2. kolokvij RK, VŠS, FRI, 1. letnik, Sežana, 9. 6. 2011

Ime: _____

Priimek: _____

Vpisna številka: _____

RKVB

*Pozorno preberite navodila! Literatura **ni** dovoljena. "Plonklistki" so literatura! Uporabljate lahko preproste kalkulatorje. Čas pisanja je **60** minut. Naloge so enakovredne.*

1. Chuck Norris ne uporablja spletnega brskalnika, ampak pošilja ukaze različnih protokolov kar s programom telnet. Njegovo povezavo na strežnik *www.lrk.si* smo zajeli s programom Wireshark:

```
Chuck:
GET / HTTP/1.1
```

```
Strežnik:
HTTP/1.1 400 Bad Request
Date: Wed, 08 Jun 2011 20:37:14 GMT
Server: Apache
Content-Length: 226
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head><title>400 Bad Request</title></head><body>
<h1>Bad Request</h1><p>Your browser sent a request that this server could not understand.<br /></p>
</body></html>
```

1. Za kateri protokol aplikacijske plasti gre?
2. Zakaj nam je strežnik odgovoril na tak način? *Bodite pozorni na različico protokola!*
3. Dopolnite Chuckovo zahtevo tako, da bo pravilna.
4. Kakšno programsko opremo uporabljamo za strežnik?
5. Strežnik je odgovoril tudi z vrstico *Connection: close*. Kaj pomeni ta vrstica? Ali lahko odjemalec na kak način vpliva na zapiranje povezave? Kako?

2. S programom Wireshark smo zajeli spodnjo sejo TCP:

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

Preučite zajete segmente in odgovorite na spodnja vprašanja:

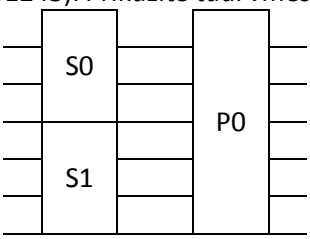
1. Kateri segmenti vsebujejo trosmerno rokovanje? *Napišite številke segmentov.*
2. Kateri segmenti vsebujejo rušenje povezave TCP? *Napišite številke segmentov.*
3. Katere segmente potrjuje segment številka **6**? *Napišite številke segmentov, ki jih potrjuje, ne pozabite upoštevati predhodnih potrditev!*
4. Koliko podatkov (v bajtih) se prenese v segmentu številka **10**?

3. Na naslednji strani je prikazan odgovor DNS, ki smo ga zajeli s programom Wireshark. S pomočjo izpisa odgovorite na spodnja vprašanja:

1. Kateri protokol transportne plasti uporablja sistem DNS? Na katerih vratih poslušajo strežniki DNS?
2. Po kakšnem tipu zapisa smo spraševali?
3. Kakšen je bil strežnikov odgovor?
4. Kakšnega tipa je zapis za *www.lrk.si*? Kakšen je IPv6 naslov strežnika *www.lrk.si*?
5. Ali imamo lahko za en strežnik več zapisov tipa A? *Odgovor na kratko utemeljite!*

```
User Datagram Protocol, Src Port: domain (53), Dst Port: 49573 (49573)
Domain Name System (response)
Transaction ID: 0x0004
Flags: 0x8180 (Standard query response, No error)
Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 0
Queries
  www.lrk.si: type AAAA, class IN
Answers
  www.lrk.si: type CNAME, class IN, cname lrk.fri.uni-lj.si
  lrk.fri.uni-lj.si: type CNAME, class IN, cname marvin.fri.uni-lj.si
  marvin.fri.uni-lj.si: type AAAA, class IN, addr 2001:1470:fffd::158
```

4. Izračunajte kako se v spodnjem kriptosistemu zašifrira niz 101110. 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

5. Protokol TCP
   1) Računalnik A ima IP naslov 22.33.44.55, računalnik B pa 55.44.33.22 . Med njima je vzpostavljena TCP povezava. Segmenti, ki potujejo od A do B imajo parameter source port 3345, segmenti, ki potujejo v obratni smeri pa 220. Kakšno vrednost parametrov source IP, destination IP in destination port imajo
      a. Segmenti, ki potujejo od A do B?
      b. Segmenti, ki potujejo od B do A?
   2) Spletni strežnik na naslovu 22.44.66.88 posluša na vratih 80 in uporablja trajne povezave (tj. TCP povezava se ne zapre po oddaji http odgovora). Denimo, da v nekem trenutku sprejema zahteve od dveh odjemalcev, P in R. Ali se na strežniku vsi odgovori pošiljajo skozi isti vtič? Če se pošiljajo skozi različna vtiča, ali imata oba številko izvornih vrat 80? Pojasnite.

6. 1) Kaj so naloge predstavitvene plasti po ISO OSI modelu?
   2) Katera plast leži pod njo in katera nad njo?
   3) Na katere (lahko različne) plasti bi po ISO OSI modelu sodile internetne storitve traceroute, http piškotki in zagotavljanje zanesljivega prenosa?

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

8. Avtentikacijski protokoli: Needham-Schroederjev protokol za avtentikacijo s centralno avtoriteto
   1) Kakšno kriptografijo predpostavlja Needham-Schroederjev protokol?
   2) Kako se imenuje napad, za katerega je ranljiv ta protokol?
   3) Opišite napad – zlasti predpogoje, ki morajo biti izpolnjeni, da lahko napadalec sploh izvede ta napad.

9. Sistem DNS
   1) Kaj je osnovni namen DNS-ja?
   2) Opišite izvajanje rekurzivnih in iterativnih poizvedb.

10. Primerjajte prenos datotek z uporabo protokolov SMTP in BitTorrent.