1. DAA (*Digital Authentication Algorithm*) je standard kojim se kreira MAC (*Message Authentication Code*) korišćenjem DES-CBC mehanizma simetričnog kriptovanja.
    a. (*3 poena*) Objasniti zajedničke osobine i razlike MAC i hash funkcija. Za koje primene se koriste MAC, a za koje hash funkcije?
    b. (*3 poena*) Objasniti mane DAA algoritma. Posebno detaljno objasniti kako može da se formira poruka M1 koja će dati istu vrednost MAC kao i neka poruka M, ako se do poruke M1 koja daje identičnu MAC vrednost kao poruka M dolazi lako (kraće od pretrage grubom silom).
    c. (*4 poena*) Na koji način je u okviru CMAC modifikovan DAA algoritam kako bi se prethodno navedeni problem rešio?
2. (*5 poena*) Skicirati proces dekodovanja poruke upotrebom DES algoritama i OFB moda funkcionisanja (bez detalja DES algoritma). Ukratko objasniti prednosti ovog moda u odnosu na CFB kao i sličnosti sa Counter modom funkcionisanja.
3. (5 poena) U sistemu koji koristi šifrovanje pomoću javnog ključa, korišćenjem RSA algoritma, presreli ste šifrovanu poruku C = 8 poslatu korisniku čiji je javni ključ e = 13 i n = 51. Koja je vrednost originalne poruke M? U čemu je propust koji je omogućio pronalaženje M?
4. (*10 poena*) Navesti i objasniti razlike između kriptografije sa javnim ključem i tradicionalne kriptografije sa tajnim ključem? Skicirati šemu koja prikazuje na koji način je moguće ostvariti autentikaciju poruke koristeći kriptografiju sa javnim ključem. Skicirati šemu koja prikazuje na koji način je moguće ostvariti autentikaciju poruke koristeći tradicionalnu kriptografiju sa tajnim ključem. Uporediti skicirane pristupe.
5. (*10 poena*) Posmatra se ćirilični *Playfair* algoritam koji koristi matricu 5x6. Prikazati postupak dekriptovanja poruke *ОЗМЕЖАУЛМОЛИЛПНХОЦ* koristeći ključ *КОЛОКВИЈУМ*. Pretpostaviti da je slovo za razdvajanje para ponovljenih slova prilikom šifrovanja bilo slovo *Х*. Da li biste kriptoanalizom uspeli da dešifrujete poruku? Obrazložiti odgovor.

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