Drugi kolokvijum iz Zaštite podataka (13S114ZP, SI4ZP) *08.05.2016.*

1. Demonstrirati *man-in-the-middle* napad kod *Diffie-Hellman* protokola iz pozicije napadača za sledeću situaciju:

   - globalni javni elementi imaju vrednosti q=101 i α=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.

2. Zbog čega se koriste arbitrirani 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 90 minuta.