پروژه **دوم** درس شبکه های کامپیوتری

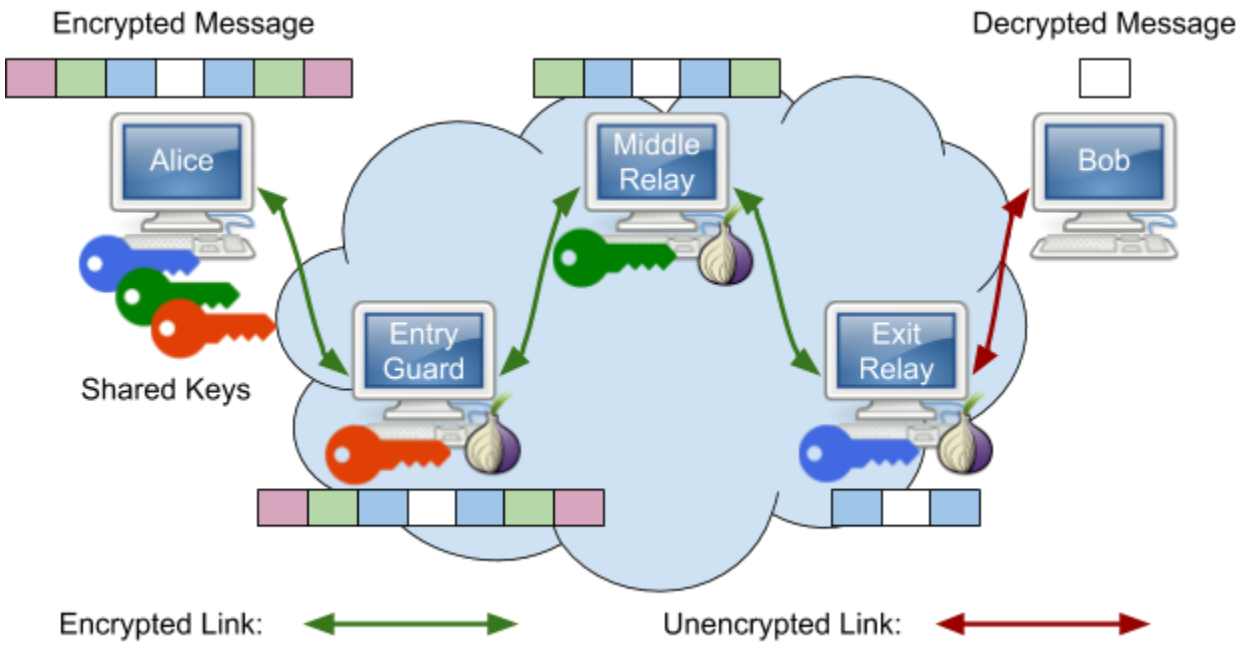
نیمسال دوم سال ۱۴۰۰-۱۴۰۱

## شرح پروژه

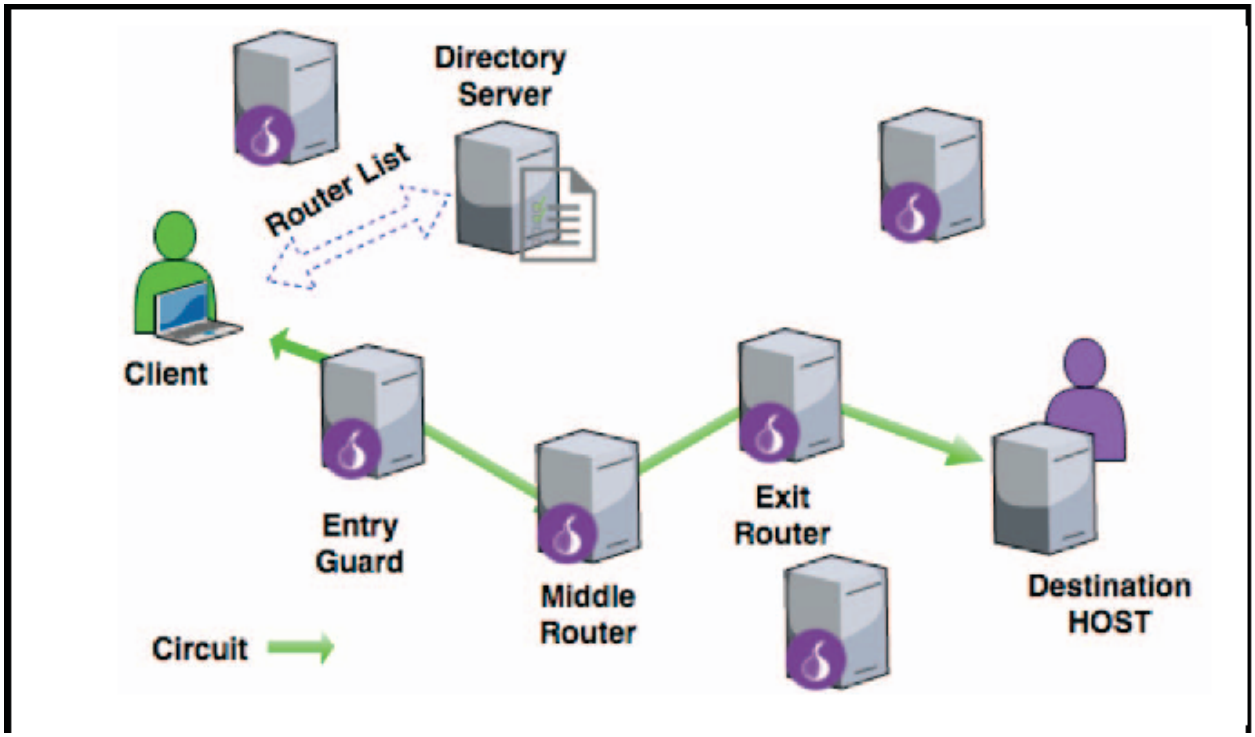
قصد داریم در این پروژه یک تابلو اعلانات را با معماری client/server پیاده سازی کنیم.ساختار این تابلو اعلانات به این صورت خواهد بود که کاربر می‌تواند یک درخواست ارسال کند و اعلانات قرار گرفته بر روی تابلو را از سرور دریافت کند و یا متن یک اعلامیه همراه با اسم خود به سرور ارسال کند و آن را "بر روی تابلو" قرار دهد. نکته مهمی که باید به آن توجه داشت این است که اعلامیه ها باید به صورت کاملا ناشناس قرار داده یا دریافت شوند.این به آن معنا است که حتی با شنود ترافیک شبکه، امکان مشخص کردن اینکه چه کسی با سرور در ارتباط بوده، نباید وجود داشته باشد.برای انجام این کار کاربر ها باید از طریق onion-routing به سرور متصل شوند. در ادامه به توضیح این روش و سایر بخش هایی که باید برای این سیستم پیاده سازی شوند می‌پردازیم.

## onion routing

نرم افزار tor یکی از معروف ترین سیستم هایی است که این پروتکل را پیاده سازی کرده است.با توجه به شکل زیر نحوه کار این پروتکل به این شکل است که در سیستم مبدا چندین مرحله رمزنگاری با کلید های مختلف بر روی بسته ارسالی انجام می‌گیرد و این بسته به شبکه tor فرستاده می‌شود. در هر node پیام دریافتی با کلیدی که در اختیار آن node هست رمزگشایی می‌شود و سپس به node بعدی ارسال می‌شود تا در نهایت به node آخر رسیده و آن node پیام را به سرور ارسال می‌کند. ویژگی که باعث می‌شود این پیام کاملا به صورت ناشناس ارسال شود این است که در circuit ای که برای ارسال پیام انتخاب شده هر نود از همسایه قبلی و بعدی خود در این circuit با خبر است و به دلیل رمزنگاری، فقط node آخر از محتوای بسته با خبر است.(**توضیح داده شده به صورت خلاصه بود حتما این لینک را مشاهده کنید**)



همچنین یک directory node نیز وجود دارد که کاربر می‌تواند لیست node های موجود در شبکه را دریافت کند و با استفاده از آن لیست سه node مورد نظر خود را انتخاب کند.در شکل زیر می‌توانید مثالی از آن را ببینید.




## رمزنگاری و تبادل کلید

حال که با معماری onion routing آشنا شدیم مراحل رمزنگاری و تبادل کلید را بررسی می‌کنیم.

ابتدا لازم است لینک های یک، دو، سه(روش Diffie-Hellman برای تبادل کلید برای قسمت نمره اضافه)، چهار و پنج(لینک های چهار و پنج مربوط به روش RSA است) را مشاهده کنید. پس کاربر باید با هر node کلیدی به اشتراک بگذارد همچنین node های همسایه در یک circuit باید با هم کلیدی به اشتراک بگذارند تا پیام های بینشان قابل شناسایی نباشد.

## پیاده سازی

- **سرور تابلو اعلانات**
- **سرور node directory**

این سرور باید بر روی یک پورت دیفالت اجرا شود تا node ها هنگام اجرا به این سرور اطلاع دهند که آنلاین شده اند و شماره پورت خود را به آن بدهند.

- **سرور های node**

برای اجرای این سرور ها یک فایل config.yml داده می‌شود. که در آن اسم سرور و شماره پورتی که این سرور باید بر روی آن اجرا شود قرار دارد ساختار این فایل به شکل زیر است:

```
name: node-1
port: 8080
directory-node: 9000
```

- **کلاینت**

کلاینت باید شماره پورت node directory را داشته باشد همچنین باید امکان گرفتن متن اعلامیه از کاربر را باید داشته باشد.

- **ثبت log**

هر یک از node ها ، directory node و کلاینت باید تمام فعالیت هایش را log کند.

## نمره اضافه

پیاده سازی روش Diffie-Hellman در عوض روش RSA برای رمز نگاری و تبادل کلید نمره اضافه در نظر گرفته می‌شود.

## نکات مهم

۱- استفاده از هر زبانی مجاز است اما زبان های جاوا و سی به هیچ وجه توصیه نمی‌شود.

۲- پروژه به صورت انفرادی باید انجام است.

۳- در صورت مشاهده هرگونه شباهت بین کد ها و اثبات تقلب نمره ۱۰۰- داده می‌شود.

۴- فایل های نهایی در قالب زیر ارسال شود :

FirstName_LastName_StudentNumber_PR2.zip

**موفق باشید**

**تیم حل پروژه شبکه های کامپیوتری**