Gimnazija A.G Matoša Đakovo

**Matematika u kriptografiji**  
Matko Ivić, 2.a

Prof. Martina Klarić  
Šk. God. 2021/2022

**Sadržaj**

[Uvod 3](#_Toc98881139)

[Razrada 3](#_Toc98881140)

[Cezarofa šifra 4](#_Toc98881141)

[Alfina šifra 4](#_Toc98881142)

[Vigenerova šifra 4](#_Toc98881143)

[Beaufortova šifra 4](#_Toc98881144)

[Zaključak 5](#_Toc98881145)

[Literatura 7](#_Toc98881146)

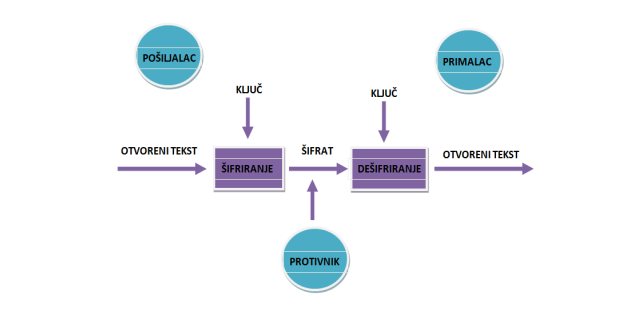
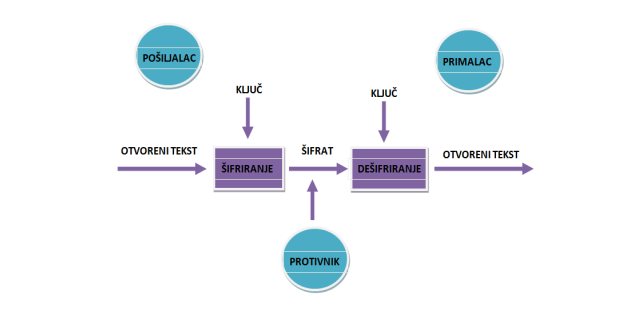
# Uvod

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati. Sama riječ kriptografija je grčkog podrijetla i mogla bi se doslovno prevesti kao tajnopis.

Zadaća je kriptografije da omogući dvjema osobama (pošiljatelj i primatelj) očuvanje tajnosti poruka, čak i u komunikaciji nesigurnim komunikacijskim kanalom (računalna mreža, telefonska linija), koji je dostupan trećim osobama. Kriptografija se stoljećima primjenjivala za osiguravanje tajnosti pretežito vojne i diplomatske komunikacije.

Grana znanosti koja obuhvaća kriptografiju, a i kriptoanalizu, naziva se kriptologija. Za razliku od dešifriranja, kriptoanaliza ili dekriptiranje je znanstvena disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa.

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

Razrada

Slika 1 Proces šifriranja i dešifriranja teksta

## Cezarofa šifra

Cezarova šifra jedna je od najranije poznatih i najjednostavnijih šifri. Šifriranje Cezarovom šifrom funkionira tako da se slovo orginalnog teksta pomakne za broj mjesta udesno te se tako dobije nova šifrirano slovo, postupak se ponavlja kroz cijeli tekst. Metoda je dobila naziv po Juliju Cezaru koji ju je koristio za komunikaciju sa svojim generalima, a za komunikaciju je najčešće koristio te bi tako orginalni tekst

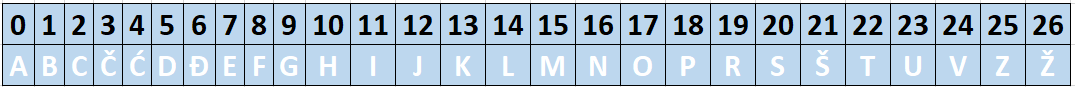
CAR

pomakom za 3 mjesta udesno dobili

EDV,

pri čemu nakon zadnjeg slova Ž, ponovo dolaze slova A, B, C, to jest abeceda se ciklički nastavlja.

Matematički slova u Cezarovoj šifri zamjenjujemo njihovim vrijednostima (redni broj u abecedi) u abecedi te tu vrijednost zbrajamo sa vrijednosti ključa i ako taj broj prelazi broj slova u abecedi koristimo modulo ukupnog broja slova u abecedi.



Tako da šifriranje Cezarove šifre (u hrvatskom jeziku bez slova Lj, Nj, Dž) možemo zapisati kao:

Gdje je vrijednost broja, a vrijednost ključa.

### Zadatak 1.

Imamo početni tekst koji glasi „Matematika“ te ključ vrijednosti 5.

1. Prvo izvučemo vrijednost svih slova:

MATEMATIKA

15 0 22 7 15 0 22 11 13 0

1. Onda na te vrijednosti dodamo vrijednost ključa koji je u ovom slučaju 5:

20 5 27 12 20 5 27 16 18 5

Uočavamo da nam neke vrijednosti prelaze preko 26 pa nakon korištenja modula dobivamo:

20 5 0 12 20 5 0 16 18 5

1. Nakon toga vrijednosti koje smo dobili vratimo nazad u slova te dobivamo šifrirani tekst:

20 5 0 12 20 5 0 16 18 5

SDAJSDANPD

Cezarovu šifru možemo lagano dešifrirati koristeći postupak tkz. Grubom silom. Taj postupak funkionira tako da isprobamo sve moguće ključeve te šifre. Postupak radi na Cezarovoj šifri jako brzo zato što nema veliki broj mogućih ključeva (u hrvatskom jeziku ih ima 26)

Postupak dešifriranja matematički možemo zapisati kao:

Gdje je vrijednost šifriranog slova i n vrijednost ključa

### Zadatak 2.

Ako ne znamo ključ u kojem je šifra pisana tada se služimo

## Alfina šifra

A

## Vigenerova šifra

V

## Beaufortova šifra

B

# Zaključak

Danas, u doba razmjene poruka globalnim računalnim i komunikacijskim mrežama, kriptografija se široko primjenjuje: bilo da se želi osigurati privatnost poruka, ili se time nastoji zaštititi njihova tajnost, kao npr. pri slanju naloga u elektroničkom bankarstvu. U oba se slučaja kriptografija bavi podatcima u digitalnom obliku, postupci kriptiranja i dekriptiranja matematičke su naravi, a provode se automatski, uz pomoć računala. Zbog toga se suvremena kriptologija, kao interdisciplinarna znanost, uglavnom oslanja na informatiku, a znatno je potpomognuta teorijom brojeva i dr. matematičkim teorijama.

# Literatura

<https://web.math.pmf.unizg.hr/~fran/clanci/kripto-poucak4.pdf>

<https://repozitorij.pmf.unizg.hr/islandora/object/pmf%3A9803/datastream/PDF/view>

<https://core.ac.uk/download/pdf/197870521.pdf>

<https://repozitorij.etfos.hr/islandora/object/etfos:807/datastream/PDF/download>

<https://privacycanada.net/mathematics/#:~:text=Cryptography%20Mathematics%20%E2%80%93%20This%20refers%20to,original%20text%20from%20encrypted%20keys>.