Cezarova šifra – Malo teorije

Poznati rimski vojskovođa i državnik Julije Cezar u komunikaciji sa svojim prijateljima koristio se šifrom u kojoj su se slova otvorenog teksta zamenjivala slovima koja su se nalazila tri mesta dalje od njih u alfabetu (A→D, B→E, itd.). Ako bismo upotrijebili današnji engleski alfabet od 26 slova, onda bi poruka:

CSLLAB

bila šifrovana ovako:

FVOODE

Cezarovu šifru možemo pregledno zapisati na sledeći način:

otvoreni tekst	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
šifrat	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

Mi ćemo se u daljnjim primjerima koristiti engleskim (međunarodnim) alfabetom od 26 slova. Cezarovu šifru možemo definisati na sledeći način:

Neka je **P** = **C** = **K** = Z_{26}. Za $0 \le K \le 25$ definišemo

šifrovanje: $y = e_K(x) = x + K \mod 26$,

dešifrovanje: $d_K(y) = y - K \mod 26$.

Znači, sva slova otvorenog i šifriranog teksta prestavljaju se brojevima iz skupa Z_{26} tj. celim brojevima od 0 do 25. Ključ K može imati bilo koju celu vrednost od 0 do 25, a njegova vrednost označava za koliko će se mesta vršiti pomeranje slova prilikom šifrovanja. Šifrovanje (enkripcija) svakog slova otvorenog teksta vrši se tako što se broju koji odgovara tom slovu doda vrednost ključa K i traži se ostatak pri dijeljenju sa brojem 26. Dekripcija (dešifrovanje) vrši se tako što se od broja koji odgovara šifrovanom slovu oduzme vrednost ključa, a potom traži ostatak pri deljenju sa 26. Deljenje po modulu 26 sprovodi se jer imamo ukupno 26 slova tako da rezultat mora biti celi broj od 0 do 25. Odgovarajuća korespodencija je:

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

Može se pokazati da je $d_K(e_K(x)) = x$, kao što se zahteva u definiciji kriptosistema. Za $K = 3$ dobija se originalna Cezarova šifra.

Zadatak 1: Šifrirati reč: "PRVEVEZBE" Cezarovom šifrom, pri čemu je ključ K=5.

Rešenje: Svakom slovu nađe se odgovarajući broj, a potom izvrši šifrovanje po formuli. Npr. slovu P odgovara broj x=15, pa je y=15+5 mod 26 = 20. Zatim se za svaki broj koji odgovara šifratu zameni odgovarajućim slovom.

P	R	V	E	V	E	Z	B	E
15	17	21	4	21	4	25	1	4

- Otvoreni tekst
- Brojevi koji odgoravarju tekstu (x)

$$y = (x + K) \bmod 26$$

20	22	0	9	0	9	4	6	9
U	W	A	J	A	J	E	G	J

- Brojevi koji odgovaraju šifratu (y)
- šifrat

Napomena: do rešenja se može doći i direktno pomoću sledeće tabele:

otvoreni tekst	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
šifrat	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

Zadatak 2: Dešifrujte tekst: "GHZAPAH" dobijen Cezarovom šifrom pomoću ključa K=7.

Rešenje: Za svako slovo u šifratu utvrdi se odgovarajući broj (y). Zatim se izračunavaju brojevi (x) koji odgovaraju otvorenom tekstu po formuli: $x=d_K(y) = (y - K) \bmod 26$, pa se na osnovu njih utvrđuje otvoreni tekst. Npr. za slovo G iz šifrata imamo:
$G \rightarrow y = 6 \rightarrow x = (6 - 7) \bmod 26 \equiv (6 - 7 + 26) \bmod 26 = 25 \rightarrow Z$.
Ponavljanjem postupka za ostala slova šifrata dobijamo rešenje: ZASTITA

G	H	Z	A	P	A	H
6	7	25	0	15	0	7

- Šifrat
- Brojevi koji odgovaraju šifratu (y)

$$x=d_K(y) = (y - K) \bmod 26$$

25	0	18	19	8	19	0
Z	A	S	T	I	T	A

- Brojevi koji odgoravarju tekstu (x)
- Otvoreni tekst

Napomena: Za ključ K=7 šifrovanje i dešifrovanje se može direktno vršiti korišćenjem sledeće tabele:

otvoreni tekst	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
šifrat	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

Zadatak 3: Dekriptujte šifrat PWNUYTLWFKNOF dobijen Cezarovom šifrom. Ključ K je nepoznat.

Rešenje: Budući da je broj mogućih 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 K=0, K=1, K=2, ... dobijamo redom:

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

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

Zadatak 4. Napisati program u programskom jeziku "C" koji šifruje neki tekst koristeći Cezarovu šifru.

Rešenje:

```
#include<stdio.h>
#include<stdlib.h>
#include<string.h>
#include<ctype.h>
#define DIM 80

int main(void){

	int i;
	char *s;

	s = malloc(DIM);
	printf("Unesite tekst koji sifrujete: ");
	gets(s);
	s = realloc(s, strlen(s)+1);

	for(i=0; i < strlen(s); i++)
		if(!isspace(s[i]))
			*(s+i) = (char)((((int)(*(s+i)) - 30) % 93) + 33);

	puts(s);

return EXIT_SUCCESS;
}
```

Zadatak 5. Napisati program u programskom jeziku "C" koji dešifruje neki tekst kriptovan Cezarovom šifrom.

Rešenje:

```
#include<stdio.h>
#include<stdlib.h>
#include<string.h>
#include<ctype.h>
#define DIM 80

int main(void){

	int i;
	char *s;

	s = malloc(DIM);
	printf("Unesite tekst koji sifrujete: ");
	gets(s);
	s = realloc(s, strlen(s)+1);

	for(i=0; i < strlen(s); i++)
		if(!isspace(s[i]))
			*(s+i) = (char)((((int)(*(s+i)) - 30) % 93) + 27);

	puts(s);

return EXIT_SUCCESS;
}
```

Afina šifra definiše se na sledeći način:

Neka se slova otvorenog teksta i šifrata označavaju brojevima kao i kod Cezarove šifre tj. neka je: **P** = **C** = $\mathbf{Z}_{26}$ i neka je ključ K definisan uređenim parom (a,b) koji su elementi skupa $\mathbf{Z}_{26}$. Za proizvoljan ključ $K = (a,b)$ definišemo:

Šifrovanje: $e_K(x) = ax + b \bmod 26$,

Dešifrovanje: $d_K(y) = a^{-1}(y - b) \bmod 26$.

Ova šifra se zove afina po funkciji kojom se vrši šifrovanje. Proverimo da li je uslov: $d_K(e_K(x)) = x$ zadovoljen. Zaista,

$$d_K(e_K(x)) = d_K(ax + b) = a^{-1}(ax + b - b) = x.$$

Ovde a^{-1} ne označava recipročnu vrijednost broja a, već je on tzv. multiplikativni inverz broja a. Brojevi a^{-1} i a zadovoljavaju jednakost: $a^{-1}a \bmod 26 = 1$. Nemaju svi brojevi iz skupa $\mathbf{Z}_{26}$ svoj multiplikativni inverz (već samo oni koji su međusobno prosti sa brojem 26 tj. da im je 1 najveći zajednički djelilac sa 26). Prikažimo te brojeve zajedno s njihovim inverzima:

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Znači broj a koji predstavlja deo ključa K ne može biti bilo koji ceo broj od 0 do 25 već samo neki od brojeva datih u prethodnoj tabeli.

Zadatak 1. Neka je $K = (7, 3)$. Šifrujte otvoreni tekst ZASTITA.

Rešenje:

$$\begin{aligned}
Z &\rightarrow 25 \cdot 7 + 3 \equiv 22 \pmod{26} \rightarrow W,\\
A &\rightarrow 0 \cdot 7 + 3 \equiv 3 \pmod{26} \rightarrow D,\\
S &\rightarrow 18 \cdot 7 + 3 \equiv 25 \pmod{26} \rightarrow Z,\\
T &\rightarrow 19 \cdot 7 + 3 \equiv 6 \pmod{26} \rightarrow G,\\
I &\rightarrow 8 \cdot 7 + 3 \equiv 7 \pmod{26} \rightarrow H,\\
T &\rightarrow 19 \cdot 7 + 3 \equiv 6 \pmod{26} \rightarrow G,\\
A &\rightarrow 0 \cdot 7 + 3 \equiv 3 \pmod{26} \rightarrow D,
\end{aligned}$$

pa je dobijeni šifrat WDZGHGD. Ispod je dat i odgovarajući tabelarni prikaz:

Z	A	S	T	I	T	A
25	0	18	19	8	19	0

- Otvoreni tekst
- Brojevi koji odgoravarju tekstu (x)

y = ax + b mod 26

22	3	25	6	7	6	3
W	D	Z	G	H	G	D

- Brojevi koji odgovaraju šifratu (y)
- Šifrat

Zadatak 2. Neka je $K = (5, 5)$. Dešifrujte šifrat: XWGXM ZSTWZ DRW.

Rešenje: Kako je a=5 iz tabele se može videti da je a^{-1}=21, pa se primjenom formule $d_K(y) = a^{-1}(y - b) \bmod 26$ tj. $d_K(y) = 21 \cdot (y - 5) \bmod 26$ dolazi do rešenja.
Npr. X→ 23 → $d_K(23) = 21 \cdot (23 - 5) = 378 \equiv 14 \pmod{26}$. Dešifrovanjem svih slova dobijaju se dešifrovane riječi: OTVORENI TEKST.

X	W	G	X	M	Z	S	T	W	Z	D	R	W
23	22	6	23	12	25	18	19	22	25	3	17	22
$d_K(y) = 21 \cdot (y - 5) \bmod 26$												
14	19	21	14	17	4	13	8	19	4	10	18	19
O	T	V	O	R	E	N	I	T	E	K	S	T

- Šifrat
- Brojevi koji odgovaraju šifratu (y)
- Brojevi koji odgoravarju tekstu (x)
- Otvoreni tekst

Zadatak 3. Dekriptujte šifrat

OZWHR YEZCV WFCTP CUWRC FPWTC HWI

dobijen afinom šifrom. Ključ nije poznat, a otvoreni tekst je pisan na našem jeziku.

Rešenje:
Kako je ključ K=(a,b) kombinacija 12 mogućih brojeva a i 26 mogućih brojeva b to postoji $12 \cdot 26 = 312$ mogućih ključeva. To je još uvek premalo, pa bi uz pomoć računara sigurno mogli primeniti "grubu silu".

Ali, postoji i elegantniji način. Ukoliko znamo kojim je jezikom pisan otvoreni tekst možemo iskoristiti statističke podatke o frekvenciji pojedinih slova u tom jeziku. Za sada nam je potrebna samo činjenica da su najfrekventnija slova u našem jeziku A, I, O, E, N(sledeća tabela), i to upravo po tom redosledu. U našem šifratu uočavamo da su najfrekventnija slova C i W, koja se javljaju po 5 puta. Iako je naš šifrat prekratak, možemo ipak očekivati da su ova dva slova šifrati od A, I, O, E ili N.

FREKVENCIJA SLOVA (u promilima)

NAŠ JEZIK	A	I	O	E	N	S	R	J	T	U	D	K	V	L	M	P	C	Z	G	B	H	F				
	115	98	90	84	66	56	54	51	48	43	37	36	35	33	31	29	28	23	16	15	8	3				
ENGLESKI	E	T	A	O	I	N	S	H	R	D	L	C	U	M	W	F	G	Y	P	B	V	K	J	Q	X	Z
	127	91	82	75	70	67	63	61	60	43	40	28	28	24	23	22	20	20	19	15	10	8	2	1	1	1
NEMAČKI	E	N	I	R	S	A	T	D	H	U	L	G	O	C	M	B	F	W	K	Z	P	V	J	Y	X	Q
	175	98	77	75	68	65	61	48	42	42	35	31	30	27	26	19	17	15	15	11	10	9	3	1	0	0

Pretpostavimo da je C šifrat slova A, kao i da je W šifrat slova I tj. $e_K(A) = C$ i $e_K(I) = W$. Korišćenjem tabele pomoću koje pretvaramo slova u brojeve imamo da je: $e_K(0) = 2$ i $e_K(8) = 22$. Sada na osnovu definicije imamo $e_K(0) = a \cdot 0 + b = b$, $e_K(8) = 8a + b$. Vidimo da je $b = 2$ i $8a + b \equiv 22 \pmod{26}$, odakle možemo izračunati $a = 9$. Dakle, dobili smo da je $e_K(x) = 9x + 2 \bmod 26$. Tada je $d_K(y) = 3(y - 2) \bmod 26$. Primenimo li funkciju d_K na naš šifrat, dobiamo otvoreni tekst:

KRIPTOGRAFIJA ZNAČI TAJNI ZAPIS.

Cezarova i afina šifra su specijalni slučajevi ***supstitucijske šifre***, kod koje za šifrovanje može izvršiti proizvoljna permutacija slova tj. svakom od 26 slova može se pridodati proizvoljno slovo kao šifrat (naravno dva slova ne smiju imati isti šifrat).