AKADEMIIJA TEHNIČKO VASPITAČKIH NAUKA
KOMUNIKACIONE TEHNOLOGIJE
ZAŠTITA PODATAKA U KOMUNIKACIONIM MREŽAMA

RAČUNSKA VEŽBA BR. 1

Cezarov algoritam – Caesar cipher

Enkripcija

K = (a_1, a_2, a_3,…), 0 ≤ a ≥ 25 – Karaktere za ključ uzimamo iz alfabeta koji koristimo, u ovom slučaju je to engleski alfabet koji ima 26 karaktera, npr. K=(10, 4, 24) vidimo da je svaki od karaktera korišćenih za ključ u okviru granica koje smo prethodno definisali izborom alfabeta.

Ključ: **K = (3)**

Enkripciju pomoću ovog algoritma vršimo tako što ključ koji smo definisali koristimo iznova, sve dok ne dođemo do kraja poruke koju želimo da kriptujemo. U našem slučaju to izgleda ovako. ***e(x) = x + K mod 26***

Dekripciju pomoću ovog algoritma vršimo tako što koristimo sledeću formulu: ***d(y) = y - K mod 26***

1. Koristeći originalni Cezarov algoritam šifrovati text:
ZASTITAPODATAKAUKOMUNIKACIONIM MREZAMA

REŠENJE:
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

Šifra je: **CDVWLWDSRGDWDNDXNRPXQLNDFLRQLPPUHCDPA**

2. **Pomoću cezarovog algoritma, izvršiti kriptovanje sledeće poruke ako je K= (4):**

Poruka: **h o w t o e n c r y p t**

Engleski alfabet																								
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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

REŠENJE:

Poruka: l s a x s i r g v c t x

3. Izvršiti dekripciju dobijenog rezultata iz prethodnog zadatka.

Poruka: **l s a x s i r g v c t x**

Engleski alfabet																								
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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

REŠENJE:

h o w t o e n c r y p t

4. Pomoću originalnog Cezarovog algoritma izvršiti enkripciju teksta POLOZICU KOLOKVIJUM:

P	O	L	O	Z	I	C	U	K	O	L	O	K	V	I	J	U	M
15	14	11	14	25	8	2	20	10	14	11	14	10	21	8	9	20	12
18	17	14	17	2	11	5	23	13	17	14	17	13	24	11	12	23	15
S	**R**	**O**	**R**	**C**	**L**	**F**	**X**	**N**	**R**	**O**	**R**	**N**	**Y**	**L**	**M**	**X**	**P**

4. Dekriptujte šifru PWNUYTLWFKNOF koja je dobijena putem originalnog Cezarovog algoritma.

REŠENJE:
Kako je prostor ključeva jako mali (ima ih 26) zadatak možemo rešiti "grubom silom", tj. tako da ispitamo sve moguće ključeve, sve dok ne dođemo do nekog smislenog teksta. Za d_0, d_1, ... dobijamo redom:

0. P W N U Y T L W F K N O F
1. O V M T X S K V E J M N E
2. N U L S W R J U D I L M D
3. M T K R V Q I T C H K L C
4. L S J Q U P H S B G J K B
5. K R I P T O G R A F I J A

Dakle, ključ je $K = 5$, a otvoreni tekst je KRIPTOGRAFIJA.

5. Dekriptujte šifru IHYOEXMZRS ako je korišen originalni Cezarov algoritam.

0. IHYOEXMZRS
1. HGXNDW
2. GFWMCV
3. FEVLBU
4. EDUKATIVNO

Rešenje je EDUKATIVNO.

Zadaci za samostalni rad studenta

Svaki od student je dužan da za poruke koje šifruje i dešifruje uzme **ime i prezime** svih članova porodice (min 4, ukoliko ima manje uzeti **ime i prezime** najboljeg prijatelja kao četvrti primer).