2. kolokvij RK 3.6.2010 Sežana

1) Na strežniku je spletna stran, ki vsebuje spodnjo kodo:

```
<html>
<head>
  <link rel="stylesheet" type="text/css" href="lrk.css" />
  <title>Področja našega dela in raziskovanja</title>
</head>
<body>
  <img border="0" src="images/omara.jpg" width="306" height="321">
  <ul>
    <li><a href="index2.html">Komunikacije</a></li>
    <li><a href="http://marvin.fri.uni-lj.si/izo.html">Izobraževanje</a></li>
  </ul>
</html>
```

   a) Koliko zahtev HTTP mora poslati naš spletni brskalnik, da nam prikaže zgornjo spletno stran?
   b) Kaj pomeni vrstica Keep-alive, če se pojavi v glavi (header) zahteve HTTP? Ali uporaba te vrstice kaj spremeni število zahtev, ki jih mora naš brskalnik poslati?
   c) Kaj pomeni, če nam strežnik odgovori s HTTP odgovorom z oznako 404 (Not found)? Gre za napako odjemalca ali napako na strežniku?

2) S programom Wireshark smo zajeli paket, katerega del prikazuje spodnja slika:

```
⊟ Domain Name System (response)
    [Request In: 82]
    [Time: 0.006503000 seconds]
    Transaction ID: 0x0004
  ⊞ Flags: 0x8180 (Standard query response, No error)
    Questions: 1
    Answer RRs: 1
    Authority RRs: 3
    Additional RRs: 2
  ⊟ Queries
    ⊟ fri.uni-lj.si: type MX, class IN
        Name: fri.uni-lj.si
        Type: MX (Mail exchange)
        Class: IN (0x0001)
  ⊟ Answers
    ⊟ fri.uni-lj.si: type MX, class IN, preference 10, mx ns.fri.uni-lj.si
        Name: fri.uni-lj.si
        Type: MX (Mail exchange)
        Class: IN (0x0001)
        Time to live: 1 minute
        Data length: 7
        Preference: 10
        Mail exchange: ns.fri.uni-lj.si
  ⊟ Authoritative nameservers
    ⊞ fri.uni-lj.si: type NS, class IN, ns metulj.uni-lj.si
    ⊞ fri.uni-lj.si: type NS, class IN, ns ns.fri.uni-lj.si
    ⊞ fri.uni-lj.si: type NS, class IN, ns ns.uni-lj.si
  ⊟ Additional records
    ⊞ ns.uni-lj.si: type A, class IN, addr 193.2.64.45
    ⊞ metulj.uni-lj.si: type A, class IN, addr 193.2.64.46
```

   a) Del katerega protokola so odgovori takšnega tipa?
   b) Po katerem tipu zapisa smo poizvedovali?
   c) Kakšen je strežnikov odgovor na našo poizvedbo? Napišite samo ime računalnika in domeno.
   d) Kaj vsebuje del odgovora Additional information? Zakaj je pomemben?

3) S programom Wireshark smo zajeli spodnjo sejo:

```
+OK POP3 server ready <1896.697170952@rk.local>
USER rdeca
+OK
PASS kapica
+OK rdeca's maildrop has 2 messages (320 octets)
STAT
+OK 2 320
LIST
+OK 2 messages (320 octets)
1 120
2 200
.
RETR 1
...
```

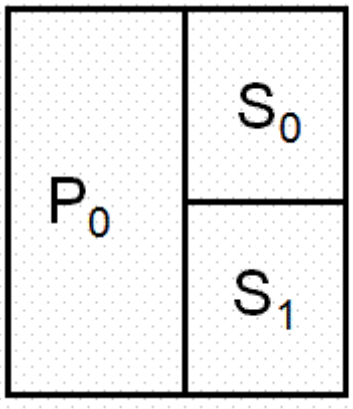
a) Za kateri protokol gre?
b) Čemu je ta protokol namenjen (kako deluje)?
c) Kaj je glavna pomanjkljivost tega protokola (prikazana je tudi v zgornji seji)?
d) Kako se lahko pred to pomanjkljivostjo zaščitimo?

4) Imamo kriptosistem, ki ga sestavlja škatla P0 in škatli S0 in S1. Kriptosistem prikazuje spodnja slika, koder in dekoder v škatlah S pa sta podana v spodnji tabeli. Permutacije v škatlah so:
   - P0 = (61047235)
   - P znotraj S0 = (3 1 7 6 12 0 8 13 15 14 9 10 11 2 4 5)
   - P znotraj S1 = (8 5 0 7 14 2 15 13 10 11 3 4 1 12 9 6)

   V kaj se kriptira 11011101? Pokažite tudi vmesne korake.

4/16	
0000	8
0001	5
0010	13
0011	1
0100	12
0101	9
0110	6
0111	10
1000	11
1001	3
1010	4
1011	14
1100	2
1101	15
1110	0
1111	7

16/4	
0	1000
1	0110
2	1100
3	1111
4	0000
5	0111
6	1001
7	1010
8	1011
9	0001
10	0010
11	1101
12	1110
13	0011
14	0100
15	0101



5) Katere od naslednjih storitev nudi TCP in katere UDP?
   a) nadzor pretoka
   b) nadzor dostopa
   c) avtentikacija
   d) navzgor omejeno zakasnitev paketa
   e) hitrost prenosa podatkov po načelu »best effort«
   f) nadzor zamašitev
   g) vzpostavljanje in rušenje povezave

6) Opišite, katere faze pozna protokol TCP pri nadzoru zamašitev. Za vsako fazo navedite njeno ime, kdaj se začne in kdaj konča ter kaj se dogaja v njej.

7) Narišite protokolarni sklad ISO OSI in navedite naloge predstavitvene plasti. V katero plast sodijo te naloge v protokolarnem skladu TCP/IP?

8) MIME
   a) Kaj je MIME in za kaj se uporablja?
   b) Na kateri plasti se uporablja?
   c) Katere vrste kodiranja besedila poznate?
   d) Kako bi kodirali izvršljivo datoteko? Zakaj?
   e) Kako bi kodirali dokument, zapisan v formatu txt? Zakaj?

9) Opišite enega od napadov na http piškotke (lahko izberete sami).

10) Kaj pomeni integriteta (celovitost) sporočila pri prenosu prek interneta? S katerimi mehanizmi jo zagotavljamo?