Marko Josifović 4494

IT210 - Sistemi IT

Domaći zadatak br. 13

Zadatak 1:

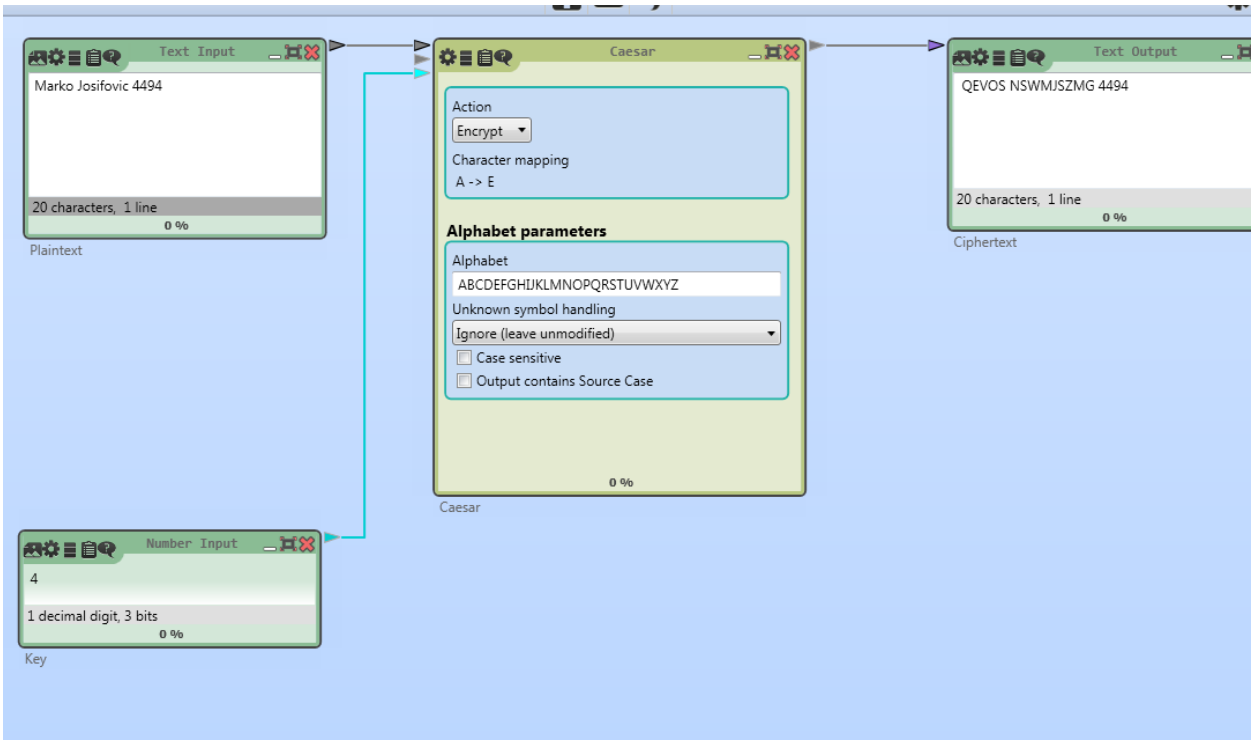
Koristeći Cezarovu šifru, šifrirajte svoje ime, prezime i broj indeksa. Kao ključ koristiti poslednju cifru u broju indeksa.

Rad:

Input text: Marko Josifovic 4494

Ključ Cezarove šifre: 4

Output text: QEVOS NSWMJSZMG 4494



Prikaz u programu CrypTool

Zadatak 2:

Sledeća poruka je šifrovana Cezarovom šifrom:

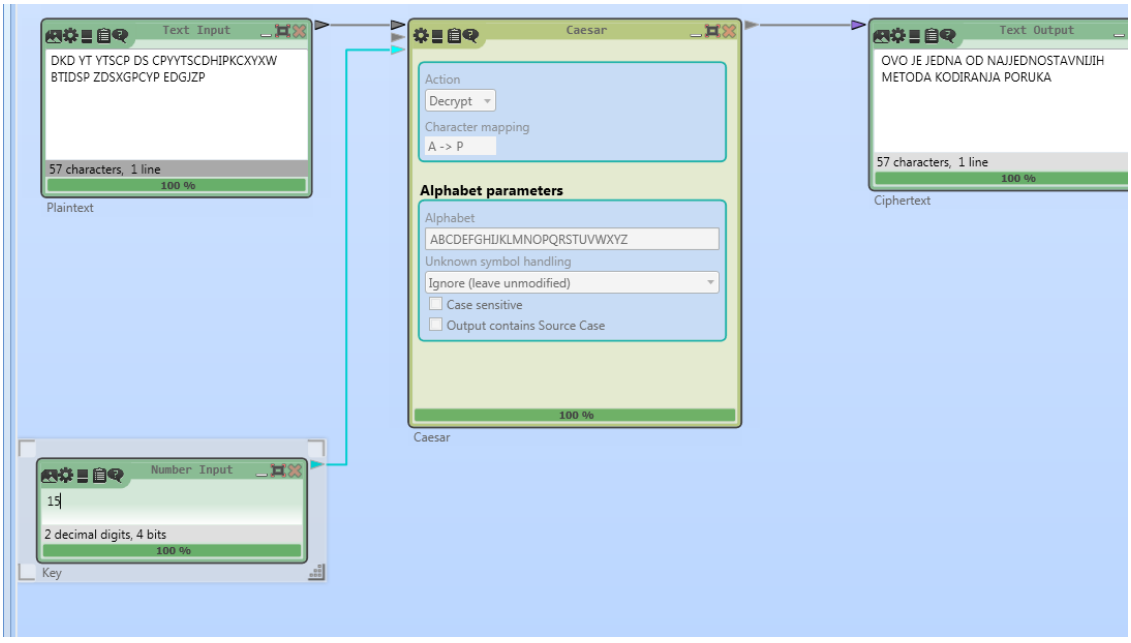
DKD YT YTSCP DS CPYYTSCDHIPKCXYXW BTIDSP ZDSXGPCYP EDGJZP

Odgovorite na pitanja:

1. Koja je tajna poruka?
2. Koliko je mogućih ključeva koje treba probati da bi dešifrovali Cezarovu šifru?
3. Kako bi sproveli napad “brute force”, šta je potrebno da znate? Drugim rečima, šta Vam je omogućilo da uradite “brute-force” napad u ovom slučaju?

Odgovor:

1. Tajna poruka je:
   OVO JE JEDNA OD NAJJEDNOSTAVNIJIH METODA KODIRANJA PORUKA
2. Postoji 25 mogućih ključeva koje treba probati da bi se dešifrovala Cezarova šifra, od pomeraja vrednosti 1 do pomeraja vrednosti 25.
3. Time što je rečeno u tekstu zadatka da se radi o Cezarovoj šifri, to me je dovelo do zaključka da treba isprobati sve moguće pomeraje radi dešifrovanja zadatog teksta, od pomeraja vrednosti 1 pa sve do 25. Kada sam došao do ključa vrednosti 15, tekst je dobio formu u čitljivom jeziku. Za "brute-force" napad potrebno je imati predznanje kako se šifriraju određene šifre, kao što je ovde bio slučaj da to bude Cezarova šifra. Samo je pitanje vremena kada ćemo otkriti koja je vrednost kojom se šifrirala poruka.



Prikaz u programu CrypTool

Zadatak 3:

Za sledeću poruku uradite analizu frekventnosti:

J lxwcnwc vjwjpnvnwc bhbcnv rb j bxocfjan jyyurljcrxw cqjc ljw kn dbnm cx vjwjpn cqn lanjcrxw jwm vxmrorljcrxw xo mrprcju lxwcnwc. LVBb jan chyrljuuh dbnm oxa nwcnayarbn lxwcnwc vjwjpnvnwc jwm fnk lxwcnwc vjwjpnvnwc. NLV chyrljuuh bdyyxacb vducryun dbnab rw j lxuujkxajcren nweraxwvnwc kh rwcnpajcrwp mxldvnwc vjwjpnvnwc, mrprcju jbbnc vjwjpnvnwc jwm anlxam ancnwcrxw. Jucnawjcrenuh, FLV rb cqn lxuujkxajcren jdcqxarwp oxa fnkbrcnb jwm vjh rwludmn cngc jwm nvknm pajyqrlb, yqxcxb, ermnx, jdmrx, vjyb jwm yaxpajvvn lxmn cqjc mrbyujh lxwcnwc jwm rwcnajlc frcq cqn dbna. NLV chyrljuuh rwludmnb j FLV odwlcrxw.

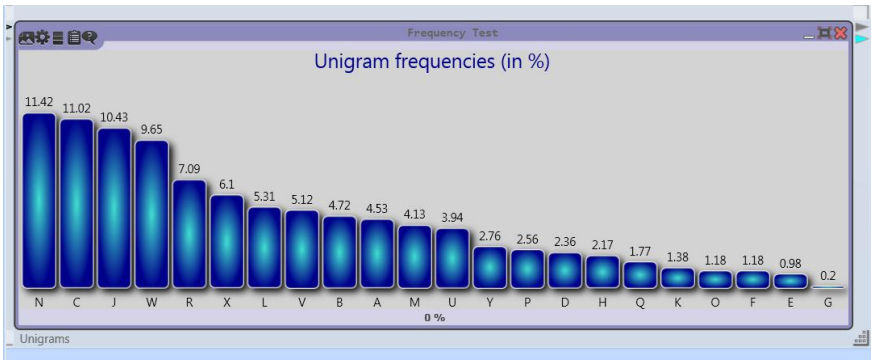
1. Koji se ključ koristio?
2. Da li je šifriran tekst dešifrovan ispravno?
3. Kako glasi prva rečenica dešifrovanog teksta?
4. Objasnite kako je CrypTool mogao da uradi dekripciju šifrovanog teksta na osnovu frekventnosti slova.

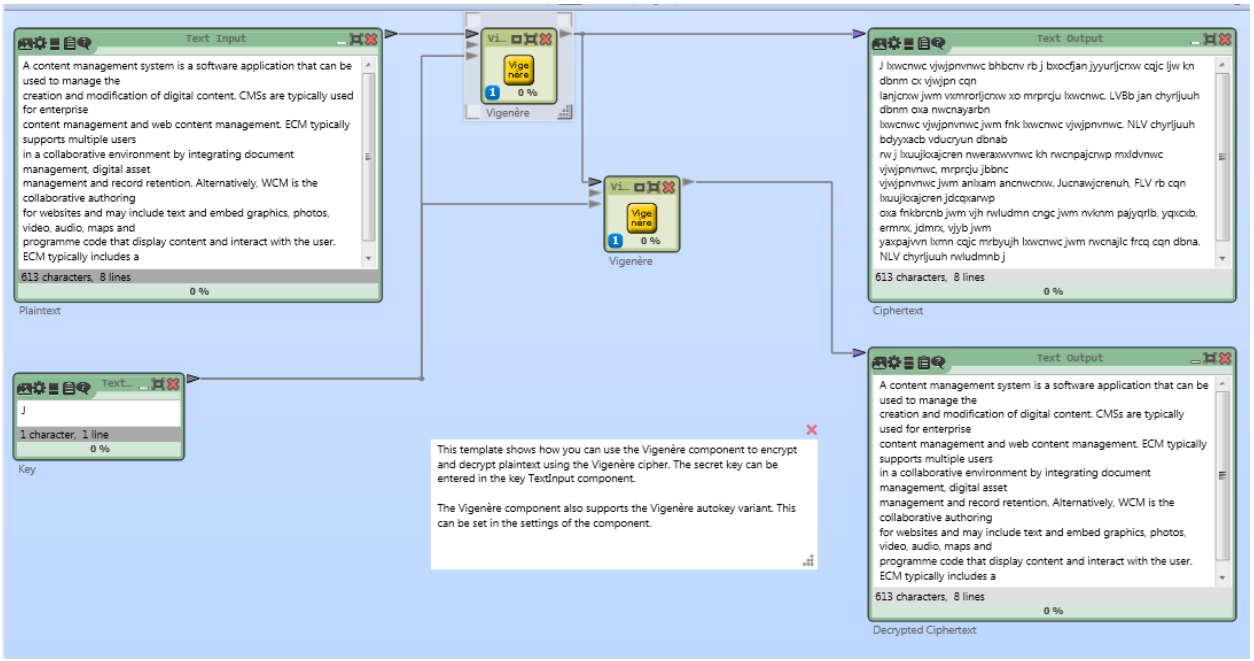
Odgovor:

Tekst je šifrovan Vigenere šifrom, ključ je bio slovo J. Ovako izgleda izvorni tekst kada se dešifruje:

A content management system is a software application that can be used to manage the creation and modification of digital content. CMSs are typically used for enterprise content management and web content management. ECM typically supports multiple users in a collaborative environment by integrating document management, digital asset management and record retention. Alternatively, WCM is the collaborative authoring for websites and may include text and embed graphics, photos, video, audio, maps and programme code that display content and interact with the user. ECM typically includes a WCM function.

Ceo tekst je ispravno dešifrovan. CrypTool pravi raspodelu po broju ponavaljanja slova u šifrovanom tekstu i na osnovu slova koja se procentualno najviše ponavljaju u svakodnevnom tekstu i govornom jeziku, vrši izmene i pokušava da pronađe reči koje postoje u rečniku.





Demonstracijom šifrovanja poruke koju smo dobili na osnovu ključa J vidimo da se dobija početni šifrovani tekst.