

Korisničko uputstvo

Tema: Algoritmi za kriptovanje i dekriptovanje

Student: Lazarević Nina

Broj indeksa: 15187

1 Uvod

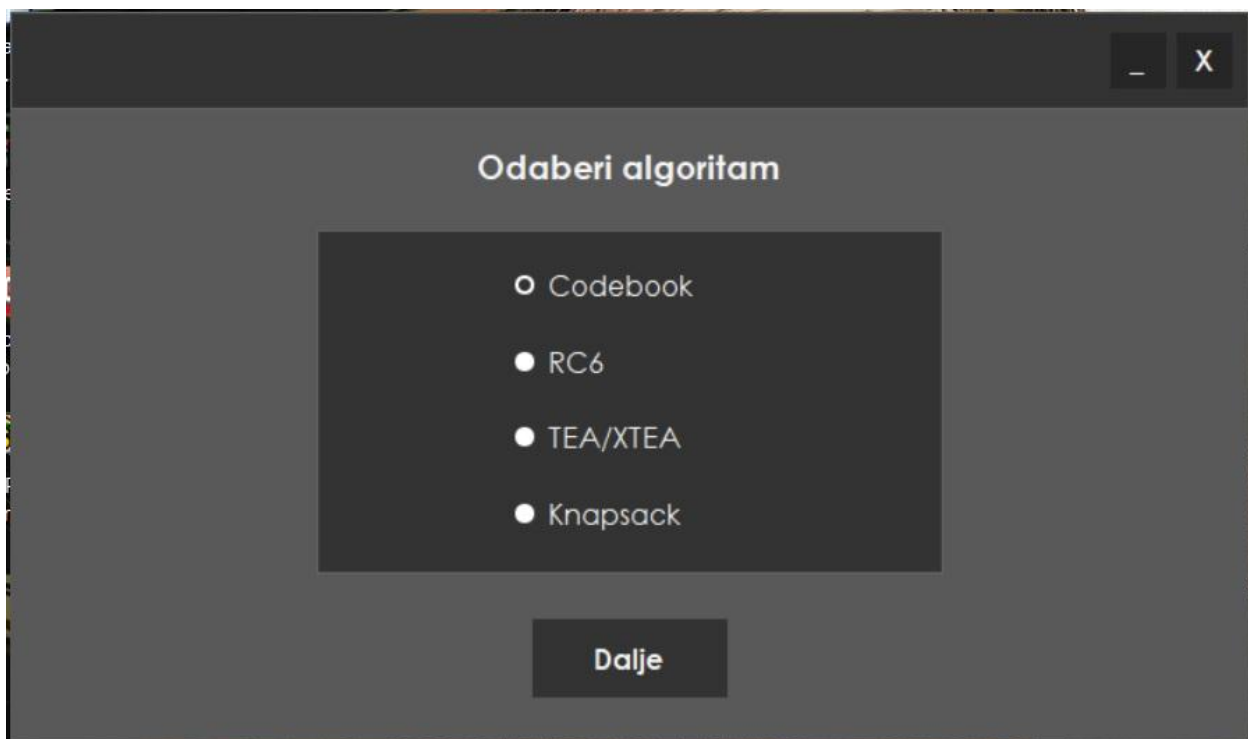
Aplikacija za kriptovanje i dekriptovanje različitih algoritama ima zadatak da na što efikasniji način izvrši kriptovanje/dekriptovanje fajla koji odabere korisnik ili proizvoljnog teksta unetog sa tastature.

Algoritmi za kriptovanje i dekriptovanje koji su implementirani su *Codebook*, *Rc6*, *Tea/Xtea* i *Knapsack*.

Ovaj document služi da korisniku približi način korišćenja ove aplikacije.

2 Pokretanje aplikacije

Kada korisnik pokrene aplikaciju bira koji od 4 ponudjena algoritama želi da koristi. Pritiskom na dugme "Dalje" otvara se stranica za odabrani algoritam.

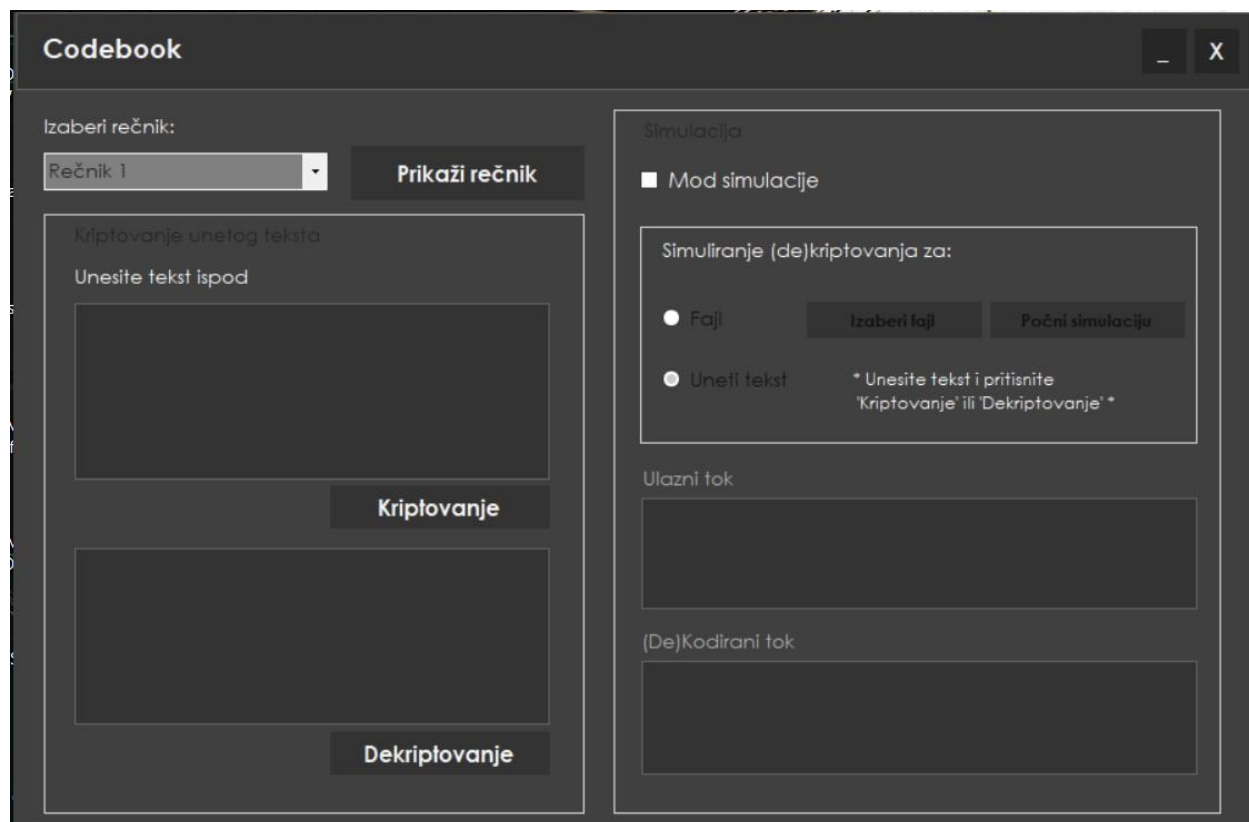


Slika 1. Početna strana

2 Codebook

Ako je korisnik odabrao algoritam "Codebook" otvara se stranica prikazana na slici 2.

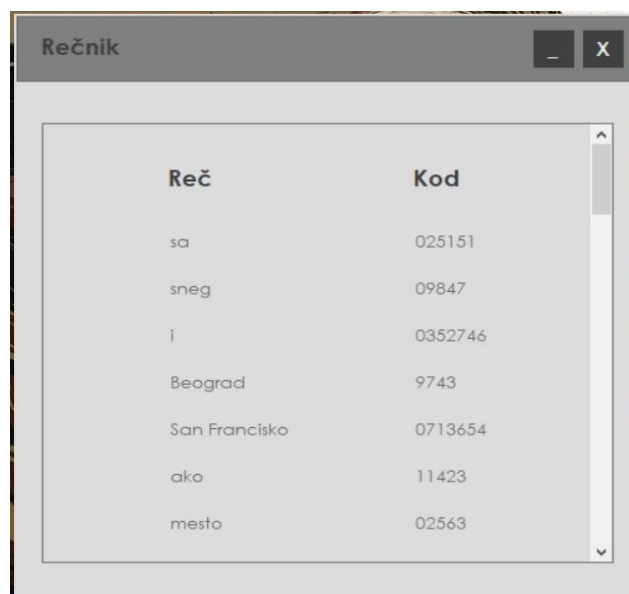
Korisnik unosi tekst koji želi da kriptuje u polje za unos teksta. Pritiskom na dugme "Kriptovanje" uneti tekst se kriptuje. Kriptovani tekst se prikazuje u tekst polju ispod polja za unos teksta. Pritiskom na dugme "Dekriptovanje" prethodno kriptovani tekst se dekriptuje.



Slika 2. Codebook strana

2.1 Rečnik

Codebook agloritam koristi rečnik za kriptovanje. Rečnik se bira u padajućem meniju. Pritiskom na dugme "Prikazi rečnik" prikazuje se odabrani rečnik.



Slika 3. Rečnik

2.1 Mod simulacije

Mod simulacije se može uključiti cekiranjem checkbox-a "Mod simulacije". Dalje se bira da li se želi simulacija (de)kriptovanja za uneti tekst ili za odabrani fajl. Ukoliko se odabere uneti tekst, korisniku se svake dve sekunde prikazuje po reč iz unetog teksta koja se kodira ili po kodirana reč koja se dekodira. Ukoliko se odabere fajl, korisniku se svake dve sekunde prikazuje po rečenica iz odabranog fajla koja se (de)kriptuje.

3 RC6

Ako je korisnik odabrao algoritam "RC6" otvara se stranica prikazana na slici 4.

Da bi korisnik mogao da (de)kriptuje mora prvo generisati ključ. To će uraditi pritiskom na dugme "Generiši ključ", nakon unosa proizvoljnog ključa u tekst polje za korisnički ključ.

Korisnik unosi tekst koji želi da kriptuje u polje za unos teksta. Pritiskom na dugme "Kriptovanje" uneti tekst se kriptuje. Kriptovani tekst se prikazuje u tekst polju ispod polja za unos teksta. Pritiskom na dugme "Dekriptovanje" prethodno kriptovani tekst se dekriptuje.

Ako korisnik želi da (de)kriptuje fajl, bira fajl pritiskom na dugme "Izaberi fajl". Kada je fajl odabran počinje se sa (de)kriptovanjem klikom na dugme "Počni". Ulaz iz fajla se prikazuje u tekst polju za ulaz, a izlaz, odnosno (de)kriptovan sadržaj fajla u tekst polju za izlaz. Svaka ovakva obrada fajla kao rezultat ima novi fajl koji je sačuvan na određenoj lokaciji na lokalnom računaru. Put do te lokacije se vidi na stranici nakon obrade fajla.

The screenshot shows a software window titled "RC6" with a dark theme. It contains several functional panels:

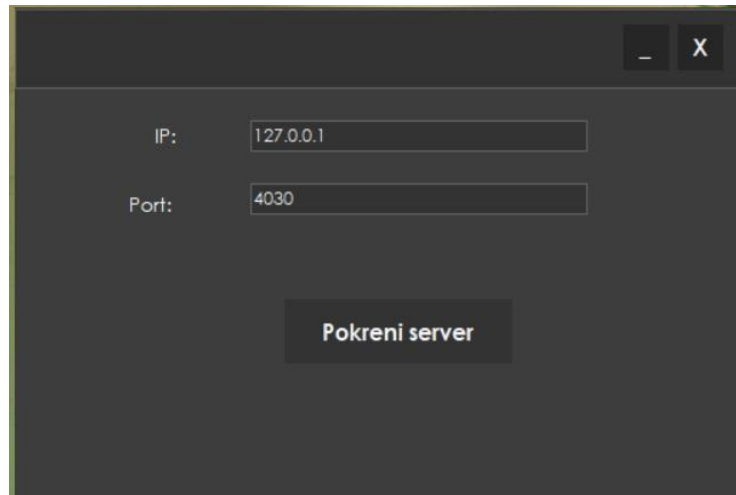
- Generisanje ključa (Key Generation):** Includes input fields for "Korisnički ključ:" (containing "264826313683"), "Broj rundi:" (20), and "Dužina reči:" (32). A "Generiši ključ" button is located to the right.
- Kriptovanje fajlova (File Encryption):** Features "Izaberi fajl" and "Počni" buttons. Below are two text areas labeled "Ulaz" and "Izlaz", each with a vertical scrollbar.
- Kriptovanje unetog teksta (Text Encryption):** Has a large text input area with the instruction "Unesite tekst ispod". Below it are buttons for "Kriptovanje" and "Dekriptovanje".
- Komunikacija (Communication):** Contains a single button labeled "Pokreni komunikaciju".

Slika 5. RC6 strana

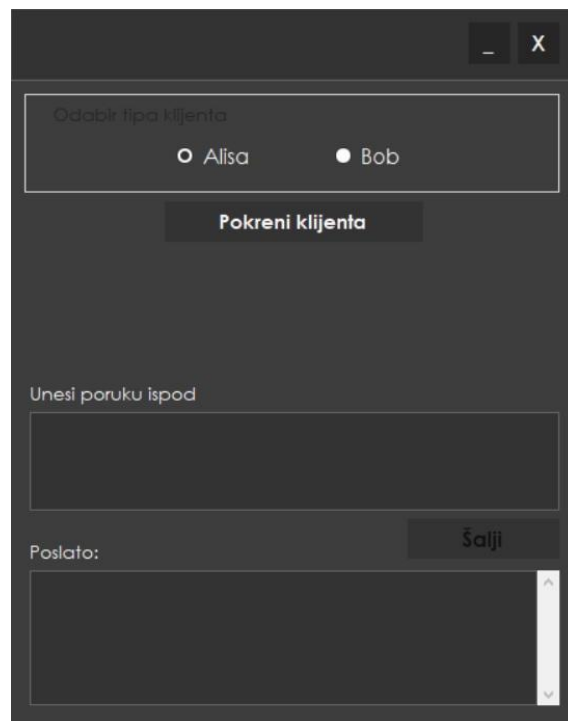
3.1 Komunikacija

Napomena: Pre nego što se uopšte počne uspostavljanje komunikacije, treba proveriti da li je server uključen. Server se uključuje pokretanjem aplikacije "Server" i pritiskom na dugme "Pokreni server". Pritiskom na dugme "Pokreni komunikaciju" korisniku se prikazuje strana za klijenta, gde on bira da li želi da učestvuje u komunikaciji kao strana koja generiše krypto poruke (Alice) ili kao strana koja dekriptuje generisane krypto poruke (Bob). Nakon sto izabere stranu on šalje kriptovane poruke (Alice) ili čeka na poruku koju će nakon prijema dekriptovati (Bob).

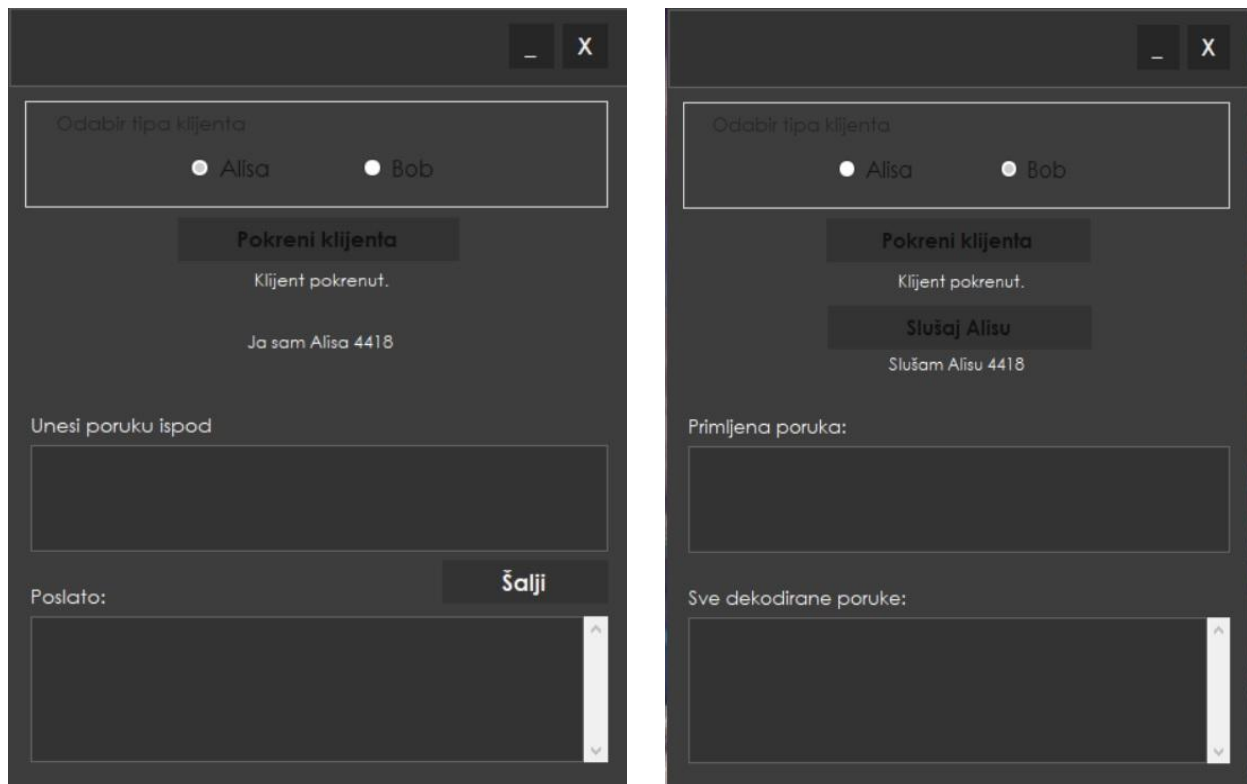
Napomena: Za komunikaciju, odnosno (de)kriptovanje poruka, koristi se RC6 algoritam.

The screenshot shows a dark-themed window titled "Server". It contains two input fields: "IP:" with the value "127.0.0.1" and "Port:" with the value "4030". Below these fields is a button labeled "Pokreni server".

Slika 6. Server strana

The screenshot shows a dark-themed window titled "Klijent". It has a section "Odabir tipa klijenta" with two radio buttons: "Alisa" (unselected) and "Bob" (selected). Below this is a button labeled "Pokreni klijenta". Further down is a text input field with the placeholder "Unesi poruku ispod". At the bottom, there is a "Poslato:" label, a "Šalji" button, and a large text area for the message with a vertical scrollbar on the right.

Slika 7. Klijent strana



Slika 7.1. Klijent strana kada su Alisa (levo) i Bob (desno) pokrenuti

4 TEA/XTEA

Ako je korisnik odabrao algoritam "TEA/XTEA" otvara se stranica prikazana na slici 8.

Korisnik može menjati zadati ključ i IV vektor.

Korisnik unosi tekst koji želi da kriptuje u polje za unos teksta. Pritiskom na dugme "Kriptovanje" uneti tekst se kriptuje. Kriptovani tekst se prikazuje u tekst polju ispod polja za unos teksta. Pritiskom na dugme "Dekriptovanje" prethodno kriptovani tekst se dekriptuje.

Ako korisnik želi da (de)kriptuje fajl, bira fajl pritiskom na dugme "Izaberi fajl". Kada je fajl odabran počinje se sa (de)kriptovanjem klikom na dugme "Pocni". Ulaz iz fajla se prikazuje u tekst polju za ulaz, a izlaz, odnosno (de)kriptovan sadržaj fajla u tekst polju za izlaz. Svaka ovakva obrada fajla kao rezultat ima novi fajl koji je sačuvan na određenoj lokaciji na lokalnom računaru. Put do te lokacije se vidi na stranici nakon obrade fajla.

TEA/XTEA (PCBC mod)

Unos ključa i IV vektora

Ključ: 1234567890123456

IV: 2589283

Kriptovanje fajlova

Izaberi fajl

Počni

Ulaz

Izlaz

Kriptovanje unetog teksta

Unesite tekst ispod

Kriptovanje

Dekriptovanje

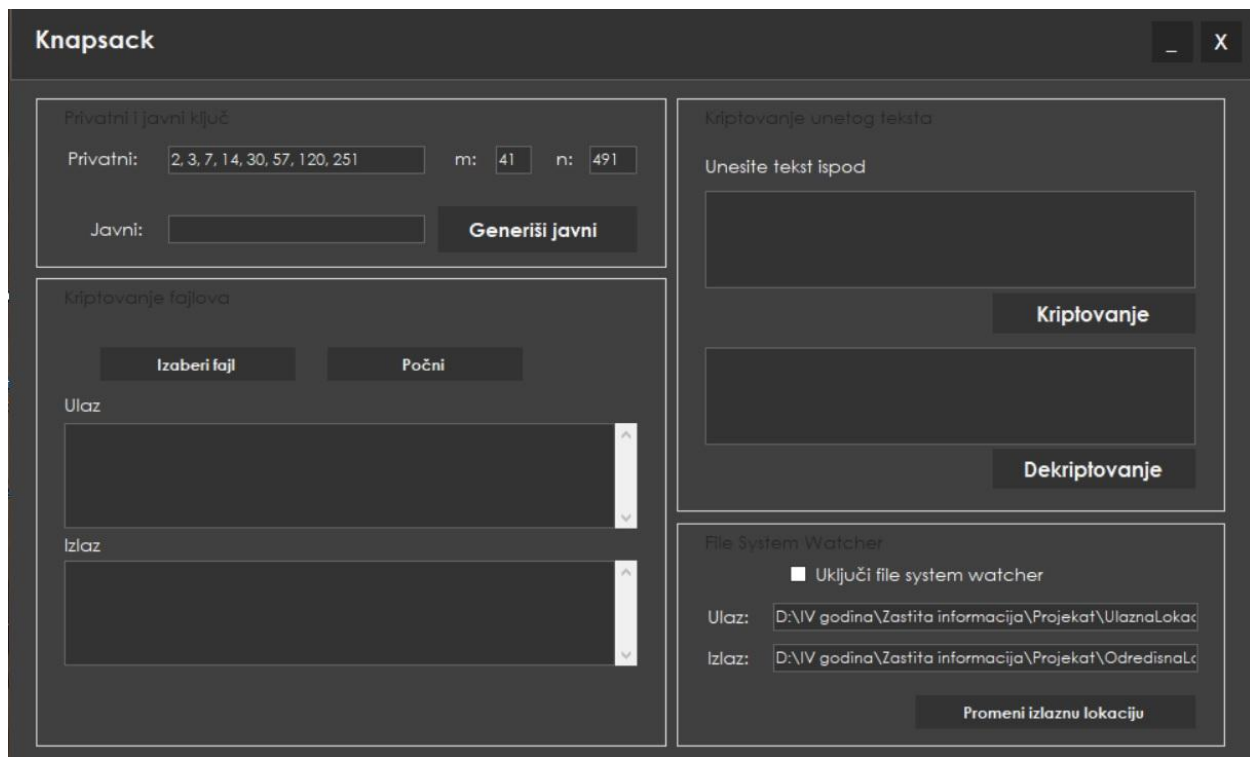
Slika 8. Tea strana

5 Knapsack

Ako je korisnik odabrao algoritam "Knapsack" otvara se stranica prikazana na slici 9.

Da bi korisnik mogao da (de)kriptuje mora prvo generisati javni ključ. To će uraditi pritiskom na dugme "Generiši javni". Korisnik može menjati zadati privatni ključ, m i n , vodeći računa da je n logički nastavak izabranog privatnog niza (tj. veći od zbira svih njegovih članova) i da je m uzajamno prost sa n . Korisnik unosi tekst koji želi da kriptuje u polje za unos teksta. Pritiskom na dugme "Kriptovanje" uneti tekst se kriptuje. Kriptovani tekst se prikazuje u tekst polju ispod polja za unos teksta. Pritiskom na dugme "Dekriptovanje" prethodno kriptovani tekst se dekriptuje.

Ako korisnik želi da (de)kriptuje fajl, bira fajl pritiskom na dugme "Izaberi fajl". Kada je fajl odabran počinje se sa (de)kriptovanjem klikom na dugme "Pocni". Ulaz iz fajla se prikazuje u tekst polju za ulaz, a izlaz, odnosno (de)kriptovan sadržaj fajla u tekst polju za izlaz. Svaka ovakva obrada fajla kao rezultat ima novi fajl koji je sačuvan na određenoj lokaciji na lokalnom računaru. Put do te lokacije se vidi na stranici nakon obrade fajla.



Slika 9. Knapsack strana

5.1 File system watcher

Korisnik može uključiti file system watcher čekanjem checkbox-a "Uključi file system watcher". Tada će se svi fajlovi koji se nalaze na ulaznoj lokaciji (Ulazna lokacija je zadata u tekst polju za ulaz) (de)kriptovati i rezultat (de)kriptovanja će se sačuvati kao novi fajl na odredišnoj lokaciji (Odredišna lokacija je zadata u tekst polju za izlaz). Takodje, svaki novi fajl koji se dodaje na ulaznoj lokaciji će se na isti način obraditi.

Korisnik ima mogućnost da menja odredišnu lokaciju. To može uraditi pritiskom na dugme "Promeni izlaznu lokaciju".

Napomena: Za file system watcher, odnosno (de)kriptovanje fajlova dok je uključen file system watcher se koristi Knapsack algoritam.

6 Završna reč

Kreator ove aplikacije se nada da će korisnici uživati u njoj i da će im ona pomoći da bolje shvate način rada kripo algoritama.

Za primedbe, pitanja i uočene nedostatke javiti se na e-mail
nina_lazarevic@live.co.uk