

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. <u>Klasični kriptografski sistemi</u> 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. <u>Savremeni kriptografski sistemi</u> 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 \rightarrow NEW. Otkucati "*all hope is gone*" u prozor za upis teksta. Iz menija Crypt/Decrypt izabrati Symmetric (classic) \rightarrow 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:

<mark>98</mark> (СгурТ	fool 1.	4.21 (EN) - Unna	amed1							-	
File	Edit	View	Crypt/Decrypt Dig	jital Signa	tures/PKI	Indiv. Procedures	Analy:	sis Options	Window	Help		
1) 등 한 가 1) 등 한 한 2) 안 3) 한	start	ingex. Innam ope is	Symmetric (node Symmetric (node Asymmetric Hybrid ead1 ggne	(c)	Caesar / Mgenerer Hill Substitu Playfair. ADFGVX ADFGVX Vernam. Vernam. Solitaire.	Rot-13 tion / Atbash tion tition ne tion / Transposition. 	L8 					
Caes	ar-/R	OT-13 e	ncryption					L:1 (:17 P:17		NUM	_//,

Key Entry: Caesar / ROT-13								
Description Here you can enter the key for the Caesar cipher. Caesar is a mono-alphabetic substitution, where the characters of the cleartext alphabet are mapped to the ciphertext alphabet by shifting. This shifting value is the key. You can enter the key as a number or as a single character of the alphabet. Rot-13 is a special variant, where the key has the fixed value of half the length of the cleartext alphabet. This variant is only selectable if the length of the alphabet is an even number.								
Select variant Options to interpret the alphabet characters © Caesar © Value of the first alphabet character = 0 (e.g. "A"=0) © Rot-13 © Value of the first alphabet character = 1 (e.g. "A"=1)								
Key entry as C Alphabet character Image: C Number value								
Properties of the choosen encryption Shift of 3 Mapping of the alphabet (26 characters) from: ABCDEFGHIJKLMNOPQRSTUVWXYZ to: DEFGHIJKLMNOPQRSTUVWXYZABC								
Encrypt Text options Cancel								



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

Key Entry: Caesar / ROT-13								
Description Here you can enter the key for the Caesar cipher. Caesar is a mono-alphabetic substitution, where the characters of the cleartext alphabet are mapped to the ciphertext alphabet by shifting. This shifting value is the key. You can enter the key as a number or as a single character of the alphabet. Rot-13 is a special variant, where the key has the fixed value of half the length of the cleartext alphabet. This variant is only selectable if the length of the alphabet is an even number.								
Select variant Options to interpret the alphabet characters • Caesar • Value of the first alphabet character = 0 (e.g. ''A''=0) © Rot-13 © Value of the first alphabet character = 1 (e.g. ''A''=1)								
Key entry as C Alphabet character Image: Comparison of the second sec								
Properties of the choosen encryption Shift of 3 Mapping of the alphabet (26 characters) from: ABCDEFGHIJKLMNOPQRSTUVWXYZ to: DEFGHIJKLMNOPQRSTUVWXYZABC								
Encrypt Decrypt Cancel								

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, ..., xm) = (x1+k1, x2+k2, ..., xm+km)Dk(y1, y2, y3, ..., ym) = (y1-k1, y2-k2, ..., 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 \rightarrow NEW, zatim otkucati "ARTOFWAR". Crypt / Decrypt \rightarrow Symetric(classic) \rightarrow 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:

Artofivar Key Entry: Vigenère Image: Second Se		
Encupit Decupt Text options Cancel	racters!	3
	Text options Cancel	



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.

<u>Hillova šifra</u>

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

 $\mathbf{K} = | \begin{array}{c} 9 \ 21 \ 17 \\ 5 \ 9 \ 22 \\ 9 \ 10 \ 20 | \end{array}$

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:
$$|2 \ 11 \ 14| \ge |9 \ 21 \ 17$$

5 9 22
9 10 20| mod26 = $|17 \ 21 \ 10| = \mathbf{RVK}$
WNS: $|22 \ 13 \ 18| \ge |9 \ 21 \ 17$
5 9 22
9 10 20| mod26 = $|9 \ 5 \ 6| = \mathbf{JFG}$

Postupak

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

Used alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Hill Key Matrix: Number Values

: INUI	nbe	r va
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).

ZADACI sa CryptTool2:

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: NEW. Levo u meniju Classic Ciphers izabrati Caesar I prevuci na radnu povrsinu. Kadav am se pojavi na radnoj povrsini Caesar imacete 3 strelice sa desne I jednu sa leve strane. Sa desne strane kliknuti prvu I prevuci na levo kako bi otvorili Text input. Isti postupak uraditi I sa levom kako bi napravili Text output. Nakon toga otkucati "*all hope is gone*" u prozor za upis teksta. Prosiriti Caesar meni kako bi mogli podesiti parametre.



• Key entry as: Number value = 3 ili Alphabet character = D

Kada se klikne Play u gornjem meniju dobija se šifra:

a 0			CrypTool 2.1 (Stable Build 9778.2) – New project	- 8 ×
Home Edit Crypt	o Tutoriais			OAbout -
New * 📄 Open	Save * Print Print Save *	Log ex 17		Startcerter CopyFlooTilizer CopyCloud Updates Setting Hep Edits: 0
Components +	Cr 🔶 Startcenter × 🕕 🛠 New	project ×		
Search				
Classic Ciphers			809	ę
ADFGVX				
Affine Cipher				
Bazeries Cipher				
Bifid Cipher				
Book Cipher				
🥙 Caesar				
Chaocipher				
Cylinder Cipher	ana ca lost 100			
ElsieFour Cipher	ALL HOPE IS GONE	¢≣BQ Carsar		
4000 Enigma		Action	Text Cutput _118	
O Fialka		Encrypt *	DOO KRSH LV JRQH	
Four-square Cipher		3 🚖		
GRANIT/160 Cipher	16 characters, 1 line	A -> D		
Grandpré Cipher	Text input	Alphabet parameters		
Hagelin Machine		Alphabet ARCDEFGHUKUMNOPORSTUWWYZ	16 characters, 1 line	
× *		Unknown symbol handling	Text Output	
Classic Ciphers		Case sensitive		
State Modern Ciphers		Output contains Source Case		
Steganography				
W Hash Functions		0%		
Cryptanalysis		Caesar		
Protocols				
Tools				
	10% (3-0			

Sada možemo proveriti svoj šifrat obrnutim procesom – tj sa istim podešvanjima odraditi Decrypt, i dobiti prvobitni tekst:

() ()		CrypTool 2.1 (Stable Build 9778.2) – New project	- ð ×
Home Edit Crypt	Tutorials		O About *
New Con	Save - Print Print Pay Stop / C Vew G		Startcerter CrypEoEllor CrypEud Usade Settings Hep
Components 👻	Cr 🔶 Startcenter 🗴 🕕 R. New project 🗴		
Search		807	0
Classic Cipners			
ADFGVX			
Affine Cipher			
Bazeries Cipher			
Bifid Cipher			
Book Cipher			
Caesar			
O Chaocipher			
Cylinder Cipher			
ElsieFour Cipher		esarH88 P	
- Enigma	Retor	-> Tet alaut HW	
O Fialka	Decrypt	* ALL HOPE IS GOIVE	
Four-square Cipher		3 *	
GRANIT/160 Cipher	16 characters, 1 line A-> D		
Grandpré Cipher	Test input Alphabet parameters		
Hagelin Machine	Alphabet	16 characters, 1 line	
×	Unknown symbol handling	Text Output	
Classic Ciphers	Ignore (reave unmodified) Case sensitive		
Modern Ciphers	Output contains Source Ca	se	
Steganography			
W Hash Functions		No.	
🔯 Cryptanalysis	Caesar		
Protocols			
Tools			
1	90%		

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, ..., xm) = (x1+k1, x2+k2, ..., xm+km)Dk(y1, y2, y3, ..., ym) = (y1-k1, y2-k2, ..., 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	Е, 4	R, 17	A, 0	P, 15	Е, 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

Otvoriti novi prozor za unos poruka: NEW. Levo u meniju Classic Ciphers izabrati Vigenere I prevuci na radnu povrsinu. Kada vam se pojavi na radnoj povrsini Vigenere imacete 3 strelice sa desne I jednu sa leve strane. Sa desne strane kliknuti prvu I prevuci na levo kako bi otvorili Text input. Isti postupak uraditi I sa levom kako bi napravili Text output. Nakon toga otkucati "ARTOFWAR" u prozor za upis teksta. Prosiriti Vigenere meni kako bi mogli podesiti parametre.

• Key treba promeniti u PERA I key integer treba sam da se promeni u 15, 4, 17, 0

Kada se klikne Play u gornjem meniju dobija se šifra:



Sada možemo proveriti svoj šifrat obrnutim procesom – tj sa istim podešvanjima odraditi Decrypt, i dobiti prvobitni tekst:



<u>Hillova šifra</u>

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

$$\mathbf{K} = | \begin{array}{c} 9 \ 21 \ 17 \\ 5 \ 9 \ 22 \\ 9 \ 10 \ 20 | \end{array}$$

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| = \mathbf{RVK}

WNS: |22 \ 13 \ 18| \ x \ |9 \ 21 \ 17

5 9 22

9 10 20| mod26 = |9 \ 5 \ 6| = \mathbf{JFG}
```

Postupak

Dakle šifrat je RVKJFG, što ćemo proveriti kroz Cryptool. Otvoriti novi prozor za unos poruka: NEW. Levo u meniju Classic Ciphers izabrati Hill Cipher I prevuci na radnu povrsinu. Kada vam se pojavi na radnoj povrsini Vigenere imacete 3 strelice sa desne I jednu sa leve strane. Sa desne strane kliknuti prvu I prevuci na levo kako bi otvorili Text input. Isti postupak uraditi I sa levom kako bi napravili Text output. Nakon toga otkucati "CLOWNS" u prozor za upis teksta.

Prosiriti Hill Cipher meni kako bi mogli podesiti parametre.

• Matrix treba promeniti I napistati:

09 21 17 05 09 22 09 10 20

Napomena: Treba ih pistati kolonu po kolonu kako bi dobili zeljeni rezultat



Kada se klikne Play u gornjem meniju dobija se šifra:

Sada možemo proveriti svoj šifrat obrnutim procesom – tj sa istim podešvanjima odraditi Decrypt, i dobiti prvobitni tekst.

Predmetni nastavnik i predmetni asistent