Nadoknada prvog kolokvijuma iz Zaštite podataka (SI4ZP, MS1ZP) 15.05.2010.

1. (**10 p**) Navesti osnovne kategorije sigurnosnih servisa prema X.800 standardu i opisati svaki od njih.

2. (**10 p**) Nacrtati šemu AES algoritma za veličinu ključa od 128 bita (2p). Objasniti strukturu jedne iteracije AES algoritma (2p). Objasniti svaku od faza iteracije (4p). Objasniti algoritam koji se koristi za ekspanziju ključa kod AES algoritma (2p).

3. (**10 p**)
   a) (5p) Nacrtati i objasniti kako izgleda CBC i CFB mod funkcionisanja, čemu služi i koje su prednosti i mane.
   b) (5p) Objasniti zbog čega nije upotrebljen 2DES da zameni DES, kada je veličina ključa postala suviše mala, već 3DES. Sa koliko različitih ključeva se može realizovati 3DES, kako i zbog čega su odabrane te varijante?

Trajanje kolokvijuma 90 minuta