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

Marina Anić

Klasične šifrirne naprave

Završni rad

Osijek, 2016.

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

Marina Anić

Klasične šifrirne naprave

Završni rad

Mentor: izv. prof. dr. sc. Ivan Matić

Osijek, 2016.

Sažetak. U ovom završnom radu navest ćemo nekoliko klasičnih šifrirnih naprava, opisati kako izgledaju te objasniti princip na kojem rade i primjenu.

Ključne riječi: Skital, Albertijev disk, Jeffersonov kotač za šifriranje, Rešetka, Trokutna šifra

Abstract. In this final paper we will cover several simple code machines, describe their looks and explain their working principles and usage.

Key words: The Scytale, The Alberti Disk, Thomas Jefferson's Wheel Cipher, Grilles, The Triangle Code

Sadržaj

1. Uvod

U današnje vrijeme svaka tehnološki razvijenija zemlja koristi računala za kodiranje i dekodiranje. Računala se koriste za razbijanje kodova neprijatelja. Ona se ne koriste samo u vojnim i diplomatskim obavještajnim službama već ih danas i velike privatne korporacije koriste u svojoj tajnoj komunikaciji koja se odvija između djelatnika iste tvrtke.

No, prije računala ljudi su skriveno komunicirali na drugačije načine, tj. putem jednostavnih šifrirnih naprava. Postoji mnogo nevjerojatno jednostavnih naprava za šifriranje, a mi ćemo spomenuti nekoliko njih u ovom radu i objasniti kako izgledaju te opisati njihov princip šifriranja i primjenu.

2. Klasične šifrirne naprave

2.1. Kodovi pisaćeg stroja

Običan pisaći stroj može poslužiti kao osnova za mnogo jednostavnih zamjenskih šifri. Umjesto da utipkamo pravi znak za svako slovo, možemo utipkati slovo izravno iznad njega i lijevo od njega, s njegove desne strane ili slovo gore i desno. Ukoliko se odlučite gore i desno, rečenica JA VOLIM MATEMATIKU će se otkucati ovako:

IW G0P9K KW64KW69O8.

A ako odaberete gore i lijevo:

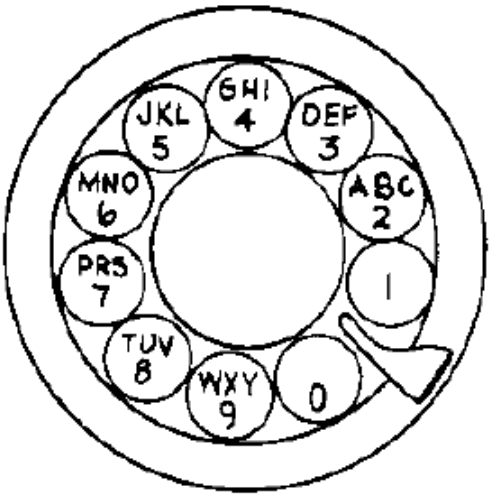
UQ F9O8J JQ53JQ58I7.

Kako bi se kod napravio težim za razbiti, mogu se prisvojiti strategije tako da se izmjenično upotrebljavaju upravo opisane dvije metode krenuvši sa gore i desno: IQ G9P8K JW54JW59I8. Tehnika dekodiranja najčešće je, kao u ovom slučaju, obrnuta postupku kodiranja. Ako kod koristi slova desno na tipkovnici pisaćeg stroja prijevod šifriranog teksta dobio bi se utipkavanjem slova lijevo svakog simbola.

Slika 1: Pisaći stroj

2.2. Telefonski kod

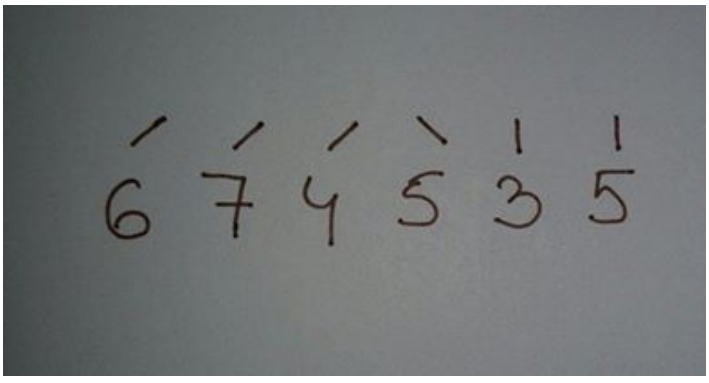
Telefonski kod služi se običnim brojčanikom telefona kako bi kreirao ključ temeljen na abecedi. Slova na brojčaniku su grupirana u trojke u kojima jedan broj vrijedi za tri slova. Primjer brojčanika možemo vidjeti na Slici 2.



Slika 2: Brojčanik

Kako bi ispisali telefonski kod trebamo pronaći svako slovo na brojčaniku i nakon toga zapisati broj kraj njega. Ako je slovo neke trojke najbliže početnom slovu abecede označimo ga s malom linijom iznad njega nagnutom ulijevo. Ako je slovo neke trojke najbliže kraju abecede označimo ga s malom linijom iznad njega nagnutom udesno te ako se slovo nalazi u sredini trojke označimo ga s okomitom linijom. Primijetimo da su Q i Z jedina slova koja se ne nalaze na brojčaniku. Budući da brojevi 1 i 0 nemaju slova uz sebe koristimo 1 umjesto slova Q i 0 umjesto slova Z.

Riječ OSIJEK izgleda ovako u telefonskom kodu:

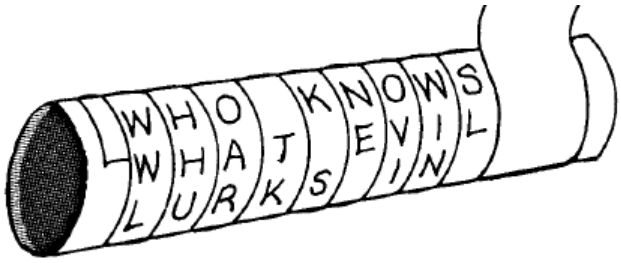


Slika 3: Riječ Osijek napisana u telefonskom kodu

2.3. Skital

Skital je naprava za kodiranje koju su upotrebljavali Spartanci već u 5. stoljeću prije Krista. Skital je imao oblik valjka i izrađivali su ga od različitih materijala. Bilo je bitno da je primatelj poruke imao valjak iste veličine.

Da bismo kodirali poruku, uzmemo dugi komad papira i omotamo ga oko valjka. Nakon što smo omotali papir, ispišemo poruku uzduž valjka. Kad se papir odmota, slova se izmiješaju te je poruka shvatljiva samo osobi koja ima valjak iste veličine.

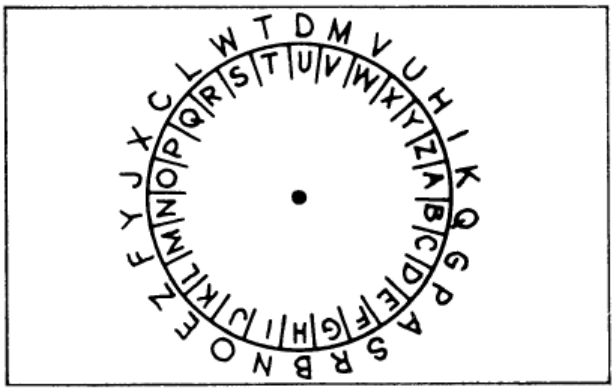


Slika 4: Skital

2.4. Albertijev disk

Još jedna klasična šifrirna naprava nam dolazi od Leona Battiste Albertija, talijanskog arhitekta iz 15. stoljeća. Ova jednostavna naprava u obliku kotača koja je prikazana na Slici 5 u kratkom roku nam omogućuje stvaranje stotine različitih kodova.

Napravu možemo izraditi tako da izrežemo disk od kartona i postavimo ga na novi komad kartona te pričvrstimo središte diska. Na unutrašnjem disku je 26 slova postavljeno po abecednom redu, dok su na vanjskom disku slova nasumično postavljena. Osoba koja prima poruku također mora imati identičnu šifrirnu napravu.



Slika 5: Albertijev disk

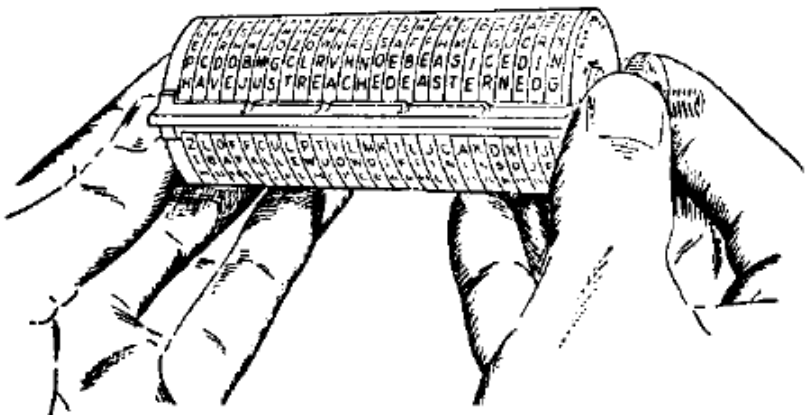
Prije nego što pošaljete poruku u obliku koda treba okrenuti disk dok slovo koje želite nije suprotno od slova A na rubu diska. Od sada je to vanjsko slovo prvo slovo vašeg šifriranog teksta i disk nadalje ostaje u istom položaju. Za svako slovo poruke pronađite slovo u unutrašnjoj abecedi i koristite slovo koje se nalazi na suprotnoj strani u vanjskom krugu. Primatelj poruke mora namjestiti svoj kotač kao i vi prema slovu s početka šifriranog teksta. Tek tada može koristiti svoj kotač kako bi preveo šifru.

Na Slici 5 kotač je postavljen tako da je K nasuprot A. Možemo zaključiti da postoji 26 različitih abecednih šifri između kojih možemo birati jer postoji 26 različitih slova koje se može postaviti nasuprot slova A. Šifru možemo mijenjati svaki put kada šaljemo našu poruku. Poruka GDJE SI izgledat će ovako: RPOA WN.

Ovo je monoalfabetska šifra. Monoalfabetska šifra je šifra u kojoj je svakom slovu pridruženo odgovarajuće slovo u šifratu, zbog čega ju je lako razbiti. Ako je poruka duža, razbijanje šifre je još lakše. Kako bismo otežali razbijanje šifre koristimo polialfabetske šifre. Polialfabetska šifra je šifra u kojoj različiti simboli (slova ili brojevi) odgovaraju istom slovu i u kojoj istim simbolima odgovara različito slovo. Ovakva šifra može biti jako komplicirana i teška za razbiti. Želimo li koristiti polialfabetsku šifru koristeći Albertijev disk, potrebno je samo okrenuti disk nakon svakog slova određujući bilo kakav sustav koji želimo. Na primjer, možemo pomicati disk za jedno mjesto u smjeru kazaljke na satu nakon što kodiramo svako pojedino slovo ili prvo okrenuti disk za jedno slovo, sljedeći put za dva mjesta, nakon toga za tri, pa opet za jedno.

2.5. Jeffersonov kotač za šifriranje

Jeffersonov kotač za šifriranje je izumio Thomas Jefferson, treći predsjednik SAD-a. Sastoji se od 36 drvenih kotača iste veličine montiranih na željeznu šipku, gdje svaki kotač ima nasumično razmještena slova abecede po svom obodu.



Slika 6: Jeffersonov kotač za šifriranje

Okretanjem valjaka slaže se poruka od 36 znakova u istom redu. Kada je poruka tako složena, šifriranje se vrši iščitavanjem bilo kojeg drugog reda od 36 znakova u

vodoravnoj liniji iznad ili ispod poruke. Da bi se izvršilo dešifriranje potrebno je imati Jeffersonov kotač s identičnim rasporedom znakova. Dešifriranje se vrši tako da se dobivena šifra složi u vodoravni red okretanjem valjaka, te se zatim pregledava po obodu cilindra dok se ne pronađe smislena poruka.

Postoje i kompaktnije verzije sa manje valjaka pri čijoj se uporabi šifrirana poruka, ukoliko ima više znakova nego što sprava za šifriranje ima kotača, mora razdijeliti na nizove znakova od kojih se svaki zasebno kodira. U kućnoj radinosti može se izraditi jednostavnija verzija ove naprave tako da se izreže šest kartonskih diskova različitog promjera koji se zajedno učvrste u sredini kako bi se mogli rotirati. Zatim se po obodu svakog diska ispiše abeceda, te se koristi jednako kao i verzija sa kotačima.

Šifru Jeffersonovog kotača je izuzetno teško probiti, no ne i nemoguće. Postoji i mala vjerojatnost da će se prilikom dešifriranja pojaviti dva smislena slijeda znakova, osobito kod verzija sa manje valjaka. 1922. godine napravu je ponovno stavila u upotrebu američka vojska, a američka mornarica koristi ju čak i danas.

2.6. Rešetke

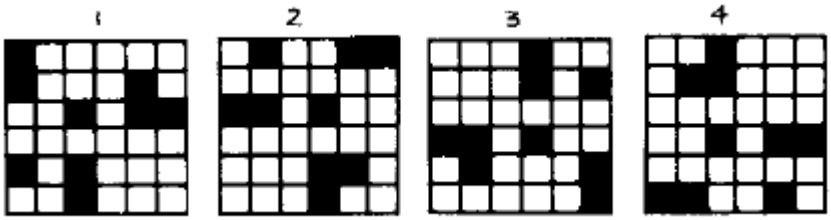
Ovu jednostavnu šifrirnu napravu je izumio Girolomo Cardiano, talijanski matematičar iz 16. stoljeća. Rešetka, nekada zvana i mreža, je kvadratnog ili pravokutnog oblika, izrađena od kartona ili nekog drugog materijala na kojem su usječeni otvori na različitim mjestima. Da bi napisali poruku, slova ili riječi poruke zapisuju se u navedene otvore. Nakon što maknemo rešetku razmaci između tih slova ispunjeni su nasumičnim slovima koja prikrivaju pravu poruku. Nakon što osoba koja je primila poruku stavi identičnu rešetku na poruku, bezvrijedna slova se pokriju i može se pročitati prava poruka.

Kasnije su izumljene rešetke koje su se mogle rotirati te je na taj način svaka ćelija matrice sadržavala slovo izvorne poruke.

Ukoliko želimo izraditi rešetku 6×6, na kartonu ucrtamo 36 kvadrata i numeriramo svaku ćeliju kao što je prikazano na Slici 7. Nakon toga izrežemo bilo koju od ćelija s brojem 1, tad još jednu s brojem 2, pa s brojem 3 te nastavimo na taj način. dok ne bude nedostajalo 9 ćelija.

Slika 7: Numerirana ćelija

Nakon toga nacrtamo kvadrat jednake veličine na komadu praznog papira. Rešetku postavimo preko tog kvadrata u bilo koji položaj i ispišemo prvih 9 slova poruke u 9 rupa. Slova se mogu upisivati na bilo koji način, npr. od dolje ka gore, u redove s desna na lijevo. Zatim se rešetka okreće za četvrt kruga te se ispisuje idućih 9 slova i tako još dvaput, dok se ne popuni svih 36 polja. Ako je poruka duža od 36 slova nastavlja se sa kodiranjem istim postupkom na drugom papiru. Bitno je da osoba koja prima poruku zna točan redoslijed i postupak popunjavanja stupaca, prvi položaj rešetke, stranu na koju je okrenuta (može se iskoristiti za dva sustava šifriranja) i smjer u kojem se rešetka okreće.

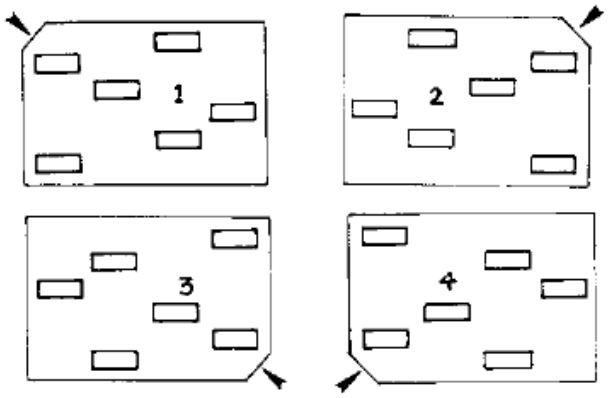


Slika 8: Rešetka u svoja četiri položaja

Može se izraditi rešetka sa bilo kojim brojem polja, ali kod rešetki sa neparnim brojem polja na stranicama, kao što su 5×5 ili 7×7 ne može se koristiti ćelija u sredini, pošto pri rotiranju ostaje na istom mjestu. Može se ostaviti prazna ili popuniti nasumičnim slovom.

Druga vrsta rešetke ima otvore pravokutnog oblika i u njih se upisuju riječi. Kao i kod rešetke sa kvadratnim otvorima, ima četiri položaja, pri čemu se u dva položaja rešetka mora okrenuti gornjom stranom prema dolje. Odrezani kut rešetke olakšava postavljanje rešetke na odgovarajući način. Mogući položaji rešetke vidljivi su na Slici 9.

Poruka šifrirana pomoću ove rešetke može sadržavati do 24 riječi, a ako je poruka

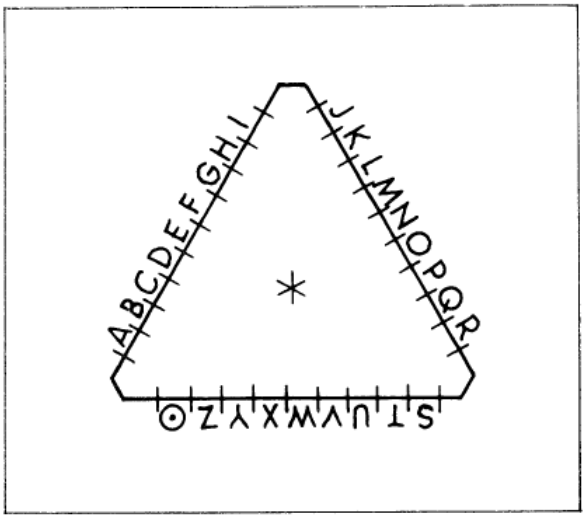


Slika 9: Četiri položaja pravokutne rešetke

duža, kao i kod kvadratne rešetke prelazi se na novi list papira. Ako je riječ predugačka da stane u jedan prozor, jedan dio riječi se piše u jedan prozor, a drugi dio u drugi prozor. Isto tako se dvije kratke riječi mogu upisati u jedan prozor.

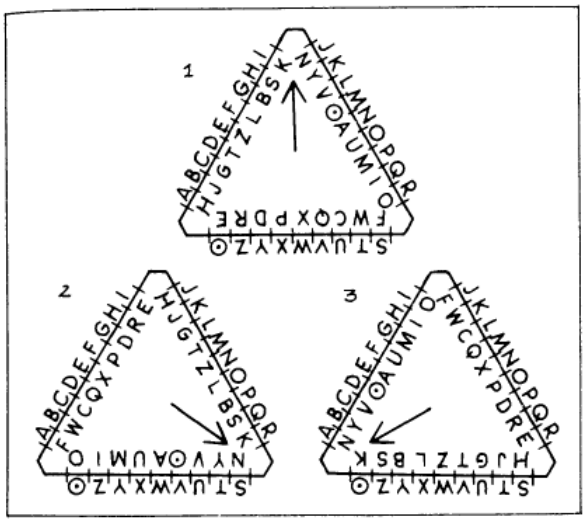
2.7. Trokutna šifra

Za izradu ove šifrirne naprave trebamo na praznom papiru nacrtati jednakostraničan trokut na središte papira. Nakon toga u pravilnom nizu oko vanjskog ruba trokuta ispišemo slova abecede. Slova moraju biti jednako udaljena jedna od drugih kao što je prikazano na Slici 10. Zatim nacrtamo identičan trokut na komadu kartona te ispišemo abecedu na rub njegove tri stranice, ali u nasumičnom redoslijedu. Potom nacrtamo strelicu koja pokazuje ka jednom od njegovih kutova i izrežemo kartonski trokut te ga postavimo na papirnati trokut. Slova s vanjske strane trokuta se koriste za šifriranje, a slova s unutarnje strane za dešifriranje. Pomičući strelice u smjeru kazaljke na satu u druge kutove trokuta za svako novo slovo dobivamo šifriranu poruku. Postupak možemo vidjeti na Slici 11.



Slika 10: Trokutna šifra

Poruka OSIJEK koristeći postupak na Slici 11 izgleda ovako: UNONXW



Slika 11: Tri položaja trokuta

Literatura

[1] M. Gardner, Codes, Ciphers and Secret Writing, Dover Publications, Inc. New York, 1984.