Fakultet elektrotehnike i računarstva
Preddiplomski studij Računarstvo

Komunikacijske mreže
Akademska godina 2021./2022.

2. domaća zadaća

Zadatak 1

Znamenke a, b i c u tekstu zadatka odnose se na posljednje tri znamenke Vašeg JMBAG-a (npr. 0036512abc). Ako je bilo koja od znamenki Vašeg JMBAG-a 0 (nula), zamijenite ju sa znamenkom 5.

Klijent K uspostavlja TCP-vezu s poslužiteljem P, a odmah po uspostavi veze poslužitelj šalje podatke duljine a000 (a tisuća) okteta. Za vrijeme trajanja veze ne dolazi do gubitaka podataka, potvrde se šalju bez odgađanja, a parametri prozora ne mijenjaju. Nakon što primi svih a000 okteta, klijent inicira raskid TCP-veze. Pretpostavite da je inicijalni apsolutni slijedni broj (prije uspostave veze) na poslužitelju P_{init} = b000, da je inicijalni apsolutni slijedni broj na klijentu K_{init} = c000, da je maksimalna veličina segmenta na poslužitelju i na klijentu *MSS* = 2000 okteta, da je veličina prozora primatelja na poslužitelju i na klijentu $rwnd_P = rwnd_K$ = 1500 okteta te da prosječno obilazno vrijeme RTT iznosi 2 vremenske jedinice.

(a) Koja je vrijednost polja *Broj u nizu* u prvom segmentu s podacima (koji šalje poslužitelj nakon uspostave veze)?
(b) Koja je vrijednost polja *Broj potvrde* u prvoj potvrdi poslanoj od strane klijenta (nakon uspostave veze)?
(c) Koliko je podataka poslano od strane poslužitelja u zadnjem segmentu (prije raskida veze)?

Očekivano rješenje zadatka je tekstualna datoteka, pohranjena kao **<JMBAG>.txt**, koja sadrži tri retka u kojima su zapisani isključivo brojevi (odgovori na pitanja pod (a), (b) i (c)).

Zadatak 2

Znamenke a, b, c, d, e i f u tekstu zadatka odnose se na posljednjih šest znamenki Vašeg JMBAG-a (npr. 0036abcdef). Ako je bilo koja od znamenki Vašeg JMBAG-a 0 (nula), zamijenite ju sa znamenkom 5.

Preuzmite topologiju *dz2_kommre.imn* s poveznice http://public.tel.fer.hr/km/dz2/dz2_kommre.imn i otvorite ju u programu IMUNES. Potrebno je stvoriti 3 podmreže (A, B i C) dodavanjem računala (čvorova tipa *PC*) i komutatora (čvorova tipa *LAN switch*) na usmjeritelje routerA, routerB i routerC. Podmreže A, B i C moraju se sastojati od po jednog čvora *LAN switch* i po dva čvora *PC*.

Adrese podmreža A, B i C su zadane kao:
A: 2*(1+ab) . 2*cd . 2*ef . 0 / 24
B: 2*(1+cd) . 2*ef . 2*ab . 0 / 26
C: 2*(1+ef) . 2*ab . 2*cd . 0 / 28

NAPOMENA: Ako je a=5, b=6 (ilustrativni primjer), onda je ab=56, a **NE** ab=30.

U tako definiranim podmrežama, konfigurirajte IP adrese i podrazumijevane usmjeritelje dodanim čvorovima, te statičke rute na **svakom** od usmjeritelja u topologiji, kako bi svi Vaši čvorovi bili dostupni sa svih ostalih čvorova u mreži (naredbom *ping*). IP adresa usmjeritelja mora biti prva valjana adresa u podmreži, a IP adrese svakog od dodanih čvorova moraju biti zadnje valjane adrese u podmreži (time isključujući adresu razašiljanja, *broadcast*).

Očekivano rješenje zadatka je topologija, .imn datoteka, pohranjena kao **<JMBAG>.imn**.

Zadatak 3

Korištenjem kriptografije javnog ključa potrebno je digitalno potpisati datoteku <JMBAG>.imn iz prethodnog zadatka. Datoteka može biti u izvornom ili promijenjenom obliku (tj. nije nužno riješiti Zadatak 2 za rješavanje Zadatka 3).

Za potpisivanje datoteke koristite naredbu *openssl*. Naredba *openssl* dostupna je na bilo kojem operacijskom sustavu, ali preporučuje se korištenje na virtualnom stroju IMUNES. Samostalno istražite naredbu *openssl* te pomoću nje generirajte RSA par ključeva potrebnih za potpisivanje datoteke. Stvorite digitalni potpis datoteke <JMBAG>.imn, te pritom zapišite sve Vaše korake u tekstualni izvještaj (<JMBAG>_log.txt).

Provjera vašeg rješenja izvodit će se na način da se pokrene naredba:

```
$ openssl rsautl -verify -inkey <kljuc> -pubin -keyform PEM -in <digitalni_potpis>
```

Naredba kao izlaz mora dati liniju nalik ovoj:

```
SHA256(0036443921.imn)=78dc88c7f2f93f7e4f0687e3afbf6e8646c38642bb87e1849b85291143b7a138
```

Ta vrijednost mora se poklapati sa sažetkom datoteke, dobivenim naredbom:

```
$ sha256 0036542199.imn
SHA256(0036443921.imn)=78dc88c7f2f93f7e4f0687e3afbf6e8646c38642bb87e1849b85291143b7a138
```

Očekivano rješenje zadatka su datoteke s kojima će se moći provjeriti digitalni potpis (**<JMBAG>.imn, <JMBAG>.pem** i **<JMBAG>.sig**) te kratki opis koraka dobivanja istih (**<JMBAG>_log.txt**).