RAČUNALNIŠKE KOMUNIKACIJE 2023/24

Ime in priimek: _____

3. izpit, 27. 8. 2024

Vpisna številka: _____

Literatura (npr. zapiski, prosojnice, knjige) ni dovoljena. Dovoljen je preprost kalkulator.
Nalogo rešujte v za to predviden prostor. Podpišite se na vse liste, ki jih oddate.
Na vprašanja odgovarjajte kratko (največ 2 povedi), daljši odgovori štejejo 0 točk.
Odgovori na vprašanja morajo biti utemeljeni. Čas pisanja je 70 minut.

izpolni ocenjevalec

SKUPAJ	

1. Denimo, da uporabljamo kvadratno modulacijo z 10 faznimi koti. Najmanj koliko različnih nivojev amplitude potrebujemo, če želimo kodirati zaporedja 6 bitov? Koliko kombinacij faznih kotov in amplitud ostane neizkoriščenih?

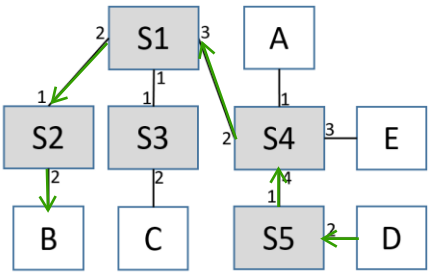
   10 * x = 2^6 = 64
   x = 7 (zaokrožujemo navzgor)

   70 - 64 = 6 neuporabljenih

2. Naštej tri družine protokolov, ki se uporabljajo za dostop do medija na povezavni plasti? Za vsako od teh treh družin navedi 2 konkretna primera protokolov

   delitev kanala: TDMA, FDMA
   navključni dostop: ALOHA, CSMA
   izmenični dostop: FDDI, Token Ring

3. Podan je sistem omrežnih stikal (S1 – S5) in vmesnikov (A – E), kot je prikazano na sliki. Ob stikalih so podane tudi številke njihovih posameznih vrat. Ob začetku so v stikalih naslednji zapisi:



   - stikalo S1: D/3, A/3
   - stikalo S2: B/2
   - stikalo S3: B/1
   - stikalo S4: D/3, B/2
   - stikalo S5: /

   V nekem trenutku pošlje pošiljatelj D okvir prejemniku B. Za vsako stikalo zapiši (1) njegovo novo vsebino stikalne tabele po pošiljanju in (2) katero akcijo izvede po prejemu okvirja.

   - stikalo S1: [D/3, A/3] flood
   - stikalo S2: [B/2, D/1] posreduj na vrata 2
   - stikalo S3: [B/1, D/1] posreduj na vrata 1
   - stikalo S4: [D/4, B/2] posreduj na vrata 2
   - stikalo S5: [D/2], flood

4. Pošiljatelj uporablja protokol TCP, ki samodejno nastavlja dolžino čakalnega intervala za čakanje na potrditve. Pri tem uporablja nastavitvi α=0,5 in β=0,5. Velja, da je IzmerjeniRTT[1]=OcenjeniRTT[1]=20 ms in DevRTT[1]=0. Na koliko se poveča čakalni interval, če naslednja meritev RTT znaša 40 ms?

   OcenjeniRTT[i] = 1/2 OcenjeniRTT[i-1] + 1/2 IzmerjeniRTT[i]
   DevRTT[i] = 1/2 DevRTT[i-1] + 1/2 |IzmerjeniRTT[i]-OcenjeniRTT[i]|
   ČakalniInterval[i] = OcenjeniRTT[i] + 4*DevRTT[i]

   IzmerjeniRTT[1]=OcenjeniRTT[1]=20
   DevRTT[1]=0
   ČakalniInterval[1] = 20ms + 4*0ms = 20ms

   IzmerjeniRTT[2] = 40ms
   OcenjeniRTT[2] = 1/2 20ms + 1/2 40ms = 30ms
   DevRTT[2] = 1/2 0 + 1/2 |40-30| = 5ms
   ČakalniInterval[2] = 30ms + 4*5ms = 50ms

5. Ana pošilja Branetu kriptograme, ki jih je izračunala z algoritmom RSA. V komunikacijo se vrine napadalec, ki se želi polastiti Aninega zasebnega ključa. Po dolgem opazovanju komunikacije med Ano in Branetom, je napadalec uspel ugotoviti, da sta Anina ključa tvorjena s parametri: p=6, n=18 in e=7. Določi najnižjo možno vrednost Aninega zasebnega ključa. Zapiši obe komponenti tega ključa.

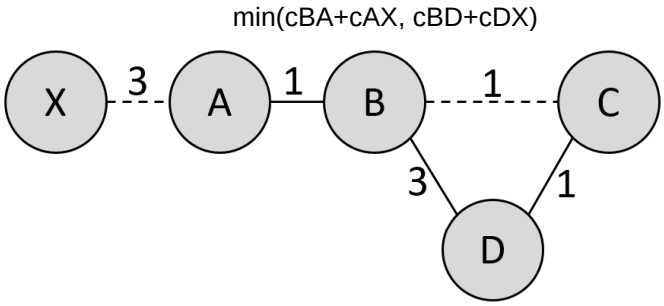
   privatni ključ je (n, d)
   n = pq =>
   q = n/p = 18/6 = 3
   z = (p-1)(q-1) = 5*2 = 10

   d mora biti tak da je edmodz=1
   e = 7
   7dmod10 = 1
   7d = 10k+1 => iščemo najmanjši k da je 10k+1 deljivo z 7

   k=0 => 1
   k=1 => 11
   k=2 => 21 / 7 = 3 nice

   torej je d = 3, ključ je (18, 3)

6. V omrežju imamo 5 usmerjevalnikov (A, B, C, D in X), ki uporabljajo usmerjanje z vektorji razdalj na podlagi cen, ki so podane na grafu na desni sliki. Usmerjevalniki imajo ob začetku opazovanja v posredovalnih tabelah naučene takšne ocene razdalj do **usmerjevalnika X**, kot je to zapisano v prvi vrstici tabele. Nato se povezavi A-X in B-C prekineta (narisano črtkano na sliki). Zapiši vrednosti ocenjenih cen povezav do usmerjevalnika X v naslednjih dveh iteracijah. V primeru enake cene preko dveh sosedov, izberi tistega, katerega oznaka je prej po abecedi. Pri tem naj bodo zapisi <u>jasno podprti z računskimi postopki</u>.



	ocenjene cene do usmerjevalnika X			
iteracija \ usmerjevalnik	**A**	**B**	**C**	**D**
začetno stanje	1/X	4/C	4/D	3/C
prekinitev povezav A-X in B-C				
nove vrednosti ocenjenih cen, 1. iteracija	1+4 = 5/B	min(1+1, 4+3) = 2/A	min(1+3) = 4/D	min(3+4, 1+4) = 5/C
2. iteracija	1+2 = 3/B	min(1+5, 3+5) = 6/A	1+5 = 6/D	min(3+2, 1+4) = 5/B

7. Podan je bločni kriptosistem nad bloki dolžine 3 bitov, ki ima ključ, ki je podan v desni tabeli. Izračunaj prve štiri kriptograme ponavljajočega čistopisa 111, če se uporablja verižno kriptiranje blokov z inicializacijskim vektorjem 101.

ključ kriptosistema	
000	010
001	000
010	100
011	011
100	111
101	110
110	001
111	101

m = 111 111 111 111
IV = c(0) = 101
c[i] = K(m[i] XOR c[i-1])

c[1] = K(111 XOR 101) = K(010) = 100
c[2] = K(111 XOR 100) = K(011) = 011
c[3] = K(111 XOR 011) = K(100) = 111
c[4] = K(111 XOR 111) = K(000) = 010

8. Na kratko odgovori na naslednja vprašanja:

A. Kje pri napadu DOS Smurf napadalec uporabi tehniko ponarejanja IP naslova (IP spoofing)?

Napadalec pošilja ICMP request pakete z ponarejenim IP naslovom (IP-jem žrtve), in potem botovi vsi naenkrat odgovarjajo na ta sporočila žrtvi in jo preplavijo

B. Katere kriptografske algoritme in/ali ključe potrebuje pošiljatelj za pripravo lastnega digitalnega podpisa?

Potrebuje zgoščevalno funkcijo in asimetrično kriptografijo npr. RSA, zasebni ključ za podpis, javni za distribucijo

C. Kako pri sodobni simetrični kriptografiji (npr. pri TLS/SSL) rešujemo problem distribucije ključev?

Simetrične ključe zakodiramo z asimetrično kriptografijo npr. RSA

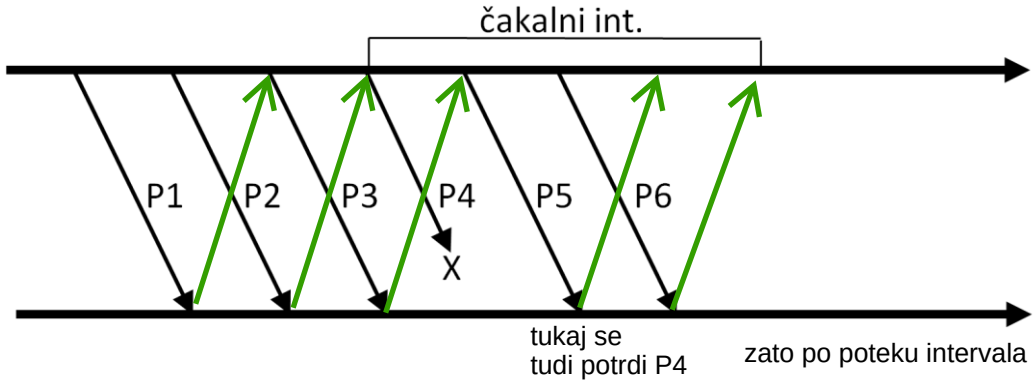
D. Kako ukrepa sistem za preprečevanje vdorov (IPS) ob zaznavi napada?

Ne vem, zavrže sumljive pakete, zapre sumljive zveze?

E. S kakšno metodo varovanja (principom varne komunikacije) preprečimo zanikanje komunikacije?

Ne vem kaj to pomeni. Ali misle na Preprečevanje zanikanja komunikacije (“Si res prejel, si res poslal?”) iz učbenika?

9. Pošiljatelj in prejemnik uporabljata protokol za potrjevanje s ponavljanjem N nepotrjenih (go-back-N). Pošiljateljevo okno je veliko 4 pakete. Na spodnji diagram doriši:
   - potrditve s strani prejemnika,
   - pošiljateljevo akcijo po preteku čakalnega intervala.



10. Za prenos izbrane datoteke, ki je sestavljena iz petih kosov (chunks) C1 - C5, uporabimo protokol BitTorrent. Pri izmenjavi datoteke sodeluje sedem odjemalcev S1 - S7, od katerih je vsak sosed (neighbor) vsem preostalim. Sosedje imajo takšno začetno razpoložljivost koščkov, kot ga prikazujejo vrednosti 0 v spodnji tabeli (vrednost "0" pomeni: košček je na razpolago že na začetku). Izmenjava naj poteka v iteracijah, ki so enako dolge. Na vsaki iteraciji lahko vsak sosed PREJME natanko en košček, razen če že ima vse koščke. Med prejemanjem lahko vsak tudi istočasno POŠILJA neomejeno število koščkov. Če sosed izbira med več enako ustreznimi koščki kot kandidati za prenos, naj izbere tistega, ki ima manjšo oznako koščka (torej npr. C3 pred C5). Spodnjo tabelo dopolni tako, da za vsakega soseda in košček izbereš, na kateri iteraciji izmenjave se bo prenesel. Vrednost 0 pri tem pomeni začetno razpoložljivost, vrednost 1 pomeni 1. iteracijo itd.

princip rarest first
prioritete po iteracijah:
1) C5, C2, C1, C4, C3
2) C2, C1, C4, C3
3) C1, C3, C4
4) C3, C4
5) C4

	C1	C2	C3	C4	C5
S1	0	2	0	0	1
S2	2	0	3	0	1
S3	3	2	0	0	1
S4	3	2	4	5	1
S5	1	0	0	2	0
S6	0	2	0	0	1
S7	0	2	0	3	1