Drugi kolokvijum iz Zaštite podataka (SI4ZP, MS1ZP) 15.05.2010.

1. (**9 p**) Dat je Needham-Shroeder protokol za sigurnu razmenu sesijskog ključa uz korišćenje nezavisnog autoriteta KDC i simetričnih algoritama enkripcije:

   1. $A \rightarrow KDC:$ $ID_A \,||\, ID_B \,||\, N_1$
   2. $KDC \rightarrow A:$ $E_{Ka}[K_s \,||\, ID_B \,||\, N_1 \,||\, E_{Kb}[K_s||ID_A]\ ]$
   3. $A \rightarrow B:$ $E_{Kb}[K_s||ID_A]$
   4. $B \rightarrow A:$ $E_{Ks}[N_2]$
   5. $A \rightarrow B:$ $E_{Ks}[f(N_2)]$

   U ovom protokolu N_x su slučajni brojevi, ID_x identifikatori učesnika u komunikaciji, E_k operacije kriptovanja simetričnim ključem, a K_S je sesijski ključ.
   Odgovoriti:
   a) (3 p) Koja je uloga slučajnih brojeva N_x u ovoj razmeni?
   b) (3 p) Koja je uloga poruka 4 i 5?
   c) (1 p) Kojim kriptografskim mehanizmom može da se realizuje funkcija *f* u poruci 5?
   d) (2 p) Kakav problem može da izazove napadač C koji bi snimio i ponovio poruku 3 i poslao je ka B i kako bi takav napad mogao da se spreči?

2. (**6 p**) X.509 sertifikati: a) (3 p) detaljno opisati sigurnosni mehanizam kojim sertifikaciono telo garantuje autentičnost podataka u sertifikatu. b) (3 p) Šta je sve potrebno da uradi učesnik u komunikaciji A koji je dobio poruku potpisanu privatnim ključem učesnika u komunikaciji B kako bi se uverio u autentičnost porekla poruke. Oba učesnika u komunikaciji imaju sertifikate potpisane od strane sertifikacionog tela CA kome veruju.

3. (**7 p**) Objasniti čemu služi i kako se koristi Diffie-Hellman algoritam (4 p). Napisati dokaz da algoritam funkcioniše (2 p). Koja je razlika između Diffie-Hellman i RSA algoritma (1 p)?

4. (**8 p**) Koje su funkcije S/MIME protokola kojim se postižu tajnost i autentikacija (2p)? Koji su koraci za pripremu podataka kada se želi tajnost podataka (2 p)? Kako izgleda i čemu služi zahtev za registraciju kod S/MIME protokola (2 p)? Koja šema se koristi u S/MIME protokolu za obradu sertifikata (2 p)?

Trajanje kolokvijuma 90 minuta