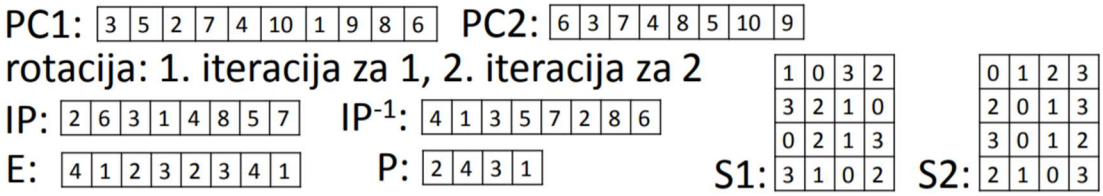
Ispit iz Zaštite podataka (13E113ZP, 13S114ZP) 22.08.2019.

1. (**20p**)
   a) (14p) Za originalnu poruku 00111100b i ključ 1111100000b dati međurezultat svake operacije, kao i vrednost šifrovane poruke, ako se koristi pojednostavljeni *DES* algoritam (*S-DES*). Parametri algoritma su u nastavku.



   b) (6p) Šta su konfuzija i difuzija? Šta je efekat lavine?

2. (**15p**)
   a) (12p) Dešifrovati poruku: AONSITNOEPORKAENIIHEAZCIILSM koja je dobijena šifrovanjem transpozicionim algoritmom sa ključem: (7,5,3,1,6,4,2). Transpozicija je primenjena dva puta.
   b) (3p) Da li analizom samo teksta šifrovanog gore opisanom metodom, bez njegovog dešifrovanja, može da se odredi na kojem jeziku je pisana originalna poruka (ako da, kako)? Odgovor obrazložiti.

3. (**15p**) Ukratko objasniti različite pristupe detekciji upada i za koje tipove uljeza daju najbolje rezultate.
4. (**15p**)

Napomena: *Na ispitu nisu dozvoljena nikakva pomoćna sredstva, ni kalkulatori ni literatura. Ispit traje 150 minuta.*