Prvi kolokvijum iz Zaštite podataka (SI4ZP, MS1ZP) *28.03.2010.* *Kolokvijum traje 90 minuta*

1. (10) Poruku „*zastita podataka*“ šifrovati Vigenère algoritmom sa autokey poboljšanjem i ključem: *kljuc*. Diskutovati zašto je uvedeno autokey poboljšanje. Napomena: koristiti 26 slova engleske abecede.

2. (15) Dopuniti dizajn, nacrtati strukturu i jednu iteraciju simetričnog blok algoritma zaštite, koji primenjuje dizajn *Feistel* algoritma. Algoritam ima sledeće parametre:
    a. veličina bloka = 16 bita,
    b. veličina ključa = 8 bita,
    c. broj iteracija = 2,
    d. funkcija za generisanje podključa:
        - K_1 = K XOR 01101010b,
        - K_2 = K_1 XOR 00110010b,
    e. funkcija iteracije:
        - prvi korak: XOR sa ključem iteracije,
        - drugi korak: 2 S-box zamene posebno za po 4 bita rezultata prvog koraka (S-box proizvoljan).

    Korišćenjem ovakvog algoritma šifrovati podatak AF0Bh, pomoću ključa CDh. Da li je kod ovog algoritma postignut efekat lavine? Objasniti.
3. (5)
    a. (1) Kako se kod simetričnih algoritama zaštite sve mogu generisati ključevi?
    b. (2) Koja je razlika između centralizovane i decentralizovane distribucije ključeva?
    c. (2) Kako izgleda ECB mod funkcionisanja, čemu služi i koje su prednosti i mane?