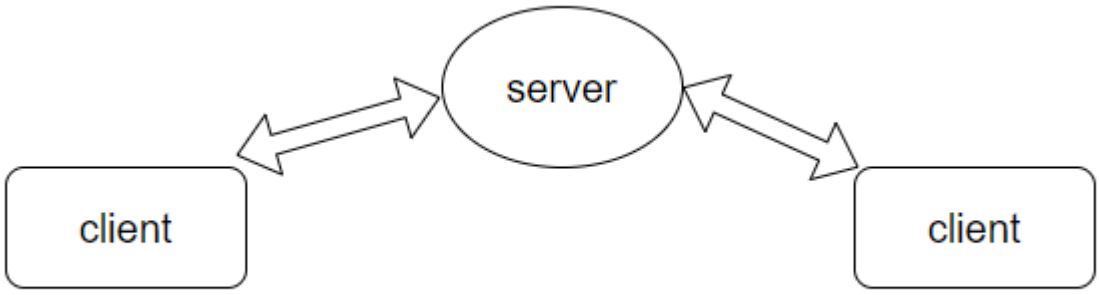
امنیت شبکه‌های کامپیوتری پیشرفته

پروژه اول

همانطور که می‌دانیم امروزه بسیاری از شبکه‌های اجتماعی از معماری client-server استفاده می‌کنند. کاربر به عنوان فرستنده پیغام خود را به سرور ارسال می‌کنند و سرور پیغام را به کاربر یا کاربران گیرنده ارسال می‌کند. آنچه در این بین مهم است مسئله امنیت است. برای ارتباط ایمن از رمزنگاری متقارن یا نامتقارن استفاده می‌شود.

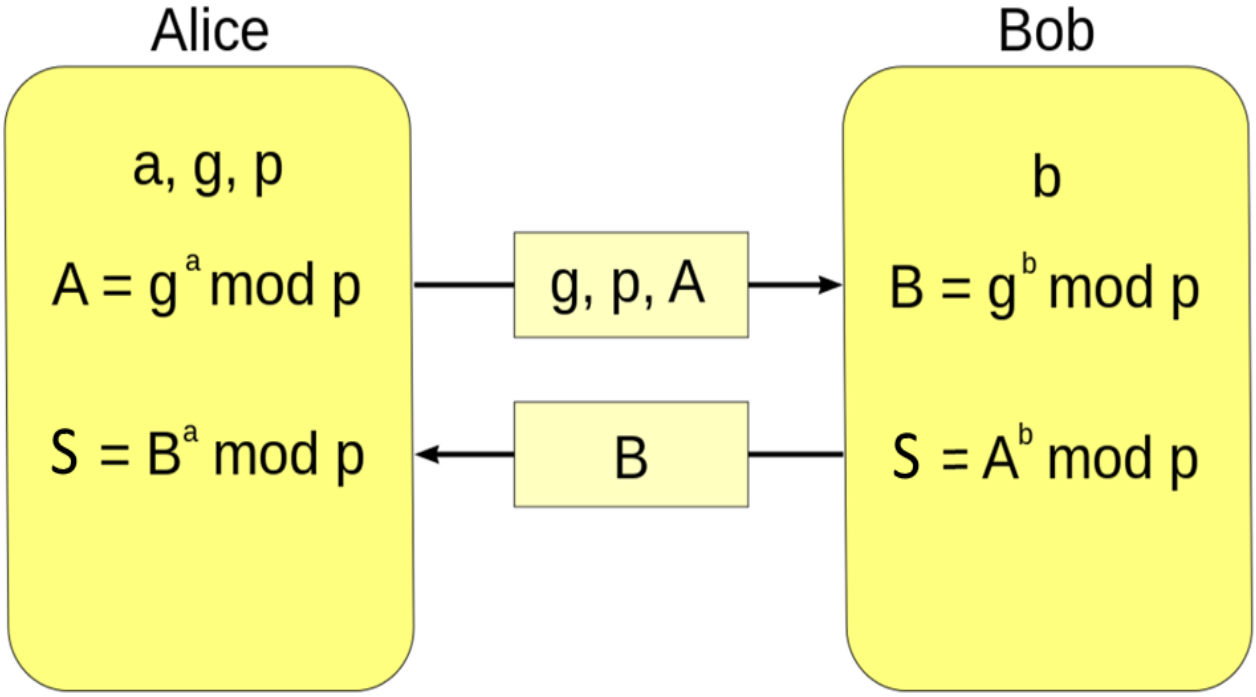
در این تمرین ابتدا با استفاده از python و socket programming معماری زیر را که متشکل از ۲ کلاینت و یک سرور است پیاده سازی کنید.



تبادل کلید :

تبادل کلید Diffie-Hellman روشی برای تبادل امن کلیدهای رمزنگاری در یک کانال ناامن است. این کار با اجازه دادن به دو طرف (آلیس و باب) در مورد یک کلید مخفی مشترک بدون اینکه هیچ طرف دیگری بتواند کلید را رهگیری کند یا چیزی در مورد آن بیاموزد، به توافق برسند. تبادل کلید شامل مراحل زیر است:

۱- **آلیس و باب بر سر دو عدد اول بزرگ p و g توافق کرده‌اند.**
۲- **آلیس یک عدد صحیح مخفی، a را انتخاب می‌کند و A = g^a mod p را محاسبه می‌کند. او A را برای باب می‌فرستد.**
۳- **باب یک عدد صحیح مخفی، b را انتخاب می‌کند و B = g^b mod p را محاسبه می‌کند. او B را برای آلیس می‌فرستد.**
۴- **آلیس s = B^a mod p را محاسبه می‌کند. باب s = A^b mod p را محاسبه می‌کند.**



امنیت شبکه‌های کامپیوتری پیشرفته
پروژه اول

در معماری ذکر شده هر کلاینت با استفاده از پروتکل تبادل کلید Diffie-Hellman فرآیند تبادل کلید با سرور را انجام می‌دهد.

ارسال و دریافت اطلاعات :

برای ارسال و دریافت اطلاعات از الگویتم رمزنگاری AES (Advanced Encryption Standard) استفاده می‌کنیم. فرستنده و گیرنده کلید عمومی یکدیگر را دارد. آنها از کلید خصوصی خود و کلید عمومی دیگری برای محاسبه یک کلید مشترک استفاده می‌کنند.

خروجی مورد انتظار:

- **فرآیند تبادل کلید بین هر کلاینت و سرور به صورت جداگانه**
- **دریافت پیام از یک کلاینت و رمزگشایی آن، رمزگذاری مجدد پیام و ارسال به کلاینت دیگر**
- **چاپ پیام آشکار(plainText) و رمزگذاری شده در ترمینال های برنامه در حال اجر**
- **گزارش توضیحات نحوه عملکرد هر بخش از کد توسعه داده شده شامل فرآیند تبادل کلید، encryption و decryption**

نکات مهم :

- **از کتابخانه های رایج پایتون برای تولید اعداد اول، اعداد تصادفی و Hash استفاده کنید.**
- **برای کاهش پیچیدگی کد لازم نیست خودتان الگوریتم AES را توسعه دهید، از کتابخانه های رایج استفاده کنید. صرفا باید ورودی های لازم برای اعمال encrypt و decrypt را به تابع مورد نظر از آن کتابخانه بدهید.**
- **فرآیند تبادل کلید باید توسط خود دانشجویان توسعه داده شود.**

موفق باشید.

رستمی