GIMNAZIJA DR. MATE UJEVIĆA ŠKOLSKA GODINA  
U IMOTSKOM 2023./2024.

SEMINARSKI RAD-INFORMATIKA

ENIGMA

UČENICI: MENTOR:

JOSIP PARLOV MARTINA MARŠIĆ  
MARIJA ČUTURA

Sadržaj

[Uvod 3](#_Toc169473698)

[Analiza problema 4](#_Toc169473699)

[Enkripcija 4](#_Toc169473700)

[Dekripcija 4](#_Toc169473701)

[Analiza rješenja 5](#_Toc169473702)

[Enkripcija 5](#_Toc169473703)

[Cezarova šifra 5](#_Toc169473704)

[Vigenèreova šifra 5](#_Toc169473705)

[ROT13 6](#_Toc169473706)

[Atbash šifra 6](#_Toc169473707)

[Dekripcija 7](#_Toc169473708)

[Cezarova šifra 7](#_Toc169473709)

[Vigenerova šifra 7](#_Toc169473710)

[ROT13 7](#_Toc169473711)

[Atbash šifra 7](#_Toc169473712)

[Izrada algoritma 8](#_Toc169473713)

[Programski kod 10](#_Toc169473714)

[Testiranje 12](#_Toc169473715)

[Zaključak 13](#_Toc169473716)

[Literatura 14](#_Toc169473717)

# Uvod

Naš zadatak bio je napraviti aplikaciju inspiriranu strojem Enigma i njegovim načinima šifriranja i dešifriranja. Aplikacija za šifriranje i dešifriranje riječi i rečenica omogućuje korisnicima da unesu tekst koji žele zaštititi i pretvore ga u šifrirani oblik, te kasnije dešifriraju taj šifrirani tekst natrag u izvorni oblik.

“Ovim projektom želim poboljšati svoje programerske vještine te napraviti konkretan algoritam optimiziran za svakodnevno korištenje. Projekt “Enigma” je odlična prilika za logičko razmišljanje i planiranje cijelog puta do savršene aplikacije. Zahtijeva detaljno kretanje kroz tekstualne datoteke međutim svaki plan uspijeva uz trud i rad."

Marija Čutura

“Mislim da će Projekt 'Enigma' biti zanimljiv te da će mi omogućiti da se zabavim s C-om i tako poboljšam svoje sposobnosti u njemu. Enkripcija i dekripcija su me oduvijek zanimale, stoga smatram da će mi to biti najdraži dio projekta za programiranje.“

Josip Parlov

# Analiza problema

Enigma  *Zadatak*

*Koristeći različite vrste kriptiranja (vidi: https://e.udzbenik.hr/pov20/g3/) kriptiranje šifriraj tekstnu datoteku kriptirano.txt. Istim ključem dešifriraj datoteku u poruka.txt. Izbornik mora imati stavke:*

*1.Enkripcija   
2. Dekripcija   
3. Ispis   
4. Kraj*

*Napraviti nekoliko datoteka kriptiranoN.txt. Korisniku omogućiti u točkama 1 – 3 upis fizičkog imena datoteke. Ako je korisnik odabrao 1. onda mu se omogućuje unos poruke koju želi šifrirati u datoteku koju je na početku odredio. Odabirom broja 2. korisnik upisuje ime datoteke koju želi dešifrirati. Ispisuje se njen sadržaj koji je bio u originalnom obliku. Odabirom broja 3. ispisuje se datoteka koju je na početku odabrao. Kraj - izlazi se iz programa. 16.4.2024.*

## Enkripcija

Enkripcija je proces pretvaranja običnog teksta (čitljivih podataka) u šifrirani tekst (nečitljive podatke) pomoću algoritma i ključa, kako bi se osigurala povjerljivost i sigurnost podataka. Enkriptirani podaci mogu se dešifrirati natrag u svoj izvorni oblik samo uz pravi ključ. Enkripcija se široko koristi u digitalnoj komunikaciji, skladištenju podataka i sigurnosti informacijskih sustava.

## Dekripcija

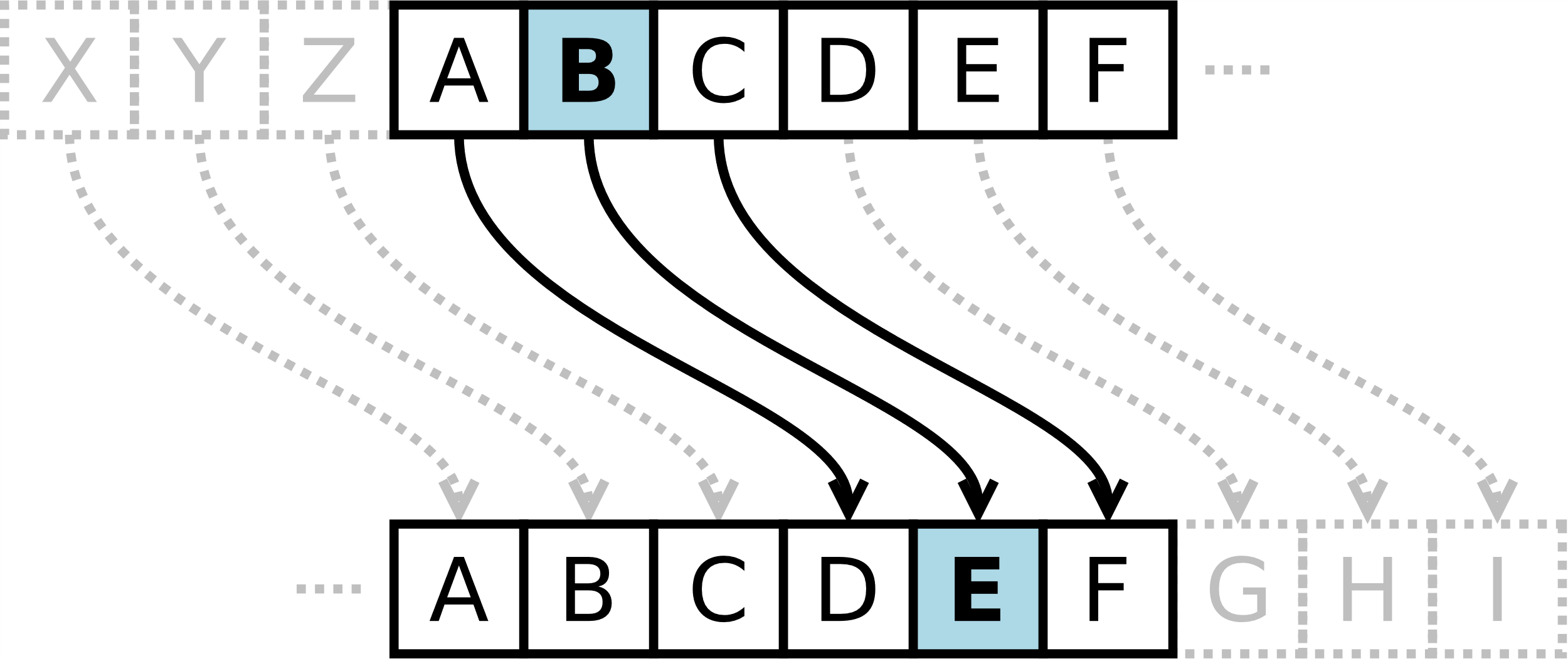
Dekripcija je proces pretvaranja šifriranog teksta (nečitljivih podataka) natrag u obični tekst (čitljive podatke) pomoću algoritma i ključa koji su korišteni za enkripciju. Cilj dekripcije je povratak izvornih podataka kako bi se oni mogli razumjeti i koristiti.

# Analiza rješenja

## Enkripcija

### Cezarova šifra

Cezarova šifra ima svoj ključ(k) koji prati tekst koji je upisan. Tijekom šifriranja svako slovo prati ključ odnosno k koji je broj I za toliko mjesta se pomakne od treutnog slova. Zamjena je ciklička što znači da zadnja slova se zamjenjuju sa zadnjim.



Slika 1. Izvor:[*https://hr.wikipedia.org/wiki/Cezarova\_%C5%A1ifra*](https://hr.wikipedia.org/wiki/Cezarova_%C5%A1ifra)

### Vigenèreova šifra

Kod Vigenèreova šifre svako slovo s otvorenog teksta može preslikati u jedno od m mogućih slova, gdje je m duljina ključa. Algoritam šifriranja definiramo na sljedeći način:

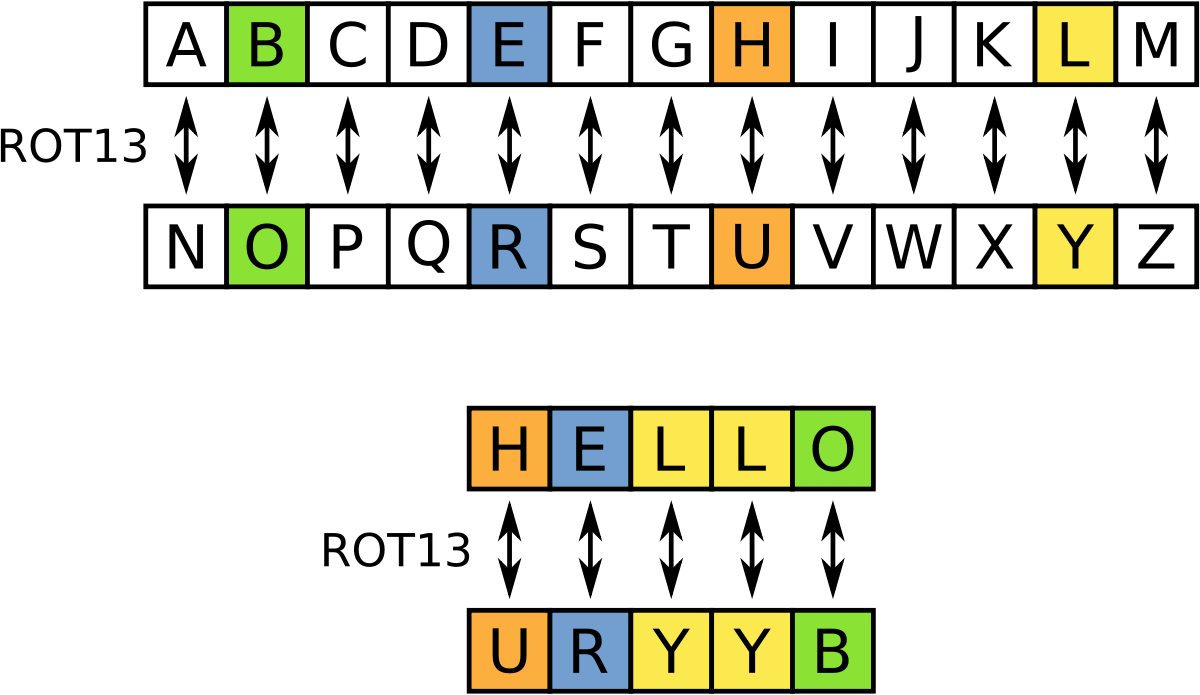
1. Zapišemo otvoreni tekst.
2. Ispod otvorenog teksta, počevši od prvog do zadnjeg slova u njemu, zapisujemo redom slova iz ključa ponavljajući postupak sve dok ne popunimo sva mjesta.
3. Svako slovo otvorenog teksta šifriramo slovom iz ključa koji je zapisan ispod njega.
4. Slovo otvorenog teksta pomičemo za k, mjesta, gdje je k, pozicija u abecedi odgovarajućeg slova iz ključa. Zamjena je ciklička, nakon slova Z dolazi opet slovo A.

Pbtral

Enigma

### ROT13

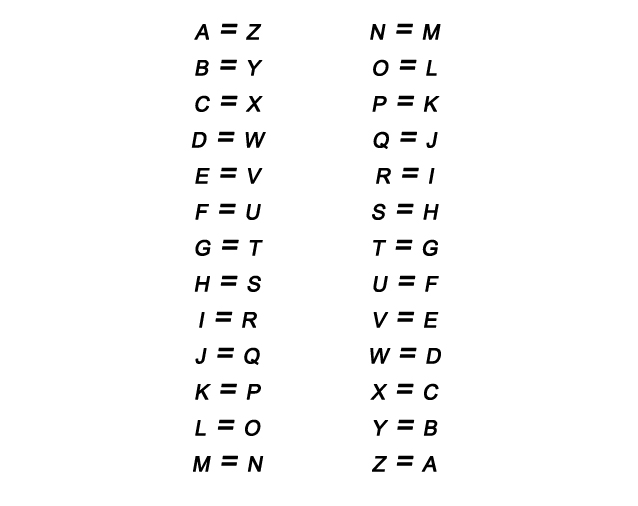
ROT13 šifriranje koristi se za miješanje problema, a funkcionira tako da je ključ k=13. Dodatno svojstvo ovog šifriranja je identično dešifriraju.



Slika 2. Izvor:[*https://en.wikipedia.org/wiki/ROT13*](https://en.wikipedia.org/wiki/ROT13)

### Atbash šifra

Atbash, pronađen u Bibliji, otvoren tekst šifrira zamjenom prvog slova abecede zadnjim, drugog slova predzadnjim… Dešifriranje se vrši na isti način. Ovakav način šifriranja se koristio u cenzuri vjerskih tekstova.

  
Slika 3. izvor: *https://highschool.spsd.org/crypt/foursquare.html*

## Dekripcija

### Cezarova šifra

Cezarova šifra za dešifriranje prati iste korake kao i za šifriranje, odnosno proces ide obratno. Unosimo tekst koji je šifriran i pomoću ključa(k) dešifriramo.

### Vigenerova šifra

Viegerova šifra radi sa obrnutim slijedom od enkrpcije. Bit je sve što se pomicalo unaprijed, vraća nazad uz ključ.

### ROT13

Šifrirani tekst, svako slovo tog teksta vraća za 13 slova unazad.

### Atbash šifra

Obrnutim slijedom, zadnji sa prvim….

# Izrada algoritma

IZBORNIK

Korisnik na početku aplikacije ima tri opcije. Jedna od opcija je enkripcija otvorenog teksta s određenim pomakom ovisno od opcije, četiri šifre koje birate imaju svoja pravila za šifriranje, odnosno način šifriranja gdje se šifrirani tekst sprema u tekstualnu datoteku sa proizvoljnim nazivom. Korisnik također može birati opciju dekripcije gdje koristi već postojanu tekstualnu datoteku s tekstom ili stvara tekstualnu datoteku s tekstom. Tada program izvrši dešifriranje i omogućeno je vidjeti dešifrirani tekst u datoteci.

ENKRIPCIJA I DEKRIPCIJA CEZAROVE ŠIFRE

ENKRIPCIJA I DEKRIPCIJA VIEGEROVE ŠIFRE

Odnosno svaka enkripcija i dekripcija ima sličan sustav međutim razlikuju se samo po obradi teksta u principu šifriranja i obrunog šifriranja, dešifriranja.

# Programski kod

Struktura izbornika

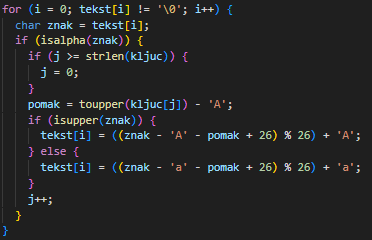
A screen shot of a computer program

Description automatically generatedA screen shot of a computer program

Description automatically generatedA screen shot of a computer program

Description automatically generatedA screen shot of a computer screen

Description automatically generatedAlgoritam enkripcije i dekripcije Cezarove šifre

A screen shot of a computer screen

Description automatically generatedAlgoritam enkripcije i dekripcije Vigenèrove šifre

A screen shot of a computer program

Description automatically generatedA screen shot of a computer code

Description automatically generatedAlgoritam enkripcije i dekripcije ROT13

A screen shot of a computer code

Description automatically generatedA screen shot of a computer code

Description automatically generatedAlgoritam enkripcije i dekripcije Atbash

# Testiranje

# [Enigma - Seminarski rad](https://www.youtube.com/embed/onYX_ZieCwM?feature=oembed)

# Zaključak

Projekt Enigma je bio odličan način kako hijararhijski osmisliti dobar I kvalitetan program. Sama ideja, odnosno funkcija nije posebno teška već je jedino bilo potrebno izvesti dobar plan, podjelu rada i pratiti neke osnovne korake i ideje. Tema je zanimljiva i praktična.

# Literatura

* Dmitrović et al. (2020.) Informatika 3: Kriptografija I Tkinter. Zagreb: SysPrint.

<https://e.udzbenik.hr/pov20/g3/>

* <https://chatgpt.com/>