Razumijevanje tajnih poruka

Škrobo, Marko

Master's thesis / Diplomski rad

2017

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Department of Mathematics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:358557

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**



Repository / Repozitorij:

Repository of School of Applied Mathematics and Computer Science







Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Diplomski studij matematike

Marko Škrobo

Razumijevanje tajnih poruka

Diplomski rad

Osijek, 2017.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Diplomski studij matematike

Marko Škrobo

Razumijevanje tajnih poruka

Diplomski rad

Voditelj: izv. prof. dr. sc. Ivan Matić

Osijek, 2017.

Sadržaj

1. UVOD **4**

2. Povijest tajnog pisanja **6**

3. Umijeće prikrivanja poruka **8**

4. Neobične metode slanja poruke **12**

5. Šifre za druge svjetove **16**

6. Ratni kodovi **20**

6.1. Spartanski skital 20

6.2. Cezarova šifra s pomakom 21

6.3. De Vigenereova tablica 22

6.4. Playfairova šifra 23

6.5. Enigma: „neprobojni“ sustav 25

7. Tajni kodovi u poznatim knjigama **29**

7.1. Biblijski kod 29

7.2. Kama sutra 30

8. Literatura **31**

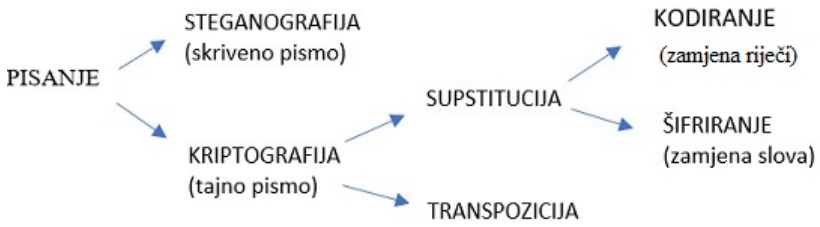
9. Sažetak **32**

10. Title and summary **33**

11. Životopis **34**

1. UVOD

Već stoljećima kraljevi, kraljice i vojskovođe pri upravljanju svojim zemljama i vođenju svojih vojski ovise o djelotvornoj komunikaciji. Međutim, bili su svjesni toga što bi se dogodilo kada bi njihove poruke došle u krive ruke i tako suparničkim državama razotkrile čuvane tajne, a protivničkim snagama odale važne informacije. Ta opasnost da bi neprijatelj mogao uhvatiti poruku, napokon je i potaknula razvoj šifri i kodova, odnosno sredstava kojima se postiže da poruku može pročitati samo onaj kome je ona namijenjena.
Šifrirati znači zamrsiti poruku pomoću šifre, a **kodirati** učiniti to isto pomoću koda. Slično tome, **dešifriranje** označava odgonetanje šifrirane, a **dekodiranje** odgonetanje kodirane poruke. Izrazi **enkriptirati** i **dekriptirati** označavaju zapletanje i raspletanje poruke pomoću i šifre i koda. Na Slici 1 imamo sažetak tih definicija.



Slika 1: Glavni ogranci umijeća tajnog pisanja

Prije nego što su osmišljeni slovni i brojčani kodovi, nastale su razne domišljate tehnike, od kojih su neke u upotrebi i danas. Informacije su se prenosile na takav način da nitko, osim pošiljatelja i namjernog primatelja, ne posumnja u postojanje poruke. Na taj način tajna se poruka skriva unutar neke druge bezazlene poruke tako da se postojanje tajne poruke ne može uočiti. Iako se u strogom smislu ne radi o kodiranju, nastojanja s ciljem skrivanja poruke primjenom tzv. „tajnog pisma“ po ciljevima su slična kriptografiji i danas su poznata pod nazivom **steganografija**. Riječ steganografija je grčkog porijekla i znači "skriveno pisanje". Sastoji se od riječi *steganos* što znači "pokriveno" ili "zaštićeno", i *graphei* što znači pisanje. Dugovječnost steganografije pokazuje da ona nudi izvjesnu sigurnost, no isto tako možemo reći i da pati od fundamentalne slabosti. Naime, ako glasnika pretraže i otkriju poruku, njezin se sadržaj smjesta razotkriva. Odnosno, hvatanje poruke smjesta razrješava tajnu. Iz tih razloga paralelno s razvojem steganografije evoluirala je i **kriptografija**. Sama riječ kriptografija dolazi od grčke riječi *kryptos*, što znači skriven. Cilj kriptografije nije zatajiti samo postojanje poruke, već prikriti njezino značenje, i to pomoću procesa zvanog enkripcija, odnosno šifriranje ili kodiranje.

Da bi poruka postala nerazumljiva, slova se u njoj ispremeću po nekom određenom pravilu, unprijed dogovorenom između pošiljatelja i primatelja. Tako primatelj može to pravilo preokrenuti, pa mu poruka postaje razumljiva. Prednost je kriptografije što neprijatelj ne može razabrati sadržaj čak ni uhvaćene poruke. Bez poznavanja tog pravila miješanja neprijatelj će teško ili nikako iz šifriranog teksta moći izvući poruku. Kriptografiju je moguće podijeliti u dvije grane, jednu u kojoj se enkriptiranje obavlja pomoću **transpozicije** (premještanja, prevođenja) i drugu, u kojoj se obavlja pomoću **supstitucije** (zamjene). Kod transpozicije se slova jednostavno premještaju i tako zapravo nastaje anagram. Kod vrlo kratkih poruka, primjerice onih koje se sastoje od samo jedne riječi, ta je metoda prilično nesigurna zato što se malen broj slova može ispremiještati na samo malen broj načina. Razvoj steganografije i kriptografije bio je uvjetovan razvojem naprava, koje su omogućavale brže i bolje prikrivanje otvorenog teksta.

2. Povijest tajnog pisanja

Premda je pojam steganografija formiran tek krajem 15. stoljeća, različite steganografske tehnike koriste se već nekoliko tisućljeća. Slijedi pregled najpoznatijih primjena tajnog pisanja kroz povijest:

- Neki od najranijih zapisa o tajnom pisanju potječu još od grčkog povjesničara Herodota. U svojim kronikama pod imenom „Povijesti“ opisuje sukob između Grčke i Perzije u petom stoljeću prije Krista. Herodot je zabilježio dvije priče u kojima se koriste steganografske tehnike u tom vremenu. U prvoj priči navodi kako je kralj Darius obrijao glavu jednom od svojih robova i tetovirao mu tajnu poruku na skalp. Kada je robu kosa natrag narasla i prekrila kraljevu poruku, Darius ga je poslao svom zetu Aristagoru u Milet sa sakrivenom porukom. U drugoj Herodotovoj priči vojnik imena Demarat je trebao poslati poruku u Spartu da Kserkso namjerava napasti Grčku. U to vrijeme podloga za pisanje bile su voskom prekrivene drvene pločice, no Demarat je uklonio vosak sa pločice, upisao skrivenu poruku u drvo te ju natrag prekrio sa voskom kako bi izgledala kao prazna pločica. Konačno, tajna poruka je bila sigurno prenesena.

- Rimljani su za sakrivanje informacija koristili nevidljive tinte, koje su se bazirale na prirodnim supstancama poput voćnih sokova ili mlijeka. Čitanje poruke se postiže zagrijavanjem skrivenog teksta i tada se prikazuje njegov sadržaj. Nevidljive tinte se naprednijim metodama i u ograničenoj uporabi koriste i danas.

- Tijekom Prvog svjetskog rata i Drugog svjetskog rata dogodio se značajan napredak u steganografskim tehnikama. Razvijene su metode „**null šifre**“ (čitanje trećeg slova u svakoj riječi u naizgled bezazlenoj poslanoj poruci). Jedan od najpoznatijih primjera primjene opisane metode vezan je uz japansku špijunku Velvalee Dickinson, poznatiju pod imenom Doll Woman (žena lutka). Velvalee se tijekom 2. svjetskog rata bavila prodajom i nabavom lutaka pa je često slala pisma iz New Yorka u neutralnu Južnu Ameriku koja su sadržavala narudžbe za lutke. Dotični tekst narudžbi je zapravo sadržavao sakrivene informacije o kretanjima brodova.

- Također, poruke su se znale prenositi korištenjem znakova Morseove abecede ili na poleđini poštanskih maraka.

- Tijekom i nakon 2. svjetskog rata Nijemci su sakrivali podatke tako da su tajnu poruku fotografirali i smanjili ju u tolikoj mjeri da bi unutar nekog poslanog dokumenta izgledala kao točka (interpunkcijski znak, „ . “).

- Talijanski znanstvenik Giovanni Porta, rođen 1535. godine, je otkrio kako sakriti poruku unutar skuhanog jajeta. Kao tintu je koristio mješavinu stipse i octa. Poruku bi nanio na skuhano jaje, a tinta od stipse i octa bi prodrla kroz ljusku jaja. Skrivena poruka bi se očitala s bjelanjka nakon što bi se jaje ogulilo.
- Drevni Kinezi su na tanki komad svile zapisivali poruku, zatim su taj komad stavljali u voštanu kuglicu koju bi glasnik progutao.

3. Umijeće prikrivanja poruka

Jedna od antičkih metoda prikrivanja poruka je pisanje pomoću **nevidljive tinte**, gdje tekst postaje vidljiv tek kada se podvrgne određenom „tretmanu“. Tako je Plinije Stariji još u prvom stoljeću objasnio kako je nevidljivu tintu moguće dobiti iz „mlijeka“ biljke mlječike. Takva je tinta kada 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. Nisu nepoznati ni slučajevi kada su moderni špijuni, ostavši bez standardne nevidljive tinte, posegnuli za improvizacijom pa poruku napisali vlastitom mokraćom.
Postoje različite vrste neividljivih tinti, a najbolje su one za čiji pripravak je potrebna rijetka kemikalija. Takvi spojevi su teško dostupni, pa samim time otežavaju otkrivanje poruke. Neki kemijski spojevi, prvobitno nevidljivi na papiru, postaju crveni ili plavi u doticaju s drugom tvari, koja se naziva reagens. Uloga reagensa je poticanje kemijske reakcije, koja će tintu učiniti vidljivom. Dosta spojeva, koji se mogu koristiti za ovakav način pisanja poruke, mogu biti opasni. Za njihovo rukovanje potrebne su velike mjere opreza.
Profesionalni špijuni su rijetko kada posebnu tintu koristili na čistom bijelom papiru jer bi u slučaju presretanja, to pobudilo veliku sumnju. Umjesto toga nevidljivom tintom bi pisali između redaka neke nevezane poruke ili na poleđini pisma ili fotografije. Često su se i označavala slova u knjizi ili časopisu. Tako da bi na prvi pogled knjiga izgledala sasvim obično, ali čitanjem slova označenih tintom prava poruka bi dobivala smisao. Nevidljivo pisanje može se kombinirati sa šifriranjem. Tada ako neželjeni promatrač uspije učiniti tintu vidljivom, sve što mu je dostupno je šifrat, kojeg ne zna dešifrirati.
Sljedeće metode nevidljivog zapisa su sigurne i djelotvorne, i korištene su supstance koje je relativno lako dobiti.

Tinte koje reagiraju na toplinu

Sok skoro svih agruma može se koristiti kao tinta koja reagira na toplinu. Poruka se piše tankim kistom za slikanje, a ne kemijskom olovkom kako na papiru ne bi ostali tragovi pisanja, što bi moglo dovesti do lakšeg otkrivanja teksta. Ako se koristi kemijska treba biti siguran da je vrh kemijske potpuno čist. Inače, neke stare tinte pomiješane s nevidljivom tintom postanu vidljive. Također, treba se pisati na hrapavom, a ne glatkom papiru, da se tinta ne osuši na površini nego upije i tako ostane očuvana. Poruka se otkriva tako da se papir lagano zagrijava pomoću žarulje koja isijava toplinu ili nekog drugog slabog izvora topline. Ukoliko bi se koristila vatra papir bi se mogao previše zagrijati ili

čak zapaliti. Zbog organskog podrijetla tinte bogate ugljikom, dolazi do izlučivanja čađe, pa napisani tekst postaje smeđe boje.

Tinte koje pocrvene

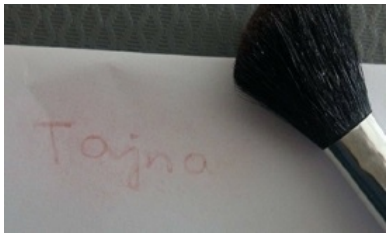
Jedan takav primjer je fenolftalein - bijeli kristalni prah netopljiv u vodi. On je jedan od najpoznatijih kemijskih indikatora. Bezbojan je u neutralnom i kiselom mediju (ispod pH 8), dok u reakciji s lužinama daje intenzivno crveno obojenje. Mađioničari ga često koriste za trik pretvaranja vode u vino. Fenolftalein je glavni sastojak laksativa pa se na taj način lako može doći do njega s obzirom da u ljekarnama najčešće ne žele prodati čisti fenolftalein.
Postupak je sljedeći. Pomiješa se prah čiste tvari ili zdrobljena tableta laksativa sa 70-postotnim alkoholom. Tableta mora biti posve otopljena. Tajna poruka piše se kistom. Zapis će biti nevidljiv sve dok je tinta suha. Poruka se otkriva tako da se krpica namoči lužnatim sredstvom, a to može biti sredstvo za čišćenje s amonijakom, i njome se pažljivo prijeđe po papiru. Odmah će se pojaviti purpurno crveni zapis. Kada se papir osuši crveni zapis će ponovno iščeznuti.

Tinte koje svijetle pod crnim svjetlom

Neke simpatetičke tinte svijetle pod ultraljubičastim zračenjem ili tzv. crnom svjetlu. Takve tinte koriste se dosta često kao žigovi u disko klubovima, klizalištima i zabavnim parkovima kako bi se identificirala osoba koja je već platila ulaznicu, a želi ponovno ući. Banke ih koriste za potpise i identifikacijske kartice.
Najlakši način stvaranja tinte koja bi bila vidljiva samo pod crnim svjetlom je otapanjem u vodi bilo kojeg praška za pranje rublja koji izbjeljuje odjeću. Ultraljubičasto zračenje iz sunčevih zraka aktivira umjetne tvari koje potiču izbjeljivanje. Kako bi se komuniciralo ovom metodom potrebno je nabaviti neku vrstu flourescentne lampe koja zrači crno svjetlo. Pri tome treba biti pažljiv i zaštititi oči. Kako bi se postigla najbolja smjesa praška i vode, potrebno je eksperimentirati. Previše vode smanjit će sjaj, a premalo vode uzrokovat će da je tinta odmah vidljiva na papiru. Vrsta papira je također bitna. Treba izbjegavati bijeli papir, kao što je papir za printanje, jer sam po sebi sjaji pod crnim svjetlom. Najbolji je tamniji s krutom površinom.

Tinte vidljive nakon pudranja

Jedan od boljih primjera tinte te vrste je obično mlijeko. Mlijeko se kistom nanese na deblji papir ili tanji karton i čeka se da se osuši. Nakon toga se utrlja puder bilo koje tamnije tvari i nevidljivi zapis postat će otkriven. Pri tome se može koristiti pepeo, rumenilo za obraze, grafitna olovka, drveni ugljen i slično. Na Slici 2 prikaz je otkrivanja poruke pomoću rumenila za obraze.



Slika 2: Zapis vidljiv nakon pudranja

Tinte koje reagiraju na vodu

Postoje mnoge kemijske formule za simpatetičku tintu, koja u doticaju s vodom postaje vidljiva. U ovom slučaju ne trebamo nikakvu nevidljivu tintu, niti kemijske tvari. Umjesto toga upotrebljava se vodeni žig.
Primjenom pritiska mijenjaju se vlakna papira ostavljajući trag vidljiv samo kada je papir mokar. Papir umočimo u vodu i stavimo na ravnu tvrdu podlogu (primjerice staklo, aluminijski list, ogledalo, granitna ploča). Preko njega stavimo novi suhi papir i napišemo poruku običnom ii kemijskom olovkom. Zatim maknemo suhi papir, dok je na donjem mokrom papiru vidljiva poruka. Kada se papir osuši poruka će postati nevidljiva. Poruka će opet postati vidljiva ukoliko se papir uroni u vodu.

Pismo vidljivo pod kosim svjetlom

Ova metoda također koristi pritisak za promjenu vlakana papira. Kao i u prethodnoj metodi stavljaju se dva papira jedan na drugi, ali oba moraju biti suha. Na gornji papirić napiše se poruka kemijskom ili grafitnom olovkom i on se pri tome ukloni. Zapis na drugom papiru najbolje se može vidjeti kada se osvijetli papir pomoću male baterije u mračnoj sobi pod određenim kutom.
Fotografi taj snop svjetlosti nazivaju koso svjetlo jer otkriva bilo kakve nepravilnosti na površini. Ukoliko nemamo na raspolaganju malu bateriju, na leću velike baterije zalijepi

se komadić crnog papira s malom rupom na njemu. Tim metodama često se koristila policija i špijuni.

Pismo vidljivo pod rasplamsanim svjetlom

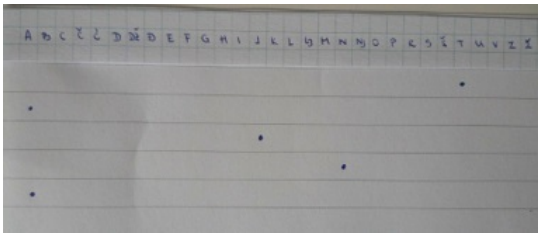
Umjesto grafitne ili kemijske olovke, pisača mašina može ostaviti odličan otisak tijekom pisanja koji je nevidljiv sve dok se ne osvijetli rasplamsanim svjetlom. Umetnu se dva lista, napiše se poruka i uništi se stranica na kojoj je vidljiva tinta. Zapis na drugom papiru je nemoguće vidjeti.
Ako se želi dodatno zaštititi od presretanja poruke, može se napisati pogrešno pismo na list papira, a zatim preko njega staviti novi papir i pisati između redaka prvog pisma pravu poruku. Nakon što se uništi gornji papir ostaje list na kojem je tajna poruka smještena između redova vidljive nevezane poruke.

4. Neobične metode slanja poruke

Nemoguće je opisati sve neobične metode koje su špijuni koristili kako bi poslali tajne poruke. Mnoge od njih su praktične metode, kao što je brijanje glave. Naime, Grci su svojim glasnicima znali poruku napisati na tjeme i čekati dok kosa naraste. Glasnik je lako mogao proći pored protivnika jer naizgled nije nosio ništa sporno. Kada bi stigao do odredišta, obrijali su mu glavu i pročitali poruku. Vrlo neobična metoda je slanje poruke putem mačke. Napisali bi poruku i dali mački da pojede. Kada bi mačka donijela poruku ubili bi je i tada pročitali poruku. Još jedan primjer je pisanje mješavinom stipse i octa po ljusci jajeta. Jaje se skuha i pošalje primatelju. Skidanjem ljuske otkriva se poruka na stjenkama kuhanog jajeta.
Netom prije 2. svjetskog rata Nijemci su razvili i koristili fotografsku metodu prikrivanja poruka pomoću sitnih točkica. Cijelu stranicu papira bi fotografirali i sliku umanjili do veličine obične točke. Proširenjem slike skrivena poruka se mogla pročitati.

Šifriranje pomoću točaka

Kako bi se komuniciralo na ovakav način potrebne su dvije trake od papira koje su identične. Na svaku traku se napišu slova abecede s jednakim razmakom. Za brže šifriranje slova trebaju biti u pravilnom poretku, ukoliko su pomiješana kôd je teže šifrirati.
Za ovu vrstu šifriranja koristi se papir s linijama. Traku s abecedom potrebno je staviti ispod prve horizontalne linije, a da se pritom poravnaju lijevi rubovi kao što je prikazano na Slici 3.



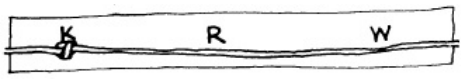
Slika 3: Šifriranje pomoću točkica

Šifriranje riječi *TAJNA* izgledalo bi ovako. Povrh prvog slova T stavi se točkica, a zatim se traka s abecedom pomakne jedan redak ispod te se točkica stavlja iznad sljedećeg slova, a to je slovo A. Postupak se ponavlja sve dok se ne ispiše cijela riječ *TAJNA*.
Ukoliko netko ima isti papirić s abecedom, bez problema će dešifrirati poruku.
Također, točkice je moguće spojiti linijama kako bi se prikrila njihova važnost ili zbunilo neprijatelja. Linije se ne smiju presijecati jer bi njihovo sjecište izgledalo kao još jedna

točkica za slovo. Još jedan način je da se umjesto točkica na papiru naprave male rupice, što će dodatno otežati dešifriranje, pogotovo ako su one dovoljno sitne. Također se na isti list može napisati i poruka za dodatno odvraćanje pažnje.

Šifriranje pomoću čvorova

Umjesto točkica šifriranje i dešifriranje obavlja se pomoću čvorova. Postupak je sličan kao i kod prethodnog šifriranja, samo se treba ostaviti veći razmak između pojedinog para slova jer je potrebno više mjesta za pravljenje čvorova.



Slika 4: Kod pomoću čvorova

Komad užeta ili niti postavi se na početak trake na koju će biti zapisana slova tako da početak s lijeve strane odgovara početku trake sa slovima. Čvor se zaveže na mjestu koje odgovara prvom slovu poruke. Zatim se uže pomakne ulijevo tako da je prvi čvor poravnat s početkom trake. Isto se ponavlja do kraja poruke. Kada je postupak završen, rezultat je komad užeta s mnogo čvorova, koji neupućenom promatraču izgledaju smješteni nasumično. Da bi primatelj dešifrirao poruku mora imati traku jednaku pošiljateljevoj.

Crveno - plava šifra

U mnogim mjesnim trgovinama može se pronaći crveni celofan za umatanje poklona koji također može poslužiti za šifriranje poruka. Može poslužiti za trenutno šifriranje tajne poruke, karte, dijagrama ili nečeg drugog što se može napisati na list papira. Prvo se crvenom kemijskom olovkom napiše lažna poruka ili se nacrta lažni crtež. Tajna poruka se potom nanosi plavom tankom kemijskom da se napisano slabo uočava. Po mogućnosti treba pisati točno na crvene tragove, a ne u bijele praznine. Kako bi se pročitala poruka, papir se prekrije crvenim celofanom. Sada linije napisane crvenom kemijskom olovkom nestaju, a plave linije su jasne i čitke.

Šifriranje pomoću igraćih karata

Kod ove neobične metode, tajnu poruku može prenijeti obični špil igraćih karata. Najbolje je koristiti špil od 52 karte. Poredak između primatelja i pošiljatelja u špilu je unaprijed dogovoren na proizvoljan način. Kada su karte u dogovorenom poretku, poruka se napiše velikim tiskanim slovima s bočne strane po rubovima. Nagnute vertikalne i horizontalne linije slova čine šifriranje još efikasnijim, kako je prikazano na Slici 5.

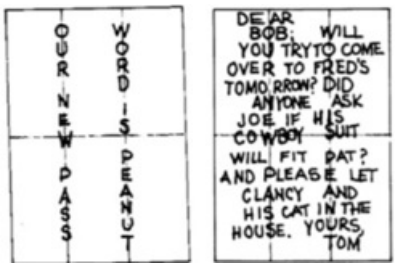


Slika 5: Šifriranje pomoću igraćih karata

Karte se zatim promiješaju što više puta i poruka više nije vidljiva. Primatelj vrati karte u dogovoreni poredak i postupak dešifriranja je gotov. Ako je tekst pisan olovkom, isti špil se može koristiti više puta. Jednostavno se obriše prethodna poruka i napiše nova.

Šifriranje presavijanjem papira

Za ovu metodu tajnog komuniciranja potreban je običan list papira i olovka. Papir se presavije tri ili više puta tako da ostanu vidljivi nabori. Ponovno se otvori i napiše poruka duž vertikalnih linija vidljivih od savijanja. Potom se ostatak ispuni različitim slovima ili se osmisli pismo, koje će zavarati protivnika kao što je prikazano na Slici 6.

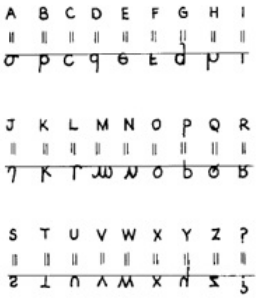


Slika 6: Šifriranje presavijanjem papira

Čitanje poruke je lako. Samo se prate slova po naborima i pravi smisao je otkriven.
Ako je u pitanju veći tekst, umjesto pisanja slova po naborima, mogu se na isti način pisati riječi. Opet se u praznine napišu riječi za zavaravanje i postupak je gotov.

Šifriranje pomoću plastičnog štapića

Plastični štapić za miješanje pića također može pomoći za šifriranje i skrivanje poruka. Kroz takve štapiće moguće je gledati jer su prozirni. Imaju neobično svojstvo, ponašaju se kao cilindrične leće. Vrlo teško je kroz njih čitati tekst jer okreću sliku naopako, odnosno stvaraju zrcalnu sliku slova. Tajna poruka se piše korištenjem zamjenske abecede prikazane na Slici 7.

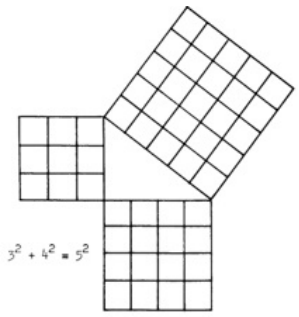


Slika 7: Zamjenska abeceda za šifriranje pomoću plastičnog štapića

Dešifriranje je gotovo istog trena kada se poruka pogleda kroz spomenuti štapić. U slučaju da primatelj pri ruci nema takav štapić, može se poslužiti sljedećim trikom. Okrenuti poruku naopako i pogledati ju pomoću zrcala.

5. Šifre za druge svjetove

Svi kodovi koje smo dosad razmatrali namijenjeni su da otežaju poruke svakome tko razumije engleski osim ako ne zna metodu dekodiranja. No, sada se razmatra suprotan problem. Kako netko može poslati poruku koju lako može pročitati netko tko ne zna naš jezik? Zaista, primatelj poruke može biti netko tko čak nije sa Zemlje.
To je problem u komunikaciji koju intenzivno proučavaju astronomi, matematičari i stručnjaci za jezik. Radi se o slanju ili primanju poruka s drugih planeta na kojima možda postoji inteligentan život.
Astronomi vjeruju da je izrazito mala mogućnost da postoji inteligentan život na bilo kojem planetu u našem sunčevom sustavu. Početkom stoljeća, prije nego što su svemirske sonde fotografirale Mars, mnogi astronomi su bili uvjereni da je Mars nastanjen inteligentnim bićima.
U vrijeme kada se postojanje marsovaca činilo kao stvarna mogućnost mnogi znanstvenici su razmišljali o pitanju: Kako bismo mogli poslati poruku na Mars u kojoj bismo rekli marsovcima da postojimo? Jedan plan je bio napraviti ogromni reflektor koji bi odašiljao treptajuće kodirane poruke, a koje bi mogao prihvatiti marsovski teleskop. Drugi plan je bio da se napravi dugački lanac od ogromnih svjetla koji bi bio u obliku jednostavnog geometrijskog tijela kao što je kvadrat ili krug ili barem dijagram osnovnog teorema geometrije. Primjerice, razumijevanje Pitagorina teorema jako je važno u geometriji ravnine jer ako Marsovci znaju geometriju i vide svojim teleskopom dijagram poput prikazanog na Slici 8, tada bi odmah razumjeli njegovo značenje.



Slika 8: Pitagorin teorem

Danas, astronomi više ne vjeruju da postoje Marsovci, stanovnici Venere, Jupitera ili Saturna. Što je s inteligentnim životom na planetima koji se kreću oko ostalih sunca na našoj Mliječnoj stazi? Ima li tamo koga? Nitko ne zna za sigurno, ali većina astronoma misli da je odgovor potvrdan. Ako inteligentna bića postoje možda već stoljećima pokušavaju komunicirati s ostalim planetima pomoću radio kodova. Godine 1960. jedan od

većih radio teleskopa u Green Banku, West Virginia počeo je skenirati nebo tražeći takve poruke. Projekt je nazvan Ozma prema djevojčici vladarici Zemlje iz Oza. Poruke nisu detektirane i projekt je napušten, ali i dalje se sluša sa drugim radio teleskopima ovdje i u drugim zemljama.

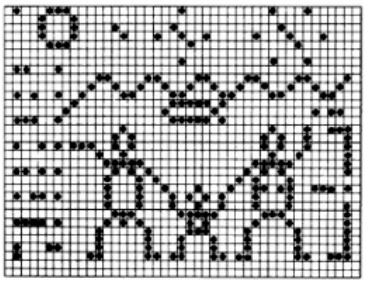
Kada bi se pokušao otkriti život na drugim planetima pomoću signala radio kodova, postavlja se pitanje kako najbolje privući pozornost slušatelja da odmah shvate da netko pokušava razgovarati s njima? Najjednostavnije bi bilo poslati niz cijelih brojeva 1, 2, 3, 4, 5, ... Najprije samo jedan zvučni signal, zatim 2 (beep-beep), zatim 3 i tako dalje. Budući da je brojenje jednako na svakom planetu, kada bi stanovnici udaljenog planeta, recimo Planet Zeta, brojili zvijezde ili kamenčiće ili bića kao što su oni ili bilo što drugo što može doći u vidljivim oblicima radili bi to na isti način kao što mi to radimo. Moguće je da bi koristili drugi bazni sustav za prikazivanje brojeva. Ako bi imali 12 prstiju umjesto 10 vjerojatno bi preferirali brojevni sustav u bazi 12 umjesto dekadskog. Ali kada je brojanje poslano kao niz zvučnih signala tada nije važno koji je brojevni sustav korišten da ih se zabilježi.

Kada bi se privukla pozornost Zetana nizom brojeva mogli bi ih početi poučavati signalima koje koristimo za zbrajanje, oduzimanje , množenje, dijeljenje i jednakosti. Na primjer, pošalje li se beep-beep, pauza, „beep“ signal znači plus, pauza, još tri beep, pauza, signal koji označava jednakost, pauza, zatim pet beep. Budući da Zetani već znaju da je dva plus tri pet, shvatili bi da je drugi signal označavao plus, a četvrti signal jednakost. Na isti način Zetani bi mogli naučiti naše signale za ostale aritmetičke operacije. Nula je važna. Mogli bismo prenijeti naš signal za nju na način da pošaljemo jednakosti kao što su $8 + 0 = 8, 0 + 7 = 7, 5 \cdot 0 = 0, 0 + 0 =$0 i tako dalje.

Sad slijedi presudni korak. Pošaljemo, iznova i iznova jednakost kao što je $31 \cdot 41 = 1\ 271$ (nakon što smo ih naučili obilježavanje mjesne vrijednosti tako da možemo poslati 1 271 bez da moramo poslati 1 271 signala!). Zatim pošaljemo niz od točno 1 271 brojeva koji se sastoji od nula i jedinica slučajnim redoslijedom. Niz od 1 271 brojeva bio bi ponovljen mnogo puta. Možda bi to Zetani snimili i puštali si koliko god bi htjeli kako bi mogli pažljivo proučiti. Što znači taj niz?

Naravno, ako su naši slušatelji dovoljno pametni da naprave instrumente koji mogu primati radio signale sa udaljenog planeta, tada su vjerojatno dovoljno pametni da znaju kako napraviti slike skeniranjem pravokutne matrice ćelija, koristeći 1 za ćeliju koja je crna, a 0 za ćeliju koja ostaje prazna. Istina, oni možda ne vide svijet na način kako ga mi vidimo i ono što mi zovemo „crno“ možda ne može biti primjenjivo u njihovim osjetilima. Ali to nije važno. Važno je samo da znaju razlikovati 1 - ćeliju od 0 - ćelije. To je tehnika kojom su slike iz novina odaslane radiom, tehnika kojom se mnoge slike pojavljuju na televizijskom ekranu i kojom su slike Mjeseca i Marsa emitirane natrag na Zemlju iz

naših kamera iz svemirskih sondi. To je tako jednostavna tehnika koju bi sigurno Zetanski znanstvenici znali koristiti.
Može li se sada naslutiti značenje broja 1 271? Brojevi 31 i 41 su prosti brojevi. Prosti brojevi mogu biti djeljivi sami sobom i sa 1, tako da su u ovom slučaju 31 i 41 jedini djelitelji broja 1 271. Brojevi sugeriraju matricu tipa 31×41, a to je jedina pravokutna matrica koja ima točno 1 271 ćeliju.
Naravno, Zetani ne bi znali kojom smo se mi skenirajućom putanjom služili. Je li s lijeva na desno u redovima, ili s desna na lijevo? Je li gore i dolje po stupcima? Krivuda li naprijed-natrag kao plug? Može li biti spirala? Zetanski kriptografi bi najprije isprobali najjednostavniji put, kao što kriptoanalitičar na zemlji koristi najjednostavniji put prilikom dešifriranja. Prva slika koju pošaljemo skeniranjem trebala bi biti jednostavna i osnovna, kao trokut ili krug. Čim bi Zetani pronašli putanju koja je proizvela takvu sliku, odmah bi znali koju smo metodu skeniranja koristili.
Od sad pa nadalje, razne vrste slika bi mogle biti poslane da prenesu kompliciranije informacije. Pored svake slike bismo poslali sliku naše riječi za tu sliku. Konačno bismo mogli prijeći na animirane crteže ili čak slike u pokretu kako bismo iskomunicirali kompliciranе ideje.
Slika 9 predstavlja sliku koja je dobivena skeniranjem 31×41 matrice od 1 271 ćelije sa nizom od 1 271 broja koji čine nule i jedninice. To je slika koju bismo mogli primiti iz svemira, možda sa Marsa. Slika je opisana na sljedeći način:



Slika 9: Slika koja bi mogla biti primljena s drugog planeta

„ Očigledno je da smo u dodiru sa rasom uspravnih dvonožaca koji se seksualno razmnožavaju. Čak postoji i nagoviještaj da bi mogli biti sisavci. Grubi krug i stupac točkica s lijeve strane sugeriraju njihovo sunce i planetarni sustav. Figura pokazuje na četvrti planet, koji je očito njihov dom. Valovita linija koja započinje kod trećeg planeta ukazuje na to da je prekriven vodom, a oblik ribe ukazuje na morski svijet. Dvonožci to znaju pa sigurno imaju i svemirska putovanja. Dijagrami na vrhu će biti prepoznati kao vodikovi, ugljikovi i kisikovi atomi, stoga je njihov život baziran na ugljikovodičnoj kemiji. Binarni broj šest iznad podignute ruke lijevog lika pokazuje na šest prstiju i ukazuje na korištenje

brojčanog sustava u bazi 12. *Na kraju, linija niže desno pokazuje da je figura visoka* 11 *nečega. Kako je valna duljina* 21 *na kojoj smo primili poruku jedina duljina koju oboje znamo, zaključili smo da su bića visoka* 231 *cm, ili sedam stopa.*

Međutim, ne možemo razgovarati sa Zetanima kao što razgovaramo jedni sa drugima telefonom ovdje na zemlji. Zvijezde su predaleko. Najbliži zvjezdani sustav-Alpha Centauri i zvijezde koje ga prate udaljen je malo više od četiri svjetlosne godine. To znači da, kada bi Zeta okružila jedan od sunca u tom sustavu, morali bismo čekati gotovo 9 godina kako bismo mogli očekivati da primimo odgovor (radio valovi putuju brzinom svjetlosti). Međutim, u tih 9 godina bismo si mogli poslati ogromne količine kodiranih informacija.

Ne možemo znati bi li Zetani bili prijateljski ili neprijateljski prema nama. Moguće je da su toliko napredniji od nas u tehnologiji i inteligenciji da bi, kada bi shvatili da smo ovdje, mogli poslati svemirski brod da pokupi neke ljudske primjerke za laboratorije i zoološke vrtove.

Ne tako davno, netko je pitao poznatog kineskog fizičara Chen Ning Yanga što bismo trebali napraviti kada bismo primili radio poruku iz svemira. Njegov odgovor je bio: Ne odgovarajte.

6. Ratni kodovi

Diplomacija i ratovanje su dva bitna područja gdje su se počeli stvarati i primjenjivati kodovi i šifre. Velika domišljatost pridavala se u osiguravanje tajnih informacija. Prvi primjeri prenošenja tajnih poruka nastali su u Sparti, što nije nimalo neobično jer su Spartanci u drevnoj Grčkoj bili na glasu kao iznimno sposobni ratnici. Naime, od najranije mladosti učili su trpjeti ekstremne uvjete, kako bi im se ojačale borbene mogućnosti i vještine preživljavanja.

6.1. Spartanski skital

Prvi poznatiji kriptografski uređaj bio je takozvani skital, kojim su se u Sparti koristili već od 7. stoljeća pr.Kr. Radi se o vrlo jednostavnom transpozicijskom šifriranju. Naprava se sastojala od drvenog štapa oko kojeg bi pošiljatelj omotao usku traku pergamenta ili kože te poruku ispisao na uzdužnim dijelovima trake, a zatim bi je odmotao. Na taj način stekao bi se dojam da je ispisan niz besmislenih slova. Ukoliko je poruka bila ispisana na koži, glasnik bi traku okrenuo da se ne vide slova i nosio je kao remen, što je ujedno i steganografska metoda. Primatelj bi zatim omotao vrpcu oko skitala te pročitao skrivenu poruku. Primateljev skital morao je biti istog promjera i imati jednak broj ploha kao i pošiljateljev.



Slika 10: Spartanski skital

Godine 404. *pr. Kr. pred Lisandrom Spartancem pojavio se glasnik, krvav i izubijan, jedini od petorice koji je preživio mukotrpan put iz Perzije. Glasnik mu je predao pojas, a Lisandar ga je omotao oko svoje scitale i tako doznao da ga Farnabas Perzijski kani napasti. Tako se zahvaljujući scitali Lisandar mogao pripremiti za napad i uspješno ga odbiti.*

6.2. Cezarova šifra s pomakom

Prvi se zapis o primjeni supstitucijske šifre u vojne svrhe pojavljuje u Galskom ratu (De bello Galico) Julija Cezara. U njemu Cezar opisuje kako je poslao poruku Ciceronu, opsjedanom i već spremnom na predaju. U toj situaciji rimska slova su bila zamijenjena grčkim, zbog čega su neprijatelju postala nerazumljiva. Cezar je za tajnim pismom posezao tako često da je Valerije Prob o šiframa napisao čitavu raspravu, no koja se nažalost nije sačuvala. Međutim, zahvaljujući Svetonijevu djelu O životu Cezara, napisanom u 2. stoljeću, do nas je dopro detaljan opis jedne vrste supstitucijske šifre kojom se služio Julije Cezar. Zamijenio bi svako slovo u poruci drugim, za tri mjesta dalje u alfabetu. Kriptografi često govore o otvorenoj abecedi, odnosno o abecedi kojom je napisana izvorna poruka, i šifriranoj abecedi, odnosno abecedi u kojoj pojedina slova zamijenjuju ona otvorena. Kada se, kao na Slici 11, postavi šifrirana abeceda, jasno se vidi da je šifrirana abeceda pomaknuta za tri mjesta, pa se takva supstitucija često naziva Cezarovom pomičnom šifrom ili jednostavnije Cezarovom šifrom. Šifrom nazivamo svako kriptografsko rješenje kod kojeg je slovo otvorenog (početnog) teksta zamijenjeno nekim drugim slovom ili simbolom.

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

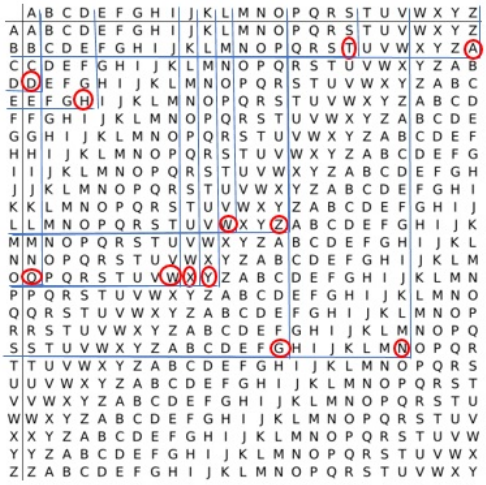
Slika 11: Cezarova šifra za pomak od tri slova

Otvoreni tekst: DOLAZI VOJSKA
Šifrirani tekst: GRODCL YRMVND

Iako Svetonije spominje samo Cezarov pomak od tri slova, jasno je da se pomicanjem slova od jednog do za dvadeset i pet mjesta može stvoriti dvadeset i pet različitih šifri. Ukoliko se ne ograničimo samo na pomicanje alfabeta, te dopustimo da šifrirna abeceda može nastati svim mogućim miješanjem otvorene abecede, onda možemo stvoriti preko $4 \cdot 10^{26}$ kombinacija, pa je toliko i različitih šifri.

6.3. De Vigenereova tablica

Tijekom povijesti su otkriveni mnogi polialfabetski sustavi, ali se posebno istaknuo matematički sustav šifriranja utemeljen na *tabuli recti*, u sklopu kojeg se poruka šifrira primjenom progresivnog Cezarova pomaka, te tako ovisi o ključu. Taj sustav šifriranja formulirao je 1553. godine Talijan Giovan Battista Bellaso, ali ga je popularizirao Francuz Blaise de Vigenere. U kriptografskoj teoriji bila je to prava prekretnica. Nova metoda ponudila je vrlo siguran, a s druge strane vrlo nespretan način prijenosa tajnih poruka. Sustav se koristio sve do kraja 19. stoljeća, posebno u kriznim ili ratnim vremenima. Smatran je toliko sigurnim da su ga prozvali neprobojni kod.
Snaga Vigenereove šifre izvire iz činjenice da se ona ne služi jednom ili dvjema šifrirnim abecedama, nego poruku enkriptira pomoću ravno njih 26. Prvi korak u šifriranju je crtanje takozvanog Vigenereova kvadrata. To je zapravo otvorena abeceda iza koje slijedi 26 šifrirnih abeceda, pri čemu je svaka od njih pomaknuta za jedno slovo u odnosu na prethodnu. To znači da tablica počinje običnim Cezarovim pomakom za samo jedno slovo. Kriptograf zatim treba pripremiti svojevrsni vodič prema kojem će se primjenjivati 26 dostupnih kombinacija, te kojim redom. On može imati oblik riječi, ili niza riječi, ali i niza brojeva. Primjenimo li razmjerno kratku riječ „SLOBODE“ ponavljat ćemo je u nizu i dobiti ključ. I pošiljatelj i primatelj tako će znati kojim su redoslijedom šifrirana slova izvorne poruke. Ključ pokazuje koji redak (počinje slovom iz ključa) valja upotrijebiti za šifriranje, a zatim se slovo „spaja“ sa slovima obične abecede ispisane iznad stupca, kako se može vidjeti na Slici 12.



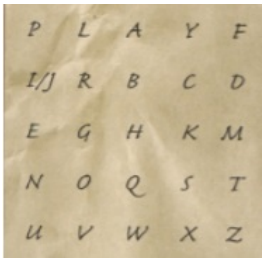
Slika 12: De Vigenereov kvadrat u kombinaciji s ključem SLOBODE

Početna poruka: Vojskadolazi
Šifrirani tekst: NZXTYDHGWOAW

Prilikom dešifriranja poruke, primjenjuje se obrnuti redoslijed. Šifrirano slovo pronalazi se u retku na koji ukazuje ključna riječ.

6.4. Playfairova šifra

Punih dvije stotine godina, od 17. do 19. stoljeća, smatralo se da složenost supstitucijske šifre osobito na temelju De Vigenereova sustava, koji se oslanjao na obostrano poznavanje ključa, te silne količine vremena potrebnog za razbijanje takvih kodova znače da su vojne šifre razmjerno sigurne. No, napredak znanosti, matematike i mehanike, proistekao iz prosvjetiteljskog doba, a koji je doveo do industrijske revolucije, ubrzo je posve izmijenio kriptografski svijet, ukazujući na nove načine pristupanja problemu sigurnog šifriranja, a isto tako i nove načine brzog dešifriranja kodova.
Playfairova šifra je jednostavna, ali učinkovita šifra koja se bazira na tome da se parovi slova šifriraju korištenjem matrice tipa 5×5. Šifru zapravo nije izumio barun Playfair nego fizičar i izumitelj Charles Wheatstone u 19. stoljeću. Playfairova uloga bila je popularizirati ju. Isprva je šifra smatrana prekompliciranom te se nije koristila često. No, pokazalo se da je jednostavnija za korištenje od većine drugih šifri koje su onda bile u uporabi.
Prvo je potrebno dogovoriti ključnu riječ, npr. PLAYFAIR. Zatim se u matricu 5×5 upiše ključna riječ, bez ponavljanja znakova, a ostala prazna mjesta popune se preostalim slovima abecede u uobičajenom poretku, pri čemu **I** i **J** idu u isto polje.



Slika 13: Playfairova tablica

Početnu poruku potrebno je razdvojiti na digrafe (parove slova). Svaki digraf mora se sastojati od različitih slova. Nađu li se dva jednaka znaka u istom digrafu, između njih se umeće **x**, a isti se dodaje i na završetku u slučaju da preostane samo jedno slovo. Na primjer, poruka *„help I really need somebody“* (*eng.“upomoć, hitno trebam nekoga“*) postaje: **he lp ir ea lx ly ne ed so me bo dy**.

Prema tablici, digrafi će se pojaviti na tri različita načina.

- Ako je u istome redu, digraf se šifrira prema slovu koje mu je zdesna. Tako da **ly** postaje **AF**. Pojavi li se slovo na završetku reda, zamjenjuje ga ono koje je na početku istog reda. Tako da **me** postaje **EG**.
- Nalazi li se u istom stupcu, slova se šifriraju slovom neposredno ispod. Pa **ne** postaje **UN**. Nalazi li se neko slovo na dnu stupca, zamjenjuje ga prvo slovo na vrhu istog stupca.
- Ne nalaze li se slova iz digrafa ni u istome redu ni u istome stupcu, valja pronaći prvo slovo u tablici, pa tražiti u tom redu, dok se ne dođe do stupca u kojem je drugo. Slovo na sjecištu tog reda i stupca postaje šifriranom zamjenom, dok kod šifriranja drugog slova treba ići istim redom , dok se ne dođe do stupca u kojem se nalazi prvo slovo, pa onda slovo na sjecištu reda i stupca postaje šifriranom zamjenom. Tako da **bo** postaje **RQ**.

Na taj način dolazimo do cjelovitog ispisa šifrirane poruke:

Početna poruka u digrafima: **he lp ir ea lx ly ne ed so me bo dy**
Šifrirani tekst: **KG AL RB HP YV AF UN MI TQ EG RQ CF**

Budući da primatelj kodirane poruke zna ključnu riječ, jednostavno ponavlja postupak obrnutim redoslijedom. Budući da se frekvencijskom analizom može utvrditi koji su najčešći digrafi, šifra nije neprobojna. Njih je moguće usporediti s najčešćim parovima slova u engleskom jeziku, a to su:
th, he, an, in, er, re i es.

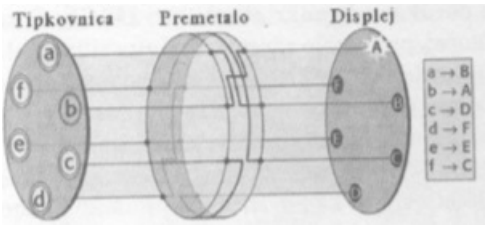
6.5. Enigma: „neprobojni“ sustav

Njemačka vojska je uvidjela da se pojavila potreba za sigurnijim sustavom šifriranja, nakon što su službeni britanski prikazi Prvoga svjetskoga rata otkrili da je neprijatelj čitao njemačke poruke. Njemački izumitelj Arthur Scherbius imao je ideju zamijeniti neadekvatni kriptografski sustav primijenjen u Prvom svjetskom ratu, i to tako da tradicionalne kodove i šifre zamijeni enkripcijom koja bi iskoristila tehnologiju dvadesetog stoljeća. Razvio je kriptografsku mašineriju koja je bila temeljena na pokretnim rotirajućim diskovima. Taj stroj nazvan je Enigma.

Enigma se sastoji od tri elementa povezana žicama:

- tipkovnice za unošenje otvorenog teksta
- premetačke jedinice koja otvorena slova enkriptira u odgovarajuća šifrirana
- displeja sastavljenog od žaruljica koje pokazuju slova šifriranog teksta.

Na Slici 14 prikazana je pojednostavljena verzija Enigme s alfabetom od šest slova.



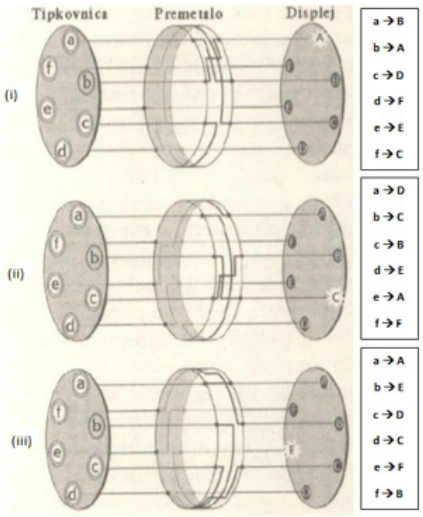
Slika 14: Pojednostavljena verzija Enigme s alfabetom od šest slova.

Da bi se enkriptiralo otvoreno slovo, operater pritišće odgovarajuće otvoreno slovo na tipkovnici i time šalje električni impuls kroz središnju premetačku jedinicu. On zatim iz nje izlazi i osvjetljava odgovarajuće šifrirano slovo na displeju s lampicama. Najvažniji dio stroja je premetalo, debeli disk isprepleten žicama. Žice prelaze od tipkovnice i na šest mjesta ulaze u premetalo, nakon čega u njemu izvode čitav niz zaokreta i preokreta, da bi napokon s druge strane izašle na šest mjesta. Taj splet žica u premetalu određuje kako će se enkriptirati slova otvorenog teksta.

Tako primjerice na Slici 14 žice određuju da će:

- Pritisak na **a** osvijetliti slovo **B**, što znači da se **a** enkriptira kao **B**.
- Pritisak na **b** osvijetliti slovo **A**, što znači da se **b** enkriptira kao **A**.
- Pritisak na **c** osvijetliti slovo **D**, što znači da se **c** enkriptira kao **D**.
- Pritisak na **d** osvijetliti slovo **F**, što znači da se **d** enkriptira kao **F**.
- Pritisak na **e** osvijetliti slovo **E**, što znači da se **e** enkriptira kao **E**.
- Pritisak na **f** osvijetliti slovo **C**, što znači da se **f** enkriptira kao **C**.

Šifrirana abeceda se nakon svake enkripcije mijenja. Scherbiusova je ideja bila da se disk premetala automatski zakrene za jednu šestinu kruga poslije enkripcije svakoga slova ili za jednu dvadesetšestinu, kada je riječ o potpunom alfabetu od dvadeset i šest slova.
Na Slici 15(i) prikazan je isti raspored kao i na Slici 14 ali tu će:
Pritisak na tipku **b** osvijetliti slovo **A**, što znači da se **b** enkriptira kao **A**.



Slika 15: Zakretanje premetala za jedno mjesto

Međutim, čim se utipka slovo i osvijetli ploča sa žaruljicama, premetalo će se zaokrenuti za jednu šestinu okreta i postaviti u položaj prikazan na Slici 15(ii).
Ponovljeno utipkavanje slova **b** ovaj bi put osvijetlilo slovo **C**. Nakon toga premetalo se zakreće još jednom, položaj prikazan na Slici 15(iii). Ovaj će put utipkavanje slova **b** osvijetliti **E**. Zahvaljujući toj rotaciji, premetalo definira šest šifrirnih abeceda.

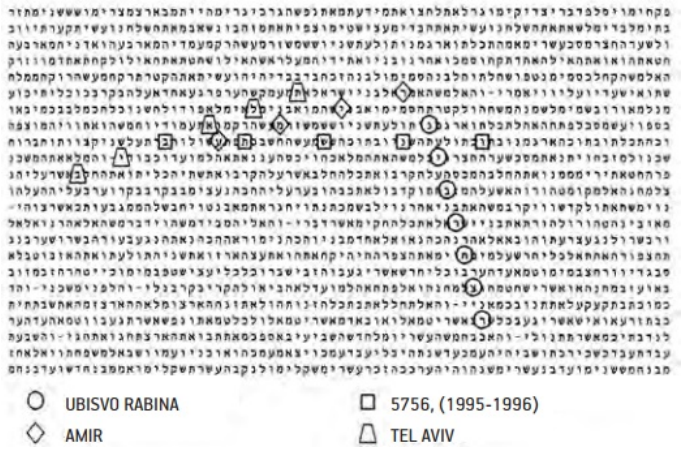
Međutim, stroj pati od jedne očite slabosti. Utipkamo li slovo **b** šest puta, premetalo će se vratiti u početni položaj, udaramo li **b** stalno, ponavljat će se i obrazac enkripcije. Kriptografi izbjegavaju ponavljanje jer ono u šifrirani tekst unosi pravilnosti i daje mu strukturu, a sve su to simptomi slabe šifre.
Iz tog razloga je dodano još jedno premetalo. Prednost je dodavanja drugog premetala da se enkripcija ne ponavlja sve dok se i to drugo premetalo ne vrati u početni položaj, za što prvo premetalo mora obaviti šest punih okretaja, što će reći dok se ne obavi enkripcija ukupno $6 \cdot 6$, to jest 36 slova. Što znači da se pri šifriranju mijenja 36 šifrirnih abeceda, odnosno 676 kada je riječ o punom alfabetu od 26 slova.
No, da bi se povećala kompleksnost šifriranja, uvedeno je i treće premetalo, što znači da su ona zajedno, kada je riječ o punom alfabetu, mogla zauzeti $26 \cdot 26 \cdot 26$, odnosno 17 576 različitih međusobnih položaja.
Da bi mogao dešifrirati poruku, i primatelj mora imati Enigmu kao i primjerak knjige šifri s početnim položajem premetala za taj dan. Primatelj namješta stroj prema knjizi, utipkava šifrirani tekst slovo po slovo, a ploča sa žaruljama javlja mu kako glasi otvoreni tekst. Drugim riječima, pošiljatelj utipkava otvoreni tekst da bi dobio šifrirani tekst, a onda primatelj utipkava šifrirani tekst da bi dobio otvoreni tekst. Dakle, šifriranje i dešifriranje su zrcalni postupci.
Iako se, 17 576 različitih početnih položaja premetala u početku činilo mnogo, neprijatelj bi u minuti mogao provjeriti jedan položaj i ako bi radio dan i noć, da provjeri sve položaje trebalo bi mu skoro dva tjedna. No, ako bi neprijatelj za taj posao odvojio puno više ljudi i više zapljenjenih Enigmi, svi položaji mogli bi se provjeriti za jedan dan. U strahu da se neprijatelj ne domogne ključa koji bi mu odgonetnuo početni položaj od kojeg kreće enkripcija, kriptoanalitičari su dodali novi element – razvodnu ploču. Ona je pošiljatelju omogućavala da umetne vodove koji će zamijeniti mjesta pojedinim slovima prije ulaska u premetalo. Operater Enigme imao je šest kablova, što znači da je 6 parova slova moglo zamijeniti mjesta. Slova kojim treba zamijeniti mjesta također tvore ključ šifre. Sljedeći popis navodi nam sve varijable stroja i odgovarajući broj mogućih položaja za svaku od njih.
Položaj premetala.
Svako od 3 premetala može se postaviti u svaki od 26 položaja. Zbog toga postoji ukupno $26 \cdot 26 \cdot 26$, odnosno 17 576 početnih položaja.
Redoslijed premetala. Tri premetala $(1, 2, 3)$ mogu se postaviti u svaki od sljedećih 6 poredaka: $123, 132, 213, 231, 312, 321$.
Razvodna ploča.
Broj načina na koji se može povezati 6 parova slova od ukupno njih 26 je ogroman: 100 391 791 500.

Ukupan broj ključeva : $17\,576 \cdot 6 \cdot 100\,391\,791\,500$ što daje preko
10 000 000 000 000 000.
Dokle god između pošiljatelja i primatelja postoji suglasnost o razmještaju kablova na razvodnoj ploči, poretku premetala i njihovoj međusobnoj orijentaciji, a što sve zajedno određuje ključ, obojica mogu lako šifrirati i dešifrirati poruke. Da bi neprijatelj provjerio svaki od 10 000 000 000 000 000 mogućih ključeva bilo bi mu potrebno više vremena no što je star svemir.

7. Tajni kodovi u poznatim knjigama

7.1. Biblijski kod

Između 800. i 1200. godine Europljani su se susretali s osnovama kriptografije. Od svih europskih institucija poučavanje su tajnog pisma poticali samo samostani u kojima su redovnici proučavali Bibliju u potrazi za skrivenim značenjima, za čime se strast održavala sve do danas. Godine 1997. knjiga Biblijski kod (The Bible Code) Michaela Drosnina dospjela je na naslovne stranice diljem svijeta. Drosnin je tvrdio da Biblija sadrži skrivene poruke koje se daju iščitati pomoću takozvanih slovnih sekvenci (equidistant letter sequences, EDLS). Do njih dolazimo tako da uzmemo tekst, izaberemo neko slovo, pa zatim počnemo preskakivati određeni broj znakova.
Drosnin je podvrgavši sličnoj analizi Bibliju, otkrio zapanjujući broj EDLS-a koji nisu sadržavali samo smislene riječi nego i čitave rečenice. Skeptike se to baš nije dojmilo i to najviše zato što je Biblija tako velika. U Drosninovoj knjizi Biblija otkriva događaje koji će se zbiti mnogo godina nakon što je ona napisana. U nekoliko dramatičnih slučajeva on je predvidio neke događaje, koji su se dogodili točno onako kako su predviđeni. Naime, nema načina da se zna je li ovaj kod ispravan što se tiče budućnosti.
U rujnu 1994. godine odletio je u Jeruzalem i pokušao o atentatu obavijestiti premijera Jichaka Rabina. Naime, u kodu je otkrio sljedeće: riječi **ubojica koji će ubiti** bile su ukrštene sa imenom **Jichaka Rabina**. Nažalost, Rabin nije povjerovao Drosninu. Četvrtog studenog 1995. godine, čovjek, koji je vjerovao da je na božjoj misiji, hicem u leđa izvršio je ubojstvo koje je prije 3 000 godina bilo najavljeno biblijskim kodom. Kodom je naknadno uočeno i ime ubojice, te kada i gdje će se dogoditi ubojstvo.



Slika 16: Biblijski kod

Atentat na Rabina nije jedini potvrđeni događaj. Uz atentate na Sadata i Kennedyja, još stotine drugih događaja od globalnog značaja također su kodirani u Bibliji – sve od 2. svjetskog rata do Watergatea, od holokausta do Hirošime, od slijetanja na Mjesec do sudara komete s Jupiterom. Također, atentat na Rabina nije bio jedini događaj koji je unaprijed dekodiran. Sudar komete s Jupiterom također je otkriven, i to s točnim datumom, prije nego što se dogodio, a datumi Zaljevskog rata nađeni su u Bibliji prije nego što je rat počeo.
Eliyahu Rips je matematičar koji je otkrio biblijski kod. Biblijski kod je kompjuterski program i otkriven je u originalnoj hebrejskoj verziji Starog zavjeta, Bibliji kakva je originalno napisana.
Međutim, postoje tvrdnje kako se skrivene šifre mogu naći u bilo kojoj knjizi. Brendan McKay s Australskog nacionalnog sveučilišta je uzeo stranicu iz knjige "Moby Dick" i izvukao sljedeće riječi korištenjem EDLS algoritma: princeza Diana, kraljevski, Dodi, Henri Paul, smrtan u tim raljama smrti.
Za mnoge je to apsolutan dokaz kako su biblijski kodovi slučajni i ne nose nikakvo inherentno značenje. Ipak, Drosnin brani svoje tvrdnje činjenicom kako su te riječi izvučene EDLS-om nađene vrlo blizu jedna drugoj, pa su šanse takvog slučajnog pojavljivanja vrlo male.

7.2. Kama sutra

Jedno od prvih opisa enkripcije supstitucijom nalazimo u Kama sutri. Kao autor teksta se tradicionalno navodi hinduistički filozof Mallanaga Vatsyayana koji je živio između 4. i 6. stoljeća. Kama sutra savjetuje ženama da izuče 64 vještine, primjerice kuhanje, odijevanje, masažu i pripravu miomirisa. Na popisu se nalaze i neke ne baš tako nužne vještine, primjerice mađioničarska, pa igranje šaha, uvezivanje knjiga i tesarski zanat. Četrdeset i peta na popisu je vještina tajnog pisanja, a koju ženama preporučuje za prikrivanje potankosti njihovih ljubavnih veza. Jedna se od preporučenih tehnika svodi na nasumično povezivanje slova abecede, dobit ćemo, na primjer, ovakve parove:

A	C	E	K	M	N	O	P	T	U
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
Z	O	L	S	E	P	T	J	D	H

Umjesto "*čekam te u ponoć*" pošiljatelj će napisati "**OLSZEDLHJTPTO**".

8. Literatura

[1] M. Gardner: Codes, ciphers and secret writing, Dover Publications, New York, 1972.

[2] G. Kipper, Investigator's Guide to Steganography, Auerbach Publications, London, 2004.

[3] P. Lunde, Tajne kodova, Novi Liber, Zagreb 2010.

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

[5] CARNet CERT, Steganografija, CCERT-PUBDOC-2006-04-154, Revizija v1.0, 2006., Dostupno na: http://sigurnost.lss.hr/documents/ LinkedDocuments/ CCERT-PUBDOC- 2006-04-154.pdf, Pristupano: Srpanj 2017.

[6] https://www.novizivot.net/2015/12/21/biblijski-kod-postoje-li-tajne-sifre-u-bibliji/ Pristupano: Rujan 2017.

9. Sažetak

Tijekom povijesti tajno komuniciranje većinom se odnosilo na vojne i državne sustave jer su ipak te tajne najčuvanije i najvažnije za veliki broj ljudi.
Informacije su se prenosile na takav način da nitko, osim pošiljatelja i namjernog primatelja, ne posumnja u postojanje poruke. Takav način tajnog komuniciranja naziva se steganografija. Paralelno s razvojem steganografije razvila se i kriptografija čiji cilj nije bio zatajiti samo postojanje poruke, već prikriti njezino značenje. Jedan od primjera prikrivanja poruke je korištenje nevidljive tinte. Od neobičnih metoda slanja poruka u ovom diplomskom radu spomenuli smo šifriranje pomoću točki i čvorova, crveno – plavu šifru, šifriranje pomoću igraćih karata, šifriranje presavijanjem papira, te šifriranje pomoću plastičnog štapića.
Od prvih ratnih kodova spominju se spartanski skital i Cezarova šifra s pomakom.
Međutim, svakoj vrsti tajnog komuniciranja može se pronaći neka mana s kojom bi se ona dešifrirala, ali isto tako može nastati novi ključ ili sama vrsta tajnog komuniciranja kako bi se razina sigurnosti vratila na odgovarajuću. Sukladno tome razvijaju se sustavi šifriranja kao što su Vigenereova tablica i Playfairova šifra. Za vrijeme 2. svjetskog rata pojavljuje se stroj zvan Enigma.
U završnom dijelu rada navedeni su neki od primjera korištenja tajnih kodova u poznatim knjigama, kao što su Biblija i Kama sutra.

Ključne riječi: šifra, šifriranje, dešifriranje, steganografija, kriptografija, nevidljiva tinta, skital, Cezarova šifra, Vigenereova šifra, Playfairova šifra, Enigma, premetalo, Biblija, Kama sutra

10. Title and summary

Understanding secret communication

Through the history secret communication was related to military and state systems because those secrets were the most guarded and most important for many people.
Information was transferred in a way that nobody, except sender and intentional receiver, doesn't suspect in existence of the message. This way of secret communication is called steganography. Parallel with the development of steganography there was development of cryptography whose aim was not to conceal the existence of the message but to cover up its meaning. The use of invisible ink was one of the examples of covering up the message. In this graduate thesis we mentioned some of the unusual methods of sending messages such as coding with dots and knots, red-blue code, coding with playing cards, coding by folding the paper, coding with plastic stick.
First war codes which are mentioned are Spartan scytale and Cesar's code with shift. However, in every type of secret communication we can find a flaw with whom it could be decoded but also it could become a new key or type of secret communication so the level of security could go back to convenient one. Accordingly, new systems of coding, such as Vigenere's table and Playfair's code are developing. A machine called Enigma appears during the Second World War.
In the last part of this work there are examples of using secret codes in famous books such as the Bible and Kama sutra.

Key words: cipher, encryption, decryption, steganography, cryptography, invisible ink, scytale, Caesar's cipher, Vigenère cipher, Playfair cipher, Enigma, cipher wheel, Bible, Kama sutra

11. Životopis

Rođen sam 11. svibnja 1987. godine u Vinkovcima. U Otoku sam pohađao Osnovnu školu Josipa Lovretića. Nakon osnovne škole upisao sam Prirodoslovno matematičku gimnaziju Matije Antuna Reljkovića u Vinkovcima. Tijekom osnovnoškolskog obrazovanja sudjelovao sam na županijskim i regionalnim natjecanjima iz matematike. Maturirao sam 2006. godine i odmah nastavio obrazovanje na Sveučilišnom preddiplomskom studiju matematike na Odjelu za matematiku u Osijeku. Titulu sveučilišnog prvostupnika matematike stekao sam 2010. godine, a potom upisao Sveučilišni diplomski studij matematike, smjer Financijska i poslovna matematika. Nakon odslušanog diplomskog studija, zapošljavam se na mjesto učitelja matematike i fizike u OŠ "Vladimir Nazor" Komletinci gdje ostajem raditi do lipnja 2015. godine. U tom razdoblju sam upisao i Pedagoško-psihološko-didaktičko-metodičku izobrazu na Filozofskom fakultetu u Osijeku, te stekao pedagoške kompetencije. Iste godine u studenom zapošljavam se u OŠ Ivane Brlić-Mažuranić u Virovitici na mjestu učitelja matematike gdje radim do kraja nastavne godine. U rujnu 2016. zapošljavam se u OŠ Josipa Kozarca u Slatini, također na mjestu učitelja matematike. Nakon dva mjeseca prelazim u OŠ Vladimira Nazora u Novoj Bukovici gdje još uvijek radim kao učitelj matematike. Trenutno živim u Slatini sa suprugom i kćerkom koja je prije 10 mjeseci obogatila naš život.