Ilustracija kriptoanalitičkih metoda pomoću aplikacije CrypTool

Takač, Edi

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Stručni studij Elektrotehnike, smjer Informatika

ILUSTRACIJA KRIPTOANALITIČKIH METODA POMOĆU APLIKACIJE CRYPTOOL

Završni rad

Edi Takač

Osijek, 2020.

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Obrazac Z1S: Obrazac za imenovanje Povjerenstva za završni ispit na preddiplomskom stručnom studiju

Osijek, 12.09.2020.

Odboru za završne i diplomske ispite

Imenovanje Povjerenstva za završni ispit na preddiplomskom stručnom studiju

Ime i prezime studenta:	Edi Takač
Studij, smjer:	Preddiplomski stručni studij Elektrotehnika, smjer Informatika
Mat. br. studenta, godina upisa:	AI4581, 25.09.2019.
OIB studenta:	47252868819
Mentor:	Izv. prof. dr. sc. Krešimir Grgić
Sumentor:	
Sumentor iz tvrtke:	
Predsjednik Povjerenstva:	Prof.dr.sc. Drago Žagar
Član Povjerenstva 1:	Izv. prof. dr. sc. Krešimir Grgić
Član Povjerenstva 2:	Doc. dr. sc. Višnja Križanović
Naslov završnog rada:	Ilustracija kriptoanalitičkih metoda pomoću aplikacije CrypTool
Znanstvena grana rada:	**Telekomunikacije i informatika (zn. polje elektrotehnika)**
Zadatak završnog rada	Kriptoanaliza uključuje različite metode otkrivanja šifriranih podataka bez poznavanja odgovarajućih ključeva potrebnih za pristup. Potrebno je analizirati i objasniti neke najčešće kriptoanalitičke metode, te ih prikazati na primjerima različitih kriptosustava (klasičnih i suvremenih) u okruženju aplikacije CrypTool.
Prijedlog ocjene pismenog dijela ispita (završnog rada):	Izvrstan (5)
Kratko obrazloženje ocjene prema Kriterijima za ocjenjivanje završnih i diplomskih radova:	Primjena znanja stečenih na fakultetu: 2 bod/boda Postignuti rezultati u odnosu na složenost zadatka: 2 bod/boda Jasnoća pismenog izražavanja: 2 bod/boda Razina samostalnosti: 3 razina
Datum prijedloga ocjene mentora:	12.09.2020.

Potpis mentora za predaju konačne verzije rada u Studentsku službu pri završetku studija:	Potpis:
	Datum:

FERIT
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA
I INFORMACIJSKIH TEHNOLOGIJA **OSIJEK**

IZJAVA O ORIGINALNOSTI RADA

Osijek, 02.10.2020.

Ime i prezime studenta:	Edi Takač
Studij:	Preddiplomski stručni studij Elektrotehnika, smjer Informatika
Mat. br. studenta, godina upisa:	AI4581, 25.09.2019.
Turnitin podudaranje [%]:	6

Ovom izjavom izjavljujem da je rad pod nazivom**: Ilustracija kriptoanalitičkih metoda pomoću aplikacije CrypTool**

izrađen pod vodstvom mentora Izv. prof. dr. sc. Krešimir Grgić

i sumentora

moj vlastiti rad i prema mom najboljem znanju ne sadrži prethodno objavljene ili neobjavljene pisane materijale drugih osoba, osim onih koji su izričito priznati navođenjem literature i drugih izvora informacija.
Izjavljujem da je intelektualni sadržaj navedenog rada proizvod mog vlastitog rada, osim u onom dijelu za koji mi je bila potrebna pomoć mentora, sumentora i drugih osoba, a što je izričito navedeno u radu.

Potpis studenta:

SADRŽAJ

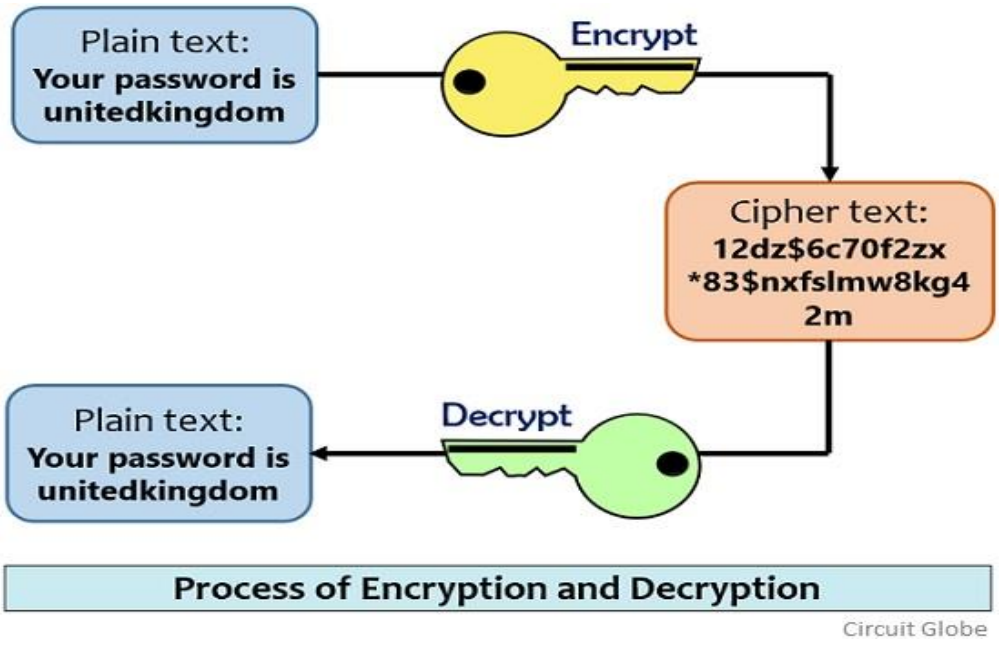
1. UVOD

U svijetu je poznato da korisnici izmjenjuju puno poruka odnosno tekstova, ali isto tako korisnici neke tekstove ne bi htjeli da svi vide, stoga oni takve poruke šifriraju iz čega nastaje šifrirani tekst koji je namijenjen samo za one koji taj tekst primaju. Pošiljalac je korisnik koji taj tekst šalje, a primatelj je onaj koji prima tekst. Kako bi primatelj znao dešifrirati tekst koji je primio, on za to koristi poseban ključ koji znaju samo on i pošiljalac.

Slika 1.1 Prikaz šifriranog i dešifriranog teksta [19]

Šifrirani tekst se najviše upotrebljava kod većih agencija, zbog toga što oni najviše povjerljivih informacija prenose između sebe i ostalih agencija.

Šifriranjem i dešifriranjem teksta se bavi znanost koja se naziva kriptografija. U kriptografiji postoje razne metode koje služe za šifriranje teksta. Za dešifriranje teksta postoji znanost koja prikuplja podatke iz kriptografije, a naziva se kriptoanaliza.



Slika 1.2 Proces šifriranja i dešifriranja teksta [20]

Šifriranje i dešifriranje teksta se koristilo puno prije tehnologije, ali koje je bilo puno lakše nego današnje šifriranje odnosno dešifriranje. Prije se koristila metoda u kojoj su se najviše zamjenjivala slova, ali takve metode su s vremenom postale lakše za dešifrirati. Kako se tehnologija poboljšavala tako je postalo bolje i šifriranje teksta, a s time i teže dešifriranje teksta. U današnje doba sve se više koriste brojevi i slova zajedno za šifriranje poruka.

S boljom tehnologijom su nastali programi i aplikacije pomoću kojih se može šifrirati i dešifrirati tekst. Takvi programi i aplikacije nam pomažu da lakše nekakav tekst šifriramo i dešifriramo, upravo zbog toga što one rade sve pomoću algoritama koji su instalirani u njih. Primjer takve aplikacije je *CrypTool*.

CrypTool je najpoznatija aplikacija na svijetu koja se najviše koristi u kriptografiji. *CrypTool* aplikacija pomaže korisnicima da lakše pošalju šifriranu poruku sa metodom koji oni izaberu ako žele da nitko osim primatelja zna za nju. Isto tako korisnik koji je poslao poruku je rekao primatelju koja je to metoda i primatelj pomoću aplikacije može lakše dešifrirati tu poruku, ali uvijek će biti korisnici odnosno napadači koji će isto tako željeti probiti tu poruku, iako nije namijenjena za njih.

Cyber napadi će se uvijek događati, a s vremenom se oni i poboljšavaju, zbog toga će eksperti za sigurnost isto tako morati poboljšavati sigurnost metoda, a isto tako praviti nove metode koje će se moći teže probiti.

1.1. Zadatak završnog rada

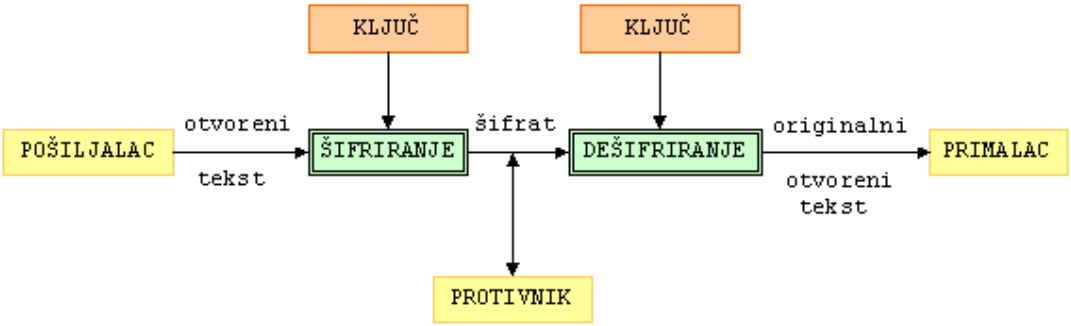
Kriptoanaliza uključuje različite metode otkrivanja šifriranih podataka bez poznavanja odgovarajućih ključeva potrebnih za pristup. Potrebno je analizirati i objasniti neke najčešće kriptoanalitičke metode, te ih prikazati na primjerima različitih kriptosustava (klasičnih i suvremenih) u okruženju aplikacije *CrypTool*.

2. KRIPTOGRAFIJA I KRIPTOANALIZA

2.1 Kriptografija

Kriptografija je metoda štićenja informacija i komuniciranja korištenjem posebnog koda kako bi mogli oni za koje je ta informacija namijenjena pročitati i procesirati je. Prefiks „kripto“ znači „skriven“ dok sufiks „grafija“ znači „pisanje“ [1].

U informatici kriptografija se odnosi na osiguranje informacije i komunikacijske tehnike izvedenih iz matematičkih koncepta i kalkuliranih pravila zvanih algoritmi za preoblikovanje poruka na načine da ih je teško dešifrirati. Takvi algoritmi su korišteni za generiranje ključeva, digitalno potpisivanje, potvrdu za zaštitu podataka i povjerljive komunikacije kao što su transakcije s karticom i e-mail. Primjer klasične kriptografije imamo prikazan na slici 2.1.



Slika 2.1 Klasična kriptografija [2]

Kriptografija je povezana sa disciplinama kriptologije i kriptoanalize. To uključuje tehnologiju kao što su mikrotočke, spajanje riječi sa slikama i ostali načini za skrivanje informacija u memoriju. Međutim, u današnjem računalnom svijetu, kriptografija se najčešće bavi s izokretanjem otvorenog teksta u šifrirani tekst (proces zvan enkripcija), i onda ponovno u otvoreni tekst (proces zvan dekripcija). Pojedinci koji su obučeni za ovo polje poznati su kao kriptografi.

Moderna kriptografija se bavi sa sljedeća četiri cilja:

1. Povjerljivost: informaciju ne može razumjeti onaj kome ta informacija nije namijenjena.

2. Integritet: informacija ne može biti promijenjena u memoriji ili prebačena između pošiljatelja i primatelja bez da je promjena primijećena.
3. Neosporavanje: pošiljatelj informacija u kasnijoj fazi ne može poreći svoje namjere u stvaranju ili prijenosu informacija.
4. Ovjera: pošiljatelj i primatelj mogu si međusobno potvrditi identitete i izvor odnosno odredište informacije

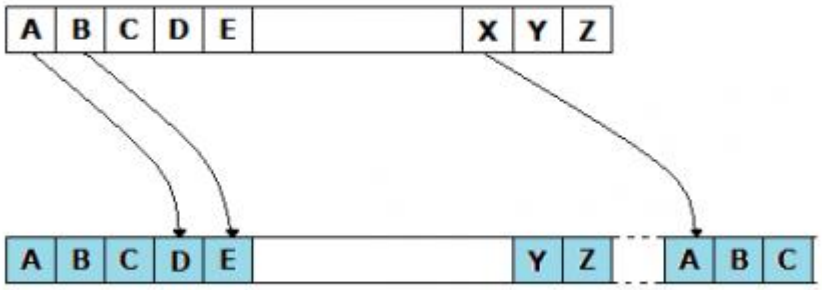
Procedure i protokoli koje se susreću s nekima ili svim ciljevima poznati su kao kriptosustavi. Za kriptosustave se često misli da se odnose samo na matematičke postupke i računalne programe, međutim, oni također uključuju regulaciju ljudskog ponašanja, kao što je biranje lozinki koje je teško pogoditi, odjavu neiskorištenih sustava i ne raspravljanje osjetljivih postupaka s vanjskim korisnicima.

Enkripcijski ili simetrični ključni algoritmi šifriranja stvaraju fiksnu duljinu bitova poznatu kao blok šifra s tajnim ključem koju pošiljatelj koristi za šifriranje podataka (enkripciju), a primatelj ga koristi za dešifriranje. Vrste kriptografije simetričnog ključa uključuju napredni standard za šifriranje (engl. *Advanced Encryption Standard* (*AES*)), specifikaciju za zaštitu osjetljivih informacija. To je specifikacija bez naknade koja se provodi u softveru i hardveru diljem svijeta.

Napadači mogu zaobići kriptografiju, upasti u računala koja su odgovorna za šifriranje i dešifriranje podataka te iskorištavati slabe implementacije, kao što je korištenje zadanih ključeva. Međutim, kriptografija napadačima otežava pristup porukama i podacima zaštićenim algoritmima šifriranja.

2.1.1. Povijest kriptografije

Prvi dokazi pojave kriptografije koji su pronađeni bili su isklesani 1900. godine prije Krista u glavnoj komori grobnice plemića Khnumhotepa II. u Egiptu. Isklesani hijeroglifi bili su neobičniji nego što su to bili pravi hijeroglifi. Oko 100. godine prije Krista, Julije Cezar je bio poznat po uporabi oblika enkripcije da pošalje skrivenu poruku svojim generalima u bitkama. Ova zamjenska šifra, poznata kao Cezarova šifra, je možda najviše spominjana povijesna šifra u akademskoj literaturi. Kod Cezarove šifre svaki znak običnog teksta zamijenjen je drugim znakom da se stvori šifrirani tekst. Verzija koju je Cezar koristio bio je pomak za 3 znaka što možemo vidjeti na slici 2.2 [3].



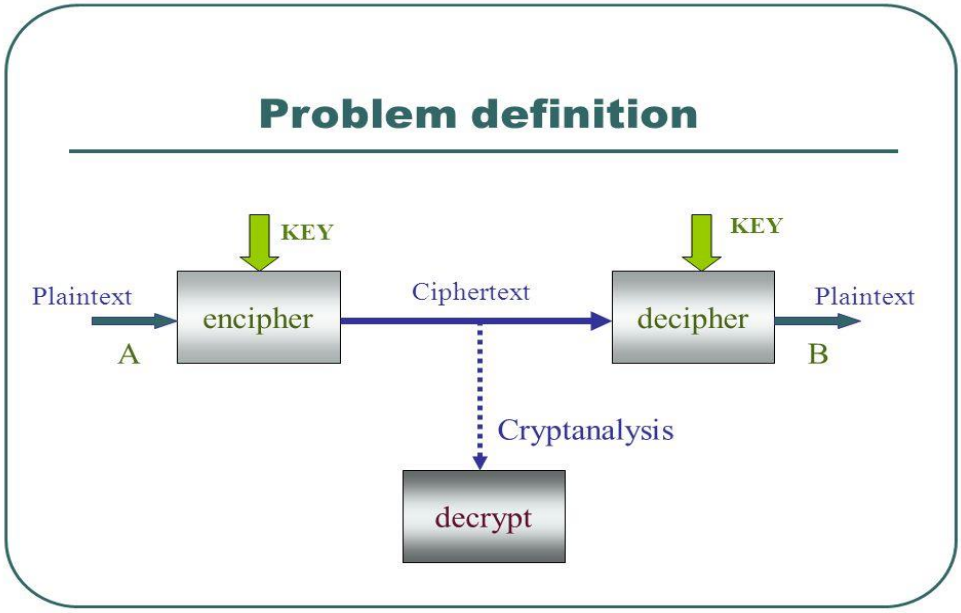
Slika 2.2 Cezarova šifra [3]

Enigma (Slika 2.3) je proizvedena od strane Nijemca Arthur Scherbiusa na kraju Prvog svjetskog rata, i puno ju je koristila Njemačka vojska tijekom Drugog svjetskog rata. Enigma je koristila 3,4 ili više rotora. Oni su se rotirali različitim brzinama kako se pisalo po tipkovnici i ispisivala su se odgovarajuća slova šifriranog teksta [3].

Slika 2.3 Enigma [4]

2.2. Kriptoanaliza

Kriptoanaliza je proučavanje šifriranih tekstova, šifri i kriptosustava s ciljem razumijevanja njihovog rada i pronalaženja i poboljšanja tehnika za njihovo pobjeđivanje ili slabljenje. Na primjer, kriptoanalitičari nastoje dešifrirati šifrirane tekstove bez poznavanja izvora otvorenog teksta, ključa za šifriranje ili algoritma koji se koristi za njegovo šifriranje; kriptoanalitičari također ciljaju sigurno raspršivanje, digitalne potpise i druge kriptografske algoritme [5].



Slika 2.4 Prikaz kritpoanalize [6]

Dok je cilj kriptoanalize pronaći slabosti ili na drugi način pobijediti kriptografske algoritme, kriptoanalitičari koriste rezultate istraživanja kriptografa za poboljšanje i jačanje ili zamjenu manjkavih algoritama. Kriptoanaliza koja se usredotočuje na dešifriranje šifriranih podataka, i kriptografija koja se fokusira na stvaranje i poboljšanje šifriranja i drugih algoritama, su aspekti kriptologije, matematičkog proučavanja kodova, šifri i povezanih algoritama.

Istraživači mogu otkriti metode napada koje potpuno prekidaju algoritam šifriranja, što znači da se šifrirani tekst šifriran s tim algoritmom može dešifrirati trivijalno bez pristupa ključu

za šifriranje. Sve češće, kriptoanalitički rezultati otkrivaju slabosti u dizajnu ili implementaciji algoritma, što može smanjiti broj ključeva koje treba pokušati na ciljnom šifriranju.

Kriptoanalizu koristi širok raspon organizacija, uključujući vlade čiji je cilj dešifrirati povjerljive komunikacije drugih nacija; tvrtke koje razvijaju sigurnosne proizvode i zapošljavaju kriptoanalitičare za testiranje njihovih sigurnosnih značajki; i hakeri, nezavisni istraživači koji traže slabosti u kriptografskim protokolima i algoritmima. Upravo ta stalna bitka između kriptografa koji pokušavaju osigurati informacije i kriptoanalitičara koji pokušavaju razbiti kriptosustave koji pomiču cijelo tijelo kriptološkog znanja unaprijed.

Zadaci kriptoanalitičara mogu uključivati razvoj algoritama, šifri i sigurnosnih sustava za šifriranje osjetljivih informacija i podataka te analiziranje i dešifriranje različitih vrsta skrivenih informacija, uključujući šifrirane podatke, šifrirane tekstove i telekomunikacijske protokole u kriptografskim sigurnosnim sustavima.

Kriptoanaliza koristi razne alate za kriptoanalizu kao što su:

1. *CrypTool*
2. *CryptoBench*
3. *Ganzua*

Kriptoanalitičari obično koriste mnoge druge alate za sigurnost podataka, uključujući softver za probijanje lozinki, iako nije neobično da kriptoanalitički istraživači kreiraju vlastite prilagođene alate za određene zadatke i izazove [5].

3. CRYPTOOL APLIKACIJA

CrypTool je projekt otvorenog koda. Glavni rezultat je besplatni softver za e-učenje *CrypTool*-a koji ilustrira kriptografske i kriptoanalitičke koncepte. *CrypTool* je u svijetu najraširenij e-learning softver u području kriptologije [7].

CrypTool implementira više od 400 algoritama. Korisnici ih mogu prilagoditi vlastitim parametrima. Grafičko sučelje, online dokumentacija, analitički alati i algoritmi *CrypTool*-a upoznaju korisnike s područjem kriptografije. *CrypTool* sadrži većinu klasičnih šifri, kao i moderne simetrične i asimetrične kriptosustave uključujući *RSA, ECC,* digitalne potpise, hibridno šifriranje, homomorfno šifriranje i *Diffie-Hellman* razmjenu ključeva. Metode iz područja kvantne kriptografije (kao *BB84* protokol za razmjenu ključeva) i područja postkvantne kriptografije su implementirane. Mnoge metode (na primjer *Huffmanov* kod, *AES*) su vizualizirane. Osim toga, sadrži: didaktičke igre (poput *Number Shark*, *Divider Game* ili *Zudo-Ku*) i interaktivne tutoriale o prostim brojevima, elementarnoj teoriji brojeva i kriptografiji na temelju rešetke [8].

Razvoj *CrypTool*-a započeo je 1998. godine. Izvorno su ga razvile njemačke tvrtke i sveučilišta, projekt je otvorenog koda još od 2001. Više od šezdeset ljudi diljem svijeta redovito doprinose projektu. Prilozi kao softverski dodaci došli su sa sveučilišta ili škola u sljedećim gradovima: Beograd, Berlin, Bochum, Brisbane, Darmstadt, Dubai, Duisburg-Essen, Eindhoven, Hagenberg, Jena, Kassel, Klagenfurth, Koblenz, London, Madrid, Mannheim, San Jose , Siegen, Utrecht, Varšava.

Trenutno se održavaju i razvijaju 4 verzije *CrypTool*-a: *CrypTool 1* (CT1) softver je dostupan na 6 jezika (engleski, njemački, poljski, španjolski, srpski i francuski). *CrypTool 2* (CT2) dostupan je na 3 jezika (engleski, njemački, ruski). Svi ostali, *JCrypTool* (JCT) i *CrypTool Online* (CTO), dostupni su samo na engleskom i njemačkom jeziku.

Cilj projekta *CrypTool* je osvijestiti korisnike o tome kako kriptografija može pomoći protiv prijetnji sigurnosti mreže i objasniti temeljne koncepte kriptologije.

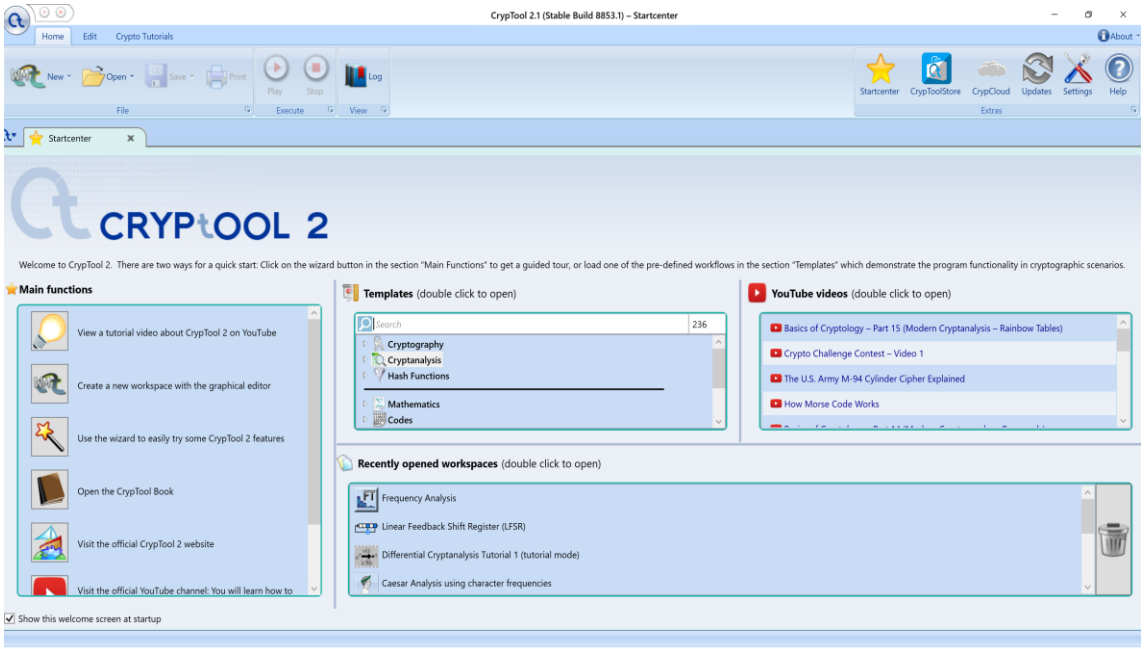
CrypTool 1 je napisan u *C++* i dizajniran je za operacijski sustav *Microsoft Windows*. U 2007, razvoj je počeo na dva dodatna projekta, oba na temelju *„pure-plugin“* arhitekture, da služe kao nasljednici izvornog *CrypTool* programa. Oba nasljednika redovito objavljuju nove stabilne verzije: *CrypTool 2* i *JCrypTool* 1.0. *CrypTool 2* koristi koncept vizualnog

programiranja kako bi razjasnio kriptografske procese. Trenutno, *Cryptool 2* sadrži više od 150 kripto funkcija. *JCrypTool* 1.0 radi na *Windowsima*, *Mac OS-u* i *Linuxu* i nudi perspektivu usredotočenu na dokumente i funkciju. Trenutno, *JCrypTool* sadrži više od 100 kripto funkcija. Jedna od glavnih točaka su moderni digitalni potpisi.

4. KORIŠTENI ALATI

4.1. CrypTool 2

CrypTool 2 je moderan nasljednik aplikacije *CrypTool 1*, dobro poznate platforme za kriptografiju i kriptoanalizu [9].



Slika 4.1 *CrypTool 2* aplikacija

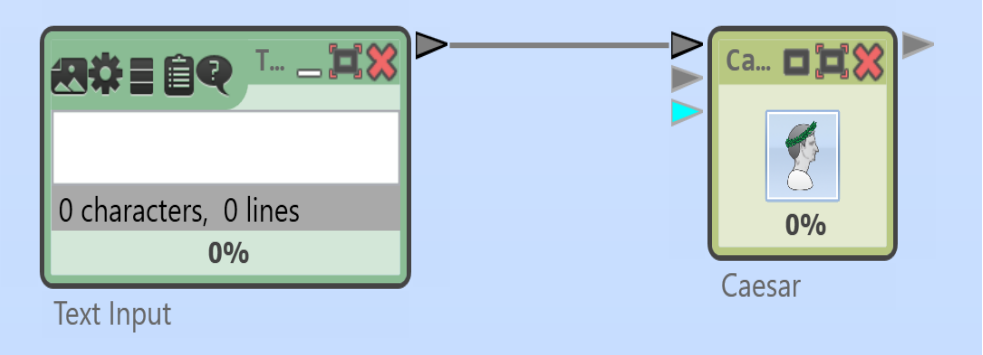
Na slici 4.1 prikazan je početni zaslon *CrypTool 2* aplikacije. U *CrypTool 2* aplikaciji opcije koje su raspoložive su: Glavne funkcije (engl. *Main functions*), Predlošci (engl. *Templates*) i *YouTube* videa.

- Glavne funkcije nude mogućnosti gledanja raznih *tutoriala* o *CrypTool 2* aplikaciji, te nudi mogućnost pravljenja novog radnog prostora u kojima korisnik može sam praviti razne predloške. Isto tako može se pokrenuti čarobnjak (engl. *Wizard*) da bi se dobio vođeni prolaz kroz *CrypTool 2* aplikaciju ili učitali neki od gotovih predložaka. Još se može pogledati *CrypTool* knjiga, posjetit *CrypTool 2 web* stranica, posjetit *YouTube* kanal i *Facebook* stranicu.

- Predlošci nude mogućnost učitavanja nekih od gotovih predložaka iz kriptografije, kriptoanalize i *Hash* funkcija. Isto tako mogu se učitati matematički, kodni, protokolni te steganografski predlošci.
- Kod *YouTube* videa može se jednim klikom otići na određeni video na *CrypTool 2 YouTube* kanalu.

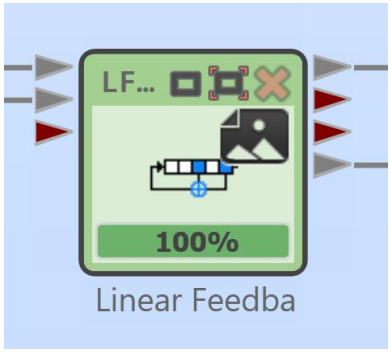
CrypTool 2 nudi mogućnosti koje nema aplikacija *CrypTool 1*, kao što su : vizualno programiranje, vizualni prikaz algoritama, opsežne funkcije kriptoanalize i internetsku pomoć.

- *CrypTool 2* nudi grafičko korisničko sučelje za vizualno programiranje (slika 3.2) kako bi tijek rada mogao biti prikazan i kontroliran da uključi intuitivnu manipulaciju i interakciju kriptografskih funckija [9].

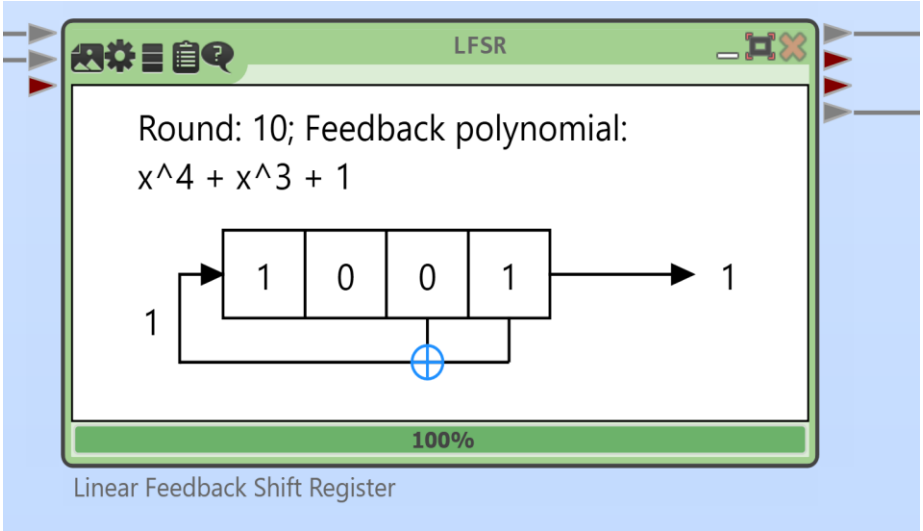


Slika 4.2 Vizualno programiranje

- Komponenta korištena (Slika 4.3) za radni tijek vizualnog programiranja može isto tako prikazati unutarnju operaciju odnosno njezin algoritam. Ta opcija korisniku čini korisnim za razumijevanje svih detalja kriptografskog algoritma dok može sagledati veću sliku kako bi taj algoritam koristio za projekt u stvarnom životu [9].

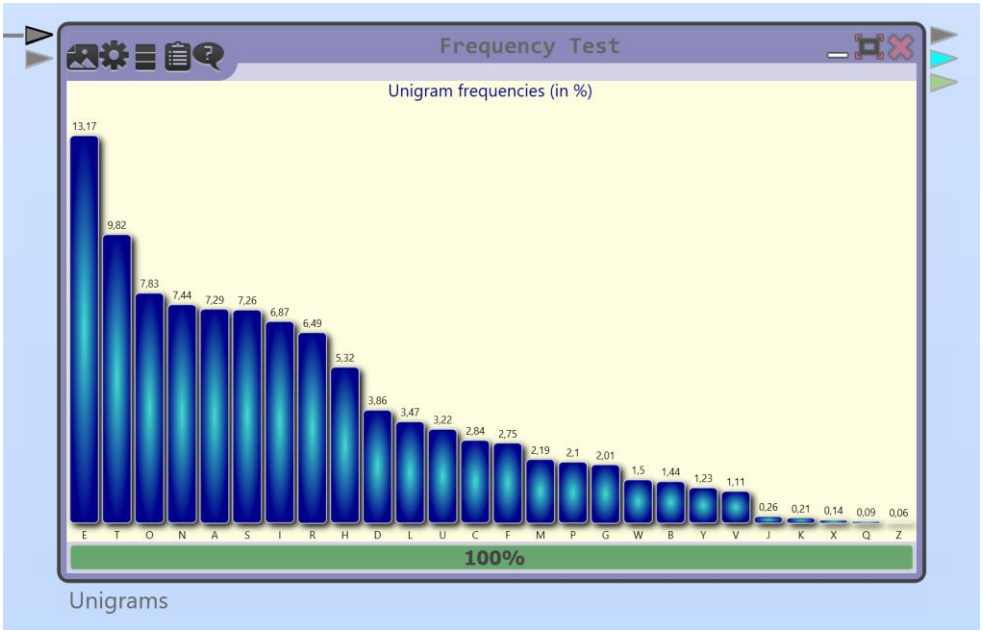


Slika 4.3 Korištena komponenta



Slika 4.4 Prikaz algoritma korištene komponente

- *CrypTool 2* nudi raznolik izbor kriptoanalitičkih alata za analiziranje ili čak razbijanje klasičnih i modernih šifri. Postoje razne kriptoanalitičke funkcije kao što je npr. frekvencijski test koji pronađe postotak određenih slova u tekstu (Slika 4.5) [9].



Slika 4.5 Frekvencijski test za slova

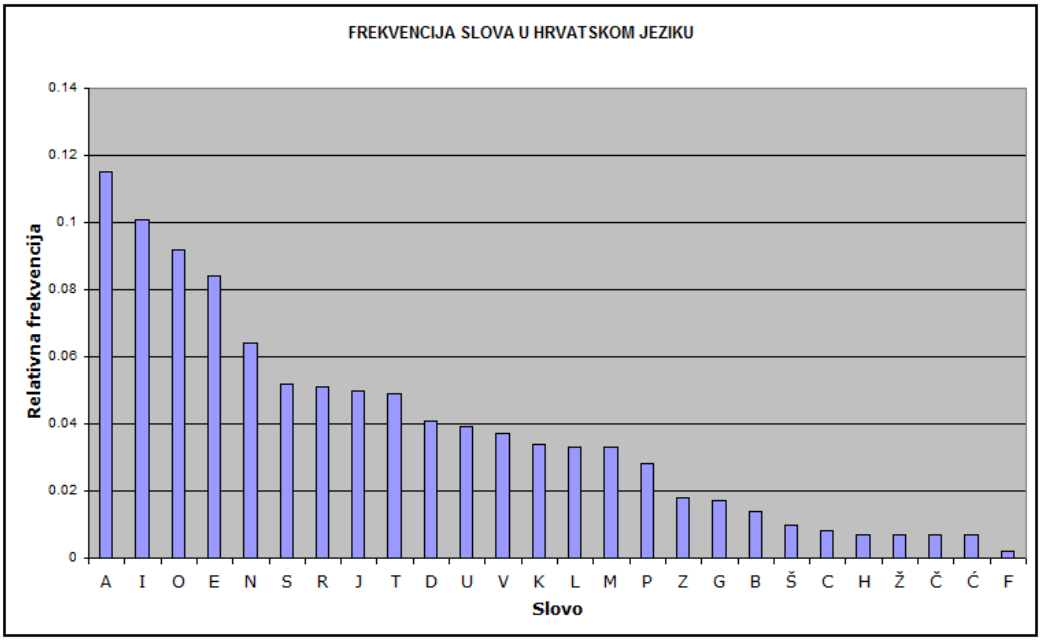
5. KRIPTOANALITIČKE METODE

U ovom odlomku prikazane su i objašnjene neke od najpoznatijih kriptoanalitičkih metoda. One su prikazane kako rade pomoću *CrypTool 2* aplikacije.

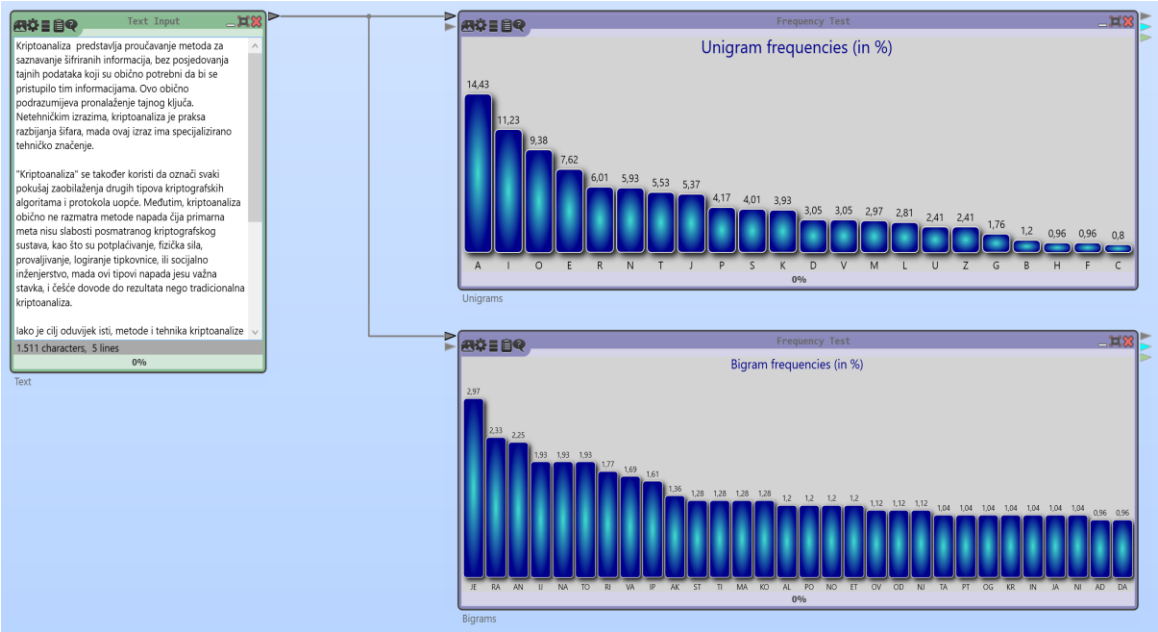
5.1. Frekvencijska analiza

Frekvencijska analiza je kriptoanalitička klasična metoda u kojoj se statistička svojstva šifriranog teksta koriste za izvlačenje zaključaka o nekodiranoj poruci [10].

U kriptografiji, frekvencijska analiza je nauka o učestalosti slova ili skupini slova u šifriranom tekstu. Metoda se koristi kako bi se razbile razne šifre kriptirane metodom zamjene. Frekvencijska analiza se radi tako da se broji pojava svakog slova u tekstu. Nakon toga se uspoređuje sa frekvencijom slova ovisno u kojem jeziku gledamo. Na primjer u hrvatskom jeziku najčešća su slova A, I, O, E dok su najrjeđa H, Ž, Č, Ć i F što možemo vidjeti na slici 5.1.

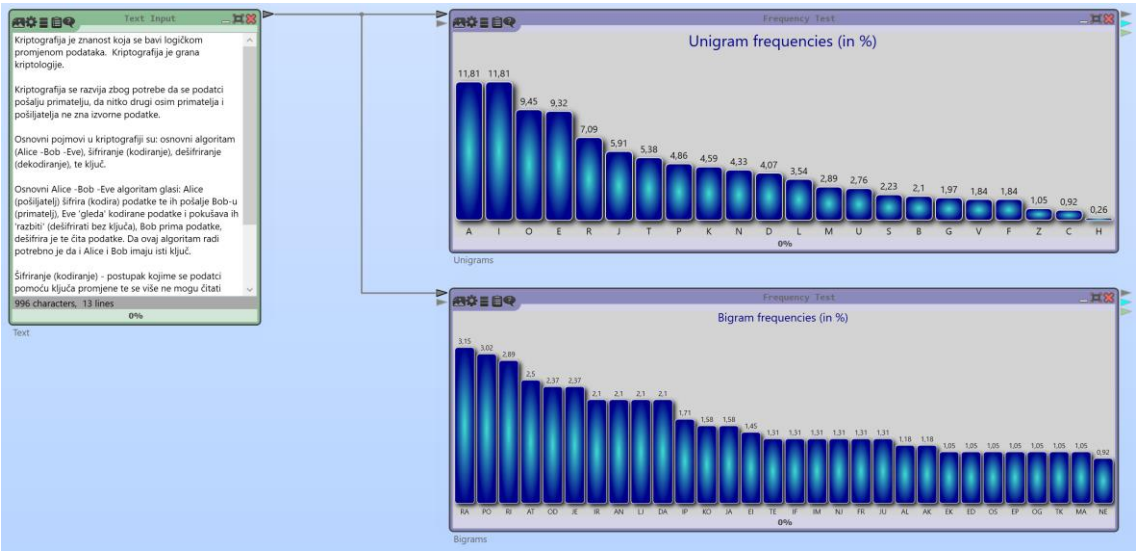


Slika 5.1 Frekvencija slova u hrvatskom jeziku [11]



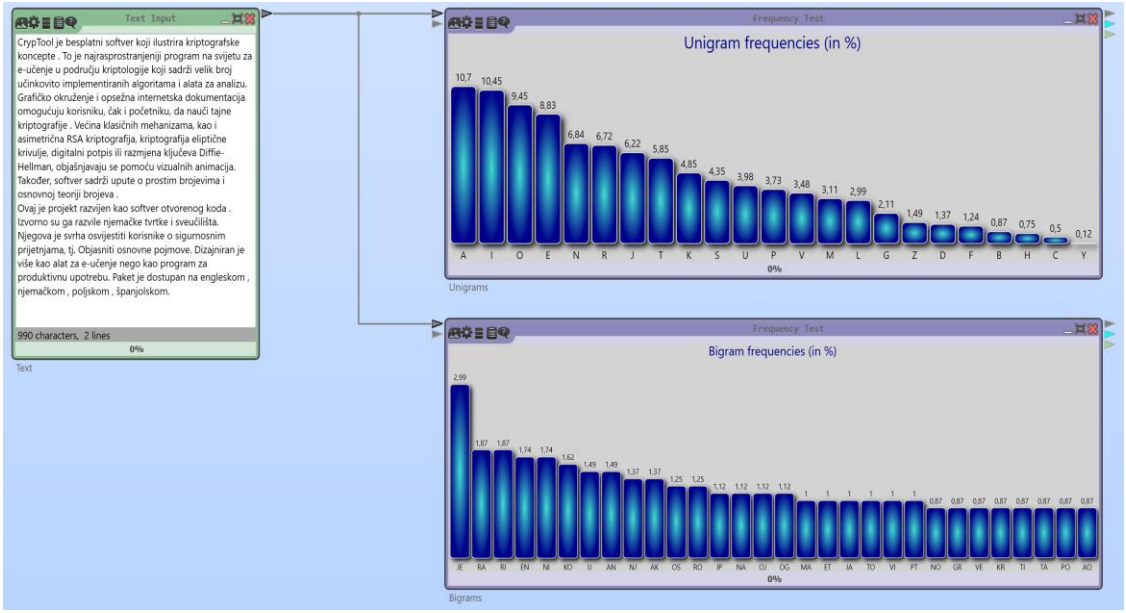
Slika 5.2 Primjer 1: Prikaz frekvencije slova

Slika 5.2 prikazuje kako frekvencijska analiza radi pomoću *CrypTool 2* aplikacije. U ovom primjeru može se vidjeti učestalost pojave jednog slova (engl. *unigram*) i može se vidjeti kako se većina *unigrama* podudara sa frekvencijom slova u hrvatskom jeziku i može se vidjeti učestalost pojave skupine od dva slova (engl. *bigram*) korištenjem frekvencijske analize u prikazanom tekstu. Ovdje je prikazano 30 najčešćih *bigrama*, ali se ta opcija može promijeniti u postavkama komponente.



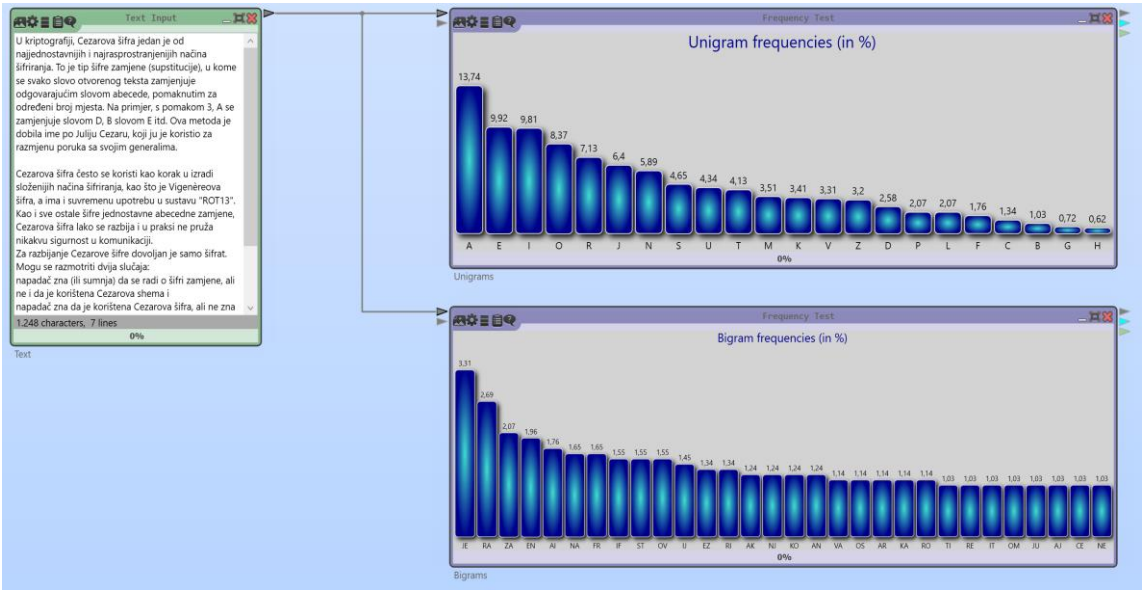
Slika 5.3 Primjer 2: Prikaz frekvencije slova

Na slici 5.3 prikazan je primjer za drugi tekst za prikaz frekvencije slova u hrvatskom jeziku. Vidi se kako je opet slično kao i u prošlom primjeru.



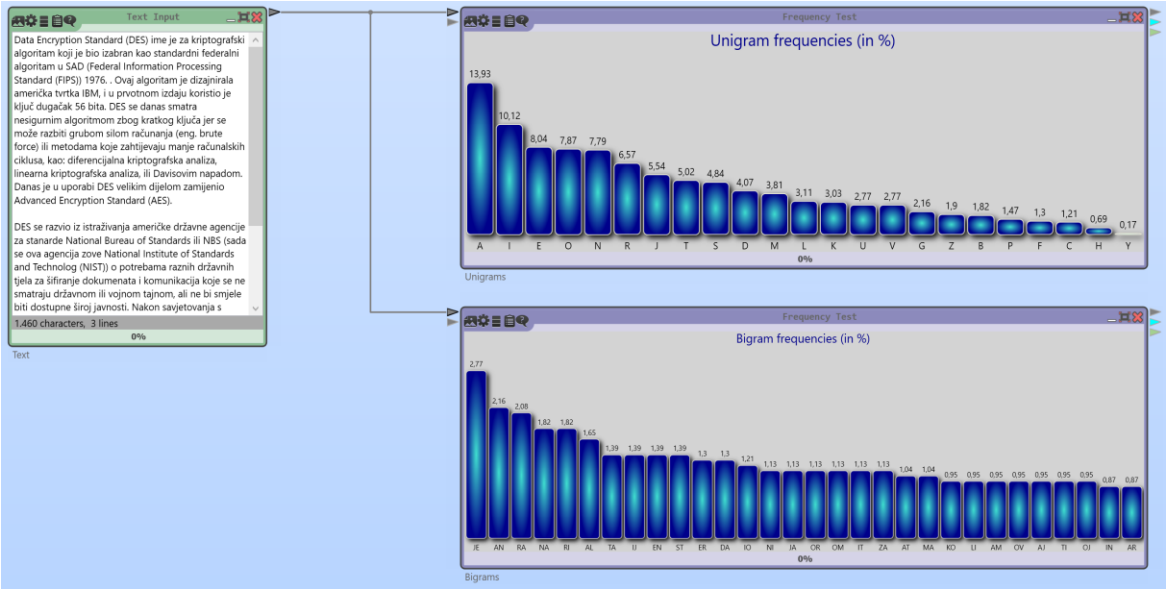
Slika 5.4 Primjer 3: Prikaz frekvencije slova

Na slici 5.4 prikazan je primjer za treći tekst za prikaz frekvencije slova u hrvatskom jeziku. *Unigrami* se većinom poklapaju sa primjerima iz prošlih tekstova.



Slika 5.5 Primjer 4: Prikaz frekvencije slova

Na slici 5.5 prikazan je primjer za četvrti tekst za prikaz frekvencije slova u hrvatskom jeziku. Vidi se kako je slovo A na prvom mjestu kao i u ostalim primjerima, ali vidi se kako se slovo E koje je inače četvrto po redu po učestalosti, nalazi na drugom mjestu što znači da učestalost slova isto tako ovisi o dužini i vrsti teksta.



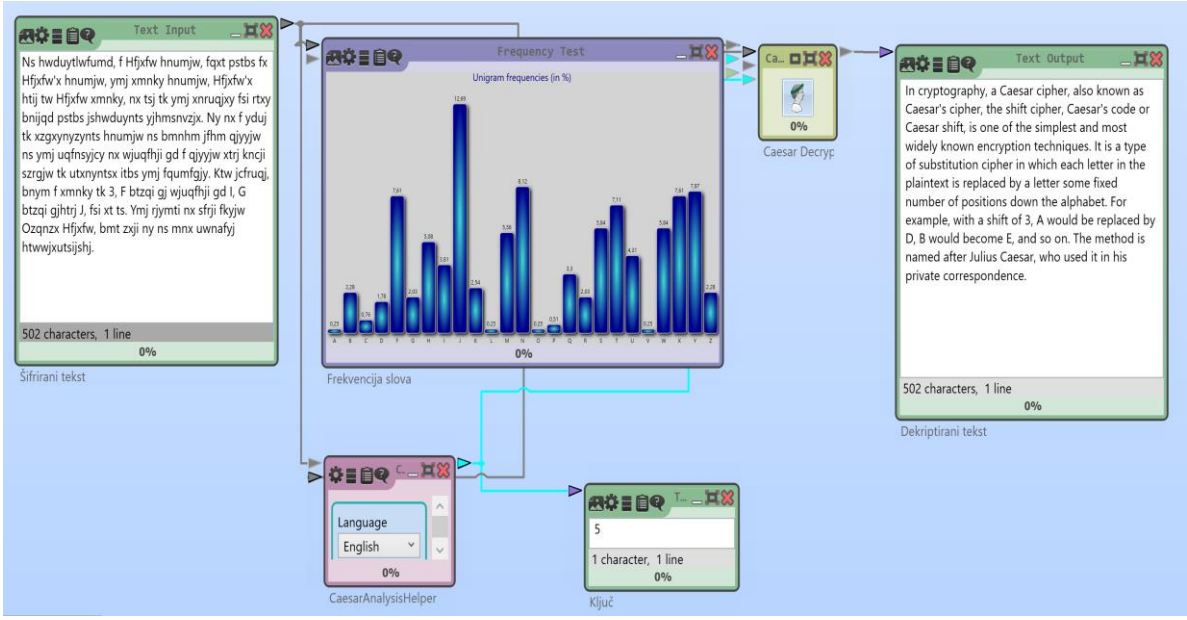
Slika 5.6 Primjer 5: Prikaz frekvencije slova

Na slici 5.6 prikazan je primjer za peti tekst za prikaz frekvencije slova u hrvatskom jeziku. Kada bi se pogledali ostali primjeri zajedno s ovim, zaključuje se da će u većini slučajeva slovo A uvijek biti najučestalije, dok će iza njega slijedit većinom slova I, O, E, kao što to prikazuje slika 5.1. što potvrđuje teoriju frekvencije slova u hrvatskom jeziku.

5.2. Kriptoanaliza Cezarove šifre korištenjem frekvencije slova

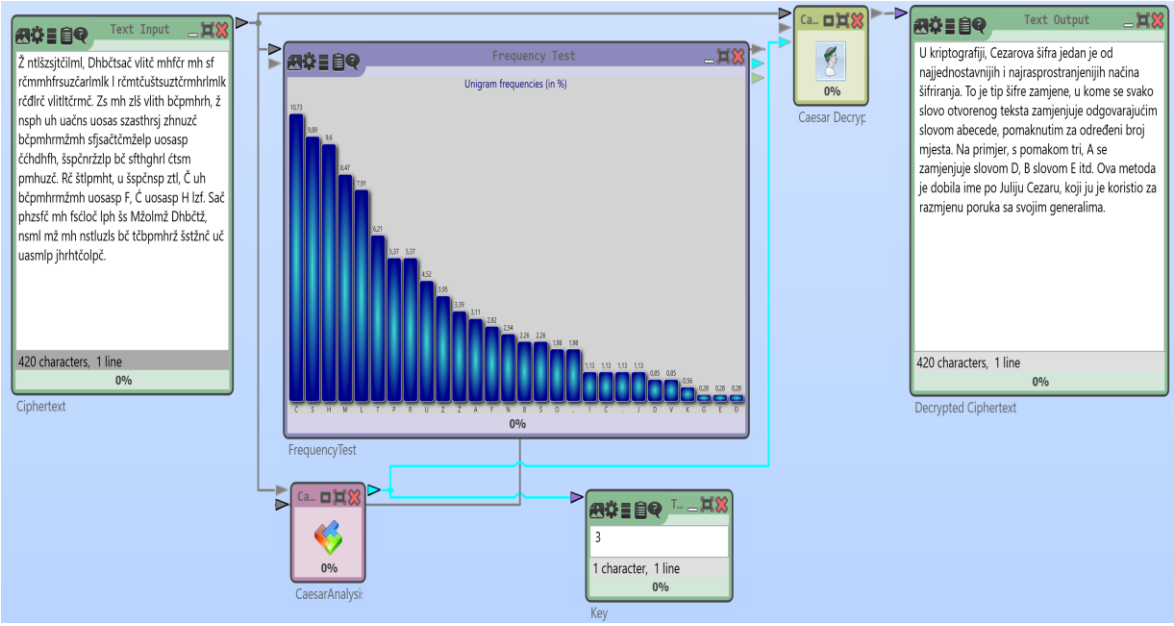
Ova klasična metoda prikazuje učestalost slova na Cezarovu šifru. Učestalost slova je analizirana i ovisno u rezultatu, slova su zamijenjena Cezarovom šifrom. Kod Cezarove šifre svaki znak običnog teksta zamijenjen je drugim znakom da se stvori šifrirani tekst. Verzija koju je Cezar koristio bio je pomak za 3 znaka.

Kriptoanaliza Cezarove šifre korištenjem frekvencije slova može biti lako razbijena. Recimo da napadač zna ili pretpostavlja da je napravljena nekakva metoda zamjene na tekstu, ali to ne mora biti isključivo Cezarova metoda. Šifra može biti razbijena ako napadač koristi metodu zamjene slova kao što je frekvencijska odnosno statistička analiza. Dok napadač razbija šifru velika je vjerojatnost da će uočiti koje se slovo najviše ponavlja i zaključit će da se radi o Cezarovoj šifri [12].



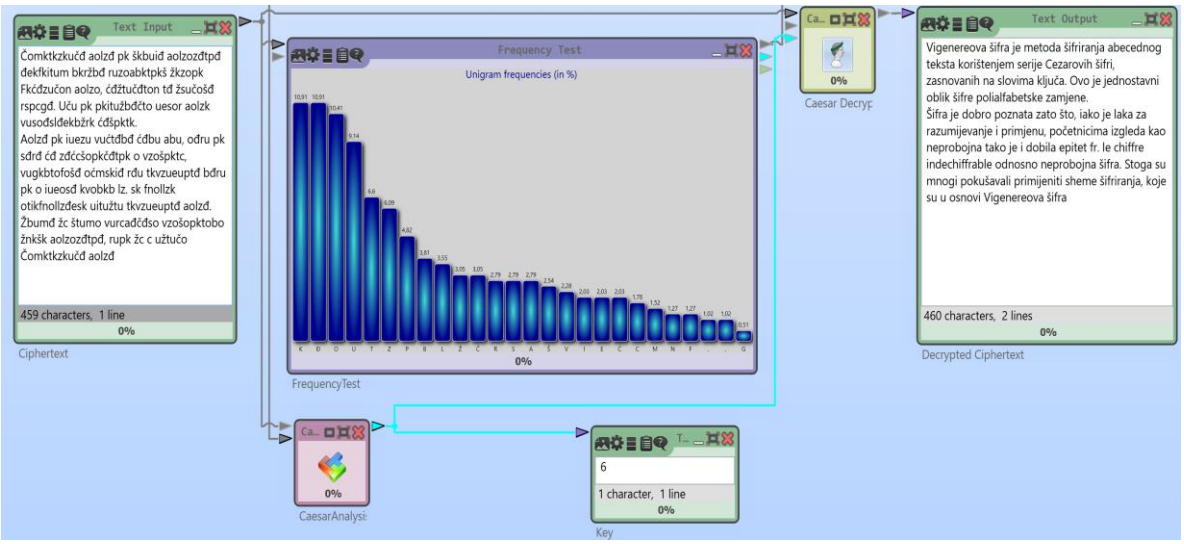
Slika 5.7 Primjer 1: Kriptoanaliza Cezarove šifre korištenjem frekvencije slova

Slika 5.3 prikazuje kako kriptoanaliza Cezarove šifre korištenjem frekvencije slova radi pomoću *CrypTool 2* aplikacije. Šifrirani tekst je proslijeđen na komponentu koja se naziva „Frekvencija slova“. Ta komponenta generira grafikon slova u postotcima koja se nalaze u šifriranom tekstu i šalje ih na komponentu koja se zove *„CaesarAnalysisHelper“*. *„CaesarAnalysisHelper“* izvodi kriptoanalizu Cezarove šifre koristeći frekvenciju jednog slova (engl. *1-grams*) u šifriranom tekstu. Izračunati ključ koji govori koliki je pomak slova, proslijeđen je Cezarovoj komponenti da dešifrira šifrirani tekst. Ključ koji govori koliki je pomak slova može se vidjeti na komponenti koja se zove „Ključ“. Komponente mogu podnijeti i frekvencije od više slova (engl. *n-grams*).



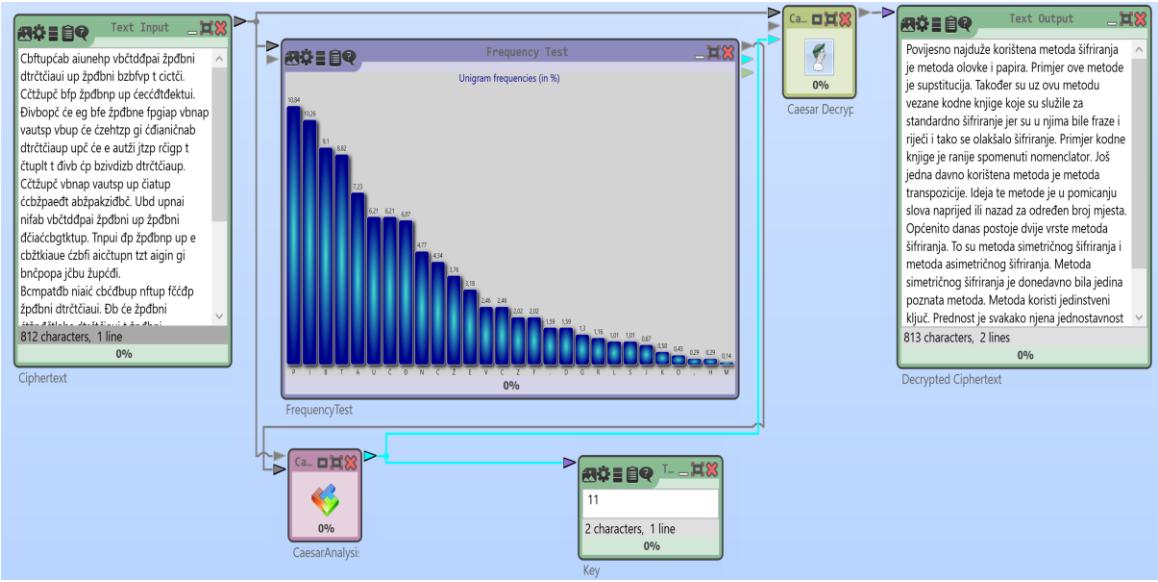
Slika 5.8 Primjer 2: Kriptoanaliza Cezarove šifre korištenjem frekvencije slova

Na slici 5.8 prikazan je primjer za drugi tekst dešifriran pomoću kriptoanalize Cezarove šifre korištenjem frekvencije slova. Može se vidjeti kako se frekvencija slova poklapa sa frekvencijom slova u hrvatskom jeziku, gdje slovo Č postaje slovo A, slovo S postaje slovo O, itd. Vidi se kako je ovdje pomak za 3 slova. Na ovoj slici su prikazane točke i zarezi zbog toga što *CrypTool 2* aplikacija ne podržava hrvatski jezik za ovu metodu, zato se u opcijama mora postaviti opcija za posebne simbole kao što su č, ć, đ, š, ž.



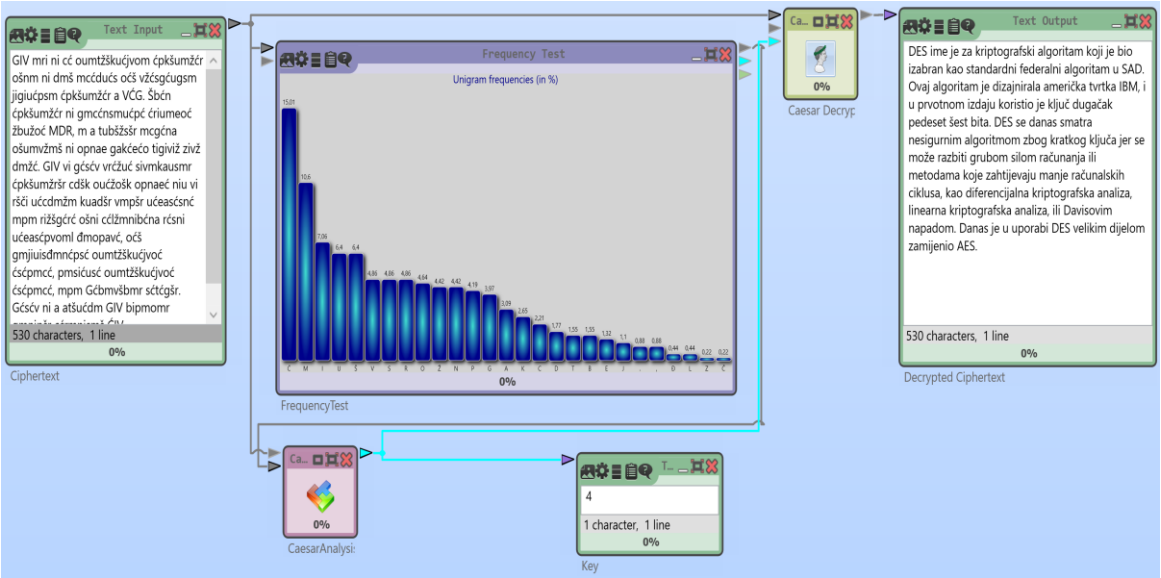
Slika 5.9 Primjer 3: Kriptoanaliza Cezarove šifre korištenjem frekvencije slova

Na slici 5.9 prikazan je primjer za treći tekst dešifriran pomoću kriptoanalize Cezarove šifre korištenjem frekvencije slova. Može se vidjeti kako slovo K i slovo Đ imaju istu učestalost u šifriranom tekstu. Vidi se kako je pomak slova za 6, pa se zaključuje kako je slovo Đ zapravo slovo A, a slovo K zapravo slovo E.



Slika 5.10 Primjer 4: Kriptoanaliza Cezarove šifre korištenjem frekvencije slova

Na slici 5.10 prikazan je primjer za četvrti tekst dešifriran pomoću kriptoanalize Cezarove šifre korištenjem frekvencije slova. Može se vidjeti kako je pomak slova za 11, tako da se zaključuje da je slovo P slovo E, a slovo I slovo A. Najučestalije slovo u ovom tekstu je E, tako da učestalost isto tako ovisi o vrsti teksta.



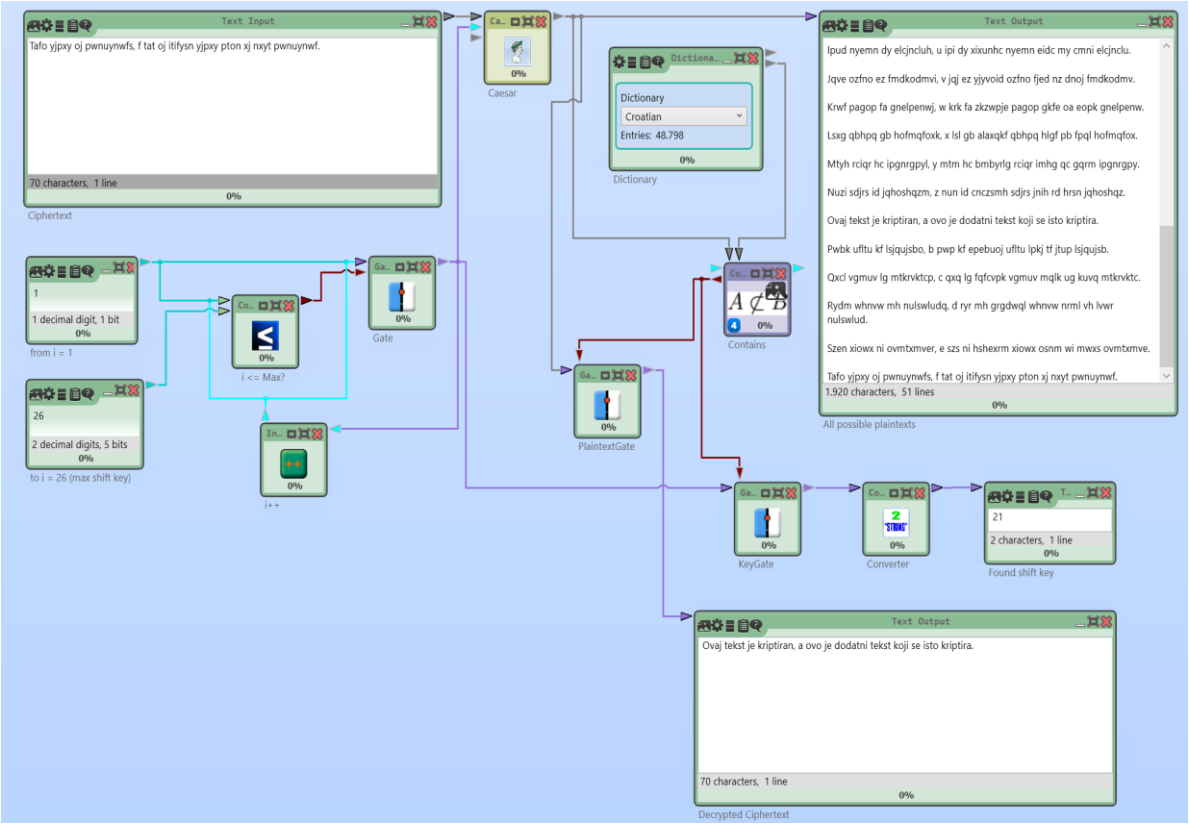
Slika 5.11 Primjer 5: Kriptoanaliza Cezarove šifre korištenjem frekvencije slova

Na slici 5.11 prikazan je primjer za peti tekst dešifriran pomoću kriptoanalize Cezarove šifre korištenjem frekvencije slova. Može se vidjeti kako je pomak slova 4, stoga slovo Ć postaje slovo A, slovo M postaje slovo I. Zaključuje se kako je u većini slučajeva slovo A uvijek najučestalije slovo.

5.3. Kriptoanaliza Cezarove šifre „grubom silom“ (brute-force)

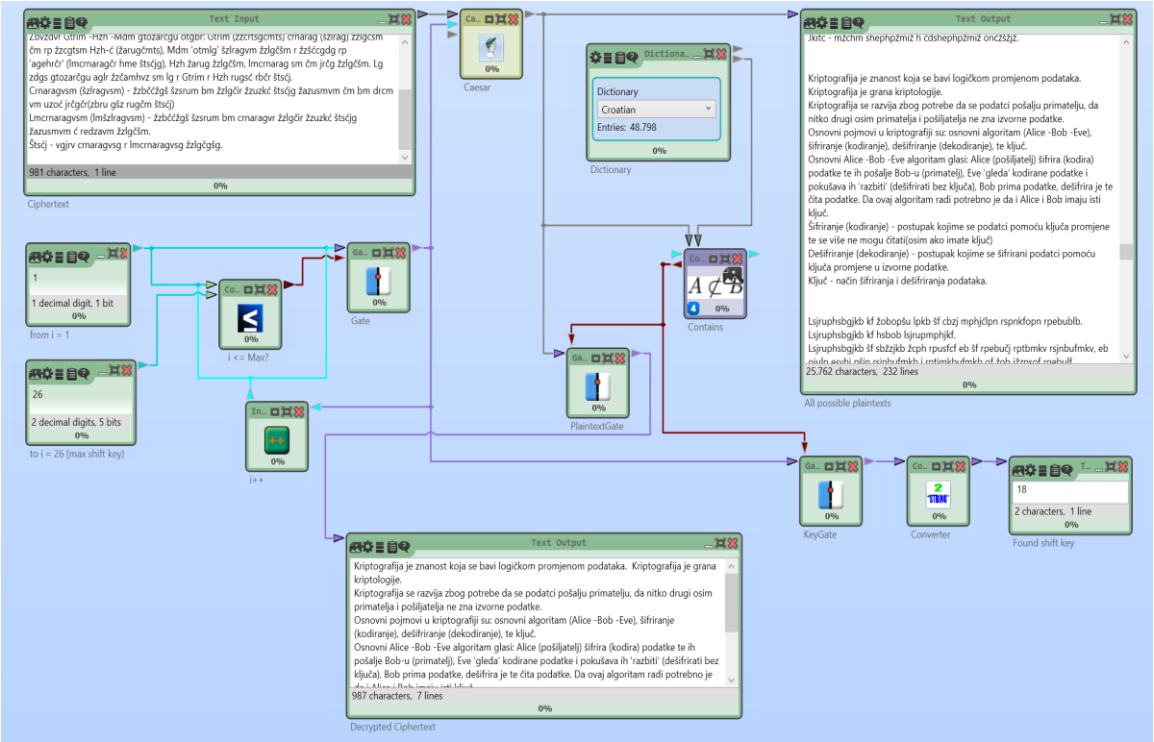
Ova klasična metoda prikazuje dešifriranje teksta pomoću kriptoanalize Cezarove šifre „grubom silom“. Osnovni princip ove metode je to da je tekst dešifriran sa svim mogućim pomacima slova odnosno određenim ključem i za svaki dešifrirani tekst je provjereno nalaze li se riječi dobivenog teksta u rječniku tog jezika. Ako je nekoliko riječi iz rječnika pronađeno u dešifriranom tekstu, vrlo je velika vjerojatnost da je to točna dekripcija.

Cezarova šifra pomoću ove metode isto kao i pomoću prošle metode može biti lako razbijena. Najlakši je način da se zapišu sve moguće kombinacije koje se dobiju pomicanjem slova na papir ili u tablicu. Kada se dođe do prepoznatljivih riječi možemo zaključiti koliki je pomak slova i dešifrirati tekst [12].



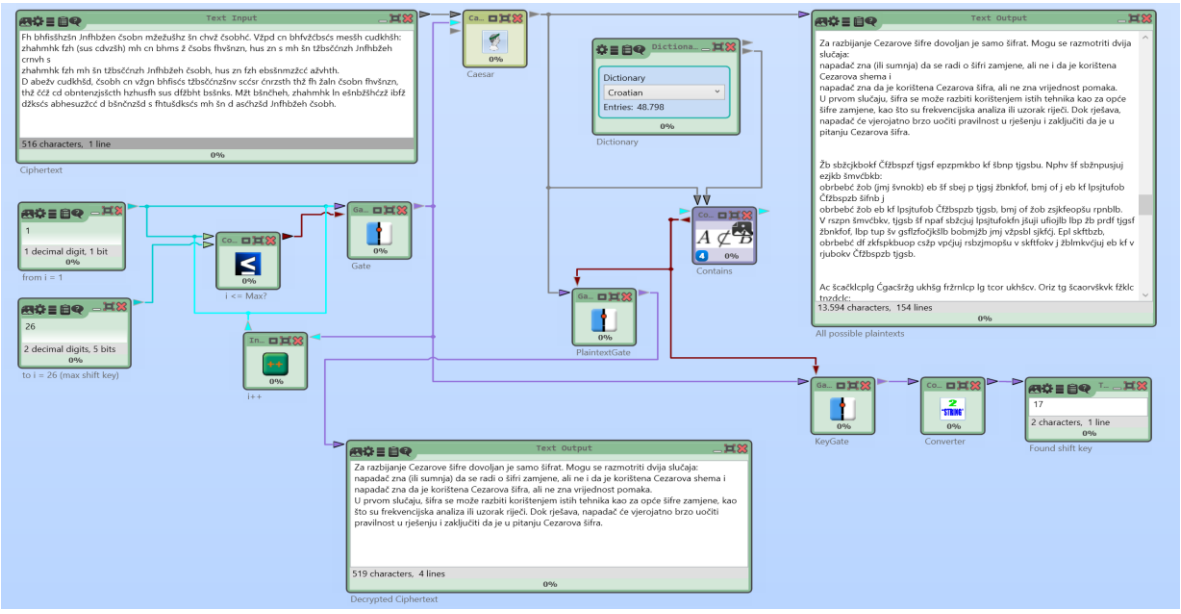
Slika 5.12 Primjer 1: Kriptoanaliza Cezarove šifre „grubom silom“

Slika 5.4 prikazuje kako kriptoanaliza Cezarove šifre „grubom silom“ radi pomoću *CrypTool 2* aplikacije. Šifrirani tekst je proslijeđen Cezarovoj komponenti. Pomak slova odnosno ključ za Cezarovu šifru je postavljen od 1 do maksimalne vrijednosti postavljene u *„max shift key“* u petlji. U petlji se nalaze brojač „i++“ i *„Gate“*. Dok god *„Gate“* ima *TRUE* vrijednost koja dolazi iz komparatora *„i <= max shift key“* petlja će raditi. Za svaki ključ koji Cezarova komponenta dobije radit će dešifriranje teksta. Rezultati dešifriranog teksta su sačuvani u komponenti *„All possible plaintexts“*. Nakon toga komponenta *„Contains“* provjerava svaki dobiveni rezultat i nalazi li se koja riječ od rezultata u rječniku. Ako se nalazi, *„Contains“* komponenta daje *TRUE* vrijednost komponenti *„PlaintextGate“* i ona šalje dobiveni rezultat odnosno dešifrirani tekst u komponentu *„Decrypted Ciphertext“*. Ako nema rezultata, onda je šifrirani tekst vjerojatno šifriran drugom šifrom ili je neki drugi jezik u pitanju.



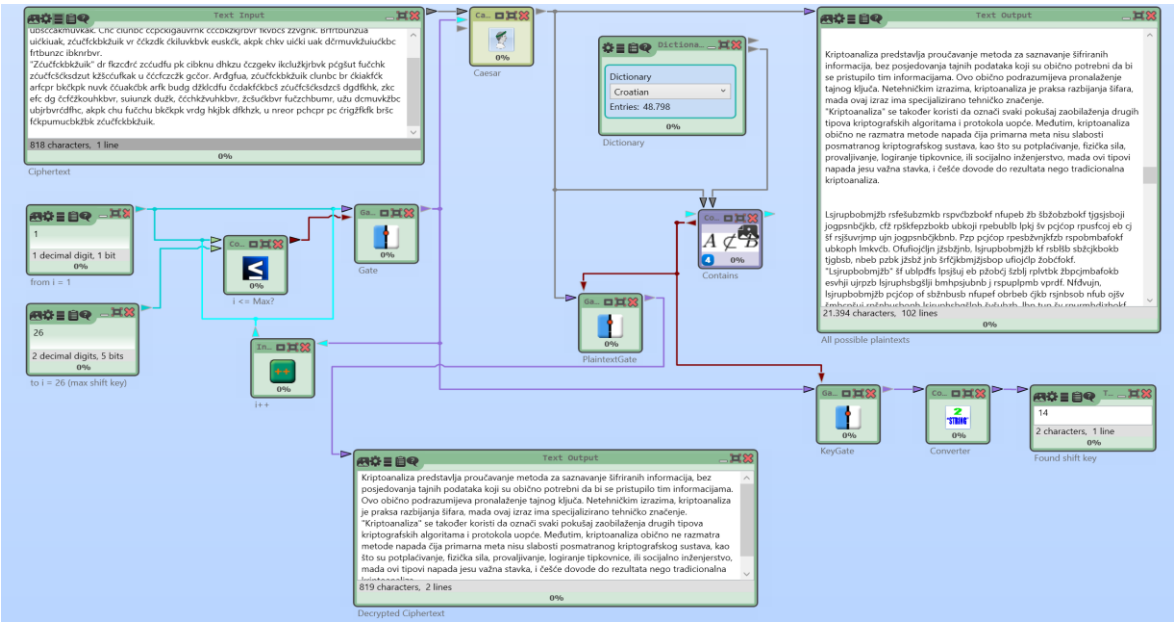
Slika 5.13 Primjer 2: Kriptoanaliza Cezarove šifre „grubom silom“

Na slici 5.13 prikazan je primjer za drugi tekst dešifriran pomoću kriptoanalize Cezarove šifre „grubom silom“. Vidi se kao i u prošlom primjeru kako se radila analiza za sva slova dok se ne pronađe tekst koji se poklapa sa ključem odnosno pomakom slova koji se traži.



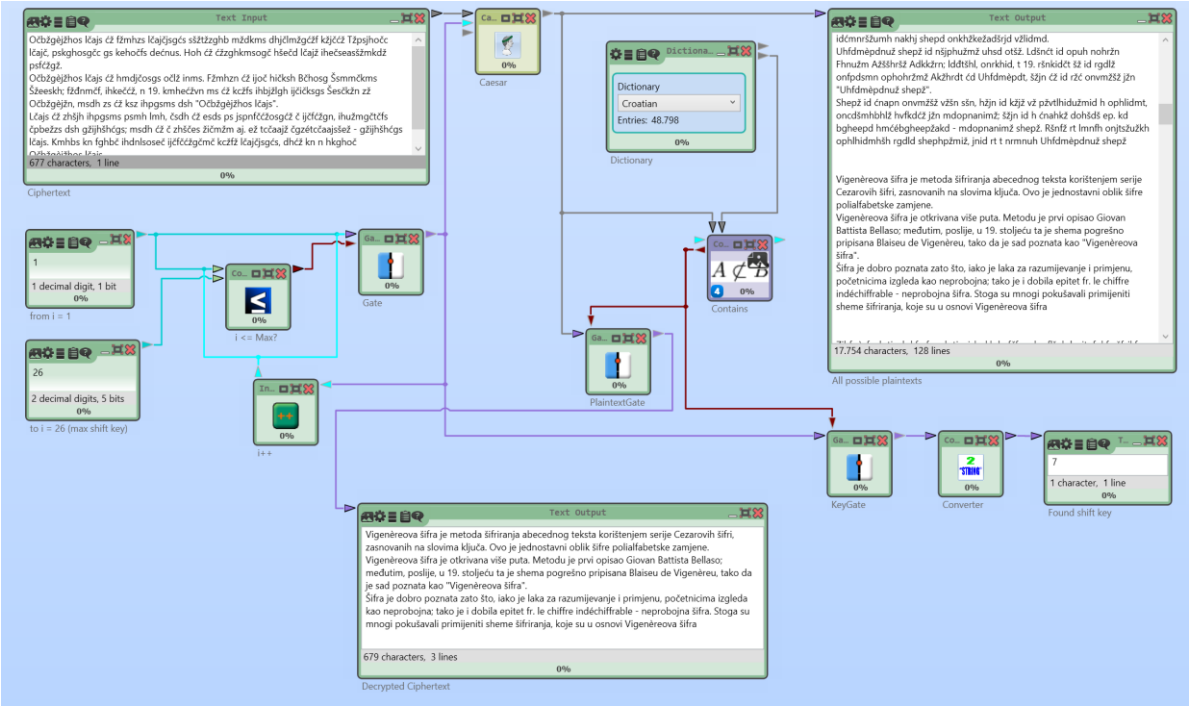
Slika 5.14 Primjer 3: Kriptoanaliza Cezarove šifre „grubom silom“

Na slici 5.14 prikazan je primjer za treći tekst dešifriran pomoću kriptoanalize Cezarove šifre „grubom silom“. Može se vidjeti kako je ovdje pronađen drugačiji ključ kao i u ostalim primjerima. Sve ovisi o tome koliki je prvo pomak slova bio za šifriranje teksta.



Slika 5.15 Primjer 4: Kriptoanaliza Cezarove šifre „grubom silom“

Na slici 5.15 prikazan je primjer za četvrti tekst dešifriran pomoću kriptoanalize Cezarove šifre „grubom silom“.



Slika 5.16 Primjer 5: Kriptoanaliza Cezarove šifre „grubom silom“

Na slici 5.16 prikazan je primjer za peti tekst dešifriran pomoću kriptoanalize Cezarove šifre „grubom silom“. Zaključuje se da je ovo dešifriranje lakši način dešifriranja, ali da za njega treba uložiti puno vremena. Isto tako zaključuje se kako pomoću *CrypTool 2* aplikacije treba svega par sekundi da se dešifrira nekakav tekst pomoću ove analize.

5.4. Vigenerova analiza

Ova klasična metoda prikazuje dešifriranje teksta skrivenog *Vigenerovom* šifrom. *Viegenerova* šifra je polialfabetska zamjena bazirana na tablici 5.1 [13].

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Tablica 5.17 *Vigenerova* tablica [14]

Vigenerova šifra koristi ovu tablicu zajedno sa ključnom riječi da bi se šifrirala ili dešifrirala poruka. Na primjer, tekst koji će se šifrirati je: TEKST ZA SIFRIRATI i korištenjem ključne riječi KRIPTOLOGIJA može se šifrirati tekst na slijedeći način: uzima se prvo slovo ključne riječ, a to je slovo K i prvo slovo teksta T. Nakon toga u tablici 5.1 u okomitom ili vodoravnom stupcu pronađe se slovo K. Ako je slovo K pronađeno u okomitom stupcu onda se uzima slovo T iz vodoravnog stupca i obrnuto. Poslije toga se gleda koje je slovo u tablici u ravnini sa slovima K i T. Pronađeno slovo će nam biti prvo slovo šifriranog teksta, a to je slovo D. Isto tako uzima se za iduće slovo ključne riječi, a to je R i iduće slovo teksta, a to je E. Kada se napravi isto što i u prvom koraku, dobije se drugo slovo šifriranog teksta, a to je V. I tako dalje se uzima za ostala slova.

Ključna riječ:	K	R	I	P	T	O	L	O	G	I	J	A	K	R	I	P
Tekst:	T	E	K	S	T	Z	A	S	I	F	R	I	R	A	T	I
Šifrirani tekst:	D	V	S	H	M	Z	L	G	O	N	A	I	B	R	B	X

Tablica 5.2 Šifriranje teksta *Vigenerovom* šifrom

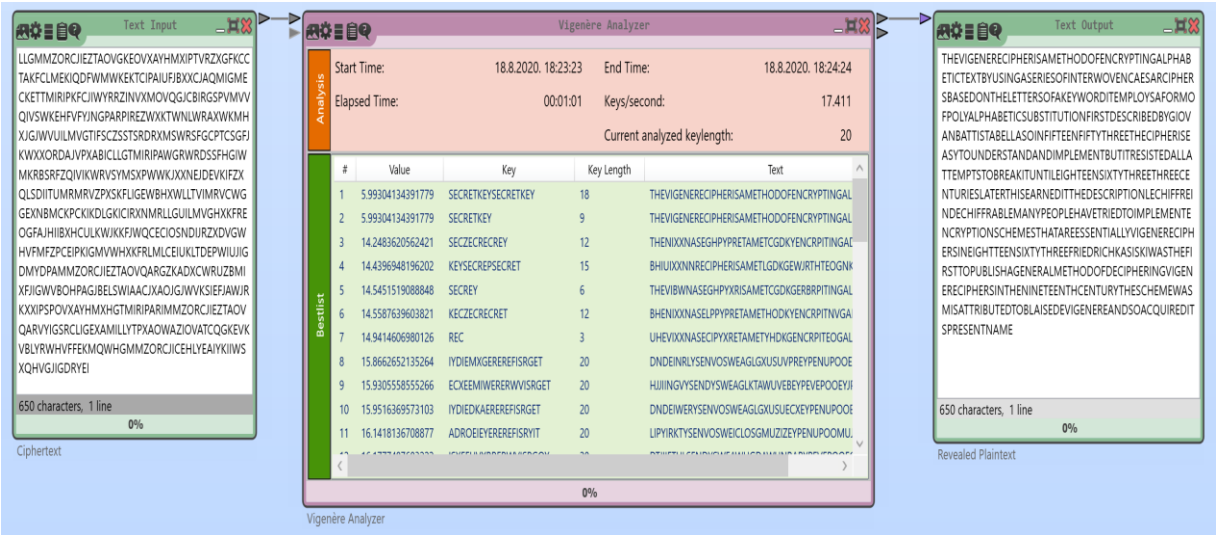
Na sličan način možemo i dešifrirati tekst:

Ključna riječ:	K	R	I	P	T	O	L	O	G	I	J	A	K	R	I	P
Šifrirani tekst:	D	V	S	H	M	Z	L	G	O	N	A	I	B	R	B	X
Tekst:	T	E	K	S	T	Z	A	S	I	F	R	I	R	A	T	I

Tablica 5.3 Dešifriranje teksta *Vigenerovom* šifrom

U ovom slučaju uzima se prvo slovo iz ključne riječi, a to je slovo K i traži se gdje se nalazi u prvom stupcu ili retku tablice 5.1. Kada se pronađe slovo K, nakon toga se u tablici traži vodoravno ili okomito od slova K, gdje se nalazi prvo slovo šifriranog teksta, a to je slovo D. Nakon što se pronađe slovo D u tablici, onda se gleda koje je slovo vodoravno ili okomito od njega, ovisno o tome kako se uzelo slovo K, i vidi se da je slovo T vodoravno ili okomito od slova D. Nakon što se pronašlo slovo T, zaključuje se da je to prvo slovo teksta koji se dešifrira. Isto tako se radi za drugo slovo ključne riječi, a to je slovo R. Pronalazi se drugo slovo šifriranog teksta u tablici, a to je slovo V koje je okomito ili vodoravno od slova R. Nakon toga opet se gleda koje je slovo okomito ili vodoravno od slova V u tablici i zaključuje se da je to slovo E. Isto tako se radi za ostala slova.

Na slijedećem primjeru prikazana je *Vigenerova* analiza u *CrypTool 2* aplikaciji.



Slika 5.18 Primjer 1: *Vigenerova* analiza

Slika 5.5 prikazuje kako *Vigenerova* analiza radi pomoću *CrypTool 2* aplikacije. Ovaj primjer pokazuje kako razbiti *Vigenerovu* šifri pomoću komponente koja se zove *Vigenerov* analizator (engl. *Vigenère Analyzer*). Ona radi na principu *„hillclimbing“* metode. *„Hillclimbing“* metoda se sastoji u 7 koraka [15] :

1. Korak: Napravi početni nasumični ključ
2. Korak: Dešifrira šifrirani tekst koristeći početni ključ i izračuna *„fitness“* (npr. *trigrame*) i dobije se vrijednost (engl. *Value*). Što je vrijednost manja to je ključ točniji.
3. Korak: Prepravi ključ (npr. nasumično mijenja slova)
4. Korak: Dešifrira šifrirani tekst koristeći prepravljeni ključ i izračuna *„fitness“*
5. Korak: Ako je *„fitness“* lošiji vrati se stari ključ
6. Korak: Poveća se uspoređivač, ako je uspoređivač iznad definirane vrijednosti, zaustavlja se algoritam
7. Korak: Vraća se na 3. korak

Ona testira veličinu ključeva između 1 i 20 slova. Kada proces završi dobije se točan ključ u stupcu *„Key“* i ako je ključ točan dobije se dešifrirani tekst u stupcu *„Text“*. Na kraju radi lakšeg pregleda dešifrirani tekst se može vidjeti u komponenti *„Revealed Plaintext“*.

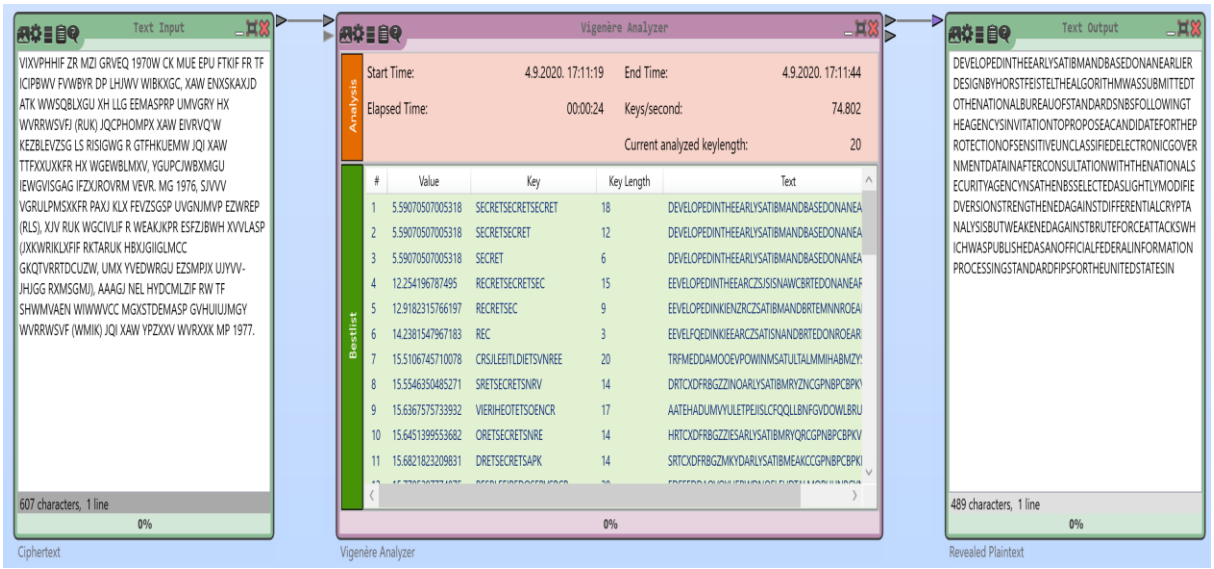
Slika 5.19 Primjer 2: *Vigenerova* analiza

Na slici 5.19 prikazan je primjer za drugi tekst dešifriran pomoću *Vigenerove* analize. Isto kao i u prošlom primjeru može se vidjeti kako se generiraju različiti ključevi sve dok se ne

dobije ključ koji odgovara. Kada se otkrije ključ isto tako se može provjeriti pomoću tablice odgovara li dešifrirani tekst pravoj vrijednosti.

Slika 5.20 Primjer 3: *Vigenerova* analiza

Na slici 5.20 prikazan je primjer za treći tekst dešifriran pomoću *Vigenerove* analize. Vidi se kako postoje više ključeva koji odgovaraju, pa se tako može zaključiti da je prvi ključ *VALUE*. Kako je veličina ključa između 1 i 20, tako će i odgovarajući ključevi *VALUEVALUE, VALUEVALUEVALUE,* itd. biti točni, sve dok veličina ključa ne dođe do 20 odnosno njene maksimalne vrijednosti.



Slika 5.21 Primjer 4: *Vigenerova* analiza

Na slici 5.21 prikazan je primjer za četvrti tekst dešifriran pomoću *Vigenerove* analize. Za razliku od prošlog primjera vidi se kako je odgovarajući ključ *SECRET* i vidi se kako je najveća vrijednost ključa 18, upravo zbog toga što vrijednost ključa ne može prijeći veličinu veću od 20.

Slika 5.22 Primjer 5: *Vigenerova* analiza

Na slici 5.22 prikazan je primjer za peti tekst dešifriran pomoću *Vigenerove* analize. Zaključuje se kako je jednostavnije i puno brže dešifrirati *Vigenerove* šifru pomoću *CrypTool 2* aplikacije, upravo zbog toga što za nekakav prosječan tekst treba najviše jedna minuta, dok ako se to radi na papiru treba jako puno vremena da se dešifrira tekst.

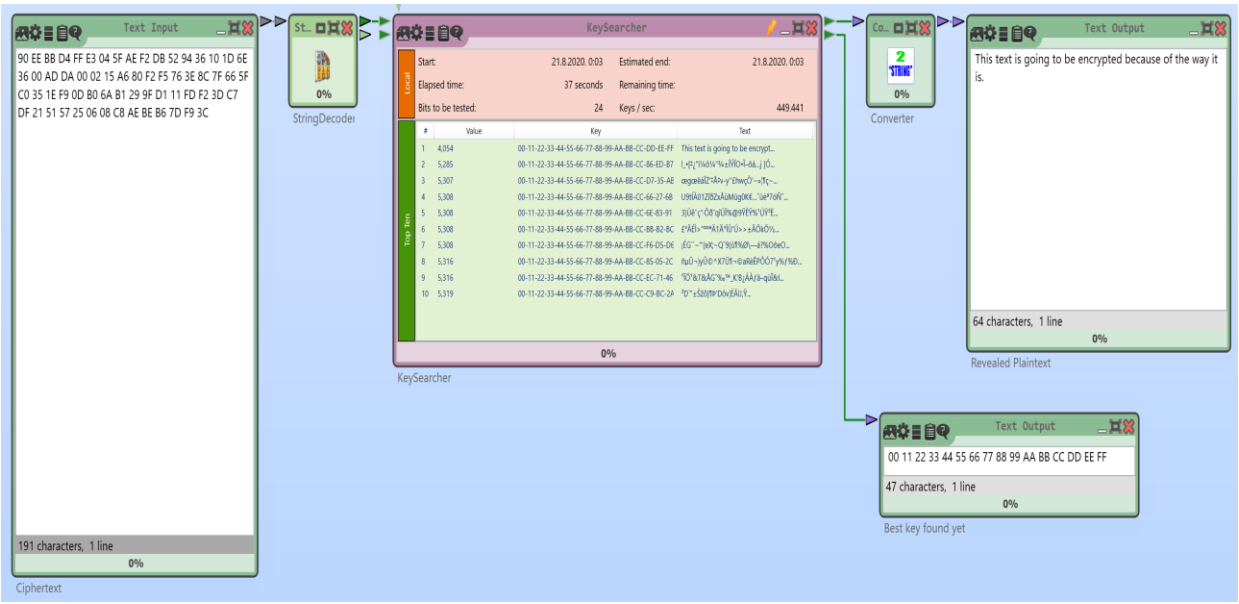
5.5. AES analiza korištenjem entropije

AES (engl. *Advanced Encryption System*) je moderna metoda. Ona je simetrična blok šifra poznata za zaštitu povjerljivih informacija. *AES* se implementira u softver i hardver širom svijeta za šifriranje osjetljivih podataka. Bitan je za državnu računalnu sigurnost, internetsku zaštitu i zaštitu elektroničkih podataka.

AES uključuje tri blok šifre: *AES-128, AES-192* i *AES-256. AES-128* koristi 128-bitnu dužinu ključa za šifriranje i dešifriranje poruka, dok *AES-192* koristi 192-bitnu dužinu ključa, a *AES-256* koristi 256-bitnu dužinu ključa.

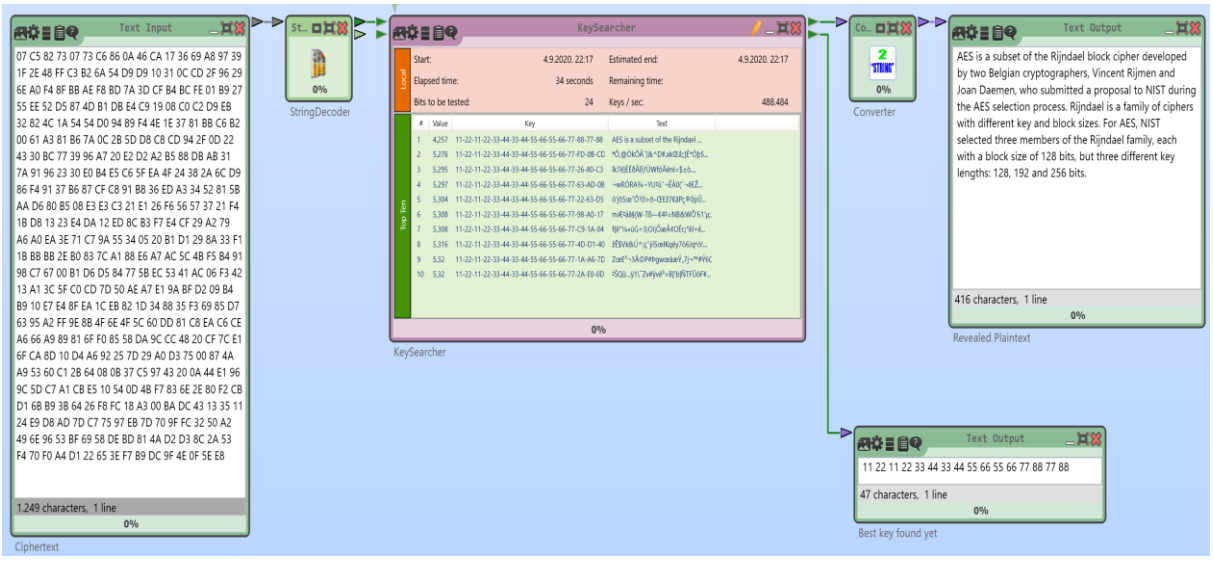
Simetrične šifre, poznate kao i tajni ključ, koriste iste ključeve za šifriranje i dešifriranje, tako da i primatelj i pošiljalac moraju znati koji je tajni ključ [16].

Entropija u kriptografiji predstavlja mjeru nepredvidivosti informacija sadržane u poruci odnosno to je očekivana vrijednost informacija sadržana u svakoj poruci [17].



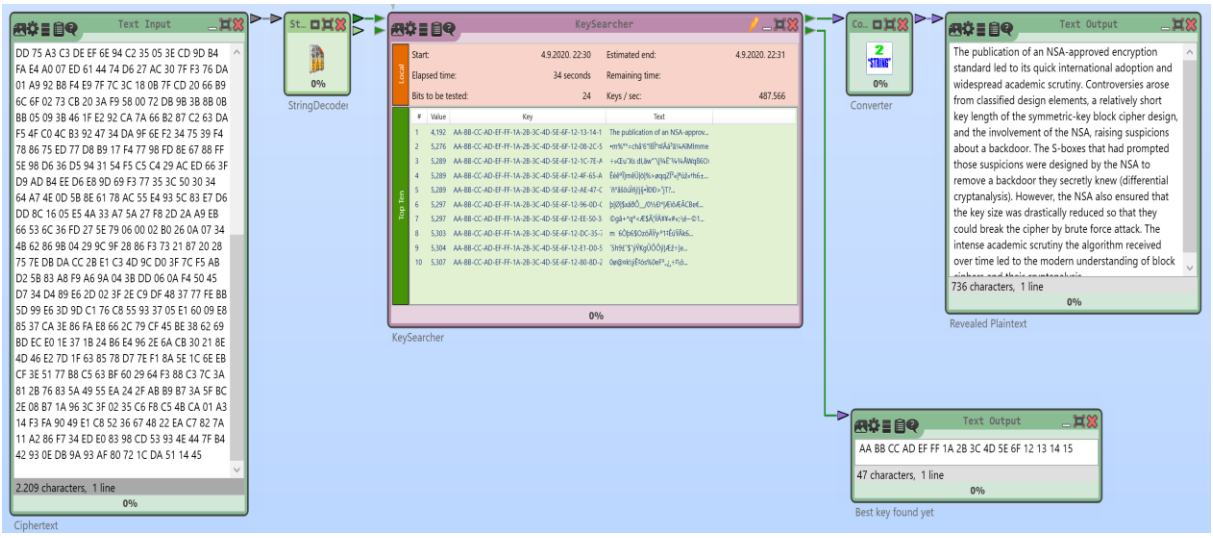
Slika 5.23 Primjer 1: *AES* analiza korištenjem entropije

Slika 5.6 prikazuje kako *AES* analiza korištenjem entropije radi pomoću *CrypTool 2* aplikacije. Ovaj primjer pokazuje kriptoanalizu *AES* algoritma korištenjem komponente *„KeySearcher“* i entropije. Na *„KeySearcher“* dolazi šifrirani tekst u heksadecimalnom obliku preko komponente *„StringDecoder“* koji taj tekst pretvara u tok ili niz bajtova. Nakon toga *„KeySearcher“* isprobava sve moguće ključeve u zadanom prostoru ključeva i koristi entropiju dešifriranog teksta da nađe onaj pravi. Dešifrirani tekst koji ima najmanju entropiju odnosno najmanju nepredvidivost teksta bit će najviše rangiran na listi. Pomoću komponente *„Converter“* dešifrirani tekst se zapisuje u komponentu *„Revealed Plaintext“*, a najbolje dobiveni ključ može se vidjeti na komponenti *„Best key found yet“*.



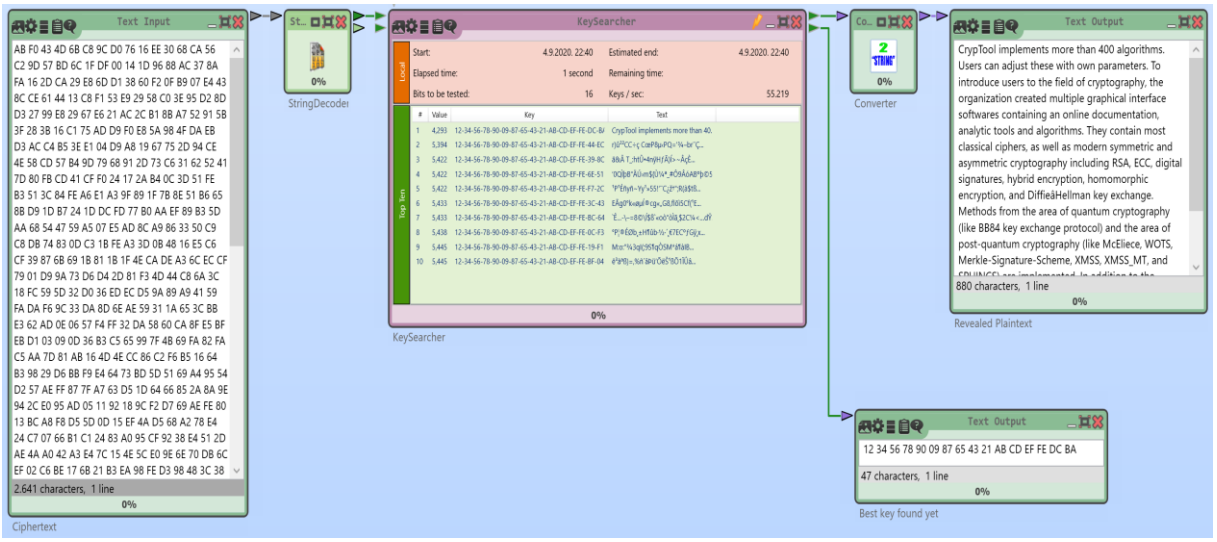
Slika 5.24 Primjer 2: *AES* analiza korištenjem entropije

Na slici 5.24 prikazan je primjer za drugi tekst dešifriran pomoću *AES* analize korištenjem entropije. Zadani ključ je bio 11-22-11-22-33-44-33-44-55-66-55-66-77-**-**-** i tražio se pravi ključ. Može se vidjeti isto kao i u prošlom primjeru kako je komponenta *„KeySearcher“* isprobavala sve ključeve u zadanom prostoru ključeva, sve dok nije pronašla pravi i dešifrirala tekst.



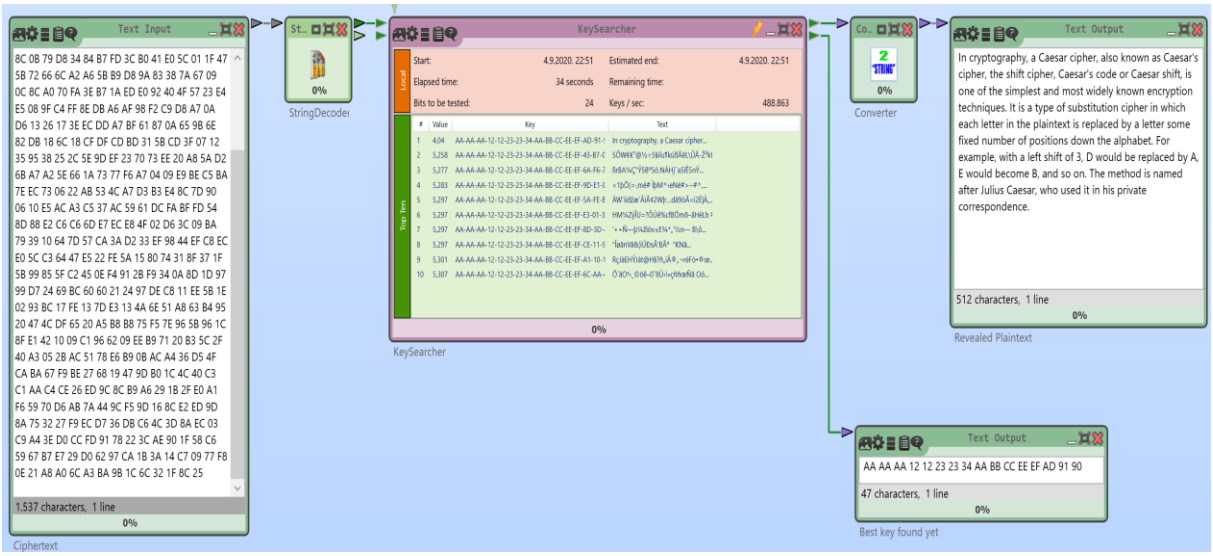
Slika 5.25 Primjer 3: *AES* analiza korištenjem entropije

Na slici 5.25 prikazan je primjer za treći tekst dešifriran pomoću *AES* analize korištenjem entropije. Zadani ključ je bio AA-BB-CC-AD-EF-FF-1A-2B-3C-4D-5E-6F-12-**-**-** i pomoću *„KeySearcher“* komponente se tražio pravi ključ.



Slika 5.26 Primjer 4: *AES* analiza korištenjem entropije

Na slici 5.26 prikazan je primjer za četvrti tekst dešifriran pomoću *AES* analize korištenjem entropije. Zadani ključ je bio 12-34-56-78-90-09-87-65-43-21-AB-CD-EF-FE-**-**. U ovom primjeru može se vidjeti ako sakrijemo zadnja dva bajta ključa koliko kraće traje dešifriranje. U komponenti *„KeySearcher“* pod pojmom *„Elapsed time“* može se vidjeti da je dekriptiranje trajalo 1 sekundu, za razliku od prošlog primjera koji je trajao 34 sekundi gdje se sakrilo zadnja tri bajta ključa.



Slika 5.27 Primjer 5: *AES* analiza korištenjem entropije

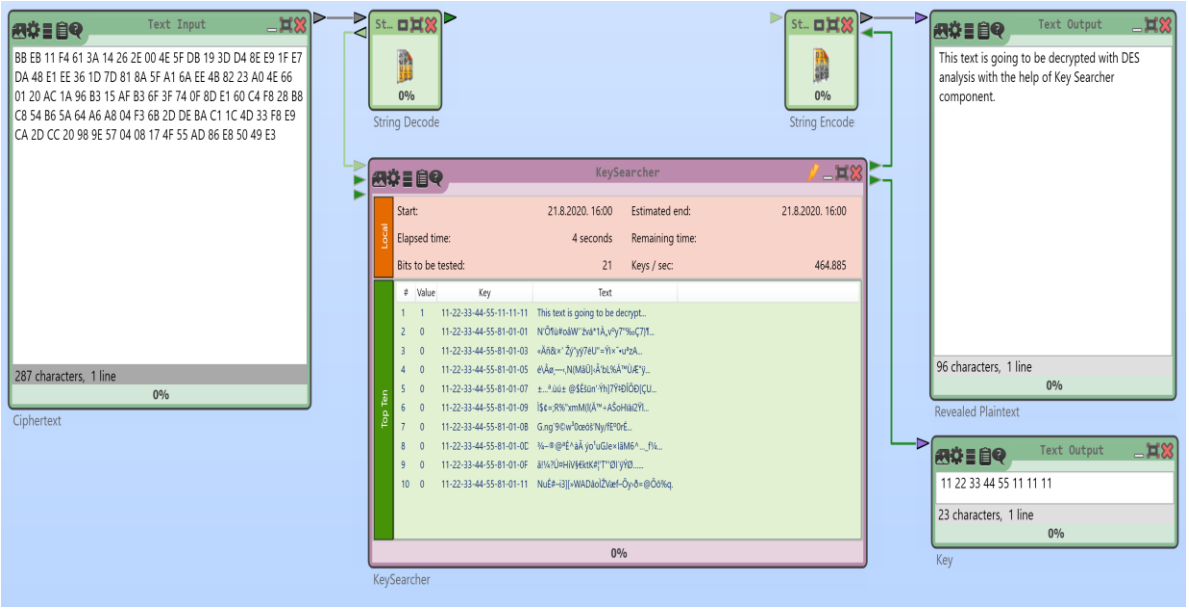
Na slici 5.27 prikazan je primjer za peti tekst dešifriran pomoću *AES* analize korištenjem entropije. Zadani ključ je bio AA-AA-AA-12-12-23-23-34-AA-BB-CC-EE-EF-**-**-** i

pronađen je pravi ključ za dešifriranje teksta. Zaključuje se kako je ovakav tip šifre puno teže dešifrirati zbog toga što su ključevi jako veliki, a kako bi se brže i lakše dekriptirao tekst mora se znati veliki dio ključa.

5.6. DES „Known-Plaintext“ analiza

Ova moderna metoda prikazuje dešifriranje *DES* šifre kada se zna neka riječ u tekstu. *DES* (engl. *Data encryption standard*) je simetrična blok šifra koja služi za zaštitu podataka. *DES* je u zadnje vrijeme ranjiva protiv jačih napada te zbog toga je njezina popularnost manja.

DES šifrira podatke u blokovima od 64 bita, što znači tekst od 64 bita stvori šifrirani tekst od 64 bita. Isti algoritam i ključ se koristi za šifriranje i dešifriranje uz vrlo male promjene. Dužina ključa je 56 bita, odnosno početni ključ se sastoji od 64 bita, ali prije nego što počne *DES* proces, svaki osmi bit je odbačen da stvori ključ od 56 bita. Pozicije bitova su 8, 16, 24, 32, 40, 48, 56 i 64 bit se odbacuje [18].



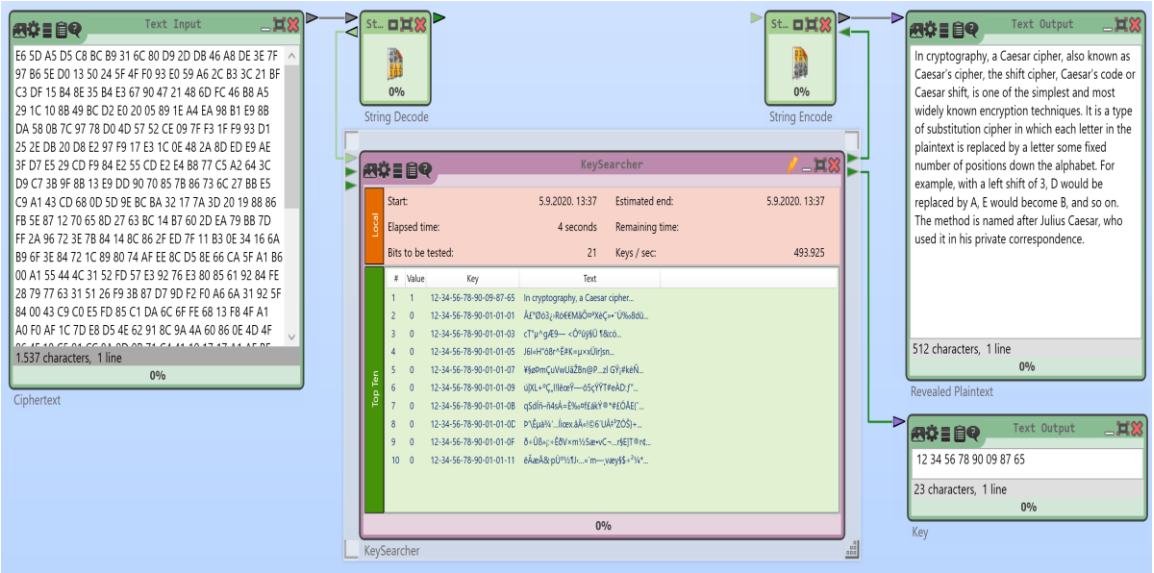
Slika 5.28 Primjer 1: *DES „Known-Plaintext“* analiza

Slika 5.7 prikazuje kako *DES „Known-Plaintext“* analiza radi pomoću *CrypTool 2* aplikacije. U ovom primjeru pomoću komponente *„KeySearcher“* pokušava se pronaći *DES* ključ koji je korišten za šifriranje teksta kako bi se dobio dešifrirani tekst. Koristi se *„brute-*

force“ metoda kako bi se pronašao zadani prostor ključeva i riječ za koju se zna da će se pojaviti u tekstu (u ovom primjeru *„decrypted“*) kako bi se pronašao točan ključ. Međutim, neće se ispitati cjelokupni ključni prostor *DES-a*, nego samo njegov podskup. Podskup može biti definiran kao pravilni izraz (engl. *Regular expression*) u postavkama od *„KeySearcher“* komponente. Ključni prostor koji će u ovom primjeru biti ispitan je 11-22-33-44-55-**-**-**, gdje prvih 5 bajtova predstavlja dio ključa koji se zna, a ostala 3 se generiraju procesom analize. Kada se dobije točan ključ ili jako malo promijenjen dobit će se dešifrirani tekst. Dešifrirani tekst se može vidjeti u komponenti *„Revealed Plaintext“*, dok se ključ može vidjeti u komponenti *„Key“*.

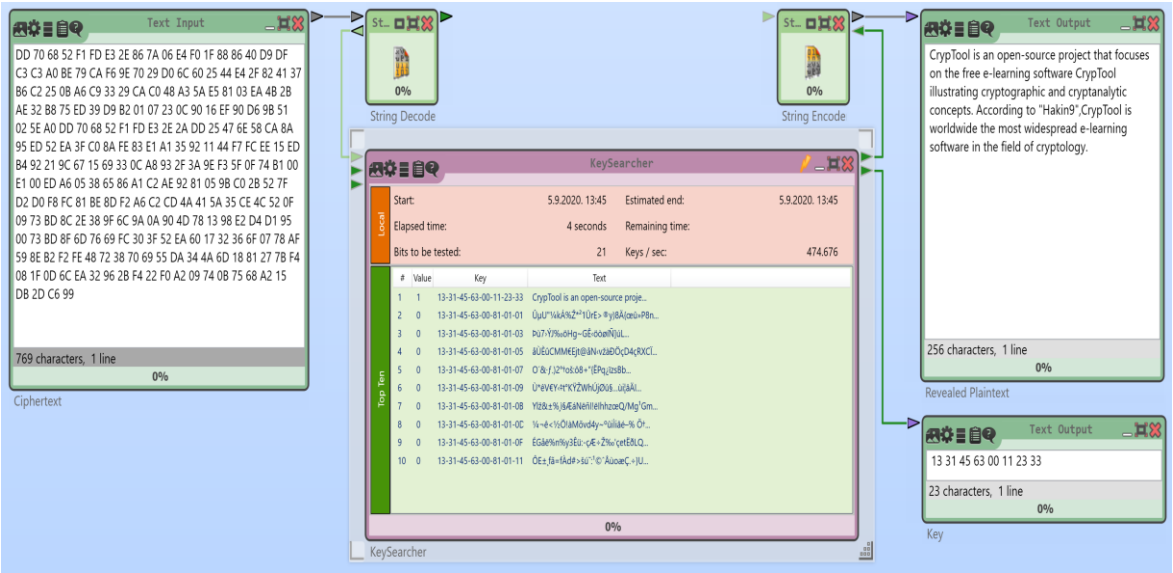
Slika 5.29 Primjer 2: *DES „Known-Plaintext“* analiza

Na slici 5.29 prikazan je primjer za drugi tekst dešifriran pomoću *DES „Known-Plaintext“* analize. Ključ koji je bio zadan je 11-11-22-22-33-44-44-55, a kada se postavljao ključ postavilo se prvih 5 bajtova 11-11-22-22-33-**-**-**. Vidi se kako ključ u ovom dešifriranju ne mora biti u potpunosti isti kao i zadani ključ kako bi se dobio dešifrirani tekst. Riječ koja se znala u tekstu bila je *„Standard“* i isto tako ona je pomogla u dešifriranju teksta.



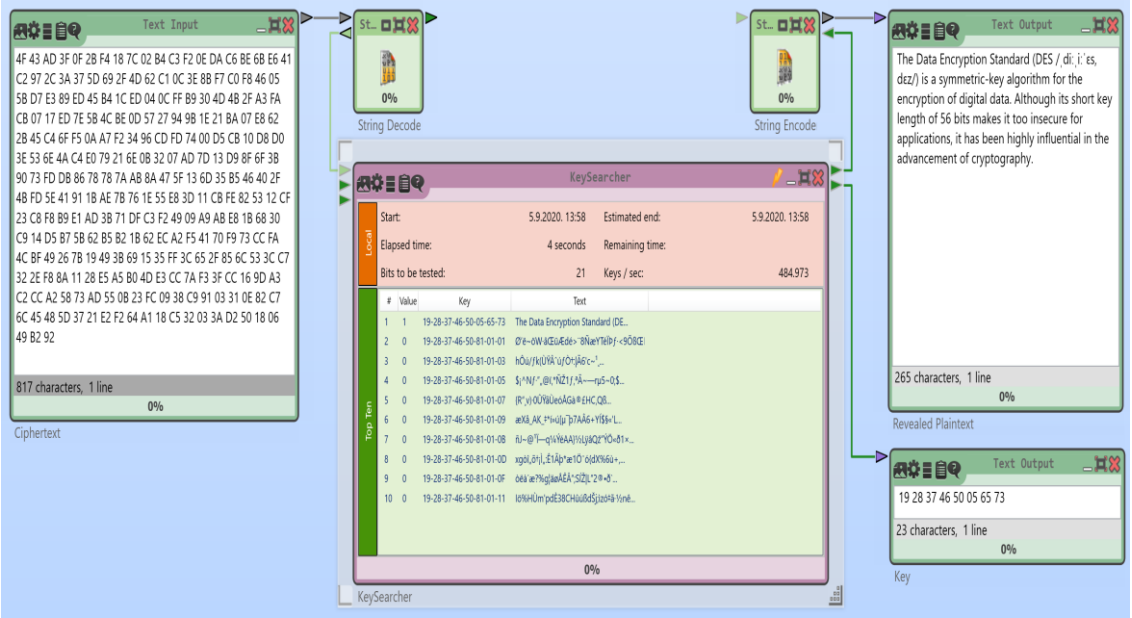
Slika 5.30 Primjer 3: *DES „Known-Plaintext“* analiza

Na slici 5.30 prikazan je primjer za treći tekst dešifriran pomoću *DES „Known-Plaintext“* analize. Zadani ključ je bio 12-34-56-78-90-09-87-65, a riječ koja se znala je *„cipher“* i vidi se kako se u ovom primjeru dobio isti ključ koji se i zadao. Vidi se ako se riječ koja se zna nalazi više puta u tekstu, ključ će biti točniji.



Slika 5.31 Primjer 4: *DES „Known-Plaintext“* analiza

Na slici 5.31 prikazan je primjer za četvrti tekst dešifriran pomoću *DES „Known-Plaintext“* analize. Zadani ključ je bio 13-31-45-63-00-11-22-33, a riječ koja se znala *„project“*. Ključ koji se dobio je 13-31-45-63-00-11-23-33.



Slika 5.32 Primjer 5: *DES „Known-Plaintext“* analiza

Na slici 5.32 prikazan je primjer za peti tekst dešifriran pomoću *DES „Known-Plaintext“* analize. Zadani ključ je bio 19-28-37-46-50-05-64-73, a riječ koja se znala *„Encryption“*. Ključ koji se dobio je 19-28-37-46-50-05-65-73. Zaključuje se kako ovakvo šifriranje nije toliko sigurno zbog toga što napadač ne mora znati cijeli ključ ako zna dovoljan dio ključa.

6. ZAKLJUČAK

Kako je danas tehnologija bolja i kako je potrebno uspješno šifrirati nekakav tekst, tako se moraju i razvijati metoda i aplikacije za šifriranje teksta kako napadači ne bi mogli lako probiti šifru. U ovom završnom radu prikazana je ilustracija kriptoanalitičkih metoda pomoću *CrypTool 2* aplikacije.

Prikazane su klasične metode „Frekvencijska analiza“, „Cezarova analiza korištena frekvencijom slova“, „Cezarova *Brute-force* analiza“ i „*Vigenerova* analiza“, i prikazane su moderne metode „*AES* analiza korištenjem entropije“ i „*DES Known-Plaintext* analiza“. Kod klasičnih metoda došlo se do zaključka da se one mogu lakše dešifrirati zbog toga što su starije pa se mogu dešifrirati pomoću papira kao i pomoću tehnologije. Većina klasičnih metoda su poznate kao i metoda substitucije odnosno metoda zamjene slova i zato je lakše probiti šifru. Moderne metode su nešto teže za prokužiti zato što kod njih postoji sistem gdje se šifrirani tekst pomoću određenog ključa pretvara u brojeve, npr. heksadecimalni sustav. Za napadače je puno teže probiti šifru jer većinom taj ključ znaju samo pošiljalac i primatelj. *CrypTool 2* aplikacija pomaže da se lako probije bilo koja šifra, ako se zna o kojoj vrsti je riječ, zbog toga što se samo ubaci šifrirani tekst u određenu kriptoanalizu i na kraju se dobije dešifrirani tekst. Isto tako *CrypTool 2* aplikacija pomaže da se šifrira tekst te se tako lakše šalju poruke ako se ne želi da netko zna za njih.

LITERATURA

[1] Margaret Rouse, *„Crypthography“* - https://searchsecurity.techtarget.com/definition/cryptography, pristup ostvaren 6.kolovoza 2020.

[2] Klasična kriptografija - https://web.math.pmf.unizg.hr/~duje/kript/osnovni.html, pristup ostvaren 6.kolovoza 2020.

[3] Huzaifa Sidhpurwala, *„A Brief History of Crypthography“* - https://access.redhat.com/blogs/766093/posts/1976023, pristup ostvaren 6.kolovoza 2020.

[4] *„Enigma“* - https://www.bonhams.com/press_release/22879/, pristup ostvaren 6.kolovoza 2020.

[5] Margaret Rouse, *„Cryptanalysis“* - https://searchsecurity.techtarget.com/definition/cryptanalysis, pristup ostvaren 8.kolovoza 2020.

[6] Prikaz kriptoanalize - https://slideplayer.com/slide/5240489/, pristup ostvaren 8.kolovoza 2020.

[7] *CrypTool* - https://www.cryptool.org/en/, pristup ostvaren 11.kolovoza 2020.

[8] *CrypTool* - https://en.wikipedia.org/wiki/CrypTool, pristup ostvaren 11.kolovoza 2020.

[9] *CrypTool 2* - https://www.cryptool.org/en/cryptool2, pristup ostvaren 13.kolovoza 2020.

[10] *„Frequency Analysis“* - https://www.101computing.net/frequency-analysis/, pristup ostvaren 16.kolovoza 2020.

[11] Frekvencijska slova u hrvatskom jeziku - https://commons.wikimedia.org/wiki/File:Frekvencija_slova_hr.png, pristup ostvaren 16.kolovoza 2020.

[12] *„Caesar Cipher“* - https://en.wikipedia.org/wiki/Caesar_cipher, pristup ostvaren 16.kolovoza 2020.

[13] *„The Vigenere Cipher“* - http://user.it.uu.se/~elenaf/Teaching/Krypto2003/vigenere.html, pristup ostvaren 17.kolovoza 2020.

[14] *Vigenerova* tablica - https://donpiorsuerte.wordpress.com/2010/05/21/vigenere-cipher/, pristup ostvaren 17.kolovoza 2020.

[15] *„Basics of Cryptology – Part 8 (Modern Cryptanalysis of Classical Ciphers – Hill Climbing)“* - https://www.youtube.com/watch?v=RB5rDdEAF7U, pristup ostvaren 17.kolovoza 2020.

[16] Margaret Rouse, *„Advanced Encryption Standard (AES)“* - https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard, pristup ostvaren 19.kolovoza 2020.

[17] Amrita Mitra, *„What is entropy in crypthography?“* - https://www.thesecuritybuddy.com/encryption/what-is-entropy-in-cryptography/, pristup ostvaren 19.kolovoza 2020.

[18] *Data Encryption Standard (DES)* - https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/, pristup ostvaren 20.kolovoza 2020.

[19] Šifriranje i dešifriranje teksta - http://ftp.magicsoftware.com/www/help/uniPaaS/mergedProjects/MasteringeDeveloper/How_Do_I_Encrypt_And_Decrypt_Data.htm, pristup ostvaren 3.rujna 2020.

[20] Proces šifriranja i dešifriranja - https://circuitglobe.com/difference-between-encryption-and-decryption.html, pristup ostvaren 3.rujna 2020.

SAŽETAK

Naslov: Ilustracija kriptoanalitičkih metoda pomoću aplikacije *CrypTool*

U ovom Završnom radu prikazane su neke od poznatijih klasičnih i modernih kriptoanalitičkih metoda pomoću *CrypTool 2* aplikacije. Klasične metode koje su prikazane su: Frekvencijska analiza, Cezarova analiza korištena frekvencijom slova, Cezarova *„Brute-force“* analiza i *Vigenerova* analiza. Moderne metode koje su prikazane: *AES* analiza korištenjem entropije i *DES „Known-Plaintext“* analiza. Navedene metode su opisane kako u teoriji rade i kako rade u *CrypTool 2* aplikaciji.

Ključne riječi: analiza, *CrypTool 2* aplikacija, kriptoanaliza, kriptoanalitička metoda, kriptografija

ABSTRACT

Title: Illustration of cryptanalytic methods using CrypTool application

The goal of this Bachelor thesis is to show some of most known classic and modern cryptanalytic methods using CrypTool application. Classic methods that are shown are: Frequency analysis, Caesar analysis using frequency characteristics, Caesar Brute-force analysis and Vigener analysis. Modern methods that are shown are: AES analysis using entropy and DES Known-Plaintext analysis. The above methods are described how they work in theory and how they work in CrypTool 2 application.

Key words: Analysis, CrypTool 2 application, Cryptanalysis, Cryptanalysis method, Cryptography