Šifriranje

Projektna naloga pri informatiki

Jakob Slak, 3.b

Mentor: Klemen Bajec

Kazalo

[Uvod 3](#_Toc200495420)

[Osnove programa 3](#_Toc200495421)

[Cezarjeva šifra 3](#_Toc200495422)

[Vigenére in autokey 4](#_Toc200495423)

[Enigma 4](#_Toc200495424)

[RSA 4](#_Toc200495425)

[Delovanje 5](#_Toc200495426)

[Zaključek 5](#_Toc200495427)

[Viri 5](#_Toc200495428)

# Uvod

Skozi zgodovino se je vedno pojavljala potreba po uporabi šifer. Naj je bilo to le osebno sporočilo, za katerega nismo želeli, da bi ga lahko kdo prebral, ali pa strogo zaupna vojaška skrivnost, zaradi katere bi lahko izgubili boj, če bi prišla v napačne roke.

V sodobnem času je uporaba šifer neznansko razširjena. Skoraj vsaka spletna stran je šifrirana, večina sporočil, katera pošiljamo, potujejo kot navidezno naključni nizi znakov do prejemnika, kjer se dešifrirajo nazaj v razumljivo besedilo.

Ko sem bil mlajši, smo si s prijatelji velikokrat želeli pisati kodirana sporočila, vendar pa se zaradi dolgotrajnega postopka šifriranja na roko to nikoli ni obneslo. Zato sem se odločil, da spišem program, ki mi bo pomagal pri dolgočasnem delu postopka, in zašifriral sporočilo namesto mene.

# Osnove programa

Program deluje z uporabo dveh seznamov črk (eden za velike, drugi za male črke), s tem da namesto dejanske črke uporablja njeno mesto v abecedi, ter poziciji prišteva ali odšteva določeno število.

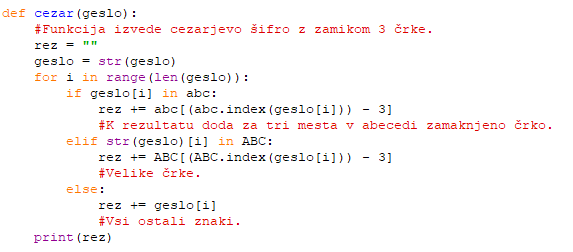
Če program ne prepozna znaka (če se znak ne nahaja v angleški abecedi – ne uporablja slovenske, saj je večina šifer zasnovana za angleško abecedo), se znak preprosto prepiše, oziroma se, če je šumnik, spremeni v črko brez strešice.





# Cezarjeva šifra

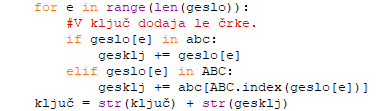
Najmanj kompleksna od vseh šifer v programu. Poziciji vsake črke odšteje 3, tako črko zamakne za tri mesta. Mogoče je nastaviti poljuben zamik. Dešifriranje je narejeno z isto operacijo, le da je zamik nasprotno enak prvotnemu.



# Vigenère in autokey

V programu zapisana podobno kot cezarjeva, le da namesto prištevanja k vsaki črki istega števila, prištejemo pozicijo pripadajoče črke ključa.

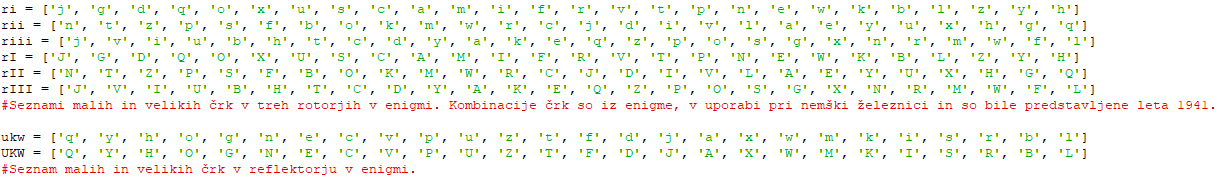
Autokey deluje enako, le da ko črk v ključu zmanjka, začne uporabljati samo besedilo kot ključ.



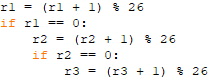
Dešifriranje je podobno šifriranju, le da se namesto seštevanja vrednosti le-te odštevajo.

# Enigma

Osnovna verzija Enigme brez plugboarda, kakšna je bila na voljo za nemške civiliste. V programu so zapisani trije rotorji in odbojnik, ki spremenijo število črke v neko drugo. To se zgodi sedemkrat.



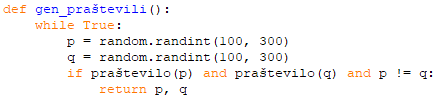
Po vsaki črki se pozicija rotorjev spremeni.



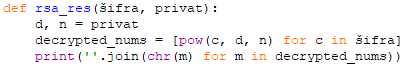
Pri Enigmi je dešifriranje enako šifriranju.

# RSA

Način šifriranja RSA je bil eden prvih asimetričnih ključev. Deluje tako, da zašifriramo besedilo z javnim ključem, dešifriramo pa ga lahko le z unikatnim zasebnim ključem, ki je sestavljen iz edinih deliteljev javnega ključa.

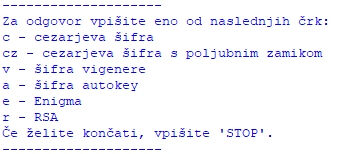


Tako šifriranje kot dešifriranje delujeta s potenciranjem števil v ključu po določenemu modulu.



# Delovanje

Program dobro deluje, in ima interaktiven besedilni vmesnik. V primeru napačno vnesenega znaka te program vodi skozi vgrajena navodila, ki se pokažejo le ob napaki. Vsebuje tudi veliko t.i. 'quality of life' dodatkov, kot na primer delovanje vmesnika le z eno črko, podpora za velike in male začetnice, itd.



# Zaključek

Izdelava programa mi je bila zelo všeč. Zdi se mi, da zdaj dosti bolj podrobno poznam šifre, ki sem se jih odločil sprogramirati. Program bi lahko izboljšal z očiščenjem svoje kode, da zavzame manj prostora, ter seveda z dodajanjem več šifer. Želel bi tudi dodati možnost za .txt datoteke. Razmišljal sem o simetrični kriptografiji, kot tudi o nekaterih slikovnih šifrah, vendar bo moralo to še počakati.

# Viri

Wikipedia [Datum zadnjega dostopa: 10.06.2025, 21:45], dostopno na naslovih:

<https://en.wikipedia.org/wiki/Enigma_rotor_details>

<https://en.wikipedia.org/wiki/Autokey_cipher>

<https://en.wikipedia.org/wiki/RSA_cryptosystem>

Orodja za preverjanje pravilnosti mojega programa:

<https://en.metools.info/enencrypt/autokey206.html>

<https://cryptii.com/pipes/vigenere-cipher>

<https://www.dcode.fr/vigenere-cipher>

ChatGPT [Datum zadnjega dostopa: 10.06.2025, 22:12]:

<https://chatgpt.com/share/6848b419-0f88-8005-8ce2-857a6826031d>