Kolokvijum iz Zaštite podataka (MS1ZP) *26.04.2014.*

1. Navedite kakav bi izabrani originalni tekst koristili u napadu na *Vigenère* šifru da bi najbrže odredili ključ. Objasnite razlog za izbor takvog originalnog teksta.
2. Objasniti ulogu, osobine i zahteve kodova za autentikaciju poruka (*MAC* kodovi). Kojim kriptografskim mehanizmima se realizuju i po čemu se razlikuju od *hash* funkcija?
3. 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.
4. Čemu služe modovi funkcionisanja blok algoritama? Nacrtati i objasniti *OFB* mod funkcionisanja blok algoritama. Kada se koristi ovaj mod funkcionisanja? U čemu je razlika u odnosu na *CFB* mod funkcionisanja?
5. Kod *Diffie-Hellman* algoritma korisnik A ima na raspolaganju globalne javne elemente: q=107 i α=103. Od korisnika B je dobio njegovu javnu vrednost Y_B=44. 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.

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