**《网络空间安全导论实践》实验报告**

实验题目：socket通信加密

姓名：

学院：网络空间安全学院

专业：网络空间安全（大类招生）

班级：

学号：

联系方式：

邮箱：

2022年 5 月 10日

# 实验内容及原理

什么是Socket？

Socket的中文翻译过来就是“套接字”。套接字是什么，我们先来看看它的英文含义：插座。

Socket就像一个电话插座，负责连通两端的电话，进行点对点通信，让电话可以进行通信，端口就像插座上的孔，端口不能同时被其他进程占用。而我们建立连接就像把插头插在这个插座上，创建一个Socket实例开始监听后，这个电话插座就时刻监听着消息的传入，谁拨通我这个“IP地址和端口”，我就接通谁。

实际上，Socket是在应用层和传输层之间的一个抽象层，它把TCP/IP层复杂的操作抽象为几个简单的接口，供应用层调用实现进程在网络中的通信。Socket起源于UNIX，在Unix一切皆文件的思想下，进程间通信就被冠名为文件描述符（file desciptor），Socket是一种“打开—读/写—关闭”模式的实现，服务器和客户端各自维护一个“文件”，在建立连接打开后，可以向文件写入内容供对方读取或者读取对方内容，通讯结束时关闭文件。

*2.实验环境（实验拓扑、节点介绍）*

服务端：win11笔记本

客户端：VMWare Station 虚拟机（centos 7）

# 程序概要设计(或使用的工具介绍)

使用工具：Pycharm

client端：利用socket库与Pycryptodome库建立起服务端和解密程序。

server端：利用socket库与Pycryptodome库建立起客户端和加密程序。

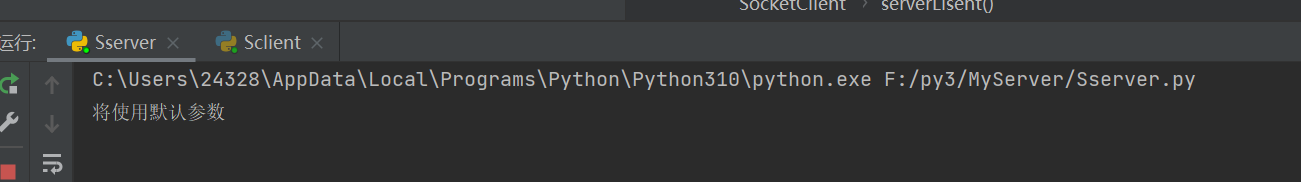
代码参考：<https://blog.gcoperation.top/posts/c961f1fb/>

https://blog.csdn.net/qq\_42693277/article/details/117040343

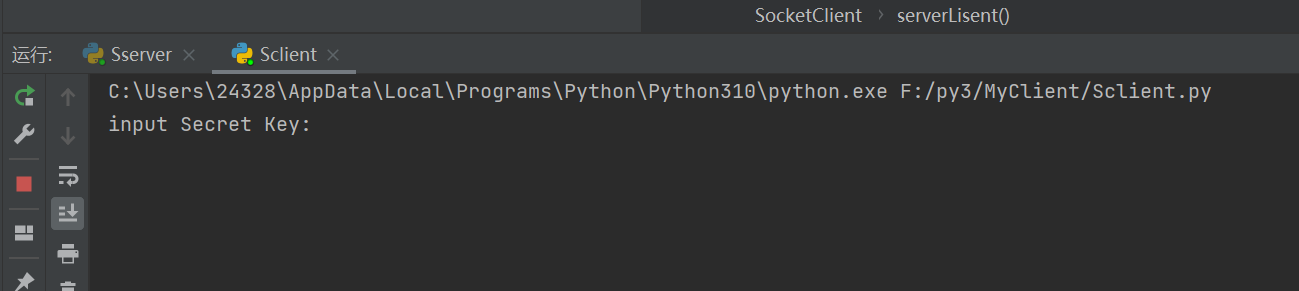
# 实验步骤、实验结果、分析

步骤：

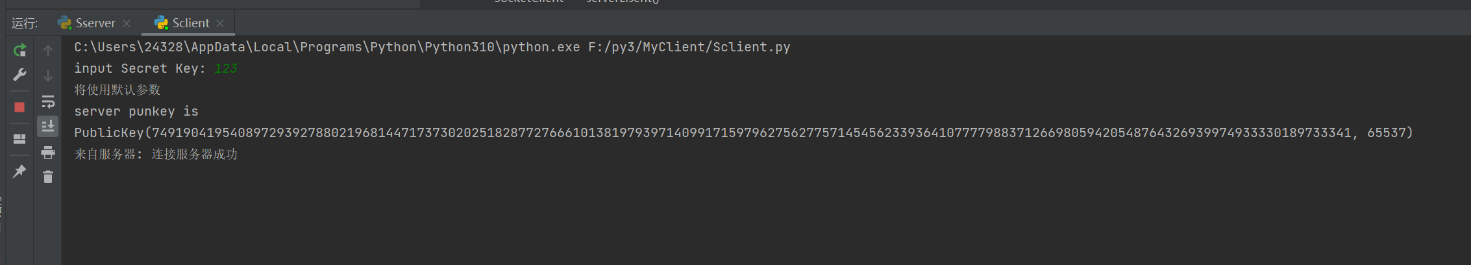
1.运行 server服务器程序

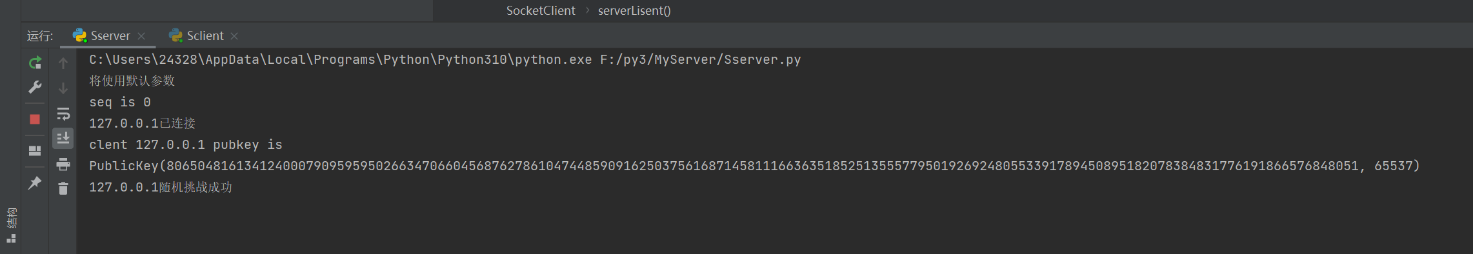


2.运行client用户程序

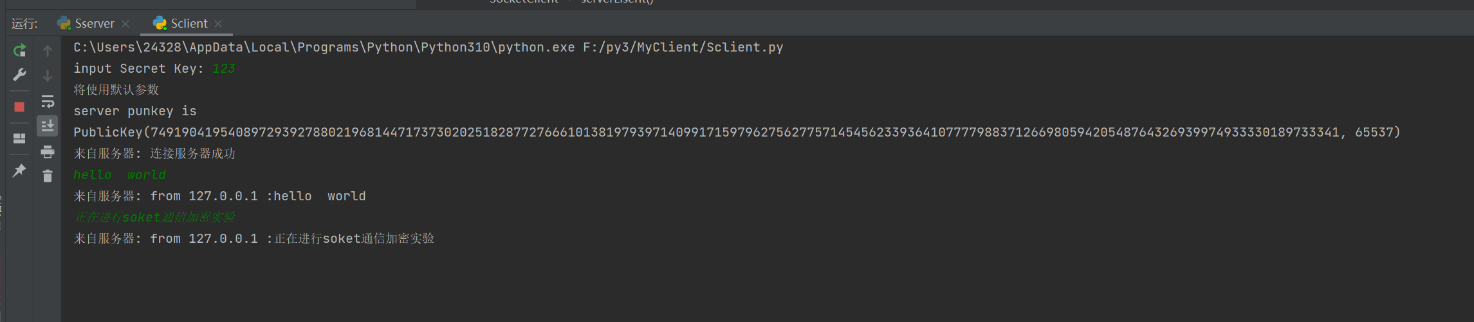


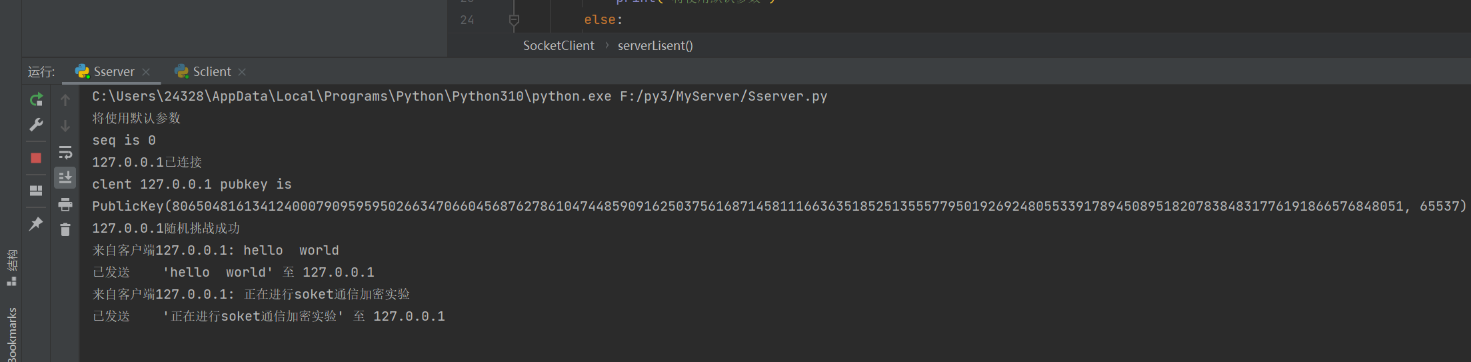
3输入key进行连接





1. *向服务器发送信息并加密，服务器接收信息并解密*





分析：

成功建立了socket网络简单的通信，并实现了信息的加解密与传输。

## 4.实现过程中遇到的问题、原因和解决

问题1：需要传输文件

解决：使用VMware tools快速传输文件

问题2：对python代码没有系统性的学习

解决：在网上寻找代码，多看多学，多了解

问题3：使用pycharm需要安装一系列的库函数 pip

解决：一步步排查原因，查找出错的问题，最后是path文件没有添加pip script路径。

## 5.实验总结

通过使用Python语言实现Socket编程，实现简单的socket通信以及通信加密。对网络通信过程中数据的传输有了一定的认识，并重新了解认识了RSA与AES加密，并了解其具体实现函数。但不可否认的是，在界面优化、缓存利用、数据传输、性能稳定，安全等诸多方面，仍然存在一些问题。还值得我们深入思索考虑。

6.思考

采取的加密算法的加密强度如何：对于目前计算能力来说1024位的RSA是安全的

对于并发的多用户要分别进行加密和解密，用分别生成对应的key进行加解密；

多个socket（套接字）如何管理？：使用高效的多路复用方法[epoll](https://so.csdn.net/so/search?q=epoll&spm=1001.2101.3001.7020" \t "_blank)解决策略