Prvi kolokvijum iz Zaštite podataka (SI4ZP, IR4ZP) *22.03.2014.*

1. Objasniti *One time pad* algoritam. Ako se ključ generiše pseudoslučajnim generatorom, da li i dalje važi da je nemoguće dekriptovati poruku? Obrazložiti odgovor.
2. Nacrtati strukturnu šemu *AES* algoritma za veličinu ključa od 128 bita i objasniti način funkcionisanja algoritma prilikom šifrovanja. Objasniti strukturu jedne iteracije *AES* algoritma. Objasniti svaku od faza iteracije. Objasniti algoritam koji se koristi za ekspanziju ključa kod *AES* algoritma.
3. Nacrtati i objasniti *CBC* i *CFB* modove funkcionisanja blok algoritama. Kada se koristi *CBC*, a kada *CFB*? Koje su razlike između ova dva moda?

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