Ispit iz zaštite podataka (SI4ZP, MS1ZP) 21.06.2010.

1. (**K2**)(**9p**) Dat je mehanizam za autorizaciju korisnika C za korišćenje servisa V korišćenjem simetričnih algoritama kriptovanja:
   (1) $C \rightarrow AS: ID_C||ID_{tgs}$
   (2) $AS \rightarrow C: E(K_c, Ticket_{tgs})$
   (3) $C \rightarrow TGS: ID_C||ID_V||Ticket_{tgs}$
   (4) $TGS \rightarrow C: Ticket_v$
   (5) $C \rightarrow V: ID_C||Ticket_v$

   Gde je: $Ticket_{tgs} = E(K_{tgs}, [ID_C||AD_C||ID_{tgs}||TS_1||Lifetime_1])$,
   $Ticket_v = E(K_v, [ID_C||AD_C||ID_v||TS_2||Lifetime_2])$, E(x,y) označava funkciju kriptovanja poruke y simetričnim algoritmom sa ključem x, AD su mrežne adrese uređaja, TS su vremena generisanja poruka, Lifetime vremena trajanja poruka, a || označava konkatenaciju delova poruka.
   a) (**4p**) Objasniti na koji način bi potencijalni napadač ponavljanjem poruka (3) ili (5) mogao da dobije pristup resursima servisa V.
   b) (**5p**) Objasniti na koji način ova vrsta napada može da se spreči (Kerberos v4 šema).

2. (**K2**)(**6p**) Objasniti ulogu, osobine i zahteve kodova za autentikaciju poruka (MAC kodovi). Kojim kriptografskim mehanizmima se realizuju i po čemu se razlikuju od hash funkcija?

3. (**K2**)(**6p**) Na koji način kod *RSA* algoritma veličina ključa utiče na veličinu bloka za šifrovanje? Kako se kod *RSA* algoritma formira par javni i privatni ključ i kako se koriste za šifrovanje, odnosno dešifrovanje? Na čemu se zasniva sigurnost *RSA* algoritma?

4. (**K2**)(**9p**) Nacrtati i objasniti postupak prilikom generisanja i prilikom prijema PGP (*Pretty Good Privacy*) poruke uz ostvarivanje tajnosti i autentikacije i uz korišćenje prstenova ključeva. Zanemariti kompresiju i konverziju. Koja je uloga prstenova ključeva kod PGP protokola? Koji mehanizam se koristi za upravljanje ključevima kod PGP protokola i na koji način se koriste prstenovi ključeva, kao podrška za taj mehanizam? Kako se izračunava legitimitet ključa?

---

5. (**K3**)(**10p**) Detaljno objasniti mehanizam duplog potpisa kod SET sistema za finansijske transakcije. Šta se postiže korišćenjem ovog mehanizma?

6. (**K3**)(**10p**) Objasniti koja je razlika između običnih i "stateful" paketskih filtera. Koju vrstu napada koju ne mogu da spreče obični filteri mogu da spreče „stateful"?

7. (**K3**)(**10p**) Šta su to zapisi osluškivanja (*audit records*) i koja je razlika između izvornih zapisa osluškivanja i zapisa osluškivanja specifičnih za detekciju? Kako funkcioniše detekcija upada u sistem zasnovana na identifikaciji penetracije (*penetration identification*)? Šta je cilj sistema za detekciju upada (šta takav sistem treba da ispuni da bi bio od koristi)?

Trajanje ispita 3 sata