

1. Objasniti napad koji onemogućava korišćenje *Double-DES* algoritma (*meet-in-the-middle*). Navesti ključne razloge zbog kojih *Triple-DES* algoritam nije ostao u upotrebi, već je zamenjen *AES* algoritmom.
2. Demonstrirati *man-in-the-middle* napad kod *Diffie-Hellman* protokola iz pozicije napadača za sledeću situaciju:
  - globalni javni elementi imaju vrednosti  $q=101$  i  $\alpha=18$ ,
  - od korisnika A presrećete njegovu javnu vrednost  $Y_A=47$ ,
  - od korisnika B presrećete njegovu javnu vrednost  $Y_B=90$ .Kod svih izračunavanja izraza sa eksponentima koristiti algoritam za brzu eksponentizaciju.
3. Objasniti razliku između tehnika distribucije javnih ključeva: kada se pristupa autoritetu za javne ključeve i kada se dobija sertifikat od sertifikacionog autoriteta. Objasniti prednosti i mane ova dva pristupa u praktičnoj primeni.
4. Zbog čega se koriste arbitrarni digitalni potpisi? Objasniti varijantu protokola kod arbitriranog digitalnog potpisivanja u kojoj se koristi simetrična enkripcija, a arbitar ne vidi poruku.

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