RK

Pisni izpit 27. 6. 2022

IME _____

PRIIMEK _____

VPISNA ŠT. _____

Pisni izpit traja 60 minut. Pišite kratko in jedrnato. Pripomočki niso dovoljeni, dovoljen je le preprost kalkulator.

1) (10) Na katero plast v TCP/IP modelu sodijo naslednje storitve (v tabelo zapišite **ime** plasti):

Storitev	Plast	Storitev	Plast
Modulacija		Aloha	
Bluetooth		Skype	
Porazdeljeno usmerjanje		Fragmentacija	
Nadzor zamašitev		WiFi	
SMTP		AIMD	

2) (20) Varnost:

a. za spodnje trditve označite, za kateri avtentikacijski protokol veljajo – v VSAKO polje tabele vpišite DA ali NE!

	Osnovni izziv-odgovor	Needham-Schroeder	PKI
Za avtentikacijo se uporablja simetrična kriptografija			
Za kriptiranje seje se uporablja simetrična kriptografija.			
Ranljivost za napad z zrcaljenjem			
Ana in Borut se avtenticirata z različnima ključema			
Ranljivost za napad s ponovitvijo seje (replay)			
Ranljivost za napad man in the middle			
Center preveri identiteto Ane ali Boruta			
Center generira sejni ključ			

b. Branko želi Angeli poslati zaupno sporočilo. Pomembno je, da se Angela lahko prepriča, da sporočilo res pošilja Branko in ne kdo drug. Kako naj Branko kriptira sporočilo, če se uporablja RSA?

i. Najprej s svojim javnim ključem, da zagotovi podpis, nato z Angelinim javnim ključem, da zagotovi zaupnost.

ii. Najprej s svojim tajnim ključem, da zagotovi podpis, nato z Angelinim javnim ključem, da zagotovi zaupnost.

iii. Najprej z Angelinim javnim ključem, da zagotovi zaupnost, nato s svojim javnim ključem, da zagotovi podpis.

iv. Najprej s svojim javnim ključem, da zagotovi zaupnost, nato z Angelinim tajnim ključem, da zagotovi podpis.

v. Najprej s svojim javnim ključem, da zagotovi podpis, nato z Angelinim javnim ključem, da zagotovi zaupnost.

vi. Najprej z Angelinim javnim ključem, da zagotovi zaupnost, nato s svojim tajnim ključem, da zagotovi podpis.

vii. Najprej z Angelinim tajnim ključem, da zagotovi zaupnost, nato s svojim tajnim ključem, da zagotovi podpis.

3) (20) Fragmentacija IPv4. IP datagram, dolg 2000 bytov, potuje po omrežju. Naleti na povezavo, kjer je MTU 1400 bytov, zato se fragmentira.
   a. Napišite dolžine nastalih fragmentov (telo + glava) in navedite njihov odmik.

   b. Nastali fragmenti potujejo naprej po omrežju. Denimo, da naletijo na povezavo, kjer znaša MTU 900 bytov. Ali se bo kateri od njih ponovno fragmentiral? Če da, zopet navedite dolžine nastalih fragmentov (glava + telo).

4) (20) TCP Potrjevanje. Katere od spodnjih trditev držijo? Za tiste, ki ne držijo, kratko pojasnite oziroma trditev spremenite tako, da bo držala.

   a. Če TCP segmentu s številko potrditve ACK 4440 sledi segment s številko potrditve 4442, to pomeni, da sta se vmes izgubili 2 potrditvi.

   b. Ko TCP oddajnik trikrat zapored sprejme segment s številko potrditve 4440, to pomeni, da je TCP prejemnik prejel tri kopije segmenta 4440.

   c. Če TCP oddajnik ne sprejme potrditve oddanih segmentov v pričakovanem času, zmanjša zamašitveno okno in s tem zmanjša tudi pretok podatkov.

   d. Če potrditve segmentov prihajajo k oddajniku tekoče in hitro, potem samo ena izjema, ki pride po dolgem času, ne bo vplivala na spremembo ocenjene vrednosti RTT.

   e. TCP prejemnik ne zna urejati segmentov v pravilen vrstni red, zato jih mora vedno dobiti v pravilnem zaporedju.

5) (20) Primerjajte ARP tabelo, stikalno tabelo in IP posredovalno tabelo tako, da izpolnite spodnjo tabelo.
   a. Opišite strukturo vsake od naštetih tabel – katere stolpce vsebuje
   b. Za vsako od njih navedite tipičen primer (scenarij), ko se v tabelo doda nova vrstica.

	Struktura (naštejte stolpce)	Kdaj se doda nova vrstica
ARP tabela		
Stikalna tabela		
IP posredovalna tabela		

6) (10) Izračunaj za omrežje **191.23.182.201/9**:
   a. Naslov omrežja

   b. Broadcast naslov

   c. Najnižji naslov

   d. Najvišji naslov

   e. Največje število naprav v tem omrežju: