
LABORATORIJSKA VEŽBA BR. 2

Klasični kriptografski algoritmi

CILJ VEŽBE

- Upoznavanje sa klasičnim kriptografskim algoritmima
- Testiranje rada Cezarovog algoritma
- Testiranje rada Vigenereovog algoritma
- Testiranje rada Hillovog algoritma

POTREBNA OPREMA

- Računar sa instaliranim Windows operativnim sistemom
- Instaliran programski paket Cryptool

TEORIJSKE OSNOVE

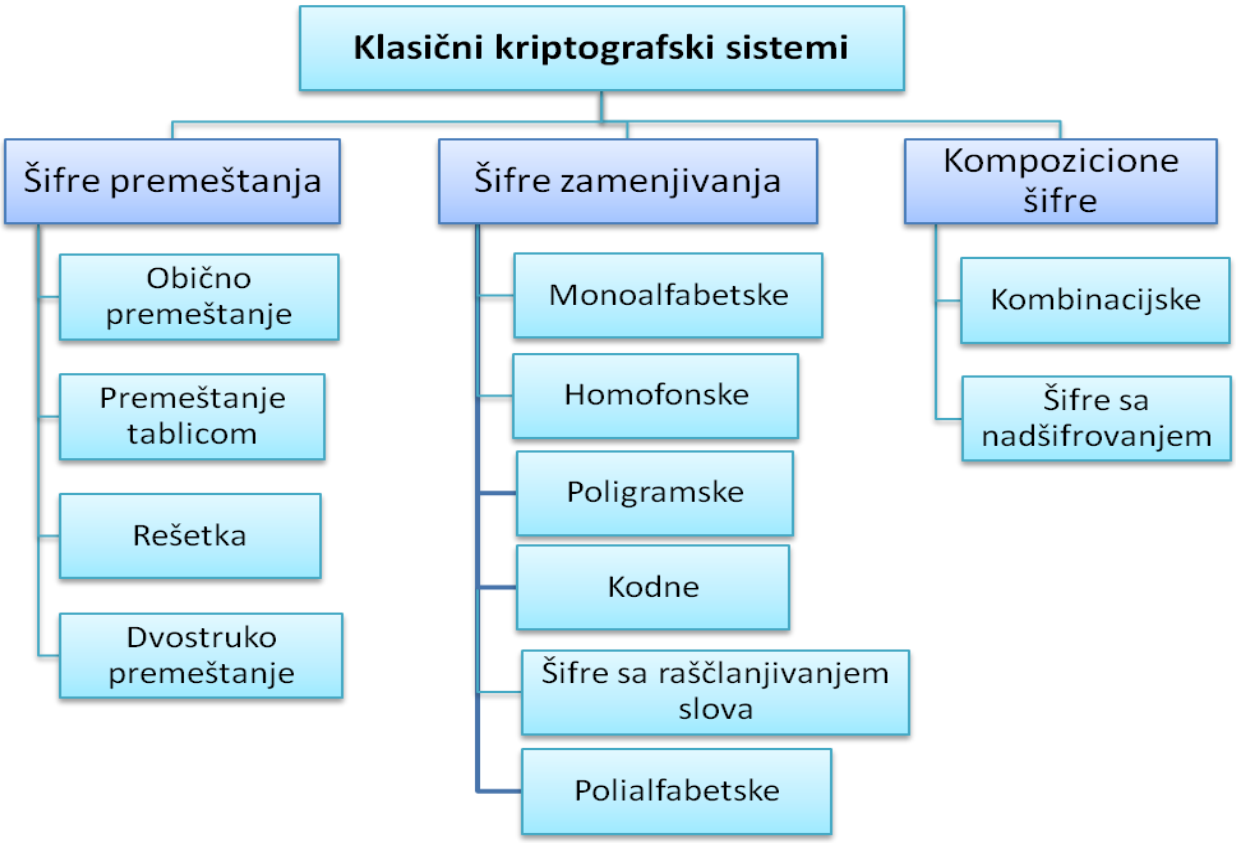
Uvod

Kriptografija je zaštita informacija sifriranjem. Pod sifriranjem se podrazumeva transformacija iz jednog oblika u drugi, odnosno preslikavanje iz skupa u kriptodomen. Kriptografski sistem je skup srodnih šifrarskih algoritama. Osnovna podela kriptografije je zasnovana na vremenskoj distanci kako su nastajali i na kompleksnosti primenjenih tehnika.

1. ***Klasični kriptografski sistemi*** koriste transformacije koje vrše:
   - ✓ **šifre premeštanja** - permutuju slova otvorenog teksta
   - ✓ **šifre zamenjivanja** - menjaju delove otvorenog teksta određenim šifarskim zamenama
   - ✓ **kompozicione šifre** - vrše dvostruku transformaciju kombinujući šifre ova dva sistema.
2. ***Savremeni kriptografski sistemi*** - realizuju se pomoću računara.

- ✓ Koriste različite transformacije klasičnih šifara, specijalne matematičke i fiksne slučajne funkcije ili višestruka šifrovanja različitim ključevima
- ✓ Razlika između **simetričnih** i **asimetričnih** algoritama (pored samog oblika i mogućnosti algoritama) je u tome što simetrični algoritmi koriste isti ključ za šifrovanje i dešifrovanje a asimetrični različite, javni i tajni, koji svoju snagu baziraju na tome da se bez dodatne informacije ne mogu dobiti jedan iz drugog.
- ✓ kriptografija bazirana na simetricnim kljucevima - isti kljuc se koristi za sifriranje i desifriranje i on je tajni (cak i da napadac presretne kljuc, on mora da zna koji algoritam je koriscen za kriptovanje)
- ✓ kriptografija bazirana na javnim kljucevima - kljucevi su razliciti (key1 i key2)-jedan je najcesce javni a drugi tajni; kljucevi nisu isti
- ✓ hash funkcija

Klasični kriptografski algoritmi



- **Šifarski sistemi premeštanja - transpozicije** obuhvataju:

1. obično premeštanje
2. premeštanje ključem
3. premeštanje rešetkama
4. dvostruko premeštanje

- **Šifarski sistemi zamenjivanja** se deli na:

I. **Šifre proste zamene** (MONOALFABETSKE) se dele na:
   a) alfabetske šifre
   b) bigramske, Trigramske i poligamske šifre
   c) kodne tablice
   d) Kodovi
   e) šifre raščlanjivanjem slova

II. **Šifre složene zamene** (POLIALFABETSKE)
   a) šifre sa sređenim alfabetom
   b) šifre sa nesređenim alfabetom

Cryptool

Program Cryptool nam nudi veoma širok raspon mogućnosti i različitih prikaza kako klasičnih tako i modernih kriptografskih algoritama koji obuhvataju šifrovanje i dešifrovanje, generisanje ključeva, generisanje sigurnih lozinki, autentikaciju, sigurnosne protokole, i td. Cryptool je kriptografski softver koji pruža uvid u način funkcionisanja algoritama za šifrovanje, od najstarijih (Cezar) do savremenih (DES, 3DES...). Ugrađeni grafički prikazi toka šifrovanja pomažu da se pojedinačno razume svaki algoritam. Koristeći Cryptool na ovim vežbama predstavićemo najznačajnije algoritme za šifrovanje i usput objasniti kako svaki od njih funkcioniše. U lab.vežbi 1 već smo se upoznali sa nekim osobinama ovog kriptografskog programa.

ZADACI:

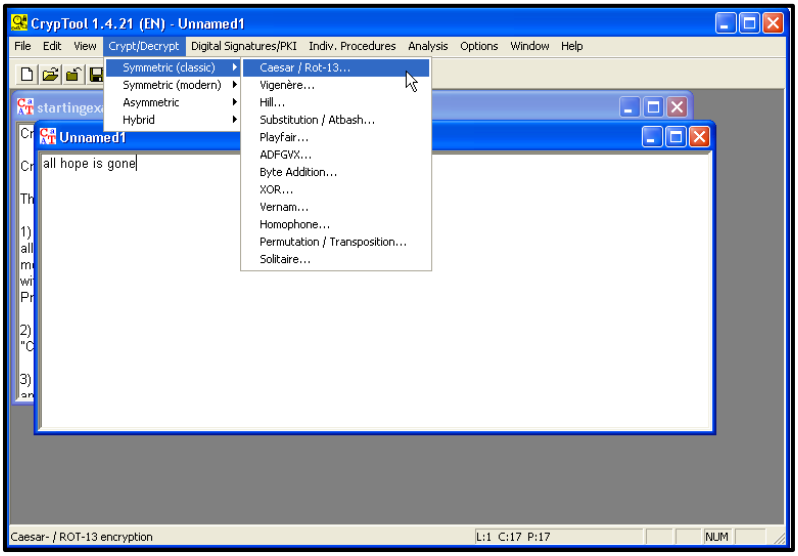
Cezarova šifra

Zadatak: Koristeći Cryptool šifrovati text "***all hope is gone***" Cezarovom šifrom.
Da bi smo ovo uradili, moramo da razumemo kako Cezarova šifra funkcioniše. U engleskoj abecedi imamo 26 slova (znakova) i za primere šifrovanja ćemo ih numerisati od 0 do 25 ili od 1 do 26. Po Cezarovoj šifri se svaki znak (slovo) pomera za tri mesta u desno tako da A postaje D, B postaje E, itd. Pogledajte sledeću tabelu:

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
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

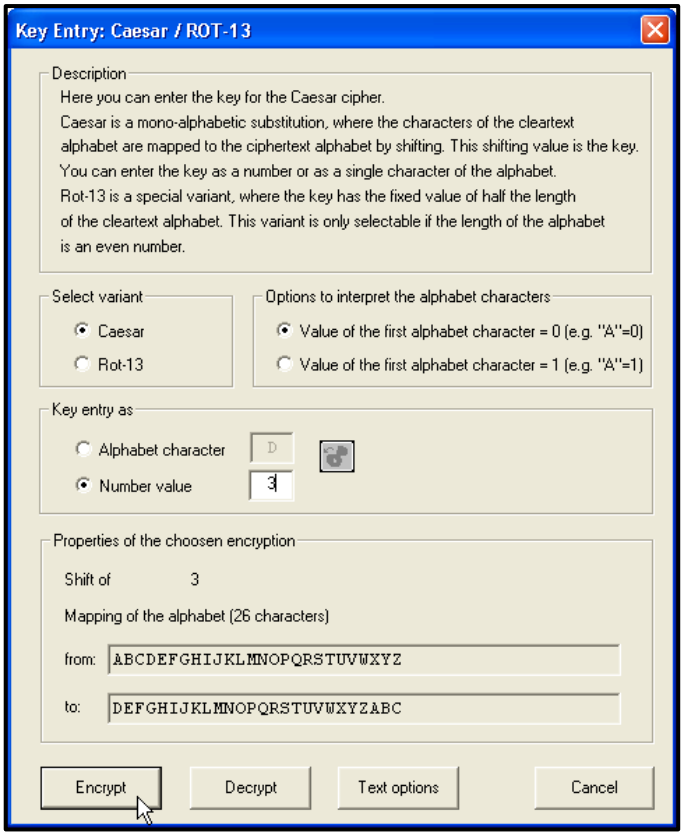
Postupak

Otvoriti novi prozor za unos poruka: FILE → NEW. Otkucati "***all hope is gone***" u prozor za upis teksta. Iz menija Crypt/Decrypt izabrati **Symmetric (classic) → Caesar/Rot 13**.
Otvara se prozor za podešavanja samog algoritma gde treba podesiti par stvari.

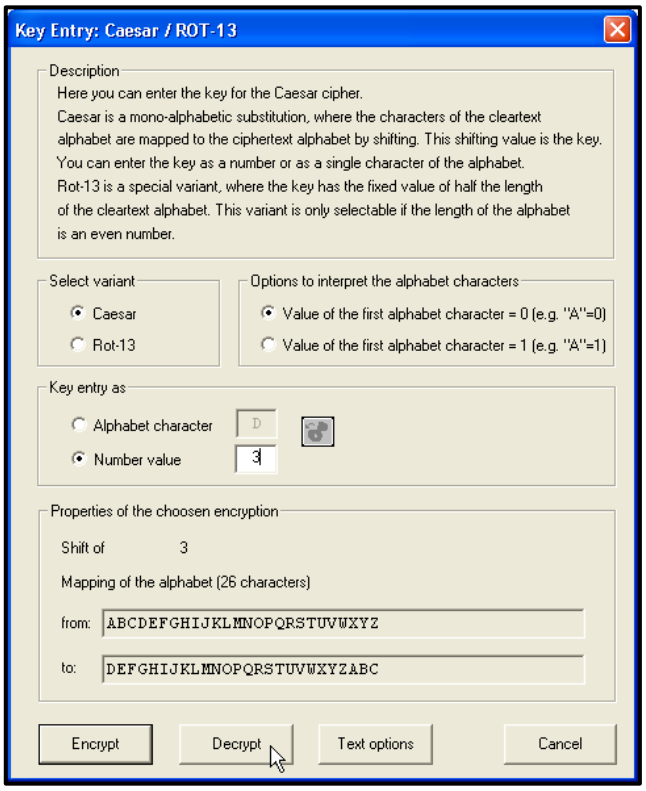


- Select Variant: Caesar
- Options to interpret the alphabet characters: A = 0
- Key entry as: Number value = 3 ili Alphabet character = D

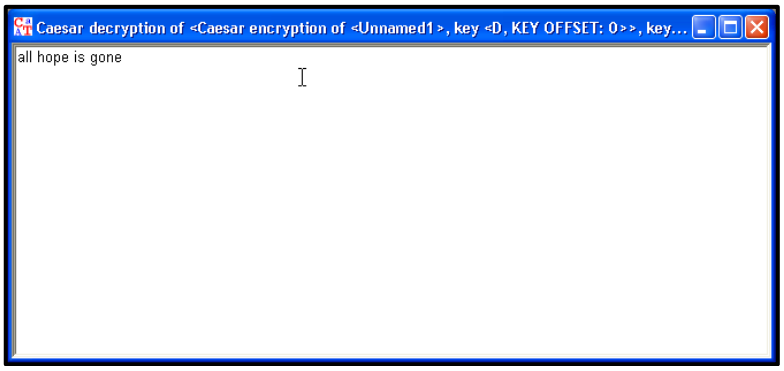
Kada se klikne na Encrypt dobija se šifrat:



Sada možemo proveriti svoj šifrat obrnutim procesom – tj sa istim podešvanjima odraditi Decrypt:



Dobija se otvoreni tekst:



Viženerova šifra

Koristeći Cryptool šifrovati i dešifrovati tekst "**ARTOFWAR**" Vigenereovom šifrom sa ključem **K=PERA**.

Viženerova šifra je polialfabetska šifra što znači da ne preslikava jedno slovo (znak) uvek u drugo slovo (znak), već jedno slovo može biti preslikano u onoliko različitih slova kolika je dužina ključa. Tj ako je ključ dužine m karaktera, jedno slovo se može preslikati u m mogućih slova u šifratu.

Ukoliko ključ predstavimo kao niz znakova K = k1, k2, k3, ... km, šifrovanje i dešifrovanje se mogu predstaviti na sledeći način:

$$Ek(x1, x2, x3, \ldots xm) = (x1+k1, x2+k2, \ldots xm+km)$$
$$Dk(y1, y2, y3, \ldots ym) = (y1–k1, y2–k2, \ldots ym–km)$$

U ovom slučaju, operacije sabiranja i oduzimanja se odvijaju po modulu 26 jer koristimo Englesku abecedu. Postavićemo numeričke ekvivalente za otvoreni tekst i ključ:

ARTOFWAR = 0, 17, 19, 14, 5, 22, 0, 17
PERA = 15, 4, 17, 0

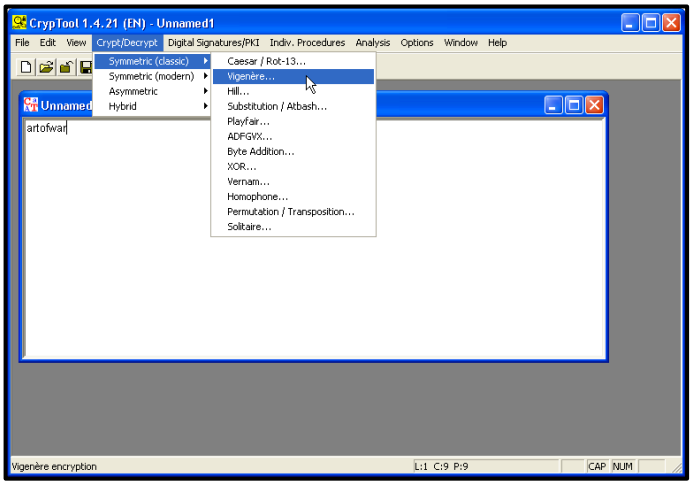
Šifrat dobijamo tako što sabiramo pojedinačne vrednosti po modulu 26. Ako je ključ kraći od otvorenog teksta, dopunjuje se slovima od početka – u ovom slučaju otvoreni tekst je dužine 8 slova a ključ 4 slova. Dakle, za sabiranje sa ARTOFWAR koristimo reč PERAPERA.

otv. Tekst	A, 0	R, 17	T, 19	O, 14	F, 5	W, 22	A, 0	R, 17
ključ	P, 15	E, 4	R, 17	A, 0	P, 15	E, 4	R, 17	A, 0
šifrat	P, 15	V, 21	K, 10	O, 15	U, 20	A, 0	R, 17	R, 17

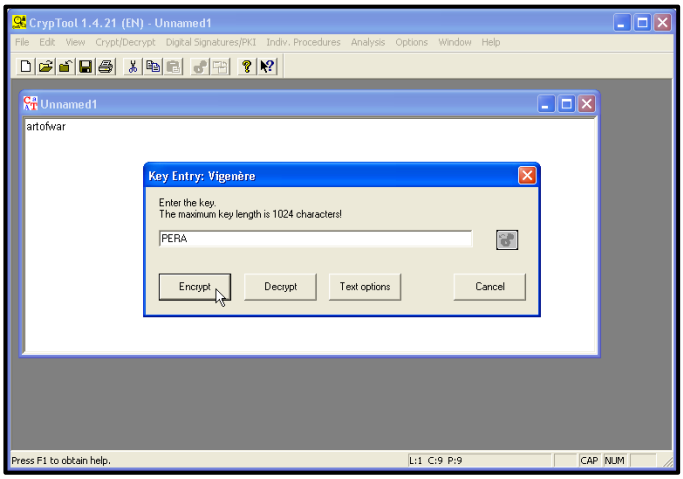
Šifrat je **PVKOUARR**.

Postupak

Sada ćemo to probati na Cryptool-u.
FILE → NEW, zatim otkucati “ARTOFWAR”.
Crypt / Decrypt → Symetric(classic) → Vigenere.
Dobijamo prozor gde nam se traži da ukucamo ključ. Naš ključ će biti PERA. Na dugmetu Text options imate podešavanja koja možete pogledati ali ćemo ih sad ostaviti na default vrednostima.



Zatim kliknemo na Encrypt. Dobija se prozor sa šifratom:



Sada možete pokušati da sa istom ključnom reči dešifrujete rezultat.
Dešifrovanje se vrši na isti način kao šifrovanje osim što se sada klikne na Decrypt.

Hillova šifra

Pomoću Cryptool-a šifrovati reč "CLOWNS" Hilovom šifrom ako je ključ dat matricom:

$$\mathbf{K} = \begin{vmatrix} 9 & 21 & 17 \\ 5 & 9 & 22 \\ 9 & 10 & 20 \end{vmatrix}$$

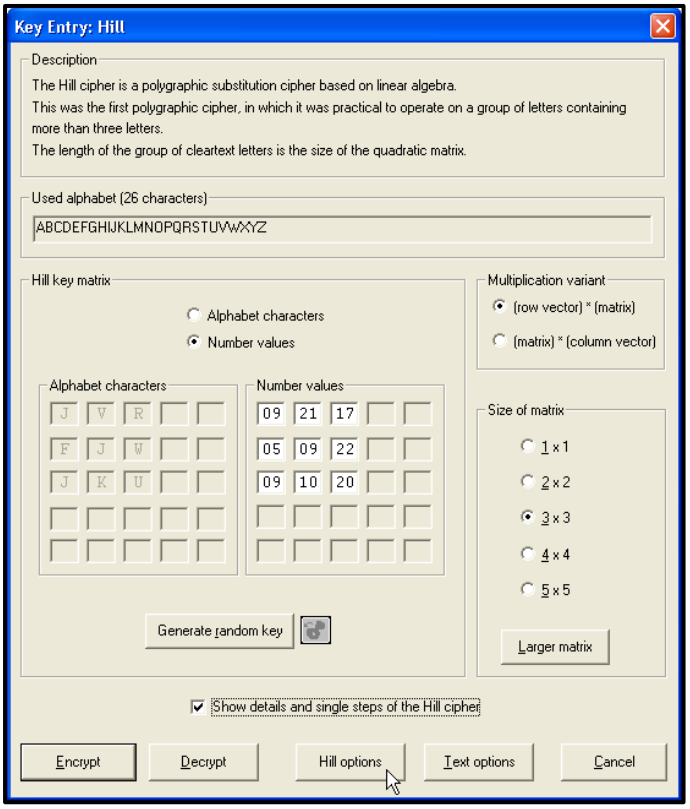
Pošto je matrica oblika 3x3, rastavljamo otvoreni tekst na dva sloga od po tri slova: CLO i WNS. Njihove numeričke vrednosti su : 2, 11, 14 i 22, 13, 18.

CLO: |2 11 14| x |9 21 17
5 9 22
9 10 20| mod26 = |17 21 10| = **RVK**

WNS: |22 13 18| x |9 21 17
5 9 22
9 10 20| mod26 = |9 5 6| = **JFG**

Postupak

Dakle šifrat je RVKJFG, što ćemo proveriti kroz Cryptool. FILE → NEW, otkucamo reč otvorenog teksta, CLOWNS. Crypt / Decrypt → Symmetric (classic) → Hill. Popunite sledeći prozor tako da bude označeno sledeće:



- •Used alphabet:
  ABCDEFGHIJKLMNOPQRSTUVWXYZ
- • Hill Key Matrix: Number Values
  09 21 17
  05 09 22
  09 10 20
- • Multiplication variant: (row vector) x (matrix)
- • Size of matrix: 3 x 3

Označite i check-box show details and single steps of Hill Cipher (nakon pokretanja Encrypt, dobićete takođe i prozor "Details" na kom je postupak šifrovanja prikazan korak po korak). Kartice Hill Options i Text Options nude podešavanja vezana za samo šifrovanje ali na njima nećemo menjati ništa.

Nakon popunjavanja dijaloga sa prethodne slike možemo da izvršimo enkripciju i dobijamo sledeće:

Pokretajući dešifrovanje dugmetom Decrypt dešifrujemo dobijeni šifrat i ponovo imamo otvoreni tekst.

Zadatak. Svaki student je dužan da pomoću gore objašnjenih algoritama šifruje **imena i prezimena** svojih članova porodice (Po četiri primera za svaki algoritam, ukoliko je broj članova porodice manji od četiri, studenti uzimaju **ime i prezime svog najboljeg prijatelja** kao četvrti primer).

Predmetni nastavnik i predmetni asistent