Prvi kolokvijum iz Zaštite podataka (MS1ZP) *05.05.2012.*

1. Objasnite *Hillovu* šifru. Pretpostavimo da engleski tekst ima jako puno reči *the* i da je broj linearnih jednačina 3. Da li bi u tom slučaju na osnovu statistike bila olakšana kriptoanaliza i zašto?
2. Navedite sve korake *Needham-Schroeder* protokola. Navedite detaljno zbog čega je moralo da se uvodi poboljšanje protokola. Objasnite poboljšanje koje je uveo *Neumann*. Zašto neko, ko se u prvom koraku lažno predstavi (npr. učesnik C se predstavi kao učesnik A), ne može da se lažno autentikuje u slučaju poboljšanja koje je uveo *Neumann*?
3. Nacrtati strukturnu šemu *AES* algoritma za veličinu ključa od 128 bita i objasniti način funkcionisanja algoritma prilikom šifrovanja. Objasniti strukturu jedne iteracije *AES* algoritma. Objasniti svaku od faza iteracije. Objasniti algoritam koji se koristi za ekspanziju ključa kod *AES* algoritma.
4. Nacrtati i objasniti *CBC* i *CFB* modove funkcionisanja blok algoritama. Kada se koristi *CBC*, a kada *CFB*? Koja je razlika između ova dva moda?
5. Objasniti čemu služi i kako se koristi *Diffie-Hellman* algoritam. Napisati dokaz da algoritam funkcioniše. Kako se izvodi *man-in-the-middle* napad i kako ga je moguće sprečiti kod *Diffie-Hellman* algoritma?

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