Prvi kolokvijum iz Zaštite podataka (SI4ZP, 13S114ZP) *27.03.2016.*

1. Koliko ima različitih reverzibilnih mapiranja za blok od n bita ako se koristi idealna blokovska šifra, a koliko ukoliko se koristi neki od simetričnih blok algoritama sa ključem dužine k bita? Zbog čega se ne koristi idealna blokovska šifra? Šta su difuzija i konfuzija i kako se postižu kod DES algoritma?
2. Skicirati i objasniti protokol kojim je moguće obaviti distribuciju tajnih (simetričnih) ključeva pomoću javnih ključeva uz autentikaciju učesnika u komunikaciji.

Napomene: Na kolokvijumu nisu dozvoljena nikakva pomoćna sredstva, ni kalkulatori ni literatura. Kolokvijum traje 90 minuta.