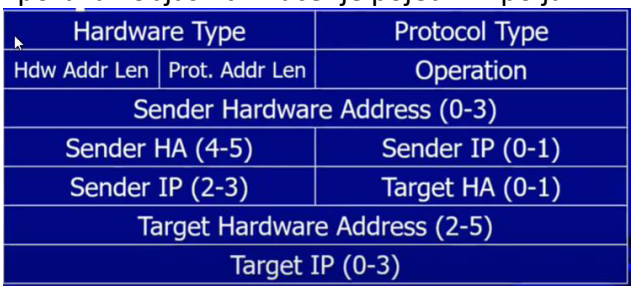
PITANJA SA PRETHODNIH BLANKETA IZ RM
(u zagradi su ponavljanja)

1. Navedeni iskazi označavaju protokol ili pojam ili mehanizam koji se koristi u računarskim mrežama. Označiti kako se zove protokol/mehanizam/pojam koji odgovara navedenom iskazu:
   a) Sprečava gubitak podataka zato što je bafer prijemnika pun - **Postavljanje window size na 0**
   b) Koristi se za raportiranje o greškama i slanje upita u IP baziranim mrežama - **ICMP**
   c)Vrši retransmisiju TCP segmenta pre isteka timeout-a - **Brza retransmisija**
   d) podela IP paketa na manje delove koji se reasembluju u odredištu - **fragmentacija**
   e)Transportni protokol koji se koristi za slanje DNS upita i odgovora - **UDP**
   f) Obavlja prevodjenje IP adresa u adrese data link nivoa - **ARP**
   g) Distribuirani servis koji obavlja preslikavanje imena hosta u IP adresu - **DNS**
   h) protokol rutiranja kod koga je oznaka za beskonačno 16 - **RIP**
   i) Koristi ga HTTP za pouzdani prenos podataka - **SSL**

2. Da bi povezali racunar na internet, potrebno je da definišete 4 parametra. Koji su to parametri i koja je njihova svrha?
   - IP adresa - sluzi za identifikaciju hosta u mrezi
   - Maska - pokazuje kojoj podmrezi host pripada
   - DNS server - prevodi ime hosta u IP adresu
   - Default gateway - host preko njega komunicira sa drugim mrezama
3. Objasniti specijalne IP adrese.
   - 0.0.0.0 host tvrdi da je to njegova adresa dok mu se ne dodeli adresa. Moze i da oznacava sve IPv4 adrese.
   - adresa koja ima sve nule na mreznim pozicijama oznacava hosta na toj mrezi
   - 255.255.255.255 je broadcast na lokalnoj mrezi
   - adresa koja ima sve jedinice na pozicijama hosta je broadcast na udaljenoj mrezi
   - adrese koje pocinju sa 127 su loopback adrese i koriste se za testiranje mreznih aplikacija.
4. Ukratko objasniti razlike izmedju port adrese, logičke adrese i fizičke adrese.
   - Fizicka adresa (MAC adresa) je adresa vezana za hardversku mreznu komponentu, koristi se na data link nivou. Logicke adrese su IP adrese, nisu povezane sa hardverom, koriste se za identifikaciju na mreznom nivou. Port adresa se koristi da identifikuje odredjeni proces na nekom hostu.
5. Objasniti zašto se kontrolna suma u zaglavlju IP paketa mora ponovo određivati pri svakom prolasku kroz ruter. (1)
   - TTL (Time to live) tajmer se smanjuje pri svakom prolasku kroz ruter, tako da se i vrednost checksum-a menja.
6. Ukratko objasniti šta je NAT i kako funkcioniše. (2)
   - NAT omogucava da lokalna mreza koristi samo jednu IP adresu sto se tice spoljnjeg sveta. NAT ruter odlaznim datagramima menja izvorisnu IP adresu i broj porta i postavlja NAT IP adresu i novi broj porta, u tabeli transliranja pamti translaciju koju je obavio. Za dolazne datagrame pronalazi u tabeli transliranja odgovarajucu IP adresu i port i postavlja njih umesto NAT IP adrese i porta koji su u datagramu.
7. Šta je ICMP i čemu služi?
   - ICMP je Internet Control Message Protocol. To je upravljacki protokol, sluzi za raportiranje o greskama i slanje upita, ali ne i korigovanje gresaka.

8. Kada polje TTL u IP paketu dostigne vrednost 0, koja ICMP poruka će biti poslata izvornom hostu:
   a) destination-unreachable, **b) time-exceeded** , c) parametar-problem, d) ništa od navedenog

9. Kolika je veličina ICMP poruka: a) 16B, b) 32B, c)8B, **d)ništa od navedenog**
   - velicina zaglavlja je 8B
   -sve poruke su razlicite velicine i formata. TO ONA KAZE
10. RIP protokol koristi nekoliko časovnika (tajmera). Koji su to časovnici i čemu služe.
    - **Period timer** - pomocu njega se odredjuje kada ce biti sledeca razmena paketa, to je random vrednost izmedju 25 i 35 sekundi
    - **Expiration timer** - kada za neku destinaciju ne stigne nijedna poruka u roku od 180 sekundi, ona postaje nevalidna i brojac skokova se postavlja na 16.
    - **Garbage Collector timer** - kada informacija za neku destinaciju postane nevalidna, ruter jos 120 sekundi saopstava da mu je broj skokova do te destinacije 16. Kada brojac dostigne vrednost 0, destinacija se brise iz tabele rutiranja.
11. Objasniti rad ARP protokola. (2)
    - ARP protokol omogucava preslikavanje IP adresa u adrese data link nivoa. Radi tako sto kada je potrebna fizicka adresa nekog rutera, ARP salje broadcast na lokalnoj mrezi sa pitanjem cija je data IP adresa, host cija je ta IP adresa odgovorice sa svojom fizickom adresom. Rezultat se kesira, da ukoliko uskoro opet kontaktira isti host nema potrebe za ponovnim broadcast-om.
12. Ko obavlja preslikavanje logičkog imena hosta u IP adresu? Ko obavlja preslikavanje IP adresa u fizičke adrese. Gde se ovi protokoli nalaze u protokol steku? (2)
    - Preslikavanje logickog imena u IP adresu radi DNS server. IP adrese u fizicku adresu radi ARP. DNS se nalazi na aplikativnom nivou, ARP se nalazi ispod IP protokola.
13. Objasniti kako se uz pomoć ARP ostvaruje preslikavanje IP adrese u fizičke adrese.
    ?? isto ko 11. ??
14. Nacrtati format ARP poruka i objasniti značenje pojedinih polja.



Hardware Type – govori o tome kog tipa je MAC adresa(u slucaju etherneta uvek se u ovom polju nalazi 0001)
Protocol Type – govori iz koje logicke adrese se obavlja preslikavanje(za ip protocol uvek je vrednost 0800)
Hdw Addr Len – koliko je dugacka fizicka adresa
Prot. Addr Len – koliko je dugacka logicka adresa
Operation – govori da li je u pitanju upit(0001) ili odgovor(0002)
Sender Hardware Address – hardverska adresa izvora(onog ko salje ARP zahtev)
Target Hardware Address – mac adresa odredista
Target IP – IP adresa odredista.

15. Objasniti rad DHCP protokola.
    - DHCP protokol sluzi za dinamicku dodelu adresa hostovima. Host prvo salje DHCPDISCOVEER poruku, koja za adresu odredista ima 255.255.255.255 a za adresu izvora 0.0.0.0. Ako se u lokalnoj mrezi nalazi DHCP server on obradjuje zahtev, ako se nalazi DHCP agent on prosledjuje poruku serveru. Nakon sto server dobije poruku salje hostu DHCPOFFER poruku, u kojoj se nalazi IP adresa, subnet maska, adresa gateway rutera i vreme vazenja dodeljene adrese. Klijent moze dobiti vise ponuda, bira jednu i odgovara sa DHCPREQUEST porukom u kojoj se nalaze podaci koje je

dobio u ponudi. Server odgovara sa DHCPACK, tako potvrdjuje parametre i oni se vezuju za dati host.

16. Pretpostavimo da IP paket koji nosi HTTP zahtev iz lokalne mreze ka internetu ide preko NAT rutera. Navesti koja će se sve polja u TCP i IP zaglavlju poslatog paketa NAT rutera morati promeniti. Obrazložiti odgovor. (1)

- NAT ruter ce zameniti privatne izvorisne IP adrese javnom NAT adresom koju ta mreza koristi za komunikaciju sa spoljasnjim svetom.

17. Host sa adresom 131.15.46.59 obavlja broadcast u lokajnoj mreži. Koja će adresa biti u polju adresa odredišta u zaglavlju IP datagrama:

a) 131.15.46.255,
b) 131.15.255.255,
c) 255.255.255.255,
d) ništa od navedenog. (1)

18. Koja od sledećih IP adresa ne može da se dodeli hostu ako se koristi subnet maska 255.255.254.0? (3 odgovora)

a) 113.10.4.0
b) 186.54.3.0
c) 175.33.3.255
d) 26.35.2.255
e) 152.135.7.0
f) 17.35.36.0

a) Ne moze jer je to adresa mreze.
b) Moze jer je adresa mreze 186.54.2.0 i maska je /23 znaci ima 2^9 = 512 hosta
c) Ne moze jer je to broadcast adresa mreze 175.33.2.0
d) Moze jer je adresa mreze 26.35.2.0 ima 512 hosta znaci da je izmedju 26.35.2.0 i 26.35.3.255 sto je broadcast.
e) Moze jer je adresa mreze 152.135.6.0 ima 512 hosta znaci da je izmedju 152.135.6.0 i 152.135.7.255 sto je broadcast.
f) Ne moze jer je to adresa te mreze.

19. Ako je IP adresa oblika 200.23.30.14/20 koja je adresa mreže?

200.23.00011110.00001110
32 – 20 = 12 bita za hostove
200.23.0001/0000.00000000 => 200.23.16.0

20. Šta je od dole navedeneog broadcast IP adresa:

a) IP adresa hosta koji šalje broadcast poruku,
b) IP adresa u kojoj su svi bitovi host adrese postavljeni na 0,
c) IP adresa u kojoj su svi bitovi mrežnog dela adrese postavljeni na 1,
d) IP adresa u kojoj su svi bitovi host adrese postavljeni na 1,
e) IP adresa u kojoj je poslednji bajt postavljen na 255.

21. Šta od sledeceg nije deo IP datagrama?

a) Fragment ofset,
b) identifikator paketa,
c) Tip servisa,
d) TTL,
e) Ethernet adresa odredista,
f) Duzina zaglavlja.

22. Klasa IP adresa se može odrediti na osnovu:

a) prvih 8bitova,
b) prva 3 bajta,
c) poslednjih 8 bitova,
d) prva tri bita,
e) prva 4 bita,
f) mrežne maske.

23. Objasniti razliku izmedju welcome soketa i connection soketa.

- Welcome soket je soket na serverskoj strani koji sluzi da ga klijent kontaktira ("pokuca na vrata") kada zeli da uspostavi konekciju. Connection soket je takodje soket na serverskoj strani, on se kreira nakon sto klijent kontaktira welcome soket i preko njega se vrsi razmena poruka.

24. Navesti primitive pomoću kojih se uspostavlja konekcioni transportni servis.

- LISTEN – server izvrsava. Server se blokira dok se ne pojhavi klijent.
CONNECT – klient izvrsava
SEND
RECEIVE
DISCONNECT – Raskidanje veze, bilo koja strana moze izvrsiti ovu primitivu.

25. Objasniti uspostavljenje veze izmedju klijenata i servera na transportnom nivou ako se koristi TCP protokol.

- Aplikativni proces u klijentu obavestava TCP sw da zeli da uspostavi konekciju sa serverom, TCP sw na klijentskoj strani salje specijalni TCP segment serveru. Server odgovara slanjem drugog specijalnog segmenta, nakon toga klijent odgovara trecim specijalnim segmentom. Prva dva segmenta ne sadrze podatke sa aplikativnog nivoa, a treci moze da ih ima. Ova procedura se zove three-way handshake procedura.
Kada se TCP konekcija uspostavi aplikativni procesi mogu da razmenjuju poiruke.

- Da bi se uspostavila veza potrebno je da klijent kontaktira server, a da bi to mogao da uradi potrebno je da je server aktivan, tj. da ima kreiran welcome soket koji klijent moze da kontaktira. Klijent kontaktira server tako sto kreira svoj soket i navodi ime servera ili njegovu IP adresu i broj port. Nakon kreiranja soketa, TCP sw na klijentskoj strani inicira three-way handshake proceduru. U toku three-way handshake procedure server kreira konekcioni soket preko koga razmenjuje poruke sa klijentom.

26. Čemu služe brojevi portova? Zašto se koriste dva broja porta u zaglavlju TCP (UDP) protokola?

- Brojevi portova sluze za identifikaciju procesa. Brojevi porta se koriste da prate trag razlicitih konverzacija kroz mrezu u isto vreme. DP je broj odredisnog porta, a SP broj izvornog porta. Koriste se dva porta zato sto se na hostu moze izvrsavati vise procesa istog tipa, pa samo broj porta aplikacije nije dovoljan da se identifikuje proces.

27. Koji je prvi TCP segment koji može sadržati podatke sa aplikativnog nivoa?

- Treci specijalni segment koji klijent salje serveru.

28. Kako se obavlja numeracija segmenata kod TCP? (1)

- TCP implicitno numerise bajtove, segmenti dobijaju redni broj jednak prvom bajtu u tom segmentu.

29. Navesti koji se segmenti razmenjuju kod uspostavljanja TCP veze.

- Kod uspostavljanja veze se razmenjuju tri specijalna segmenta. Prvi salje klijent serveru i bit SYN je postavlje na 1, a ACK na 0. Drugi salje server klijentu, ukoliko prihvata konekciju SYN=1 i ACK=1, ako odbija konekciju RST=1. Treci salje klijent serveru ako dobije potvrdu konekcije i u njemu je SYN postavljen na 0. Prva dva ne sadrze podatke sa aplikativnog nivoa, treci moze da ih ima.

30. Šta radi TCP prijemnik kada primi segment van očekivanog rednog broja?

- Salje se duplikat prethodnog ACK-a i ukazuje na broj ocekivanog segmenta. Nije definisano sta radi sa segmentima koji su primljeni van reda, postoje dve mogucnosti. Prva je da odbaci sve segmente koji su primljeni van redosleda, to je lakse za programiranje, ali je lose za propusnost mreze. Druga opcija se cesce koristi, to je da zapamti segment koji je primljen van redosleda dok se ne popuni praznina, ona je teza za programiranje, ali je efikasnija.

31. Objasniti brzu retransmisiju kod TCP. (3)

- Kod brze retransmisije nakon sto izvor dobije 3 puta ACK za istu poruku, pretpostavi da se sledeca poruka izgubila i radi retransmisiju i pre nego sto istekne timeout.

32. Da li TCP koristi selektivnu retransmisiju ili go-back-N? Obrazložiti odgovor. (1)

- TCP je hibrid, ne potvrdjuje segmente primljenje van redosleda, vrsi retransmisiju samo segmenata za koje je istekao timeout.

33. Ko obavlja preslikavanje logičkog imena hosta u IP adresu? Ko obavlja preslikavanje IP adresa u fizičke adrese. Gde se ovi protokoli nalaze u protokol steku? (2)

- DNS. ARP. DNS se nalazi u aplikativnom nivou, a ARP u mreznom ispod IP-a.

34. Kako se obavlja kontrola zagušenja kod TCP? (3)

- Zagusenje se detektuje kada se prime 3 ACK-a sa istim rednim brojem ili kada istekne timeout. TCP obavlja kontrolu zagusenja tako sto podesava velicinu prozora u izvoru prema trenutnim mogucnostima mreze i odredista. Koristi dve vrednosti, prozor zagusenja (maksimalni broj segmenata koji mogu biti poslati a nepotvrdjeni) i prozor koji je odobrilo odrediste. Stvarna velicina prozora je uvek manja vrednost od te dve. Ako nema simptoma zagusenja prozor se postepeno i kontinualno povecava da bi se iskoristio trenutno raspoloziv kapacitet mreze. Kada se detektuje zagusenje dolazi do trenutnog i velikog smanjenja prozora.

35. Kako se obavlja kontrola toka kod TCP? (1)

- Obavlja se uz pomoc polja Window size u TCP zaglavlju. Window size odredjuje koliko bajtova moze biti poslato, pocev od poslednjeg potvrdjenog. Ukoliko se postavi na 0 kaze izvoru da privremeno prestane sa slanjem.

36. Šta je funkcija transportnog nivoa u TCP/IP protokol steku.

- Funkcija transportnog nivoa je da pruzi aplikativnim procesima konekcioni i bezkonekcioni servis. On obezbedjuje pouzdan komunikacioni kanal, multipleksiranje, demultipleksiranje, kontrolu gresaka, kotrolu toka, kotrolu zagusenja, full-duplex.

Osnovna funkcija je da poboljsa kvalitet usluga koje pruza mrezni nivo.
Zaduzen je za pouzdan prenos poruka sa aplikativnog nivoa.
Transportni nivo vrsi segmentiranje i reasembliranje poruka sa aplikativnog nivoa.
Vrsi multipleksiranje i demultipleksiranje poruka.
Obavlja kontrolu toka i kontrolu zagusenja.

37. Koji od navedenih protokola su primeri transportnih protokola u TCP/Ip protokolsteku?

a) Ethernet,
b) HTTP,
c) IP,
d) UDP,
e) SMTP,
f) TCP

38. Koji od sledećih protokola se bave pristupom prenosnom medijumu u TCP/IP?

a) Ethernet,
b) HTTP,
c) IP,
d) UDP,
e) SMTP,
f) TCP

39. Koja od sledecih tvrdnji se odnose na TCP protokol – tačno (T), netačno (N):

a) To je konekciono orijentisani protokol, **T**
b) pruža best effort uslugu, **N**
c) obezbedjuje je polu-duplex komunikaciju, **N**
d) To je protokol nivoa sesije, **N**
e) izmedju dva računara u jednom trenutku može postojati samo jedna TCP sesija, **N**
f) koristi piggybacking za potvrdjivanje, **T – REKLA JE NA TERMINU 9** pocetak
g) podržava do 256 portova, **N**
h) Koristi se da implementira IP protokol **N**

40. Koji tipovi servera imena (name server) postoje?

- lokalni name server
- root name server
- serveri vrsnih domena (TLD)
- autorizovani name serveri

41. Kako izgleda struktura zapisa u bazi servera imena (resource records)?

- (name, value, type, ttl)

42. Šta je DNS?

- DNS (Domen Name System) je distribuirana baza podataka, koristi veliki broj name servera koji su hijerarhijski uredjeni. Sluzi za preslikavanje imena hostova u IP adrese.

-DNS je protokol aplikativnog nivoa koji dozvoljava hostovima i name serverima da komuniciraju da bi obezbedili uslugu preslikavanja.
Usluge DNS koriste i drugi protokoli aplikativnog nivoa da bi preveli korisnicku adresu u IP adresu.

43. Dati format DNS zapisa i objasniti značenje pojedinih polja.

Zapisi u DNS bazi se zovu Resource Records (RR)
Svaki zapis sadrzi 4 polja:

RR format: `(name, value, type,ttl)`

Znacenje polja name i value zavisi od toga sta se nalazi u polju type.
Postoji vise tipova koji mogu da stoje u polju type a ovi su osnovni:

Type = A

name je ime hosta
value je IP adresa hosta
pr. (relay1.bar.foo.com, 45.37.93.126, A)

Type = NS

name je domen (npr. foo.com)
value je ime autorizovanog DNS servera za ovaj domen
koristi se da prosledi DNS upit kroz lanac upita
pr. (foo.com, dns.foo.com, NS)

Type = CNAME

name je alias za neko "kanoničko" (realno) ime
value je kanoničko ime

Type = MX

name je domen
value je ime mail servera za taj domen
omogućava da se mail serverima obraća na osnovu aliasa
pr. (foo.com, mail.bar.foo.com, MX)

44. U čemu je razlika izmedju iterativnih i rekurzivnih DNS upita? (4)

Razlika je u tome sto kod rekurzivnih upita teziste razresenja je na kontaktiranom name serveru, a kod iterativnih upita uvek je teziste na lokalnom DNS serveru, i ovi upiti funkcionisu po principu „Ja ne znam ali pitaj ovoga mozda on zna"

45. Pretpostavimo da ste osnovali kompaniju SNOOPY i da zelite da je registrujete pod tim imenom ispod domena .rs. Ime vašeg autorizovanog servera imena (Name servera) je dnsl.snoopy.rs, mail servera mail.snoopy.rs i web servera www.snoopy.rs. Objasniti koje zapise je neophodno ubaciti u DNS bazu TLD servera za domen RS, a koje u autorizovani server dnsl.snoopy.rs da bi moglo da se iz spoljnjeg sveta pristupa vasem web serveru i mail serveru?

NE ZNAM DAL JE DOBRO PROVERITE

Zapisi za DNS bazu TLD:

(snoopy.rs, dns.snoopy.rs, NS)
(dns.snoopy.rs, 212.212.212.1, A)

Zapisi za autorizovani server dns.snoopy.rs:

Treba da se ubace zapisi tipa A koji kazu koje je ime naseg web servera i ip adresa, i zapis tipa MX koji kaze koje je ime mail servera za domen snoopy.rs i tip A(odnosno njegova IP adresa)

(snoopy.rs, mail.snoopy.rs, MX)
(www.snoopy.rs, nesto.snoopy.rs, CNAME)
(nesto.snoopy.rs, 140.14.14.14, A)

46. Pretpostavimo da želimo da promenimo IP adresu hosta gaia.cs.umass.edu sa 128.119.49.186 na 128.119.40.187 i da smo te promene zapamtili u autorizovanom DNS serveru za host gaia.cs.umass.edu. Da li će nakon što smo izvršili promene u autorizovanom DNS serveru sva buduća obraćanja hostu gaia.cs.umass.edu inicirana sa bilo kog hosta u Internetu biti poslata na IP adresu 128.119.40.187? Objasniti odgovor. (1)

OVO NIJE VALIDAN ODG NA PITANJE NEGO MOJE SKROMNO MISLJENJE.

Trebalo bi da sva buduca obracanja hostu gaia.cs.umass.edu inicirana sa hostova KOJI DO TADA NISU KONTAKTIRALI host gaia.cs.umass.edu budu poslata na ip adresu 128.119.40.187

E sad ovi koji su im prethodno pristupali imaju kesiranu ip adresu u svom lokalnom name serveru pa ce oni gaia.cs.umass.edu da traze na adresi 128.119.49.186. posto on vise nije na toj adresi mozda opet iniciraju pretragu preko root name servera ili se to resava na drugaciji nacin.

47. Objasniti razliku izmedju simetričnih i asimetričnih sistema za šifriranje.

Kod simetricnih sistema obe strane (i posiljac i primalac) koriste isti tajni kljuc. Posiljalac za sifriranje a primalac za desifriranje.

Kod asimetricnih sistema posiljalac i primalac koriste razlicite kljuceve. Kljuc za sifriranje moze biti javni, tj. Dostupan svima, dok je kljuc za desifriranje tajni(privatni). Javni i tajni kljuc cine par.

48. Pobrojati redom korake prilikom kreiranja digitalnog potpisa.

1. Hash funkcijom posaljilac racuna sazetak poruke koju salje.
2. Posaljilac sifrira svojim tajnim kljucem sazetak poruke i na taj nacin kreira digitalni potpis.
3. Zajedno sa originalnim dokumentom posaljilac salje i digitalni potpis.
4. Primalac dobija potpisanu poruku. Iz originalne poruke izracuna sazetak.
5. Primalac desifruje digitalni potpis javnim kljucem posaljioca i uporedjuje desifrovani sazetak sa onim koje je sam primalac izracunao.

49. Šta je funkcija sažetka (hash) i koje osobine ima? (1)

Hash funkcija H (funkcija sazetka) je jednosmerna funkcija koja ulazni niz proizvoljne duzine, poruku m, pretvara u niz fiksne duzine koji se naziva sazetak poruke h.

$$h = H(m)$$

Osobine:

- Iz dobijenog sazetka poruke h je nemoguce dobiti izvornu poruku m, zbog jednosmernosti funkcije sazetka, te je na taj nacin osiguran integritet poruke.
- Najmanja promena originalne poruke uzrokuje drasticne promene u njenom sazetku.
- Verovatnoca da se za dve razlicite poruke generise isti sazetak je jako mala.

50. Gde se SSL nalazi u protokl steku? Od kojih protokola se sastoji SSL protokol? (2)
SSL se u protokol steku nalazi izmedju sloja aplikacija i trasnportnog sloja. SSL se sastoji od 2 podprotokola:

- Protokol za uspostavljanje bezbedne konekcije
- Protokol koji koristi bezbednu konekciju za prenos podataka

51. Koja osobina RSA algoritma je ključna za kreiranje digitalnog potpisa?
Potrebna je da ima sledece osobine:
E(D(P)) = P i D(E(P)) = P, pri cemu je E javni kljuc za sifriranje a D tajni.

52. Ako par (e,n) čini javni ključ za šifriranje, a par (d,n) tajni ključ za dešifriranje kako se obavlja šifriranje i dešifriranje kod RSA algoritma?

1. Odabrati dva velika prosta broja p i q veca od 10^100.
2. Izvracunati n = pq i z = (p - 1)(q - 1);
3. Izabrati broj d koje je relativno prost u odnosu na z.
4. Naci e tako da vazi $(e \times d) \bmod z = 1$
5. Podeliti tekst koji treba da se sifrira na blokove velicine k bitova, pri cemu je k najveci ceo broj za koji vazi 2^k < n.
6. Sifrovana poruka se dobija na osnovu $C = P^e \bmod n$
7. Da bi se desifrovala poruka potrebno je izracunati $P = C^d \bmod n$

53. Ako par (e,n) čini javni ključ za šifriranje, a par (d,n) tajni ključ za dešifriranje. Koji od sledecih parova kljuceva moze iskoristiti u RSA (zanemarujucu cinjenicu da su vrednosti male):

a) (5,31) (11,31) – ne, zato sto n = 31 ne moze da se zapise kao n = p * q
b) (7,77) (43,77) – da, zato sto je n = 77 = 7*11, z = 6*10 = 60
pa je (e*d)mod z = (7 * 43)mod 60 = 1
c) (7,55) (41,55) – ne, zato sto je n = 55 = 5*11, z = 4*10 = 40
pa je (e*d)mod z = (7 * 41)mod 40 = 7

54. Pretpostavimo da Alisa i Bob koriste kriptografiju sa javnim ključem i svako od njih ima svoj par privatni/javni ključ. Alisin par ključeva je K_A^P i K_A^J, a Bobovi K_B^P i K_B^J. Alisa želi da pošalje poruku m Bobu tako da se može garantovati autentičnost poruke (tj. da ona zaista potiče od Alise), integritet i tajnost. Alisa šalje Bobu prouku koja je prvo šifrirana Bobovim javnim ključem K_B^J, a zatim Alisinim privatnim ključem K_A^P.

a) Da li ovaj prilaz obezbedjuje ostvarivanje bezbednosnih ciljeva koje je Alisa postavila?
b) Ako ne, šta je potrebno za modifikovati?
Prvo alisa sifrira svojim tajnim kljucem a zatim i bobovim javnim kljucem.

55. Ako Alisa želi da pošalje šifrovanu poruku Bobu, koji od dole navedenih ključeva će koristiti:

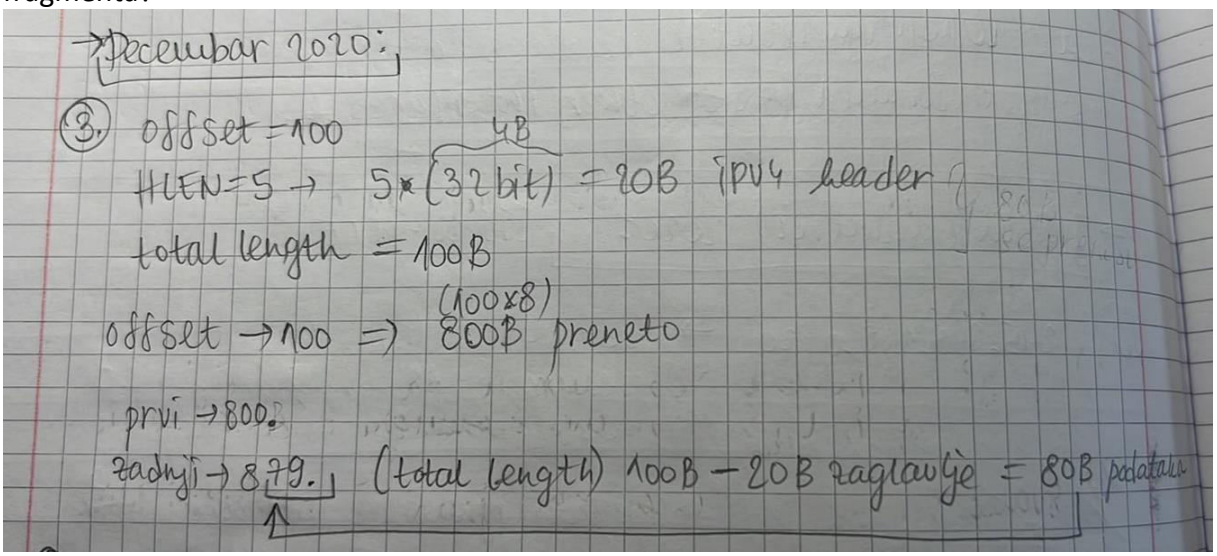
a) Alisin javni ključ
b) Alisin tajni (privatni) ključ
c) Bobov javni ključ
d) Bobov tajni (privatni) ključ

56. Ako Alisa želi da pošalje digitalno potpisanu poruku Bobu, koji od dole navedenih ključeva će koristiti:

a) Alisin javni ključ
b) Alisin tajni (privatni) ključ
c) Bobov javni ključ
d) Bobov tajni (privatni) ključ

NOVA PITANJA

1. Navesti bar 4 razlike izmedju TCP i UDP protokola.
    1. TCP je konekcioni servis, UDP je bezkonekcioni servis.
    2. TCP garantuje isporuku poruka po redosledu preko mehanizma potvrdjivanja i numeracije, UDP ne garantuje isporuku, ne koristi potvrdjivanje i numeraciju.
    3. Programima koji koriste TCP je garantovan pouzdan prenos dok kod programa koji kroriste UDP sami moraju voditi racuna o greskama.
    4. TCP je sporiji i podrzava samo point-to-point komunikaciju, UDP je brz moze podrzati point-to-point i point-to-multipoint komunikaciju(UDP je do 40% brzi nego TCP).
2. Koje su minimalne i maksimalne velicine zaglavlja kod TCP i Ipv4 protokola?
   Ipv4 i TCP: Min je 20 max je 60 (20 fiksno + 40 opciono).
3. Kada ruter generise ICMP poruke kome se one salju? Pored zaglavlja sta se jos u svakoj ICMP poruci nalazi?
   Poruke se salju hostu. Pored zaglavlja se nalazi polje podataka.
4. Pretpostavimo da host A salje dva TCP segmenta hostu B preko TCP konekcije. Prvi segment ima redni broj 90. drugi segment ima redni brojh 110. Koliko je podataka preneto u prvom segmentu?
   Preneto je u prvom segmentu 19 bajtova.
   Pretpostavimo da je prvi segment izgubljen a da je drugi stigao korektno u B. Koji broj ce biti u polju ack number u segmentu koji host B salje hostu A?
   U polju ack number bice 90.
5. Pristigao je IP paket u kome je vrednost u offset polju 100, u polju HLEN 5, a u polju ukupna duzina (total length) 100. Koji je redni broj prvog i poslednjeg bajta ovog fragmenta?



6. Pretpostavimo da grupa od 20 ljudi zeli medjusobno da komunicira. Svaki clan grupe treba da posalje tajnu poruku preostalim clanoviuma grupe. Sva komunikacija izmedju bilo koja dva clana grupe, p i q, je vidljiva svima osim clanovima grupe, ali ni jedan drugi clan grupe ne moze da otkrije sadrzaj poruke koja se razmenjuje izmedju p i q. Ako grupa odluci da koristi simetricnu kriptografiju sa tajnim kljucem za sifriranje, koliko je ukupno tajnih kljuceva u sistemu potrebno? Ako se koristi kriptografija sa javnim kljudcem, koliko ce kljuceva biti potrebno?
   (ISTI ZAD KAO SEPTEMBAR2019 samo sto je grupa od 10 ljudi)

7. Na transpornom nivou se koristi TCP protokol, verzija Reno. Veličina prozora zagušenja je u startu (trenutak T=1) jednaka 2 MSS (maximum segment size), a prag sporog starta 8 MSS.Pretpostavimo da je u trenutku T=5 nastupio time out. Kolika je veličina prozora zagušenja u trenutku T=10:
   (A) 8 MSS
   (B) 14 MSS
   (C) 7 MSS
   (D) 12 MSS

   Obrazloženje: U trenutku T=3 dostiže se prag sporog starta, pa nakon toga prozor zagušenja linearno raste. To znači da će u trenutku T=5 prozor zagušenja biti 10, a pošto tada nastupa time out, prozor zagušenja će se u sledećem trenutku postaviti na početnu vrednost, tj na 2, a nova vrednost praga sporog starta će biti polovina od trenutne vrednosti tj. 10/2 =5. U trenutku T=6 prozor zagušenja će biti 2, u T=7 će biti 4, u T=8 je premašen prag sporog starta pa se prozor povećava linearno, tj. ima vrednost 5, u T=9 biće 6, a u T=10 imaće vrednost 7.

8. Host A salje hostu B TCP segment enkapsuliran u IP datagramu. Kada host B primi datagram, kako mrezni nivo u hostu B zna da treba da prosledi segment TCP-u a ne UDP-u ili nekom drugom protokolu?
   Zaglavlje IP datagrama sadrzi u sebi polje protocol koje se koristi kada kompletan datagram stigne u odrediste i govori o tome kom protokolu trasnportnog nivoa je datagram namenjen. (TCP protocol = 6, UDP protocol = 17)
9. Hostovi A i B komuniciraju i na transportnom nivou koriste TCP protokol. Pretpostavimo da su nakon three-way-handshake procedure oba hosta krenula sa numeracijom svojih segmenata od nule. Pretpostavimo da su zaglavlja svih segmenata velicine 20byte. Neka se komunikacija izmedju A i B odvija na sledeci nacin:
   - A salje segment sa 20byte podataka
   - B odgovara slanjem segmenata sa 30byte podataka
   - B salje novi segment sa 40 byte podataka
   - A odgovara slanjem segmenta sa 50 byte podataka.

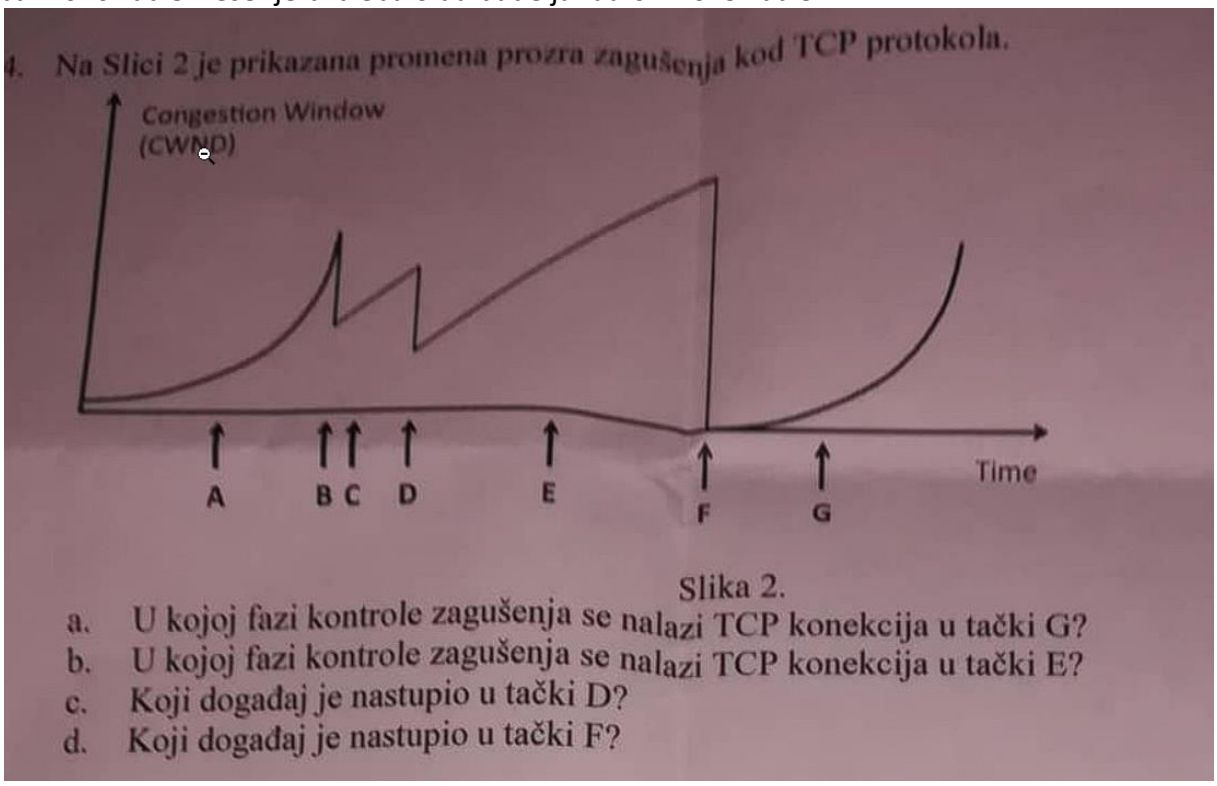
   Za svaki od poslatih segmenata navesti koje vrednosti ce se naci u poljima redni broj(sequence number) i redni broj potvrde(acknowledgement number).
   A sn = 0 ack = 0 -> B
   B sn = 0 ack = 20 -> A
   B sn = 30 ack = 20 -> A
   A sn = 20 ack = 70 -> B
10. Pretpostavimo da UDP prijemnik izracuna ceksumu za primljeni UDP segment i ustanovi da se ona slaze sa vrednoscu koja se nalazi u ceksum polju u primljenom segmentu. Moze li prijemnik biti potpuno siguran da nije nastupila ni jedna greska u toku prenosa? Objasniti odgovor. Da li bi stvari bile drugacije ako bi se koristio TCP?
    Pricala je za to.

11. Velicina adrese izvornog i odredisnog porta u TCP zaglavlju je, redom:
    a) 16-bitova i 32-bita
    b) 16-bitova i 16-bitova
    c) 32 bita I 16-bitova
    d) 32 bita i 32 bita
12. Ipv6 adrese mogu imati do __32__ hexadecimalnih cifra
    a) 16
    b) 32
    c) 8
    d) Nista od navedenog
13. Da bi proverio da li se moze pristupiti novopridodatom hostu 192.168.2.5, mrezni administrator je u komand promptu otkucao ping 192.168.2.5. Koji protokoli su korisceni tokom ovog testiranja:
    a) ARP
    b) RARP

c) DHCP
d) DNS
e) ICMP

14. Kolika je velicina zaglavlja kod Ipv6:
    a) Ista kao kod Ipv4
    b) Promenljiva
    c) 20 byte
    d) 40 byte
    e) 60 byte

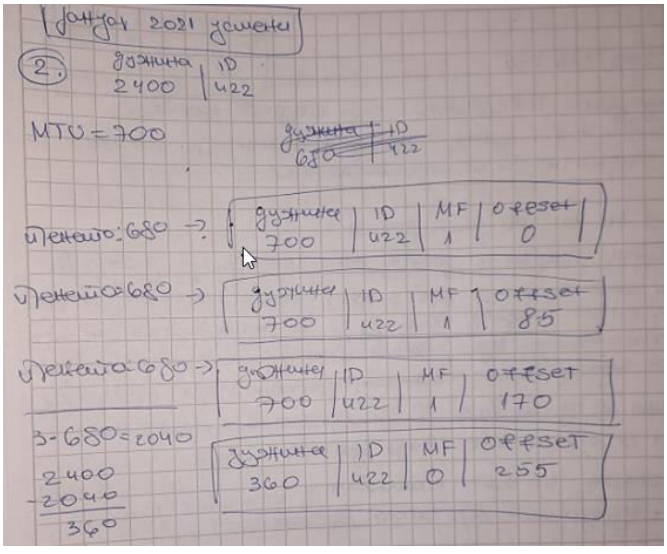
15. Jan2020 zad 5. resenje bi trebalo da bude januarski 2019 zad 5.



A i G – spori start.
C i E – kontinualni rast.
B i D – brza retransmisija.
F – timeout.

16. Potrebno je poslati datagram velicine 2400 byte preko linka cija je MTU 700 byte. Pretpostavimo da originalni datagram ima identifikator 422. Koliko fragmenta ce biti generisano? Koje vrednosti ce se naci u poljima identification number, fragment offset i MF bit u svakom fragmentu?

4 FRAGMENTA



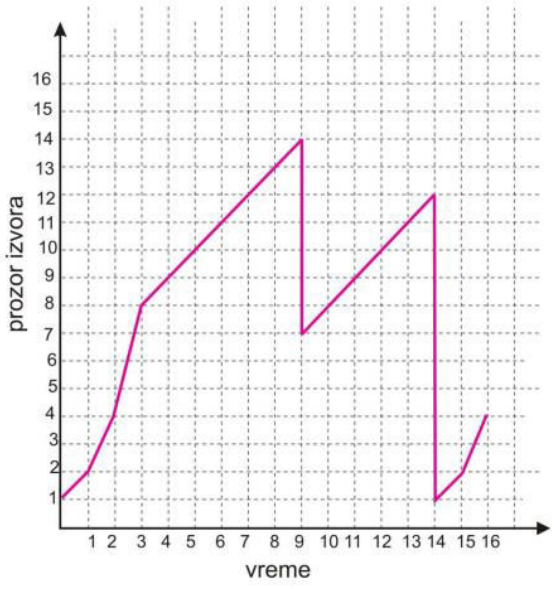
17. Pretpostavimo da je veličina datagrama koji se prenose između hosa A i hosta B ograničena na 1500 byte (uključujući i zaglavlje). Ako je veličina IP zaglavlja 20 byte, koliko datagrama je potrebno da bi se preneo MP3 fajl veličine 5 miliona byte? Prikazati računicu kojom se došlo do odgovora.

    U 1500 byte treba uključiti 20 byte IP zaglavlja i 20 byte TCP zaglavlja, tako da se broj datagrama dobija kao:
    5000000 / 1460 = 3425
    Svi datagrami, izuzev poslednjeg su veličine 1500 byte, a poslednji 960+40=1000byte.
    3424 su od po 1500 byte, 1460 * 3424 = 4 999 040, 5000000 – 4999040 = 960

18. Da li je checksum u TCP zaglavlju visak jer IP vec ima u svom zaglavlju checksumu?
    Checksum u IP zaglavlju predstavlja samo checksumu za zaglavlje (ne uključuje podatke), dok checksum u TCP zaglavlju predstavlja checksum-u za ceo segment. Zato checksum u TCP zaglavlju nije suvišna.
19. TCP obavlja kontrolu zagusenja tako sto menja velicinu prozora kada detektuje simptome zagusenja u mrezi. Kako se menja prozor kada u TCP izvor stignu tri duplikata istog ACK-a?
    Kod TCP tahoe cwnd = 1
    Kod TCP Reno cwnd = jedna polovina trenutnog cwnd-a
    Kako se menja prozor zagusenja kada u TCP izvoru nastupi timeout dogadjaj?
    Kod TCP tahoe cwnd = 1
    Kod TCP reno cwnd = 1
    Sta je razlog ponasanja TCP izora u ova dva dogadjaja?
    Sprecavanje zagusenja servera.

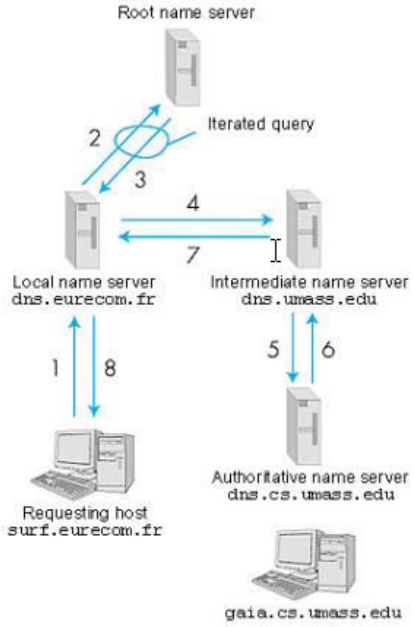
4. Nacrtati dijagram promene veličine prozora TCP izvora ako je inicijalno prag sporog starta postavljen na 8. Kada veličina prozora dostigne vrednost 14 u izvor pristignu tri duplikata ACK. Kasnije, kada veličina prozora izvora dostigne vrednost 12 nastupi time out.

Rešenje:



20.

5. U sledećem primeru izvršenja DNS protokola, navesti koji će se zapisi vratiti u odgovorima 3, 6, 7 i 8 kada host **surf.eurecom.fr** želi da pristupi hostu **gaia.cs.umass.edu**. Navesti tip zapisa i dati izgled odgovarajućih polja u zapisu. Kao oznaku **IP** adrese nekog hosta **A** pisati **IP(A).** Odgovor dati u obliku **(name, value, type)**



Rešenje:

Poruka 3:

(umas.edu, dns.umas.edu, NS)
(dns.umas.edu, IP(dns.umas.edu), A)

Poruka 6: (gaia.cs.umas.edu, IP(gaia.cs.umas.edu), A)

Poruka 7: (gaia.cs.umas.edu, IP(gaia.cs.umas.edu), A))

Poruka 8: (gaia.cs.umas.edu, IP(gaia.cs.umas.edu), A)

21.

22.