2. kolokvij RK, VŠS, FRI, 1. letnik, 6. 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. V programu Wireshark smo zajeli spodnjo zahtevo in odgovor nanjo (uporabili smo možnost Follow TCP Stream):

```
GET /si/novice_in_dogodki/aktivne/59460/novica.html HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: sl-SI
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept-Encoding: gzip, deflate
Host: www.fri.uni-lj.si
Connection: Keep-Alive

HTTP/1.1 500 Server error
Date: Mon, 06 Jun 2011 06:42:22 GMT
Server: Apache/2.2.3 (Debian) mod_ssl/2.2.3 OpenSSL/0.9.8c
Content-Length: 347
Connection: close
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML>
<HEAD><TITLE>500 Internal server error</TITLE></HEAD>
<BODY><H1>Internal server error</H1></BODY>
</HTML>
```

1. Za kateri protokol aplikacijske plasti gre?
2. Kaj pomeni strežnikov odgovor?
3. Odjemalec je v zahtevi poslal tudi vrstico *Connection: Keep-Alive*, razložite pomen te vrstice.
4. Kakšno programsko opremo uporablja strežnik?
5. Kaj pomeni vrstica *Accept* v zahtevi, ki jo je poslal odjemalec?

2. S programom Wireshark smo zajeli spodnje pakete:

Št	Izvorni IP	Ponorni IP	Protokol	Opis
63	212.235.189.155	212.235.189.151	TCP	56418 > 2207 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=2
64	212.235.189.151	212.235.189.155	TCP	2207 > 56418 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=0
65	212.235.189.155	212.235.189.151	TCP	56418 > 2207 [ACK] Seq=1 Ack=1 Win=262140 Len=0
67	212.235.189.151	212.235.189.155	FTP-DATA	FTP Data: 365 bytes
68	212.235.189.151	212.235.189.155	TCP	2207 > 56418 [FIN, ACK] Seq=366 Ack=1 Win=64240 Len=0
69	212.235.189.155	212.235.189.151	TCP	56418 > 2207 [ACK] Seq=1 Ack=367 Win=262140 Len=0
70	212.235.189.155	212.235.189.151	TCP	56418 > 2207 [FIN, ACK] Seq=1 Ack=367 Win=262140 Len=0
71	212.235.189.151	212.235.189.155	TCP	2207 > 56418 [ACK] Seq=367 Ack=2 Win=64240 Len=0

1. Za kateri protokol na aplikacijski plasti gre, če veste da zgornji paketi predstavljajo njegovo podatkovno povezavo?
2. Za katerega od načinov delovanja protokola gre, če je strežnikov IP 212.235.189.151 in odjemalčev IP 212.235.189.155?
3. Kako se imenuje drugi način delovanja tega protokola?
4. Pojasnite razliko med delovanjem obeh načinov.

3. S programom Wireshark smo zajeli sejo TCP, ki je prikazana na naslednji strani. Preučite zajete segmente in odgovorite na spodnja vprašanja:

1. Kateri segmenti (številke) vsebujejo trosmerno rokovanje?
2. Kateri segmenti (številke) vsebujejo rušenje povezave TCP?
3. Katere segmente potrjuje segment številka **9**? *Napišite številke segmentov, ki jih potrjuje, ne pozabite upoštevati predhodnih potrditev!*
4. Koliko podatkov (v bajtih) se prenese v segmentu številka **4**?

```
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 [FIN, ACK] Seq=703 Ack=19 Win=5840 Len=0
12  10.0.0.200      10.0.0.197   TCP        1043 > 80 [ACK] Seq=19 Ack=704 Win=63538 Len=0
13  10.0.0.200      10.0.0.197   TCP        1043 > 80 [FIN, ACK] Seq=19 Ack=704 Win=63538 Len=0
14  10.0.0.197      10.0.0.200   TCP        80 > 1043 [ACK] Seq=704 Ack=20 Win=5840 Len=0
```

4. S programom Wireshark smo zajeli spodnji paket:

```
Secure Socket Layer
  TLSv1 Record Layer: Handshake Protocol: Multiple...
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 571
  Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 77
    Version: TLS 1.0 (0x0301)
  Random
    gmt_unix_time: Jun  6, 2011 09:49:42.000000000
    random_bytes: 79aeba12ce22a8abcd51be006ca...
  Session ID Length: 32
  Session ID: 4dec8696cf5...
  Cipher Suite: TLS_RSA_WITH_3DES_CBC_SHA
  Compression Method: null (0)
  Extensions Length: 5
  Extension: renegotiation_info
```

```
Handshake Protocol: Certificate
  Handshake Type: Certificate (11)
  Length: 425
  Certificates Length: 422
  Certificates (422 bytes)
    Certificate Length: 419
    Certificate (id-at-commonName=localhost)
  Handshake Protocol: Certificate Request
    Handshake Type: Certificate Request (13)
    Length: 53
    Certificate types count: 2
    Certificate types (2 types)
    Distinguished Names Length: 48
    Distinguished Names (48 bytes)
  Handshake Protocol: Server Hello Done
    Handshake Type: Server Hello Done (14)
    Length: 0
```

1. Za kateri protokol gre?
2. Kateri šifrirni algoritmi se bodo uporabili v tej seji? Naštejte jih in *na kratko* opišite nalogo vsakega izmed njih.
3. Kakšno ime (hostname) je zapisano v certifikatu (digitalnem potrdilu), ki ga pošlje strežnik?

5. Opišite delovanje in namen uporabe posredniških http strežnikov (http proxy).

6. Navedite, na katero plast po ISO OSI modelu sodijo naslednji protokoli in storitve:

Protokol/storitev	**PLAST**	**Protokol/storitev**	**PLAST**
Prenos elektronske pošte		MIME	
Prenos okvirja		IEEE 802.11n	
Prenos datagrama od izvornega do ciljnega IP		IPv6	
Prenos signala		DNS	
Nadzor zamašitev		AES	

7. Kriptografija

1. Za kriptiranje RSA želimo uporabiti p=5, q=7, n=35, z=24, d=5, e=245. Ali števila ustrezajo pogojem za ključ? Odgovor utemeljite.
2. Ne glede na zgornji odgovor izračunajte: uporabljamo bloke dolžine 2 desetiški mesti in želimo kriptirati blok »06«. Kakšen je rezultat enkripcije?
3. Ne glede na vaš prejšnji odgovor izračunajte: uporabljamo bloke dolžine 2 desetiški mesti in želimo dekriptirati blok »12«. Kakšen je rezultat dekripcije?
4. Uporabljamo mini simetrični kriptosistem, ki deluje nad 8-bitnimi bloki. Uporabljamo tudi CBC. Zadnji kriptirani blok ima vrednost 1111 0000. Naslednji je za kriptiranje na vrsti blok 1000 1011. Če bi ga kriptirali z našim sistemom, bi dobili vrednost 0101 0101. Kaj se bo zgodilo v naslednjem koraku? Lahko napišete kak rezultat?

8. Opišite napad z zrcaljenjem na osnovni avtentikacijski protokol izziv – odgovor. Kometirajte, kako bi odpravili ranljivosti tega protokola.

9. Primerjajte polja v glavi pri UDP in TCP in pojasnite, zakaj so potrebna polja, ki jih pri drugem protokolu ni.

10. Kaj je čas vrnitve, kaj je odmik in kako vplivata na interval časovne kontrole pri TCP? Zakaj je lahko narobe, če je ta interval predolg ali prekratek?