2. kolokvij RKVB, VSS, FRI, 1. letnik, 29. 5. 2012

Ime: _____

Priimek: _____

RKVB Ljubljana

Vpisna številka: _____

*Pozorno preberite navodila! Literatura **ni** dovoljena. Odgovarjajte kratko (z eno, največ dvema povedima)! Čas pisanja je **45** minut. Naloge so enakovredne.*

1. Na katero plast po TCP/IP arhitekturnem modelu po svoji vsebini sodijo naslednje storitve in protokoli?

a) Kompresija podatkov	f) Rekurzivno poizvedovanje
b) IPsec	g) Trojna potrditev
c) Trojno rokovanje	h) Kerberos
d) SSL in TLS	i) Bluetooth
e) UDP	j) Nadzor zamašitev

2. Štirje odjemalci pošiljajo strežniku zahteve z naslednjimi lastnostmi:

	IP izvora	Št.vrat izvora	IP cilja	Št.vrat cilja
1	223.34.45.56	22345	223.34.56.78	12345
2	223.34.45.67	22355	223.34.56.78	12345
3	223.34.45.78	22365	223.34.56.78	23456
4	223.34.45.98	22365	223.34.56.78	23456
5	223.34.45.98	22365	223.34.56.78	12345
6	223.34.45.78	22365	223.34.56.78	23456

a) Koliko različnih vtičev je odprtih na strežniku, če se uporablja TCP?
b) Koliko različnih vtičev je odprtih na strežniku, če se uporablja UDP?
c) Katere od zgornjih zahtev pridejo do strežnika preko istega vtiča pri TCP in katere pri UDP?

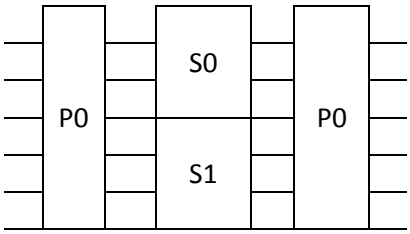
3. Kriptografske metode
a) Opišite, kako deluje trojni DES v primerjavi z enojnim DES.
b) Katera je najbolj očitna prednost in slabost trojnega DES-a v primerjavi z enojnim DES in AES?
c) Kako in zakaj uporabljamo kombinacijo simetrične in asimetrične kriptografije – zakaj ne samo eno od obeh?

4. Primerjajte prenos datoteke po elektronski pošti s prenosom datoteke prek protokola FTP.

5. Opišite napad na Diffie-Hellmanov protokol.

6. Nadzor zamašitev: uporabljamo najbolj osnovno različico TCP (Tahoe), ki ni optimizirana za zelo učinkovite prenose. Največja velikost segmenta (MSS) je 1000 bytov. Vsi poslani segmenti so velikosti 1000 bytov. V zaporednih časovnih intervalih (po en RTT) pošiljamo naslednje število segmentov: 1, 2, 4, 8, 16, 32, 33, 34, 35, 36, 18, 19, 20, 10, 11, 1, 2.
a) Kakšne težave so se najverjetneje dogajale na omrežju?
b) Kakšen je bil prag v 10. In kakšen v 11. časovnem intervalu?
c) Katere faze nadzora zamašitev prepoznate in v katerih zaporednih časovnih intervalih so se odvijale?
d) Kolikšen je bil povprečen pretok podatkov (v bit/s) v opazovanem scenariju, če vemo, da je RTT ves čas približno 50 ms?

7. Izračunajte kako se v spodnjem kriptosistemu zašifrira niz 111000. Kodirnika in dekodirnika v škatlah S0 in S1 sta enaka, delujeta pa v skladu s tabelo prikazano spodaj desno. P v S0 je (65730421), P v S1 je (17260354), P0 pa je (051243). *Prikažite tudi vmesne korake!*



000	2
001	5
010	7
011	4
100	1
101	0
110	3
111	6

0	000
1	101
2	010
3	111
4	001
5	110
6	011
7	100

8. Spodnji izpis prikazuje del odgovora, ki smo ga zajeli s programom Wireshark:

1. Za kateri protokol aplikacijske plasti gre?
2. Po kakšnem tipu zapisa smo spraševali strežnik? Kakšno storitev opravljajo strežniki s tem tipom zapisa?
3. Kakšen je bil strežnikov odgovor?
4. Kaj pomeni *Transaction ID* v odgovoru?
5. Čemu je namenjen del odgovora *Additional records*?

```
Domain Name System (response)
  Transaction ID: 0x0005
  Flags: 0x8180 (Standard query response, No error)
  Questions: 1
  Answer RRs: 1
  Authority RRs: 0
  Additional RRs: 1
  Queries
    facebook.com: type MX, class IN
  Answers
    facebook.com: type MX, class IN, preference 10, mx smtpin.mx.facebook.com
  Additional records
    smtpin.mx.facebook.com: type A, class IN, addr 69.171.244.16
```

9. Preučite zajete segmente in odgovorite na spodnja vprašanja:

Št	Izvorni IP	Ponorni IP	Protokol	Opis
1	10.0.0.200	10.0.0.197	TCP	1043 > 80 [SYN] Seq=0 Win=64240
2	10.0.0.197	10.0.0.200	TCP	80 > 1043 [SYN, ACK] Seq=0 Ack=1 Win=5840
3	10.0.0.200	10.0.0.197	TCP	1043 > 80 [ACK] Seq=1 Ack=1 Win=64240
4	10.0.0.200	10.0.0.197	TCP	1043 > 80 [PSH, ACK] Seq=1 Ack=1 Win=64240
5	10.0.0.200	10.0.0.197	TCP	1043 > 80 [PSH, ACK] Seq=15 Ack=1 Win=64240
6	10.0.0.197	10.0.0.200	TCP	80 > 1043 [ACK] Seq=1 Ack=15 Win=5840
7	10.0.0.197	10.0.0.200	TCP	80 > 1043 [ACK] Seq=1 Ack=17 Win=5840
8	10.0.0.200	10.0.0.197	TCP	1043 > 80 [PSH, ACK] Seq=17 Ack=1 Win=64240
9	10.0.0.197	10.0.0.200	TCP	80 > 1043 [ACK] Seq=1 Ack=19 Win=5840
10	10.0.0.197	10.0.0.200	TCP	80 > 1043 [PSH, ACK] Seq=1 Ack=19 Win=5840
11	10.0.0.197	10.0.0.200	TCP	80 > 1043 [RST] Seq=703 Ack=19 Win=5840 Len=0

1. Kateri segmenti predstavljajo vzpostavitev povezave TCP? *Napišite številke segmentov.*
2. Kateri segmenti predstavljajo rušenje povezave TCP? *Napišite številke segmentov.*
3. Računalnik z naslovom 10.0.0.197 je v tej seji poslal 6 segmentov. Za vsakega od njih napišite, katere segmente potrjuje. *Napišite številke segmentov, ki jih potrjuje, brez segmentov, ki so že potrjeni.*
4. Koliko podatkov (v bajtih) se prenese v segmentu številka **5**?

10. Za vsakega od spodnjih naslovov določite, ali je sintaktično pravilen IPv6 naslov (obrazložite).

a. 2001:0001::AFG3
b. ::0
c. 2001:1470:1211:0001::1.2.3.4
d. 2001::AF:DEAD::0001
e. ::AF13:1

Kakšne vrste so naslednji IPv6 naslovi:

f. ::1
g. FF02::1
h. FE80::BA8C:12FF:FE80:D82D%en0