Zadatak 1: Za kodiranje po RC4 algoritmu dato je trenutno stanje ključa $S = [5\ 7\ 0\ 4\ 1\ 3\ 2\ 6]$ i trenutne vrednosti indeksa $i = 4$ i $j = 3$. Kodirati broj $14340_{(8)}$ po RC4 algoritmu i rezultat predstaviti kao oktalni broj.

Rešenje:
Prevešćemo cifre datog broja u binarni oblik:
$1 \rightarrow 001$
$4 \rightarrow 100$
$3 \rightarrow 011$
$0 \rightarrow 000$
Dalje, dati su trenutno stanje ključa $S = [5\ 7\ 0\ 4\ 1\ 3\ 2\ 6]$ i trenutne vrednosti brojača $i = 3$ i $j = 4$.

U odnosu na standardni RC4 algoritam, ovaj problem se specijalizuje na sledeći način:

```
i := 3
j := 4
while GeneratingOutput:
        i := (i + 1) mod 8
        j := (j + S[i]) mod 8
        swap(S[i], S[j])
        output S[(S[i] + S[j]) mod 8]
endwhile
```

Operacija mod se ne vrši sa 256 već sa 8 jer u datom primeru niz S ima 8 elemenata. Kako je broj petocifren, do ključa dolazimo primenom datog algoritma kroz pet iteracija:

Pocetak: $S = [5\ 7\ 0\ 4\ 1\ 3\ 2\ 6]$ i trenutne vrednosti brojača $i = 3$ i $j = 4$.

Prva iteracija:
$i = 4\ mod\ 8 = 4$
$j = (4 + S[4])\ mod\ 8 = (4 + 1)\ mod\ 8 = 5$
$S = [5\ 7\ 0\ 4\ 3\ 1\ 2\ 6]$
$output = S[(S[i] + S[j])\ mod\ 8] = S[(S[4] + S[5])\ mod\ 8] = S[(3 + 1)\ mod\ 8] = S[4] = 3$

Druga iteracija:
$i = 5\ mod\ 8 = 5$
$j = (5 + S[5])\ mod\ 8 = (5 + 1)\ mod\ 8 = 6$
$S = [5\ 7\ 0\ 4\ 3\ 2\ 1\ 6]$
$output = S[(S[i] + S[j])\ mod\ 8] = S[(S[5] + S[6])\ mod\ 8] = S[(2 + 1)\ mod\ 8] = S[3] = 4$

Treća iteracija:
$i = 6\ mod\ 8 = 6$
$j = (6 + S[6])\ mod\ 8 = (6 + 1)\ mod\ 8 = 7$
$S = [5\ 7\ 0\ 4\ 3\ 2\ 6\ 1]$
$output = S[(S[i] + S[j])\ mod\ 8] = S[(S[6] + S[7])\ mod\ 8] = S[(6 + 1)\ mod\ 8] = S[7] = 1$

Četvrta iteracija:
$i = 7\ mod\ 8 = 7$
$j = (7 + S[7])\ mod\ 8 = (7 + 1)\ mod\ 8 = 0$
$S = [1\ 7\ 0\ 4\ 3\ 2\ 6\ 5]$
$output = S[(S[i] + S[j])\ mod\ 8] = S[(S[7] + S[0])\ mod\ 8] = S[(5 + 1)\ mod\ 8] = S[6] = 6$

Peta iteracija:
$i = 8\ mod\ 8 = 0$
$j = (0 + S[0])\ mod\ 8 =\ 1\ mod\ 8 = 1$
$S = [7\ 1\ 0\ 4\ 3\ 2\ 6\ 5]$
$output = S[(S[i] + S[j])\ mod\ 8] = S[(S[0] + S[1])\ mod\ 8] = S[(7 + 1)\ mod\ 8] = S[0] = 7$

Kako se svaki generisani triplet ključa (a iz svake iteracije dobili smo po jedan) uparuje sa jednim tripletom originalnog podatka, kodirani podatak dobićemo na sledeći način:

Nazovimo $output$ iz i-te iteracije $output[i]$. Dakle imamo da je $output[1] = 3, output[2] = 4, output[3] = 1, output[4] = 6, output[5] = 7$. $output$ takođe treba biti kodiran binarno tako da je
$output[1] = 011,$
$output[2] = 100,$
$output[3] = 001,$
$output[4] = 110,$
$output[5] = 111.$

Svaki bajt triplet podatka obeležimo sa $data[i]$, odakle sledi da je
$data[1] = 001,$
$data[2] = 100,$
$data[3] = 011,$
$data[4] = 100,$
$data[5] = 000.$

Primenom XOR $(\oplus)$ operacije među parovima ključ – podatak dobijamo:
$data[1] \oplus output[1] = 001\ \oplus 011 = 010$
$data[2] \oplus output[2] = 100\ \oplus 100 = 000$
$data[3] \oplus output[3] = 011\ \oplus 001 = 010$
$data[4] \oplus output[4] = 110\ \oplus 100 = 010$
$data[5] \oplus output[5] = 000\ \oplus 111 = 111$

Dakle dobijeni kodirani podatak je:
010 000 010 010 111
Odnosno, predstavljeno oktalno:
20227

Zadatak 2: Odrediti sadržaj niza S od 16 elemenata nakon postupka generisanja ključa standardnim RC4 algoritmom. Za spoljni ključ uzeti niz hex cifara 0x2FFFA113.

Spoljni ključ je 0x2FFFA113. Kako se sastoji od 8 hex cifara, vrednost parametra keylength je 8. Broj elemenata niza S je 16, po uslovu zadatka. Dakle, N = 16 i za dobijanje ključa potrebno je 16 iteracija.

U priloženoj tabeli su date promene vektora S uz prateće određivanje indeksa koji menjaju vrednosti.

S					
0	0	2	8		
1	1	0	3	A	C
2	2	0	1		
3	3	4			
4	4	3	0		
5	5	7			
6	6	E	5	6	D
7	7	5	E		
8	8	2	9		
9	9	2			
A	A	3			
B	B				
C	C	A			
D	D	F			
E	E	6	5		
F	F	D	6		

i = 0; j = (0 + 0 + 2) % 16 = 2;	i = 8; j = (6 + 8 + 2) % 16 = 0
i = 1; j = (2 + 1 + F) % 16 = 2;	i = 9; j = (0 + 9 + F) % 16 = 8;
i = 2; j = (2 + 1 + F) % 16 = 2	i = A; j = (8 + A + F) % 16 = 1
i = 3; j = (2 + 3 + F) % 16 = 4	i = B j = (1 + B + F) % 16 = 11
i = 4; j = (4 + 3 + A) % 16 = 1	i = C; j = (B + C + A) % 16 = 1
i = 5; j = (1 + 5 + 1) % 16 = 7;	i = D j = (1 + D + 1) % 16 = F
i = 6; j = (7 + 6 + 1) % 10 = E	i = E j = (F + 6 + 1) % 10 = 6
i = 7; j = (E + 5 +3) % 10 = 6	i = F j = (6 + D + 3) % 10 = 6

S = [8 C 1 4 0 7 D E 9 2 3 B A F 5 6]