Prezime, Ime	JMBAG

Bodovi
/50

Napredni operacijski sustavi — Završni ispit

1. srpnja 2021.

1. (6 boda ukupno) Kriptosustavi i sigurnosni protokoli.

   (a) (0.5) Na čemu se temelji sigurnost kriptosustava RSA?

   (b) (1) Navedite dva načina kriptiranja blokova kod kojih se pogreška u kriptiranom tekstu propagira na sljedeći blok čistog teksta.

   (c) (1) Razmatramo Diffie-Hellmanov postupak. Je li par (p, g) modula $p = 8$ i generatora $g = 3$ korektan? Obrazložite.

   (d) (2) Razmatramo raspodijelu ključeva u zatvorenom simetričnom kriptosustavu prema Needhamu i Schroederu. Hoće li sigurnost kriptosustava biti narušena ako za unaprijed dogovorenu funkciju F iskoristimo funkciju identiteta $F(x) = x$? Obrazložite.

   (e) (1.5) Od čega se sastoji čvor Kerberos poslužitelja?

2. (4 boda ukupno) Skicirajte protokol jednostrane autentifikacije uz pomoć certifikata, navedite sadržaj svih poruka i značenje svih simbola koje koristite.
   Rješenje:

3. (5 bodova ukupno) Pretpostavimo da je riječ o kriptosustavu RSA (bez nadopunjavanja i sažetka) s javnim ključem $pk = (3, 55)$ i privatnim ključem $sk = (27, 55)$.

   (a) (1) $\varphi(N) =$

   (b) (1) Pokažite da je par (sk, pk) javnog i privatnog ključa korektan.

   (c) (1) Odredite enkripciju poruke „2” (poruka je broj 2).

   (d) (2) Odredite dekripciju poruke „5” (poruka je broj 5) koristeći algoritam uzastopnog kvadriranja. Obavezno navesti postupak. *Rješenje:*

4. (4 boda ukupno) Funkcije za izračunavanje sažetka i nadopunjavanje.

   (a) (2) Objasnite na jednom primjeru zašto je kriptosustav RSA bez nadopunjavanja nesiguran.

   (b) (1) U čemu se razlikuje izračunavanje funkcija sažetka SHA-0 i SHA-1?

   (c) (1) Na koji način se provjerava RSA digitalni potpis σ poruke m pomoću javnog ključa (e, N) ako se prilikom potpisivanja koristi funkcija sažetka SHA256.

5. (4 boda ukupno) Neka su H_1 i H_2 dvije funkcije sažetka. Želimo izgraditi novu funkciju sažetka koja će biti sigurna čak i ako se pokaže da jedna od funkcija H_1 i H_2 nije. Funkciju sažetka H gradimo tako da samo spojimo izlaz obje funkcije sažetka:

$$H_3(M) = H_1(M) \parallel H_2(M).$$

   Funkciju sažetka H_4 gradimo tako da ulaz podijelimo na pola, svakom funkcijom obradimo pola ulaza i spojimo izlaz:

$$H_4(M_1 \parallel M_2) = H_1(M_1) \parallel H_1(M_2).$$

   (a) (2) Ako je jedna od funkcija H_1 i H_2 otporna na kolizije, je li posljedično i funkcija H_3 otporna na koliziije? Obrazložite.

(b) (2) Ako je jedna od funkcija H_1 i H_2 otporna na kolizije, je li posljedično i funkcija H_4 otporna na koliziije? Obrazložite.

6. (8 bodova ukupno) Komunikacija između procesa.

   (a) (2.5) Nabrojite 5 načina komuniciranja između procesa na istom računalu.

   (b) (2) Proces P_i šalje zahtjev za ulazak u kritični odsječak procesu P_j protokolom Ricart-Agrawal. Definirajte poruku zahtjev koju prima i poruku odgovor koju proces P_j šalje.
   Zahtjev: Odgovor:

   (c) (0.5) Navesti najmanji mogući broj diskova u sustavu RAID 10:

   (d) (3) Između sustava RAID 10 i RAID 0+1, koji je pouzdaniji i zašto?

7. (4 bodova ukupno, *postupak obavezno navesti na košuljici*). Međusobno isključivanje u raspodijeljenim sustavima. Neki sustav sastoji se od 6 čvorova i u svakom čvoru nalazi se po jedan proces. Niti jedan od procesa P_1, P_2, P_3, P_4, P_5 i P_6 do trenutka t_1 nije zaželio ući u kritični odsječak. Sinkronizacija procesa odvija se prema pravilima **protokola Ricarta i Agrawala**. Između t_1 i t_2 svaki od procesa P_i uđe i izađe iz kritičnog odsječka i puta (proces P_1 jednaput, P_2 dvaput, P_3 triput, itd.).

   (a) (1) Koliko je ukupno poruka razaslano u intervalu (t_1, t_2)?

   (b) (3) Za svaki proces navesti **tip i broj** poruka koje su razaslali te **tip i broj** poruke koje su primili u (t_1, t_2).
   Proces P_1 je primio: i poslao: .
   Proces P_2 je primio: i poslao: .
   Proces P_3 je primio: i poslao: .
   Proces P_4 je primio: i poslao: .
   Proces P_5 je primio: i poslao: .
   Proces P_6 je primio: i poslao: .

8. (5 bodova ukupno, *postupak obavezno navesti na košuljici.*) Neka se višediskovni sustav sastoji od N istovrsnih diskova. Koliki može biti najveći N ako srednje vrijeme do pojave kvara u sustavu mora biti barem 4 godine? Za svaki disk zadano je srednje vrijeme do pojave kvara $MTTF = 20$ godina i srednje vrijeme popravka $MTTR = 5$ dana. Pretpostavimo da je sustav neispravan ako se dogodi

   (a) (4) dvostruki kvar.

   (b) (1) jednostruki kvar.

9. (10 bodova ukupno) Višediskovni zalihosni spremnici.
Za ostvarenje višediskovnog zalihosnog sustava RAID 5 na raspolaganju je 6 istovrsnih diskova svaki po 2TB.

(a) (1) RAID 5 sustav ulazi u kvarno stanje ako se dogodi kvar (zaokružiti jedan ili više točnih odgovora):
   a) jednog diska.
   b) dva diska.
   c) tri diska.
   d) četiri diska.
   e) svih raspoloživih diskova.

(b) (1) Skicirati RAID 5 sustav s raspoloživim diskovima, te istaknuti redundatne dijelove pojasa.
Rješenje:

(c) (1) Ukupan kapacitet raspoloživih diskova sastavljenih u RAID 5 sustav iznosi _____ TB, od kojih _____ TB otpada na korisne podatke, _____ TB na redundantne podatke.

(d) (3) Skicirati Markovljev lanac za takav višediskovni RAID 5 sustav. Svi diskovi imaju konstantne brzine kvarenja i popravljanja. Markovljev lanac neka se sastoji od potrebnog broja stanja gdje oznaka stanja odgovara broju neispravnih komponenti, npr. (0) sve komponente su ispravne, (1) jedna neispravna, (2) dvije neispravne itd. te (K) kvarno stanje. Naznačiti vjerojatnosti prijelaska iz stanja u stanje kao i vjerojatnost ostanka u istom stanju. Zanemariti vjerojatnosti da se u nekom trenutku odjednom pokvare ili poprave dvije ili više komponenti.
Rješenje:

(e) (3) Postaviti sustav diferencijalnih jednadžbi za navedeni sustav i navesti početne vrijednosti vjerojatnosti.
$p_0'(t) =$ _____, $p_0(0) =$ _____,
$p_1'(t) =$ _____, $p_1(0) =$ _____,
$p_2'(t) =$ _____, $p_2(0) =$ _____,
$p_3'(t) =$ _____, $p_3(0) =$ _____.

(f) (1) Navesti izraze za raspoloživost $A_s(t)$ i neraspoloživost $Q_s(t)$ navedenog sustava.
$A_s(t) =$ _____, $Q_s(t) =$ _____.