	4	5
2. Metode šifriranja i dešifriranja su bile preteške za razumjeti.	1	2	3	4	5
3. Pojedine sadržaje iskoristio/la bih u nastavi matematike.	1	2	3	4	5
4. Pojedine sadržaje iskoristio/la bih u dodatnoj nastavi matematike.	1	2	3	4	5
5. Smatram da je šifriranje i dešifriranje zanimljivo.	1	2	3	4	5
6. Šifriranje poruka sam već upotrebljavao/upotrebljavala prije.	1	2	3	4	5
7. U budućnosti ću upotrebljavati šifriranje poruka.	1	2	3	4	5