Prvi kolokvijum iz Zaštite podataka (SI4ZP, IR4ZP) *24.03.2012.*

1. Kako se može uspostaviti međusobna komunikacija učesnika u kojoj se postiže tajnost bez prethodne razmene tajnih ključeva, a zahvaljujući postojanju javnih ključeva. Na kojim osobinama sistema sa javnim ključem je zasnovano postizanje tajnosti.
2. Nacrtati strukturnu šemu *DES* algoritma i objasniti način funkcionisanja algoritma prilikom šifrovanja. Detaljno objasniti kako izgleda jedna iteracija i kako se od ključa prave ključevi iteracije.
3. Nacrtati i objasniti CFB i OFB modove funkcionisanja blok algoritama. Kada se koristi CFB, a kada OFB? Koja je razlika između ova dva moda?

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