Kolokvijum iz Zaštite podataka (MS1ZP) *27.04.2013.*

1. Objasniti ulogu, osobine i zahteve kodova za autentikaciju poruka (*MAC* kodovi). Kojim kriptografskim mehanizmima se realizuju i po čemu se razlikuju od *hash* funkcija?
2. Šta su *replay* napadi i kako izbegavamo te napade? Navedite elementarni primer lažnog predstavljanja korišćenjem *replay* napada.
3. Koje parametre treba uzeti u obzir prilikom dizajna algoritma koji koristi *Feistel* strukturu i na koji način promena svakog od parametara utiče na algoritam? Objasniti kako ovi parametri izgledaju u *DES* algoritmu.
4. Nacrtati i objasniti *EBC* i *OFB* modove funkcionisanja blok algoritama. Kada se koristi *EBC*, a kada *OFB*? Koja je razlika između ova dva moda?
5. Objasniti *RSA* algoritam za šifrovanje pomoću javnog ključa. Opisati način formiranja privatnog i javnog ključa, kao i postupak prilikom šifrovanja, odnosno dešifrovanja ovim algoritmom. Šifrovati poruku M=2, koristeći javni ključ PU={11, 91}. Za izračunavanje šifrovane vrednosti koristiti algoritam za brzu eksponentizaciju.

Napomene: Na kolokvijumu nisu dozvoljena nikakva pomoćna sredstva, ni kalkulatori ni literatura. Kolokvijum traje 120 minuta.