

PRAKTIKUM IZ PROGRAMIRANJA 2

- domaći zadatak broj 5 -

Sastaviti program na programskom jeziku C kojim se vrši šifrovanje ili dešifrovanje teksta na način kako je to opisano u pojedinačnim zadacima. Program treba da pročita ulaznu datoteku sa tekstom koji treba šifrovati ili dešifrovati, smesti podatke u odgovarajuću listu, izvrši odgovarajuću obradu nad ulaznim podacima, upiše rezultat u datoteku i dealocira svu alociranu dinamičku memoriju.

Zavisno od rednog broja problema, sastaviti **jedan** od sledećih programa:

0. Pera i Mika su jako čudni dečaci koji vole da pričaju o socijalno neprihvatljivim stvarima poput „Ane Karenjine“ i „Ratu i miru“. Normalno, njihovi roditelji, kojima je stalo do socijalnog statusa, ne dozvoljavaju svojoj deci da pričaju o ovim tabu temama. Stoga su Pera i Mika rešili da šifruju svoje poruke! Kada se vide, njih dvojica, tajno, razmene ključ. Ključ i poruka su nizovi znakova tajnog alfabeta. Pera ode kući i napravi niz znakova kojim šifruje poruku, tako što ponavlja ključ dok broj znakova u nizu ne dostigne dužinu poruke koja se šifruje (na primer, niz kojim se poruka šifruje za poruku dužine 23 izgleda ovako: `k1jučk1jučk1jučk1jučk1j`). Zatim Pera napiše svoju poruku u drugom nizu. Onda uradi operaciju isključivo ILI nad bitovima elemenata poruke i ključa sa odgovarajućim indeksima i tako dobijeni niz pošalje Miki. Mika primi i na isti način dešifruje niz i pročita Perinu poruku. Kako Pera i Mika ne znaju programiranje, oni su se obratili Vama da im napišete program koji će raditi ovo šifrovanje i dešifrovanje.
1. Peri i Miki iz nultog zadatka je život bio lep dok nisu upoznali Vljaka. Jednog dana Vljako je rekao Peri: „Vidiš, Pero, dobra ti je ova fora sa šifrom, ali ako ne menjaš ključ dovoljno često, i ako ti nije dovoljno dugačak, lako će da te provale“. Nesretni Pera je pomislio da mu je algoritam loš i rešio da ga zameni novim i boljim. Setio se Pera da je [Cezar](#) imao običaj da svako slovo u poruci zameni sledećim slovom u alfabetu kako bi zbunio neprijatelje. Umesto `Gal1i`, on bi napisao `Гбmј` (pomerio svako slovo za jedno mesto) ili `Јао1` (pomerio svako slovo za 3 mesta). Pera pored slova mora da vodi računa i o ciframa, razmaku i tački. Peri je bilo jasno da pomeranje svih znakova za isti broj mesta unapred nije sigurno rešenje. Rešio je da pomeri svaki znak unapred za poziciju u tajnom alfabetu (istom kao u varijanti 0) odgovarajućeg znaka u ključu. Znakovi se pomeraju kružno (posle znaka `.` dolazi znak `a`). Kako Pera još uvek nije naučio programiranje, on Vas opet moli da mu napravite program za šifrovanje i dešifrovanje.
2. Romeo i Julija su očajni! Njihovi roditelji su im zabranili ne samo da se viđaju, nego i da šalju pisma. Na svu sreću po njih, njihove palate se nalaze na susednim brdima, tako da imaju optičku vidljivost. Romeo se dosetio da ode unapred kroz vreme i kupi na buvljaku par minijaturnih lasera, pa da šalje Juliji poruke [Morzeovom azbukom](#). Avaj, Romeo ne zna Morzeovu azbuku, pa je zamolio vas, njegove verne prijatelje, da mu napišete program za kontrolu lasera, koji će njegove poruke pretvarati u niz tačaka i crta.
3. Romeova sreća je bila neopisiva kada je koristeći program iz prethodnog zadatka uspeo da pošalje Juliji poruku i da joj kaže koliko je voli. Julija je, naravno, odmah pocrvenela, uzela svoj laser i odgovorila Romeu (pošto je i ona putovala unapred kroz vreme i bila školovana na odseku za telekomunikacije na fakultetu iz sredine XIX veka, ona zna Morzeovu azbuku). Kako je Romeo na sedmom nebu i nema vremena ručno da dešifruje poruku, zadužio je Vas da mu napravite program koji Julijinu poruku napisanu [Morzeovom azbukom](#) prevodi u slova i brojeve koji su mu razumljivi.

4. Radašin je kopao po tavanu kuće svoje pokojne prababe Paraskeve i nakon nekog vremena je pronašao nekakav stari svitak pun rupa. Posle malo istraživanja porodične istorije, saznao je da je Paraskeva zapravo bila jedan od izumitelja teleprinteru. Sem toga, Paraskeva je bila vrlo pogana veštica. Ona je svoje blago zakopala negde u dvorištu. Put do blaga je zapisala u [Bodoovom kodu](#) na bušenim karticama. Radašin želi da se dokopa blaga, ali ne ume da dešifruje Bodoov kod. Pomozite mu da dešifruje kod, ako su simboli kodirane poruke dati u heksadecimalnom zapisu.
5. Uz vašu pomoć i malo iskopavanja po dvorištu, Radašin je našao bočicu sa nekom tečnošću. Kako ne zna hemiju, zaključio je da je lakše da kontaktira svoju prababu Paraskevu (iz prošlog zadatka) u svetu mrtvih. Nažalost, baba je izlapela, te se od zemaljskih jezika seća samo [Bodoovog koda](#). Stoga Radašinu treba program koji pretvara poruke pisane korišćenjem alfabeta u Bodoov kod, kodiran u heksadecimalnom zapisu. Pomozite Radašinu da se obrati prababi i sazna šta je u bočici, tako što ćete mu napisati potreban program.

Alfabet za varijante 0 i 1 se sastoji od velikih i malih slova engleskog alfabeta, cifara, znaka razmaka i tačke:

abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123465789 .
--

Alfabet za varijante 2, 3, 4 i 5 sadrži velika slova engleskog alfabeta, cifre i neke specijalne znakove:

ABCDEFGHIJKLMNOPQRSTUVWXYZ0123465789-?:!&' () . , ; / "

Primeri i objašnjenja upotrebljenih algoritama šifriranja/kodiranja su u prilogu. Pre odbrane, priložiti makar tri suštinski različita test primera i očekivane rezultate. Poruka koja se šifruje ili dešifruje se uvek nalazi u tekstualnoj datoteci. Prilikom formiranja izlazne datoteke očuvati uredenost teksta u redove.

Glavni program treba da poziva funkcije koje obavljaju radnje potrebne za sprovođenje obrade. Sve funkcije smestiti u odgovarajuće **.c** datoteke (prema donjem spisku), a prototipove svih funkcija smestiti u zajedničku **.h** datoteku. Svaku obradu koja se ponavlja više od jednom smestiti u zasebnu funkciju. Nije dozvoljeno korišćenje globalnih promenljivih, sva razmena podataka između funkcija mora ići preko liste argumenata i povratne vrednosti funkcija.

U zavisnosti od rednog broja problema koji se rešava osmisлити sopstvenu strukturu/strukture za smeštanje podataka iz ulazne datoteke. Element liste koja sadrži podatke iz ulazne/ulaznih datoteka treba realizovati kao strukturu koja ima **tačno** tri polja – pokazivače na prethodni i sledeći element, i pokazivač na strukturu koja sadrži podatke. Voditi računa o pravilnoj alokaciji i dealokaciji dinamičke memorije.

U zavisnosti da li je definisana simbolička konstanta **CMD_LINE**, omogućiti da program sa korisnikom komunicira putem komandne linije ili putem interaktivnog menija, što se određuje uslovnim prevođenjem, u zavisnosti od trenutne aktivne konfiguracije za prevođenje programa. U slučaju rada putem komandne linije, korisnik zadaje ime ulazne i izlazne datoteke. U varijantama 0 i 1, kao dodatni argument komandne linije se navodi ključ za šifrovanje i dešifrovanje poruke. U slučaju rada preko glavnog ulaza, ključ se zadaje putem posebne stavke u meniju.

U slučaju bilo kakve greške (poziv programa sa neodgovarajućim brojem argumenata komandne linije, neuspešna dodela dinamičke memorije, greška pri radu sa datotekom), kod za grešku proslediti do glavnog programa preko povratne vrednosti funkcije, ispisati odgovarajuću poruku i prekinuti izvršavanje. Ispisivanje poruke o greškama vršiti samo iz glavnog programa.

Ako nešto u postavci zadatka nije dovoljno precizno definisano ili ako su neki od zahteva međusobno suprotstavljeni, usvojiti razumnu pretpostavku i rešiti zadatak korišćenjem te pretpostavke. Na samoj odbrani obavestiti demonstratora o usvojenoj pretpostavci/pretpostavkama.

Napomene:

1. Odbrana petog domaćeg zadatka je u četvrtak, 25.05.2017. po rasporedu dostupnom na sajtu predmeta.
2. Primeri ulaza i izlaza za gornje probleme su dostupni u prilogu ovog dokumenta.
3. Formula za redni broj problema **i** koji treba rešavati je sledeća (R – redni broj indeksa, G – poslednje dve cifre godine upisa): **$i = (R + G) \bmod 6$**
4. Kao rešenje domaćeg zadatka potrebno je na odbrani pokazati sledeće datoteke:
 - **dz5.h**, koja sadrži prototipe svih funkcija opisanih u postavci zadatka;
 - **dz5.c**, koja sadrži izvorni tekst osnovnog programa na programskom jeziku C;
 - **dz5_load.c, dz5_save.c, dz5_process.c**, koje sadrže izvorne tekstove funkcija potrebnih za inicijalizaciju programa, čitanje, snimanje i obradu teksta;
 - **dz5_test1.txt, dz5_test2.txt, dz5_test3.txt** koje sadrže nekoliko test primera koje su kandidati sami osmislili.

12.05.2017. godine

sa predmeta

Primer za varijantu 0

Ključ: tajni ključ

Poruka: Ovo treba sifrovati super tajnom sifrom.

Prva kolona je i, indeks znaka u poruci.

Druga kolona je i-ti znak u poruci.

Treća kolona je vrednost i-tog znaka poruke u tajnom alfabetu.

Četvrta kolona je i-ti znak (po modulu dužine ključa) ključa.

Peta kolona je vrednost i-tog znaka ključa u tajnom alfabetu.

Šesta kolona je operacija XOR (isključivo ILI) nad vrednostima treće i pete kolone (6 bita).

Sedma kolona je znak u tajnom alfabetu koje odgovara broju iz šeste kolone.

0	o	40	t	19	59	7
1	v	21	a	0	21	v
2	o	14	j	9	7	h
3		62	n	13	51	Z
4	t	19	i	8	27	B
5	r	17		62	47	V
6	e	4	k	10	14	o
7	b	1	l	11	10	k
8	a	0	j	9	9	j
9		62	u	20	42	Q
10	s	18	c	2	16	q
11	i	8	t	19	27	B
12	f	5	a	0	5	f
13	r	17	j	9	24	y
14	o	14	n	13	3	d
15	v	21	i	8	29	D
16	a	0		62	62	
17	t	19	k	10	25	z
18	i	8	l	11	3	d
19		62	j	9	55	3
20	s	18	u	20	6	g
21	u	20	c	2	22	w
22	p	15	t	19	28	C
23	e	4	a	0	4	e
24	r	17	j	9	24	y
25		62	n	13	51	Z
26	t	19	i	8	27	B
27	a	0		62	62	
28	j	9	k	10	3	d
29	n	13	l	11	6	g
30	o	14	j	9	7	h
31	m	12	u	20	24	y
32		62	c	2	60	8
33	s	18	t	19	1	b
34	i	8	a	0	8	i
35	f	5	j	9	12	m
36	r	17	n	13	28	C
37	o	14	i	8	6	g
38	m	12		62	50	Y
39	.	63	k	10	53	l

Primer za varijantu 1

Ključ: tajni ključ

Poruka: Ovo treba sifrovati super tajnom sifrom.

Prva kolona je i, indeks znaka u poruci.

Druga kolona je i-ti znak u poruci.

Treća kolona je vrednost i-tog znaka poruke u tajnom alfabetu.

Četvrta kolona je i-ti znak (po modulu dužine ključa) ključa.

Peta kolona je vrednost i-tog znaka ključa u tajnom alfabetu.

Šesta kolona je sabrana vrednost treće i pete kolone po modulu 64.

Sedma kolona je znak u tajnom alfabetu koje odgovara broju iz šeste kolone.

0	o	40	t	19	59	7
1	v	21	a	0	21	v
2	o	14	j	9	23	x
3		62	n	13	11	l
4	t	19	i	8	27	B
5	r	17		62	15	p
6	e	4	k	10	14	o
7	b	1	l	11	12	m
8	a	0	j	9	9	j
9		62	u	20	18	s
10	s	18	c	2	20	u
11	i	8	t	19	27	B
12	f	5	a	0	5	f
13	r	17	j	9	26	A
14	o	14	n	13	27	B
15	v	21	i	8	29	D
16	a	0		62	62	
17	t	19	k	10	29	D
18	i	8	l	11	19	t
19		62	j	9	7	h
20	s	18	u	20	38	M
21	u	20	c	2	22	w
22	p	15	t	19	34	I
23	e	4	a	0	4	e
24	r	17	j	9	26	A
25		62	n	13	11	l
26	t	19	i	8	27	B
27	a	0		62	62	
28	j	9	k	10	19	t
29	n	13	l	11	24	y
30	o	14	j	9	23	x
31	m	12	u	20	32	G
32		62	c	2	0	a
33	s	18	t	19	37	L
34	i	8	a	0	8	i
35	f	5	j	9	14	o
36	r	17	n	13	30	E
37	o	14	i	8	22	w
38	m	12		62	10	k
39	.	63	k	10	9	j

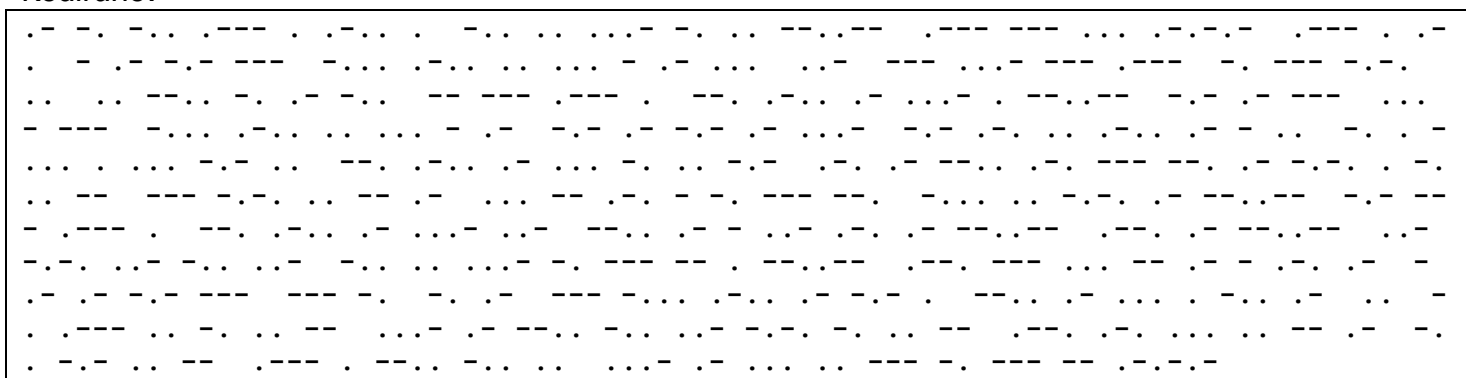
Primer za varijante 2 i 3

Morzeova azbuka koja treba da se koristi je data u sledećoj tabeli.

Znak	Kod	Znak	Kod	Znak	Kod	Znak	Kod	Znak	Kod	Znak	Kod
A	·—	J	·— —	S	···	1	·— — —	Tačka [.]	·—· —· —	Dvotačka [:]	— —· ·
B	—·· ·	K	—· —	T	—	2	··— —	Zapeta [,]	— ··— —	Tačka zapeta [;]	—· —· —·
C	—· —·	L	·—· ·	U	··—	3	··· —	Znak pitanja [?]	··— —··	Jednako [=]	—·· ·—
D	—··	M	—	V	··· —	4	···· —	Apostrof [']	·— — —·	Plus [+]	·—· —·
E	·	N	—·	W	·— —	5	···· ·	Znak uzvike [!]	—· —· —	Crta [-]	—·· ··—
F	··— ·	O	— —	X	—·· —	6	—·· ··	Kosa crta [/]	—·· —·	Donja crta [_]	··— —· —
G	— ·	P	·— —·	Y	—· —	7	— ···	Otvorena zagrada [(]	—· — ·	Navodnici ["]	·—· ·—·
H	····	Q	— ·—	Z	— ··	8	— —··	Zatvorena zagrada [)]	—· — ·—	Dolar [\$]	··· —·· —
I	··	R	·—·	0	— — —	9	— — ·	<i>Ampersand</i> [&]	·—· ··	<i>At sign</i> [@]	·— —· —·

Sivi znaci su regularni, ali ih za potrebe zadatka treba ignorisati i nije potrebno implementirati. Smatrati da nakon svakog znaka iz Morzeove azbuke sledi pauza u vidu jednog blanko znaka. Tamo gde u poruci postoji blanko znak, u kodiranoj poruci se blanko znak javlja dva puta.

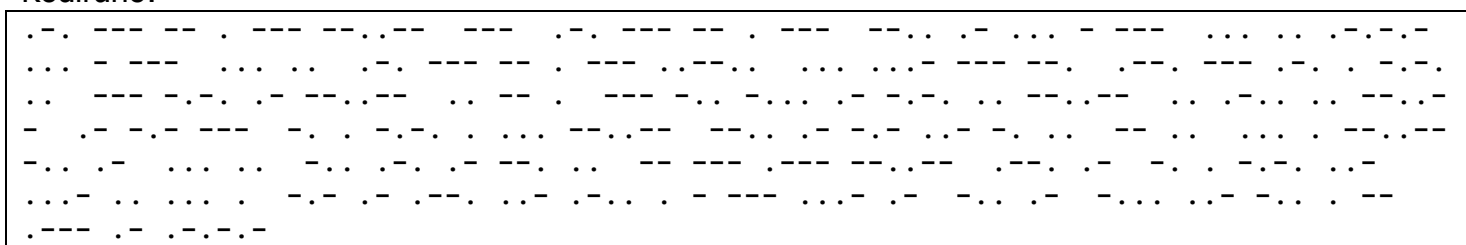
Romeo:
Kodirano:



Prevod:

ANDJELE DIVNI, JOS. JER TAKO BLISTAS U OVOJ NOCI IZNAD MOJE GLAVE, KAO STO BLISTA
KAKAV KRILATI NEBESKI GLASNIK RAZROGACENIM OCIMA SMRTNOG BICA, KOJE GLAVU ZATURA,
PA, U CUDU DIVNOME, POSMATRA KAKO ON NA OBLAKE ZASEDA I NJINIM VAZDUCNIM PRSIMA
NEKIM JEZDI VASIONOM.

Julija:
Kodirano:



Prevod:

ROMEO, O ROMEO! ZASTO SI. STO SI ROMEO? SVOG PORECI OCA, IME ODBACI, ILI, AKO
NECES, ZAKUNI MI SE, DA SI DRAGI MOJ, PA NECU VISE KAPULETOVA DA BUDEM JA.

Primer za varijante 4 i 5

Bodoov kod je kod u kome su karakteri podeljeni na dva dela: slova (leva kolona) i cifre i znakovi (desna kolona). Svako slovo (leva kolona) se obeležava određenim brojem (od 01 do 1F), i tu oznaku "deli" sa još jednim znakom ili brojem iz desne kolone. Kako bi se označilo da li će se kod tumačiti kao slova ili cifre i znakovi, koriste se brojevi 1F, koji označava da se radi o slovima (levoj koloni), i 1B, koji označava da se radi o ciframa i specijalnim znakovima (desnoj koloni).

BITS	LETTERS	FIGURES	HEX
00011	A	-	03
11001	B	?	19
01110	C	:	0E
01001	D	\$	09
00001	E	3	01
01101	F	!	0D
11010	G	&	1A
10100	H	STOP	14
00110	I	8	06
01011	J	'	0B
01111	K	(0F
10010	L)	12
11100	M	.	1C
01100	N	,	0C
11000	O	9	18
10110	P	0	16
10111	Q	1	17
01010	R	4	0A
00101	S	BELL	05
10000	T	5	10
00111	U	7	07
11110	V	;	1E
10011	W	2	13
11101	X	/	1D
10101	Y	6	15
10001	Z	"	11
00000	Nelegalno	Nelegalno	00
01000	CR (\r)	CR (\r)	08
00010	LF (\n)	LF (\n)	02
00100	SP (razmak)	SP (razmak)	04
11111	slede slova	slede slova	1F
11011	slede brojevi	slede brojevi	1B

BELL predstavlja audio signal. Na predajnoj strani nije potrebno realizovati podršku za slanje BELL i STOP kodova. Na prijemnoj strani ignorisati ih. Broj 0 se nikada ne pojavljuje u Bodoovom kodu.

Poruka: **BAUDOT**

KOD	1F	19	03	07	09	18	10
ZNAK		B	A	U	D	O	T

Poruka: **PERA1**

KOD	1F	16	01	0A	03	1B	17
ZNAK		P	E	R	A		1

Poruka: **SARMA**

KOD	1F	05	03	0A	1C	03
ZNAK		S	A	R	M	A

Poruka: **OO1PP2**

KOD	1F	18	18	1B	1	1F	16	16	1B	13
ZNAK		O	O		1		P	P		2