



## عنوان

پیاده‌سازی یک تالار گفتگو ساده

## هدف

با توجه به مفاهیم ارائه شده در درس شبکه‌های کامپیوتری، اهداف زیر در این پروژه مورد نظر می‌باشد.

- آشنایی عملی با برنامه‌نویسی شبکه
- آشنایی کامل با نحوه عملکرد پروتکل‌های شبکه در لایه کاربرد
- آشنایی عمیق با معماری Client/Server در لایه کاربرد

## توصیف

در این پروژه می‌خواهیم یک تالار گفتگو (Chat Room) برای حضور تعداد کاربر (Users) پیاده‌سازی کنیم. در یک تالار گفتگو و در هر لحظه از زمان تعداد کاربران حضور دارند و اقدام به ارسال پیام‌های خصوصی و عمومی می‌کنند. معماری سیستم به صورت Client/Server است. به عبارت دیگر هر کاربر باید از طریق یک کارفرما (Client) به سرور متصل شده و پیام‌های خود را ارسال نموده و یا پیام‌های تالار را دریافت نماید. ارتباط بین کارفرما و سرور از طریق یک سوکت TCP برقرار می‌شود و در این ارتباط سرور بر روی پورت 15000 گوش می‌دهد.

در این تالار گفتگو هر کاربر دارای یک نام کاربری منحصر به فرد و یک گذرواژه است. فرایند ثبت نام برای کاربران در نظر گرفته شده است که در این فرایند کاربر می‌تواند با یک نام کاربری و یک گذرواژه ثبت نام انجام دهد و در صورتی که نام کاربری آن قبلاً اخذ نشده باشد، سرور درخواست ثبت نام را تایید می‌کند. در سمت سرور لیست کاربران به همراه گذرواژه آن‌ها ذخیره می‌شود. همچنین سرور تاریخچه‌ای از رخدادهای تالار گفتگو نیز نگهداری می‌کند.

هر کاربر ثبت نام شده می‌تواند در هر زمان وارد تالار گفتگو شود. لازم به ذکر است که یک کاربر نمی‌تواند همزمان از طریق بیش از یک کارفرما وارد تالار شود. در صورتی که یک کاربر درخواست ورود به تالار دهد، در حالی که هم اکنون داخل تالار باشد، سرور آن کاربر را ابتدا از کارفرمای قبلی خارج نموده و سپس درخواست جدید را پذیرش می‌نماید.

کارفرما به محض اتصال به سرور می‌تواند درخواست ثبت نام و یا درخواست ورود به تالار دهد. برای درخواست ثبت نام، لازم است که اطلاعات ثبت نام شامل نام منحصر به فرد برای نام کاربری و گذرواژه ارسال گردد. سرور درخواست ثبت نام را بررسی نموده و درخواست را تایید و یا رد می‌نماید. پس از پاسخ درخواست ثبت نام، اتصال بین کارفرما و سرور قطع می‌گردد.

در صورتی که کاربر درخواست ورود به تالار داشته باشد، کارفرما به محض اتصال به سرور، پیام درخواست ورود به تالار ارسال می‌کند و در این پیام نام کاربری خود را برای سرور ارسال می‌کند. در سمت سرور و با دریافت پیام درخواست ورود، سرور ابتدا از وجود نام کاربری درخواست دهنده مطمئن می‌شود و سپس یک کلید رمزنگاری تصادفی ایجاد نموده و این کلید را رمزگذاری نموده و مقدار رمز شده را برای کارفرما ارسال می‌کند. کلید رمزگذاری در این بخش برابر با گذرواژه آن کاربر درخواست کننده است. کارفرما مقدار رمز



شده را دریافت کرده و در صورت داشتن مقدار گذرواژه آن را رمزگشایی نموده و تا پایان حضورش در تالار نگهداری می‌کند. تمامی پیام‌های بعدی که توسط کارفرما به سمت سرور ارسال می‌شود و یا توسط سرور به کارفرما ارسال می‌شود باید توسط این کلید رمزگذاری و رمزگشایی شود.

**نکته:** در تمامی عملیات رمزگذاری/رمزگشایی از یکی از الگوریتم‌های رمزنگاری متقارن نظیر AES استفاده نمایید. مد کاری الگوریتم را نیز ECB یا CBC در نظر بگیرید.

کارفرما پس از دریافت کلید رمزنگاری، باید یک درخواست «سلام» برای سرور ارسال نماید و سرور کاربر مورد نظر را به تالار گفتگو اضافه نموده و پیامی مبنی بر اضافه شدن کاربر جدید به تمامی کاربران حاضر در تالار ارسال می‌نماید. همچنین پاسخی به کاربر جدید ارسال می‌شود که حاوی خوش‌آمدگویی به کاربر برای ورود به تالار است. کاربر جدید بعد از دریافت پیام خوش‌آمدگویی، درخواستی برای گرفتن لیست نام حضار به سرور ارسال نموده و در پاسخ سرور لیست حضار را برایش ارسال می‌کند.

هر کاربر حاضر در تالار گفتگو می‌تواند پیامی را به صورت عمومی ارسال نماید و البته در این صورت تمامی کاربران حاضر دیگر آن پیام را دریافت می‌کنند. برای ارسال یک پیام در تالار گفتگو، یک کاربر باید متنی را به عنوان پیام عمومی به سمت سرور ارسال می‌کند. سرور آن پیام را ذخیره نموده و همچنین به تمامی کاربران ارسال می‌کند. البته سرور برای ارسال یک پیام عمومی به تمامی حضار، باید به نحو مناسب مشخص نماید که پیام عمومی ارسال شده است.

هر کاربر حاضر در تالار گفتگو می‌تواند پیامی را به صورت خصوصی به یک یا چند کاربر حاضر دیگری ارسال نماید و البته در این صورت تنها کاربران مشخص شده آن پیام را دریافت می‌کند. برای ارسال یک پیام خصوصی در تالار گفتگو، یک کاربر باید متنی را به عنوان پیام خصوصی به سمت سرور ارسال می‌کند که در آن گیرنده و یا گیرندگان را مشخص می‌کند. سرور آن پیام را ذخیره نموده و همچنین به تمامی کاربران مشخص شده در لیست گیرندگان ارسال می‌کند. البته سرور برای ارسال یک پیام خصوصی به لیست محدودی از گیرندگان، باید به نحو مناسب مشخص نماید که پیام خصوصی ارسال شده است.

هر کاربر حاضر در تالار گفتگو می‌تواند تالار را ترک کند. برای این منظور می‌تواند یک پیام ترک برای سرور ارسال نماید و سرور پیامی مبنی بر ترک تالار برای تمامی حضار ارسال می‌کند. البته ممکن است که یک کاربر بدون ارسال پیام ترک، و به دلیل قطعی شبکه و یا اتصال با سرور، تالار را ترک کند و در صورت تشخیص توسط سرور، پیام ترک کاربر مذکور برای تمامی اعضا ارسال می‌گردد. سرور پس از تشخیص خروج یک کاربر، کلید رمزنگاری آن کاربر را از لیست کلیدهای فعال حذف می‌نماید.

## نیازمندی‌های غیرعملیاتی

- در صورتی که دستوری اشتباه وارد شود، باید پیام مناسب به کاربر داده شود.
- در صورت پیاده‌سازی برنامه با امکانات متنوع‌تر، نظیر واسط کاربری گرافیکی، نمره اضافه کسب خواهید نمود.
- برنامه باید در قالب (code style) مناسبی نوشته شود. همچنین برنامه باید comment گذاری شده باشد.
- نامگذاری متغیرها، فایل‌ها، کلاس‌ها و متدها باید به درستی (معنی‌دار) انجام شود.



## توصیف پروتکل

توصیف پروتکل ارتباطی شامل شرح دقیق فرمت پیام‌های ارسالی بین کارفرما و سرور در شرایط مختلف است. با توجه به توصیف فوق از برنامه، پیام‌های اصلی به ترتیب زیر شرح داده می‌شود. باید توجه داشت که تمامی ارتباطات در لایه کاربرد به صورت متنی است و هر پیام در قالب مشخص یک دستور بین کارفرما و سرور مبادله می‌شود. لازم به ذکر است که خروجی محتوای رمز شده را می‌توانید در قالب Base64 ارسال نمایید. بدیهی است که برخی از پیام‌ها از سمت کارفرما به سرور و مابقی برعکس ارسال می‌شوند. در صورتی که پیامی به طور دقیق شرح داده نشده است، می‌توانید فرضیات خود را در پروتکل در نظر بگیرید و در زمان تحویل آن فرضیات را توضیح دهید.

### پیام ثبت نام کاربر

این پیام در ابتدای اتصال کارفرما به سرور و از سمت کارفرما به سرور ارسال می‌شود. هدف از این پیام ثبت نام کاربر و ارسال نام کاربری و گذرواژه است. در این پیام کلمه Registration یک رشته ثابت و بخش <user\_name> نام کاربر و <password> حاوی گذرواژه است که البته هر کاربر یک نام کاربری مشخص و یکتا دارد. به طور کلی و در ادامه این مستند، متغیرها در توصیف پروتکل بین دو علامت <> خواهند آمد. امکان استفاده از فاصله خالی (هرگونه White Space) در نام کاربری و گذرواژه وجود ندارد.

```
Registration <user_name> <password>
```

### پیام درخواست ورود کاربر

این پیام در ابتدای اتصال کارفرما به سرور و از سمت کارفرما به سرور ارسال می‌شود. هدف از این پیام درخواست ورود کاربر برای حضور در تالار گفتگو است. در این پیام کلمه Login یک رشته ثابت و بخش <user\_name> نام کاربر است که البته هر کاربر یک نام مشخص و یکتا دارد.

```
Login <user_name>
```

پس از ارسال درخواست فوق از سمت کارفرما به سرور، سرور درخواست را بررسی نموده و در صورت عدم وجود چنین کاربری در لیست کاربران ثبت نام شده، یک پیام خطا برای کارفرما ارسال نموده و اتصال را قطع می‌کند. در صورت وجود نام کاربری در لیست کاربران ثبت نام شده، کلید رمزنگاری را به صورت تصادفی تولید نموده و با پیام زیر برای کارفرما ارسال می‌کند. در پیام زیر کلمه Key یک رشته ثابت و متغیر key\_value حاوی مقدار کلید رمزنگاری است که توسط الگوریتم رمزنگاری رمز شده است. در این بخش برای رمزنگاری از گذرواژه به عنوان کلید رمزنگاری استفاده می‌شود. در صورتی که تولید گذرواژه با اندازه کلید الگوریتم مطابقت ندارد، می‌توانید به صورت توافقی تنها بخشی از گذرواژه را استفاده نمایی و یا اینکه بیت‌های صفر را به ابتدا یا انتهای گذرواژه اضافه کنید تا به



طول مشخص برای الگوریتم رمزنگاری برسید. دقت کنید که این مکانیسم باید در هر دو سمت کارفرما و سرور به یک صورت پیاده‌سازی گردد.

Key <key\_value>

کارفرما به محض دریافت پیام فوق، کلید را استخراج نموده و این کلید را برای تمامی فعالیت‌های بعدی خود در داخل تالار استفاده می‌کند. لذا ابتدا پیام Hello را برای سرور به صورت زیر ارسال می‌کند. محتوای این پیام و پیام‌های بعدی بین طرفین باید رمزگذاری شده باشد.

Hello <user\_name>

### پیغام اضافه شدن یک کاربر جدید به تالار

سرور به محض دریافت پیام Hello از سمت یک کاربر، یک پیغام مبنی بر اضافه شدن یک کاربر جدید به تالار به تمامی حضار ارسال می‌کند. فرمت این پیغام به صورت زیر است. دقت کنید که سرور باید مشخصات کامل تمامی حضار را در هر لحظه از زمان نگهداری کند که بتواند پیغام‌های همگانی را برای تمامی حضار ارسال نماید. بدیهی است که پیام هر کاربر باید با کلید رمزنگاری همان کاربر رمز شود.

<user\_name> join the chat room.

### خوش آمدگویی به کاربر

سرور به محض دریافت پیام Hello از سمت یک کاربر، یک پیغام خوش‌آمدگویی به آن کاربر ارسال می‌کند. فرمت این پیغام به صورت زیر است.

Hi <user\_name>, welcome to the chat room.

### درخواست ارسال لیست حضار

هر کارفرما می‌تواند درخواستی مبنی بر ارسال لیست حضار به سرور بدهد. فرمت پیغام این درخواست به صورت زیر است.

Please send the list of attendees.



### پاسخ به درخواست ارسال لیست حضار

سرور به محض دریافت درخواست لیست حضار از سمت یک کاربر، این لیست را آماده نموده و به فرمت زیر برای آن کاربر ارسال می‌کند. دقت کنید که در مثال زیر تعداد حضار 4 بوده است و البته این تعداد می‌تواند کمتر یا بیشتر باشد. خط اول و دوم باید با کاراکترهای “\r\n” جدا شوند. نام حضار باید با کاما جدا شوند و کل لیست حضار باید در یک خط قرار گیرد. به عبارت دیگر پایان لیست حضار با New Line نمایش داده می‌شود. برای این منظور می‌توانید در انتهای لیست حضار از کاراکترهای “\r\n” استفاده کنید.

Here is the list of attendees:

<user\_name1>,<user\_name2>,<user\_name3>,<user\_name4>

### ارسال پیام عمومی از یک کاربر به سرور

هر کاربر می‌تواند یک پیام را به صورت عمومی در تالار ارسال کند. برای این منظور باید پیامی در قالب زیر به سرور ارسال کند. دقت کنید که خط اول و دوم باید با کاراکترهای “\r\n” جدا شوند. همچنین message\_len طول پیام بر مبنای تعداد بایت‌ها و message\_body شامل محتوای پیام است. دقت کنید که طول پیام برای شناسایی پایان پیام ضروری است.

Public message, length=<message\_len>:

<message\_body>

### ارسال پیام عمومی از سرور به هر کاربر

سرور به محض دریافت یک پیام عمومی از یک کاربر، متن زیر را آماده نموده و برای تمامی حضار (از جمله فرستنده) ارسال می‌کند. دقت کنید که خط اول و دوم باید با کاراکترهای “\r\n” جدا شوند. همچنین message\_len طول پیام بر مبنای تعداد بایت‌ها، message\_body شامل محتوای پیام و user\_name نام کاربری است که پیام را ارسال نموده است.

Public message from <user\_name>, length=<message\_len>:

<message\_body>

### ارسال پیام خصوصی از یک کاربر به سرور

هر کاربر می‌تواند یک پیام را به صورت خصوصی به یک یا بیش از یک نفر از حضار در تالار ارسال کند. برای این منظور باید پیامی در قالب زیر به سرور ارسال کند. دقت کنید که خط اول و دوم باید با کاراکترهای “\r\n” جدا شوند. همچنین message\_len طول پیام بر مبنای تعداد بایت‌ها و message\_body شامل محتوای پیام است. لازم به ذکر است که نام کاربرانی که باید این پیام برایشان ارسال شود در خط اول آمده است. این لیست باید حداقل شامل یک نام کاربری باشد.

Private message, length=<message\_len> to <user\_name1>,<user\_name2>,<user\_name3>,<user\_name4>:

<message\_body>



### ارسال پیام خصوصی از سرور به هر کاربر

سرور به محض دریافت یک پیام خصوصی از یک کاربر، متن زیر را آماده نموده و برای تمامی حضار مورد نظر که در لیست گیرندگان آمده است، ارسال می‌کند. دقت کنید که خط اول و دوم باید با کاراکترهای “\r\n” جدا شوند. همچنین message\_len طول پیام بر مبنای تعداد بایت‌ها، message\_body شامل محتوای پیام و user\_name نام کاربری است که پیام را ارسال نموده است.

```
Private message, length=<message_len> from <user_name> to <user_name1>,<user_name2>,<user_name3>:
<message_body>
```

### درخواست ترک تالار از یک کاربر به سرور

هر کاربر در صورتی که بخواهد تالار را ترک کند، پیامی با فرمت زیر برای سرور ارسال نموده و بعد از اتصال خود با سرور را قطع می‌کند.

```
Bye.
```

### اعلان ترک یک کاربر توسط سرور به تمامی حضار

سرور به محض دریافت یک پیام ترک تالار از یک کاربر، این موضوع را با پیام زیر به تمامی حضار اعلان می‌کند.

```
<user_name> left the chat room.
```

## قابلیت‌های اضافی

در صورتی که علاقه‌مند هستید که قابلیت‌های بیشتری به این تالار گفتگو اضافه کنید، ابتدا توصیف کاملی از پیام‌های اضافی مورد نیاز تدوین کنید و سپس قابلیت‌های مورد نظر را در سمت کارفرما و سرور پیاده‌سازی کنید. نمونه قابلیت‌های اضافه تر که می‌توانید اضافه کنید شامل موارد زیر می‌تواند باشد:

- طراحی واسط گرافیکی برای کلاینت‌ها
- امکان انتقال فایل بین کاربران و یا در یک تالار
- امکان استفاده از Tag در انتقال متن با هدف نمایش متون Bold، متون رنگی، متن با قابلیت لینک و سایر موارد مشابه
- امکان فشرده‌سازی در فرآیند انتقال فایل (نیاز به Header برای معرفی الگوریتم فشرده‌سازی دارد)
- امکان ارسال پیام‌های کنترلی نظیر BUZZ بین کاربران و یا در تالار

## برنامه کارفرما

برنامه کارفرما باید ضمن پیاده‌سازی دقیق پروتکل ارتباطی واسط کاربری (متنی یا گرافیکی) مناسبی به کاربر خود ارائه نماید که محتوای پیام‌های دریافتی از سمت سرور را به کاربر نمایش دهد. برای این منظور باید به‌طور مناسب پیام‌های عمومی و خصوصی را با



کاربر نشان دهد. همچنین کاربر باید بتواند در صورت نیاز پیغامی را به صورت خصوصی یا عمومی به تالار ارسال نماید. امکان ورود و خروج به تالار نیز باید برای کاربر فراهم گردد. همچنین کاربر باید بتواند در صورت نیاز لیست حضار را ببیند.

## برنامه سرور

برنامه سرور علاوه بر پیاده‌سازی کامل پروتکل، باید یک کپی از تمامی پیغام‌های ارسالی در کنسول نمایش دهد. همچنین تمامی ورود و خروج‌ها را باید در کنسول نمایش دهد.

## نکات مهم

- پروژه را می‌توانید در گروه‌های حداکثر یک نفری انجام دهید.
- موعد تحویل پروژه هفته آخر فروردین ماه ۱۴۰۳ است و زمان دقیق آن متعاقبا اعلان می‌گردد.
- در نوشتن کد برنامه باید Coding Style رعایت شود.
- هرگونه رفتار که از مصادیق تقلب تشخیص داده شود، منجر به اعمال مقررات بر تمامی افراد درگیر در آن رفتار خواهد شد.
- هرگونه سؤال تنها از طریق گروه تشکیل شده برای کلاس قابل پاسخگویی است.