

# Preizkus klienta in strežnika v Javi

Komunikacije v avtomatiki – Laboratorijske Vaje

16. december 2013

## Povzetek

V tej vaji se boste preizkusili v razumevanju protokola TCP in implementacije strežnik-klient. Vaja je sestavljena iz dveh nalog. V prvi nalogi boste napisali program, s katerim se priklopite na strežnik – vendar ne poznate protokola, niti gesla za priklop. Uporabiti boste morali Wireshark in z njim analizirati mrežni promet, preko katerega boste ugotovili vaše neznanke. V drugi nalogi boste demonstrirali vaše poznavanje postopka Cezarjeve šifre. Tretja naloga je neobvezna, je pa dobra vaja za programiranje v Javi in demonstracija zelo osnovnega šifrirnega postopka. Rešitve vseh nalog boste dodali na koncu poročila, ki ste ga napisali na prejšnjih vajah in poročilo poslali na naslov `janez.pers@fe.uni-lj.si` ob koncu teh vaj. V polje zadeva vpišite `KA_vaja5_<ime priimek, ime priimek>`. Poročilo poimenujte enako kot vpis v polje zadeva, torej, `KA_vaja5_<ime priimek, ime priimek>.doc`. Vsako poročilo, katerega datum in ura v prejetem elektronskem sporočilu presežeta konec vaje po urniku za več kot 10 minut, se upošteva kot oddano z zamudo in se mu zniža ocena.

**Pozor:** Lahko komunicirate s svojim kolegom v skupini, ne smete pa komunicirati z ostalimi kolegi v razredu. V primeru vsakokratnega pogovora ali prepisovanja (tudi elektronskega) se vam odbije po 10% od ocene Vaje 5.

## 1 Naloga 1 (70%)

Scenarij te naloge bo sledeč. Na oddaljenem računalniku bo tekel strežnik, na katerega boste morali narediti priklop, mu poslati vaše uporabniško ime in nato še geslo (naslov IP, port strežnika in vaše uporabniško ime vam pove asistent). Priklop boste izvedli s klientom, ki ga boste napisali v Javi – izhajali boste kar iz kode s prejšnje vaje. (V kolikor ste preveč pokvarili vaš program, si lahko prenesete s spletne strani predmeta originalen program za klienta `http://vision.fe.uni-lj.si/classes/KA-vaje/vaje/2012/TCPCClient.java`.) V primeru pravega gesla, vam bo strežnik odgovoril s sporočilom, da ste nalogo uspešno opravili in s tem pridobili 70% ocene. **Prej pa boste morali rešiti dva problema:**

1. Ne poznate pravega gesla, ki ustreza vašemu uporabniškemu imenu.
2. Ne poznate protokola, oziroma, kakšno mora biti zaporedje sporočil med strežnikom in klientom. Namreč, mogoče mora najprej strežnik poslati neko sporočilo, nato klient odgovori, nato strežnik spet pošlje nekaj, in tako naprej. Lahko pa je (*seveda je*) zaporedje in število sporočil popolnoma drugačno.

Ta problem boste rešili tako, da si boste pomagali z v naprej napisanim klientom. Če prihajate iz cikla1, potem uporabite program `http://vision.fe.uni-lj.si/classes/KA-vaje/vaje/2013/TCPCClientHidden1.class`, sicer pa si prenesite `http://vision.fe.uni-lj.si/classes/KA-vaje/vaje/2013/TCPCClientHidden2.class`. Ker nimate na voljo izvirne kode, lahko tega klienta samo poganjate. Ta klient ima spravljena vsa gesla za vašo uporabniška imena, pozna zaporedje sporočil, ki jih mora poslati/prejeti s strežnika in zna uspešno izvesti priklop na strežnik. Tako lahko na svojem računalniku zaženete `TCPCClientHidden` (s pravnimi parametri) in preko prestrežanja paketkov v Wiresharku prestrežete pravilno geslo, kakor tudi *pravilno zaporedje ukazov*. Nato spremenite *vaš program* `TCPCClient.java` iz prejšnjih vaj tako,

da se bo *uspešno priklopil na strežnik* in v pravilnem zaporedju izmenjal pravilne podatke. Z vaj 1 do 4 veste, da v Wiresharku lahko prestrežemo zaporedje paketkov med dvema procesi. Spomnite se, da lahko prikažemo le pakete poslane na, oziroma prejeti iz, nekega računalnika. Veste tudi, da pretoke sporočil lahko pregledujete preko **Flow graph** ali preko **Follow TCP stream**. Pri nalogi uporabite tisto vizualizacijo, ki vam najbolj ustreza.

Primere uspešnega priklopa, razlago, kako ste določili pravilno zaporedje sporočil in geslo, zapišite v poročilo. Dodajte tudi slike iz Wiresharka za lažjo razlago. Ob uspešnem priklopu tudi pokličite asistenta, da zabeleži opravljen praktični del naloge.

## 2 Naloga 2(30%)

Predpostavite, da je geslo, ki ga pošljete na strežnik, z nekim kodirnim protokolom zakodirano vaše uporabniško ime in predpostavite, da je ta kodirni protokol Cezarjeva šifra [1] (ogledate si lahko tudi [http://en.wikipedia.org/wiki/Caesar\\_cipher](http://en.wikipedia.org/wiki/Caesar_cipher)). Sedaj predpostavite, da je abeceda za Cezarjevo šifro enaka ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 in abeceda ne razločuje med velikimi in malimi črkami (spomnite se, da je abeceda ciklična – ko pridete do 9, nadaljujete z A). Izračunajte vrednost ključa ali *premika* (angl., shift) tako, da bo vaše zakodirano uporabniško ime enako pravilnemu geslu, ki ste ga poslali na strežnik! Rešitev naloge obrazložite v svojem poročilu.

## 3 Dodatna neobvezna naloga

Poskusite spisati kodo v Javi, ki bo implementirala Cezarjevo šifro, z njo šifrirala vaše uporabniško ime, in to poslala kot geslo na strežnik. Preizkusite program.

## Literatura

- [1] J.F. Kurose and K.W Ross, *Computer networking – a top-down approach*, Addison Wesley, 2009.