1. (K)(**10p**) Polialfabetske substitucione šifre – osobine i razlog uvođenja. Posebno analizirajte *Vigenère* šifru i prodiskutujte uticaj dužine ključa na sigurnost.

2. (K)(**10p**) Šta su *replay* napadi i kako izbegavamo te napade? Navedite elementarni primer lažnog predstavljanja korišćenjem *replay* napada.

3. (K)(**10p**) Nacrtati strukturnu šemu *DES* algoritma i objasniti način funkcionisanja algoritma prilikom šifrovanja. Detaljno objasniti kako izgleda jedna iteracija i kako se od ključa prave ključevi iteracije.

4. (K)(**10p**) Čemu služe modovi funkcionisanja blok algoritama? Nacrtati i objasniti *ECB* i *OFB* modove funkcionisanja blok algoritama. Kada se koristi *ECB*, a kada *OFB*? Koja je razlika između ova dva moda?

5. (K)(**10p**) Objasniti *RSA* algoritam za šifrovanje pomoću javnog ključa. Opisati način formiranja privatnog i javnog ključa, kao i postupak prilikom šifrovanja, odnosno dešifrovanja ovim algoritmom. Šifrovati poruku M=10, koristeći javni ključ PU={23, 91}. Za izračunavanje šifrovane vrednosti koristiti algoritam za brzu eksponentizaciju.

---

1. (I)(**10p**) Navedite poruke u *Kerberos* verziji 4. Pokušajte da objasnite zašto je potrebno da postoji puno *timestamp*-ova (5) i *lifetime*-a (2)?

2. (I)(**10p**) Detaljno objasniti mehanizam duplog potpisa kod SET sistema za finansijske transakcije. Šta se postiže korišćenjem ovog mehanizma?

3. (I)(**10p**) Koje funkcije se koriste u *S/MIME* za obezbeđivanje tajnosti, autentikacije (razmatrati obe varijante autentikacije) i tajnosti i autentikacije? Objasniti na koji način se vrši osiguravanje *MIME* entiteta u slučaju da želimo da postignemo tajnost. Objasniti na koji način se vrši osiguravanje *MIME* entiteta u slučaju da želimo da postignemo autentikaciju (razmatrati obe varijante autentikacije).

4. (I)(**10p**) Prikazati strukturu virusa koristeći pseudokod. Koje su to faze kroz koje tipičan virus prolazi i šta se dešava u svakoj od faza?

5. (I)(**10p**) Koje tri klase uljeza postoje? Opisati kratko svaku od njih. Za svaku klasu uljeza navesti koji pristup detekcije upada može detektovati upade iz te klase i objasniti zašto.

Napomena: Na ispitu nisu dozvoljena nikakva pomoćna sredstva, ni kalkulatori ni literatura. Potrebno je na svesci naznačiti ukoliko želite da Vam se poeni sa prvog kolokvijuma računaju umesto zadataka označenih sa K. Ispit traje 180 minuta.