Prezime, Ime	JMBAG

Bodovi
/30

Napredni operacijski sustavi — Međuispit

29. travnja 2021.

1. (5 boda ukupno) Komunikacija između ~~protokola~~ procesa.
   (a) (0.5) Prema čemu procesi znaju da je poruka upućena njima?
   (b) (0.5) Mogu li već stvoreni procesi međusobno komunicirati preko neimenovanih cjevovoda?
   (c) (2) Napišite redom sustavske pozive koji se koriste u postupku povezivanja cjevovoda na standarni ulaz.
   (d) (0.5) Koja je posljedica kvara centralnog čvora u centraliziranom protokolu?
   (e) (1) Nakon kojih karakterističnih događaja će se povećati vrijednost logičkog sata procesa u protokolu Ricart-Agrawala?
   (f) (0.5) Koliki je ukupni broj poruka u sustavu s N. čvorova kada proces želi ući u kritični odsječak, a komunikacija između procesa je putem protokola Ricart-Agrawal?

2. (5 boda ukupno) Protokol Ricart-Agrawal.
   U sustavu se nalaze tri čvora i na svakom čvoru po jedan proces P_1, P_2 i P_3 koji imaju u svojim lokalnim logičkim satovima vrijednosti $C_1 = 6$, $C_2 = 12$ i $C_3 = 6$ gdje je C_i lokalni logički sat procesa P_i. Sinkronizacija procesa odvija se prema pravilima protokola Ricarta i Agrawala. Svi procesi žele ući u kritični odsječak.
   (a) (1.5) Skicirati protokol.
   (b) (0.5) Kojim redoslijedom su procesi ulazili u kritični odsječak?
   (c) (3) Koje su sve moguće vrijednosti lokalnih logičkih satova na kraju?

3. (5 bodova ukupno) Lamportov raspodijeljeni protokol.
   Neki sustav sastoji se od 4 čvora i u svakom čvoru nalazi se po jedan proces. Niti jedan od procesa P_1, P_2, P_3 i P_4 do trenutka t_1 nije zaželio ući u kritični odsječak. Sinkronizacija procesa odvija se prema pravilima Lamprotovog raspodijeljenog protokola. 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, itd.).

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

(b) (4) Za svaki proces navesti broj poruka koje su razaslali te broj poruke koje su primili u intervalu (t_1, t_2).

4. (3 boda ukupno) Sigurnosni zahtjevi, kriptosustav jednokratne bilježnice, DES i 3DES.

(a) (0.5) Kako asimetričnim kriptosustavom osiguravamo neporecivost?

(b) (0.5) Možemo li simetričnim kriptosustavom osigurati neporecivost? Ukratko obrazložite.

(c) (0.5) Koristimo kriptosustav jednokratne bilježnice (one-time padding). Za jasni tekst $P = 1001$ i skriveni (kriptirani) tekst $C = 1100$ izračunajte ključ K.

(d) (0.5) Navedite barem dva nedostatka kriptosustava jednokratne bilježnice.

(e) (0.5) Definirajte funkciju kriptiranja kriptosustava 3DES za jasni tekst P i ključeve K_i, $i \in \{1, 2, 3\}$.

(f) (0.5) Kada je funkcija kriptiranja kriptosustava 3DES jednaka funkciji kriptiranja kriptosustava DES?

5. (4 bodova ukupno) Kriptosustav AES.

(a) (1) Navedite dva načina kriptiranja u kojima kriptirani tekst ne ovisi o prethodnim blokovima skrivenog teksta.

(b) (0.5) Kako nazivamo strukturu unutar koje su definirane AES funkcije zbrajanja i množenja bajtova bloka?

(c) (2.5) Pretpostavimo da kriptiramo dva toka podataka koristeći „Output Feedback" (OFB) tako da u oba toka iskoristimo isti inicijalizacijski vektor (IV). Neka je prvi kriptirani blok jasnog teksta prvog toka $C_1 = (\texttt{10 39 23 3C 26})_{Hex}$ i neka je prvi kriptirani blok jasnog teksta drugog toka $C_2 = (\texttt{19 3C 23 30 26})_{Hex}$. Ako napadač zna da je jedan od blokova jasnog teksta prvog ili drugog toka jednak $M = (\texttt{45 6C 76 69 73})_{Hex} \in \{M_1, M_2\}$ (ne zna je li M_1 ili M_2), što time može zaključiti o bloku jasnog teksta drugog toka podataka $M' \in \{M_1, M_2\}, M' \neq M$? Napadaču je na raspolaganju sljedeća tablica.

ASCII Char	Binary	Hex	ASCII Char	Binary	Hex
E	01000101	45	NUL	00000000	00
l	01101100	6C	FF	00001100	0C
v	01110110	76	DLE	00010000	10
i	01101001	69	9	00111001	39
s	01110011	73	#	00100011	23
L	01001100	4C	<	00111100	3C
HT	00001001	09	&	00100110	26
ENQ	00000101	05	EM	00011001	19
0	00110000	30			

Zbog greške, u tablici nije navedeno slovo "e" pa su se priznavala rješenja bez istog.

6. (5 bodova ukupno) Kriptosustav RSA.

   (a) ~~(0.5)~~ (1) Kako je definirana Eulerova funkcija φ?

   (b) (1) Neka je $N = p * q$ umožak dva prosta broja. Može li javni eksponent $e \in \mathbb{Z}^*_{\varphi(N)}$ biti paran broj? Ukratko obrazložite.

   (c) Pretpostavimo da je riječ o kriptosustavu RSA (bez nadopunjavanja i sažetka) s javnim ključem $pk = (5, 65)$ i privatnim ključem $sk = (29, 65)$.

      (1) (0.5) Izračunajte $\varphi(N)$.

      (2) (0.5) Pokažite da je par (sk, pk) javnog i privatnog ključa korektan.

      (3) (0.5) Odredite enkripciju jasnog teksta „4".

      (4) (1.5) Odredite dekripciju skrivenog teksta „17" koristeći algoritam uzastopnog kvadriranja. Obavezno napišite postupak.

7. (3 boda ukupno) Sustav digitalnog potpisa.

   (a) (1) Definirajte sustav digitalnog potpisa.

   (b) (0.5) Navedite sigurnosna svojstva koja pruža sustav digitalnog potpisa.

   (c) (1) Jednim primjerom pokažite zašto kriptosustav RSA bez nadopunjavanja i funkcije sažetka nije siguran sustav digitalnog potpisa. Označite sve simbole koje koristite.

(d) (0.5) Zašto je u kriptosustavu RSA, u praksi, provjera potpisa znatno brža od potpisivanja? Ukratko obrazložite.