RK 2. kolokvij 2. 6. 2010

1) TCP oddajnik s širino okna 4000 bytov odda segmente z zaporednimi številkami 3000, 4000, 5000 in 6000. Nato sprejme potrditev ACK 6000. Katere od naslednjih trditev so resnične in katere ne ? Vse odgovore utemeljite!
    a. (2t) Vsi oddani paketi so sedaj potrjeni.
    b. (2t) Po prejemu naslednje potrditve (ACK 7000) se bo zamašitveno okno povečalo.
    c. (1t) Max. velikost segmenta je najverjetneje 1000 bytov. DA.
    d. (2t) Če bo naslednja potrditev ACK 6000, pomeni da prejemnik dobil segment 6000 podvojen.
    e. (1t) Če bo naslednja potrditev ACK 6000, pomeni da je bilo s segmentom 6000 najbrž nekaj narobe.
    f. (1t) Če bo naslednja potrditev imela vrednost Receive window nastavljeno na več kot 1000, lahko oddamo naslednji segment.
    g. (1t) Če bo namesto naslednje potrditve zazvonil alarm časovne kontrole za segment 6000, je to lažni alarm in segmenta ni treba ponovno oddati, saj smo že 2x dobili njegovo potrditev.
2) Navedite naloge transportne plasti in en standardni protokol transportne plasti. Na transportni plasti se med transportnima entitetama vzpostavi:
    a. fizična povezava
    b. logična povezava
    c. virtualna zveza
    d. aplikacijska povezava
3) Navedite 3 od petih metod, ki jih uporabljamo v http zahtevi po http 1.1, ter pojasnite njihovo uporabo. (10 točk)
4) Hash funkcije (10 točk = 5x po 2)
    a. Kaj je hash funkcija?
    b. Navedite tri lastnosti dobre hash funkcije.
    c. Navedite dva hash algoritma.
    d. Kje se uporablja na področju varnosti (zadošča en primer)?
    e. Kaj je rojstnodnevni napad (navedite le namen napada, ne mehanizma izvedbe)?
5) Elektronski podpis
    a. (5 točk) Kaj je elektronski podpis in kako ga izvedemo s pomočjo kriptografije? Opišite le osnovno različico brez centralne avtoritete in navedite tudi slabosti takega načina podpisovanja.
    b. (3 točke) Ali vidite kako možnost napada na opisani mehanizem?
    c. (2 točki) Je podpisano besedilo je varno pred napadalčevimi očmi?
6) Needham- Schroeder:
    a. (5 točk)Za kakšen namen in v kakšnih sistemih se uporablja Needham-Schroeder-jev protokol?
    b. (2 točki) Ali uporablja simetrično ali asimetrično kriptografijo?
    c. (3 točke) Za kateri napad je občutljiv (kratek oris izvedbe napada)?

7) Brskalnik prenaša s spletnega strežnika html datoteko, ki vključuje še tri majhne objekte, npr. jpeg sličice. Čas vrnitve (RTT) naj bo r, časi prenosa datotek pa naj bodo kar vsi enaki in sicer t. Predpostavimo, da na omrežju ni zamašitev. Koliko http zahtev je potrebnih? Koliko časa preteče, da brskalnik dobi vse objekte, če
    a. Uporablja ne-trajne povezave in vzporedne prenose po več TCP povezavah?
    b. Uporablja ne-trajne povezave brez vzporednih prenosov?
    c. Uporablja trajne povezave, okno je ob vzpostavitvi povezave enako 1 in se povečuje v skladu s pravili delovanja TCP?

    (10 točk)

Odg: 4 http zahteve (1 točka)

a- 4 povezave : 2 RTT + t za prvi html, nato tri vzporedni prenosi 2RTT+t za one tri objekte

b- 4 zaporedne TCP povezave: (2 RTT + t)*4 : vzpostavljanje + prenos za vsak objekt

c- 1 TCP povezava, po kateri 4 prenosi zapored: 2RTT+ t + 3*(RTT+t)

8) S programom Wireshark smo zajeli spodnjo sejo SMTP:

```
220 ns.fri.uni-lj.si ESMTP Postfix (Debian/GNU)
EHLO fri.uni-lj.si
250-ns.fri.uni-lj.si
250-PIPELINING
250-SIZE 60000000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
MAIL FROM: <mojca.ciglaric@fri.uni-lj.si>
250 2.1.0 Ok
RCPT TO: <andrej.krevl@fri.uni-lj.si>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: Janez Novak <janez@example.com>
To: Andrej Krevl <andrej.krevl@fri.uni-lj.si>
Subject: Domaca naloga

Zal nisem uspel narediti domace naloge.

Lp, Janez
.
250 2.0.0 Ok: queued as 6FAE48322
```

a. Kaj bo kot pošiljatelja sporočila prikazal prejemnikov odjemalec za e-pošto (npr. Thunderbird)?

b. Kako se lahko zavarujemo pred poneverjanjem pošiljatelja?

c. Vidimo, da protokol SMTP prenaša podatke kot golo besedilo. Kaj lahko storimo, da naši podatki ne bodo vidni morebitnim prisluškovalcem na omrežju?

9) S programom Wireshark smo zajeli spodnji promet:

```
Št          Čas        Izvorni IP   Ponorni IP       Info
71   53.256762  212.235.189.155  193.2.1.66       DNS Standard query A www.fri.uni-lj.si
72   53.259022  193.2.1.66       212.235.189.155  DNS Standard query response
                                                      A 212.235.188.25
97   69.926157  212.235.189.155  193.2.1.66       DNS Standard query MX fri.uni-lj.si
98   69.929198  193.2.1.66       212.235.189.155  DNS Standard query response
                                                      MX 10 ns.fri.uni-lj.si
117  85.699318  212.235.189.155  193.2.1.66       DNS Standard query
                                                      PTR 158.189.235.212.in-addr.arpa
118  85.702795  193.2.1.66       212.235.189.155  DNS Standard query response
                                                      PTR marvin.fri.uni-lj.si
```

a. Za kateri protokol gre?

b. Strežnik sprašujemo po 3 različnih tipih zapisih v tem protokolu. Po katerih treh?

c. Čemu so namenjeni zapisi PTR (po takšnem zapisu sprašuje paket št. 117)?

10) S programom Wireshark smo zajeli spodnjo zahtevo in odgovor HTTP:

```
GET / HTTP/1.1
Host: marvin.fri.uni-lj.si
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.3)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
If-Modified-Since: Fri, 20 Feb 2009 14:41:51 GMT
If-None-Match: "076195e6993c91:ae8"
Cache-Control: max-age=0

HTTP/1.1 304 Not Modified
Content-Location: http://marvin.fri.uni-lj.si/Default.htm
Last-Modified: Fri, 20 Feb 2009 14:41:51 GMT
Accept-Ranges: bytes
```

```
ETag: "076195e6993c91:ae8"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Wed, 02 Jun 2010 08:15:28 GMT
```

1. Zahtevo smo zajeli pri dostopu do spletnega naslova http://marvin.fri.uni-lj.si. Zakaj nam strežnik odgovori s takšnim odgovorom namesto s spletno stranjo (navedite tudi ustrezne vrstice zahteve, ki so »krivi« za to)?
2. Kakšno programsko opremo (spletni strežnik) uporablja marvin.fri.uni-lj.si? Kje lahko to preberemo?