Prvi kolokvijum iz Zaštite podataka (SI4ZP, IR4ZP) *23.03.2013.*

1. Koja je suštinska razlika između *Vernamove* šifre i *One time pad* šifre primenjene na binarne podatke. Ako je na dve poruke iste dužine primenjen isti ključ kod *One time pad* algoritma i dođe se do originalnog teksta jedne od te dve poruke, da li je moguće otkriti drugu poruku i kako?
2. Projektovati simetrični blok algoritam zaštite zasnovan na *Feistel* strukturi. Veličina blokova za šifrovanje treba da bude 8b, veličina ključa 6b, broj iteracija 1. Kao funkciju iteracije treba upotrebiti funkciju iteracije iz *DES* algoritma sa modifikacijom da postoji samo jedna S-box zamena (umesto osam S-box tabela, koristi se samo jedna). Ne postoji funkcija za generisanje ključeva iteracije, već se originalni ključ koristi kao ključ iteracije. Konkretne tablice za permutaciju i substituciju usvojiti proizvoljno. Nacrtati šemu projektovanog algoritma, ispisati usvojene tablice, šifrovati podatak 10100001 koristeći ključ 110011, a zatim dobijeni šifrovani blok dešifrovati istim ključem.
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.

Napomene: Na kolokvijumu nisu dozvoljena nikakva pomoćna sredstva, ni kalkulatori ni literatura. Kolokvijum traje 90 minuta.