Drugi kolokvijum iz Zaštite podataka (SI4ZP, IR4ZP) *26.04.2014.*

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. Kod *Diffie-Hellman* algoritma korisnik A ima na raspolaganju globalne javne elemente: q=113 i α=101. Od korisnika B je dobio njegovu javnu vrednost Y_B=99. Odabrati privatnu vrednost korisnika A tako da bude barem dvocifrena i izračunati zajedničku tajnu vrednost na strani korisnika A. Zatim šifrovati dobijenu zajedničku tajnu vrednost korišćenjem *RSA* algoritma i javnog ključa korisnika C: PU={17, 187}. Kod svih izračunavanja izraza sa eksponentima koristiti algoritam za brzu eksponentizaciju.
3. Nacrtati i objasniti postupak prilikom generisanja i prilikom prijema *PGP* poruke uz ostvarivanje tajnosti i autentikacije i uz korišćenje prstenova ključeva. Zanemariti kompresiju i konverziju.

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