进度报告

组名：三人行

组长姓名：周磊

组长学号：2017210494

项目目标：实现建立一个C-S模型的私密聊天平台，实现身份认证、访问控制、多用户接入，并酌情加入文件传输、小游戏等附加功能。

关键问题：

* 1.Python网络套接字编程实现客户端与服务端、客户端与客户端的连接。
* 2.消息加密机制：服务器与客户端的通讯在初次建立时应采用RSA非对称加密机制，因为服务端与客户端可能先前没有商议好预共享密钥。初次通信时建立共享密钥。但首次连接后应该采取用共享密钥对称加密，因为这样效率较高。这需要pycrypto之类高级加密算法库的支持，并有较高的编程难度。

若不加密则存在消息被抓包获取的危险。

* 3.多线程问题，提高服务器的运行效率。
* 4. 以及消息的及时性和用户的个性化区别。

主要特性：

1.实现用户的个性分类，实现平台的趣味性。（后期可加标签功能）

2.进行信息的加密，以实现高级别安全。

3.后期可能加入gui界面。

4.后期可能实现程序的打包成exe功能。

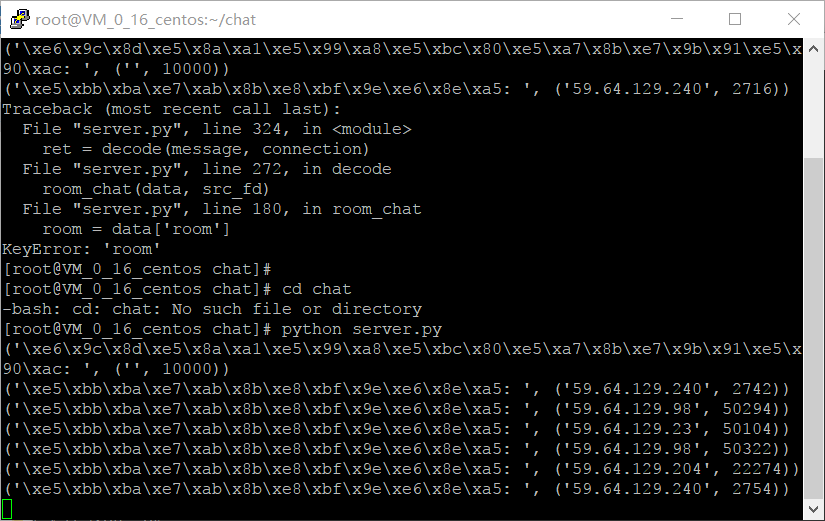
总体流程设计：

* 1. Client-Server架构基础功能:
* 客户端登录
* 私聊发信
* 在线情况核查
* 2.拓展功能：
* 文件传输与小游戏
* 账号事务管理：
  1. 客户端可以向服务器提交密码修改请求
  2. 服务端管理员可以重置用户密码
  3. 服务端管理员可以添加与删除用户
  4. 服务端管理员可以查看统计信息
* 客户端离线消息缓存（服务器存储的消息经过加密）

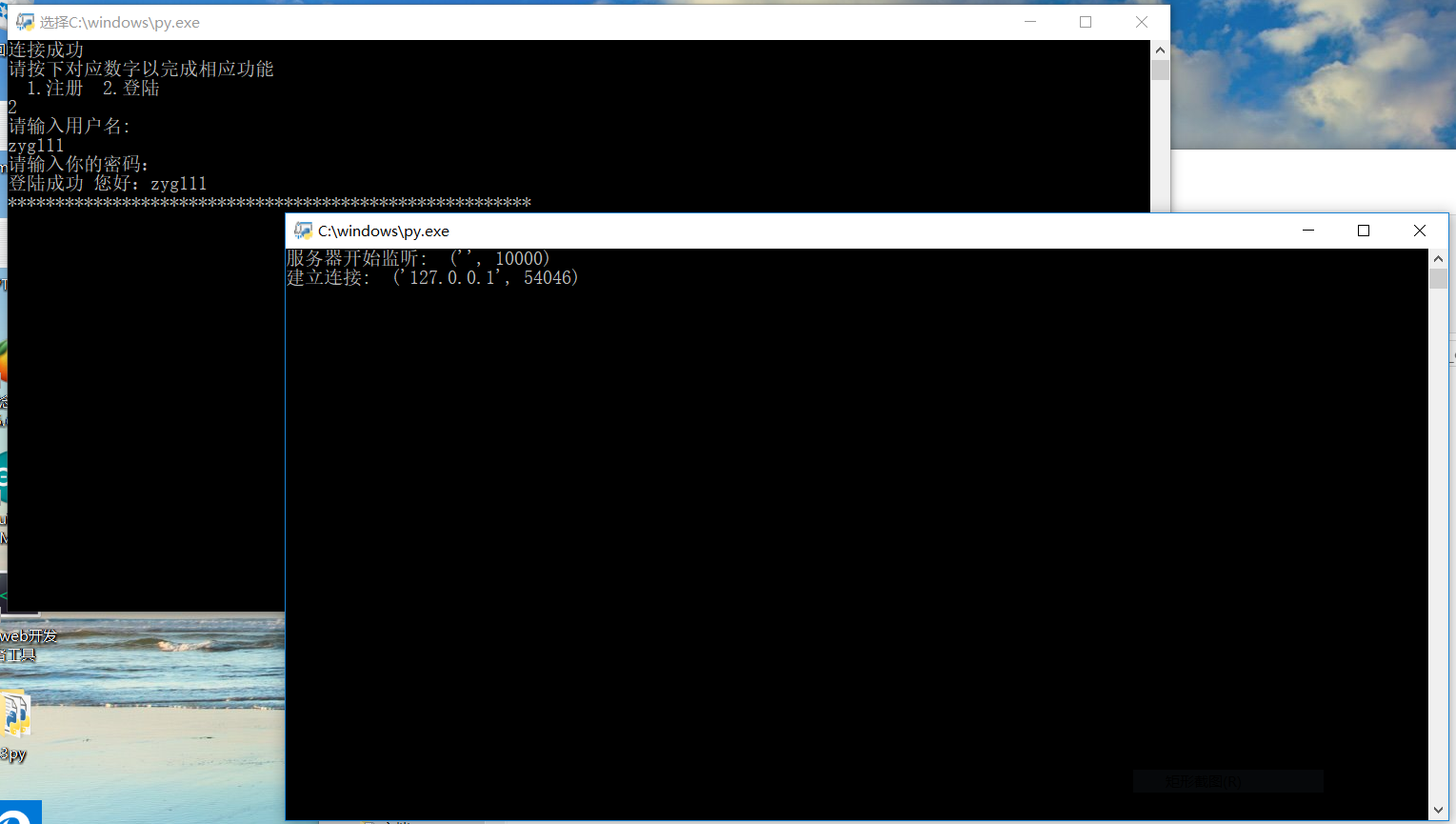
目前进展状况：

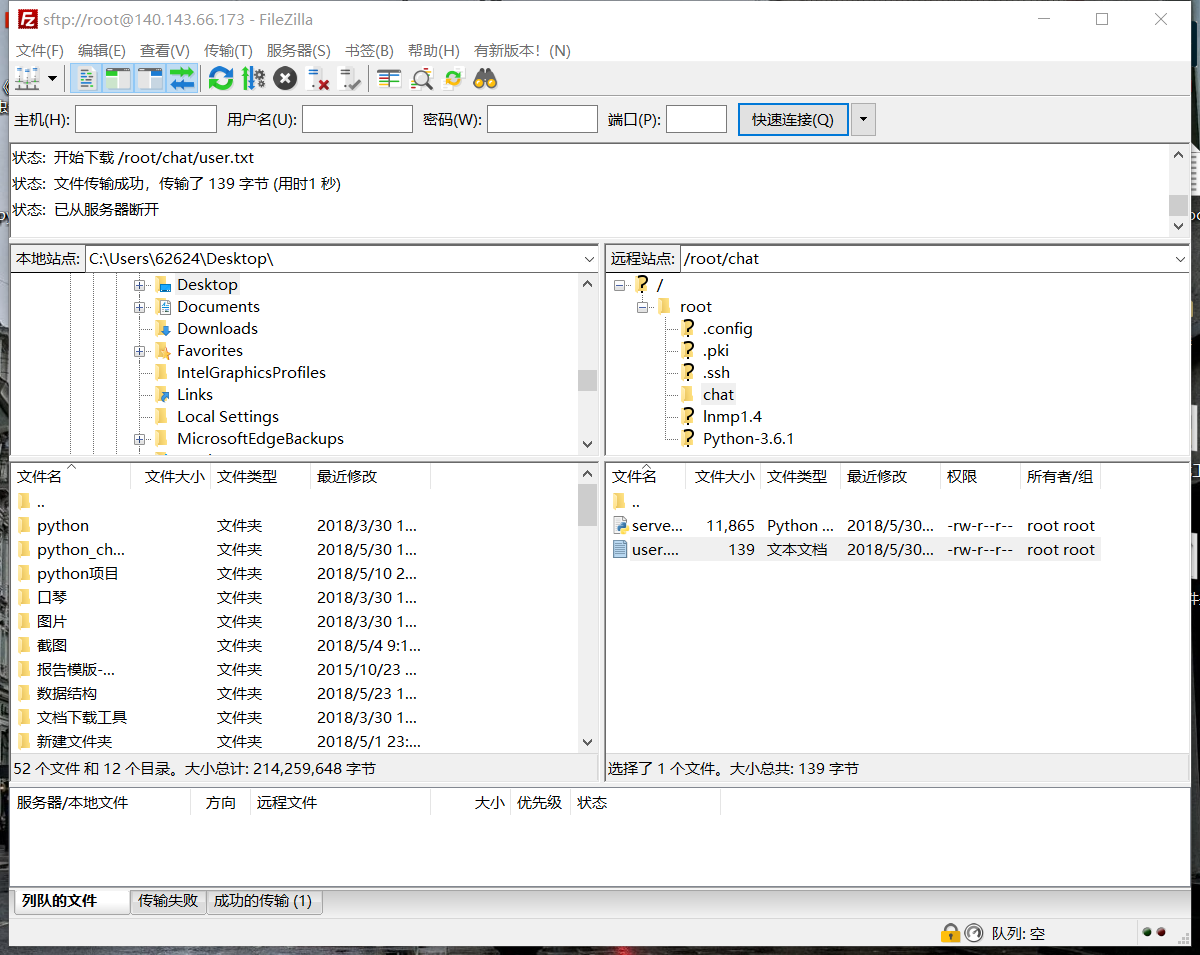
1.在云服务器上配置python3环境，并将初步的server.py部署到云服务器。

（5.31）

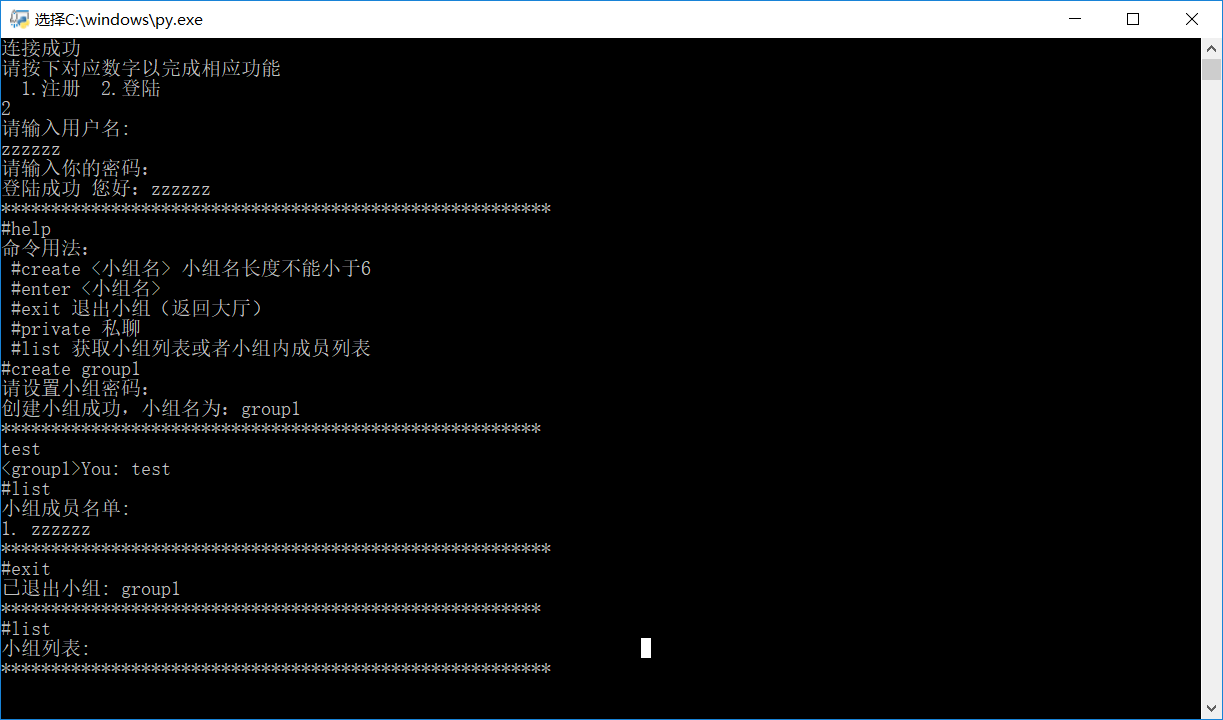


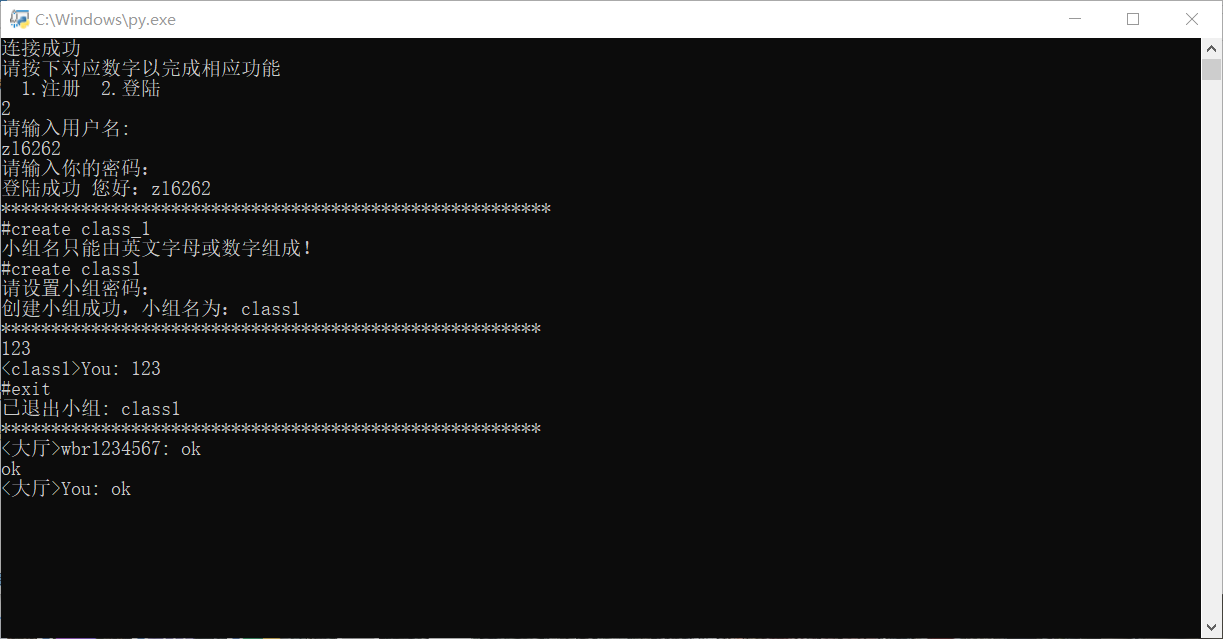
（由于服务器非中文环境，中文无法显示。在本地中文环境可正常显示，如下图所示。）



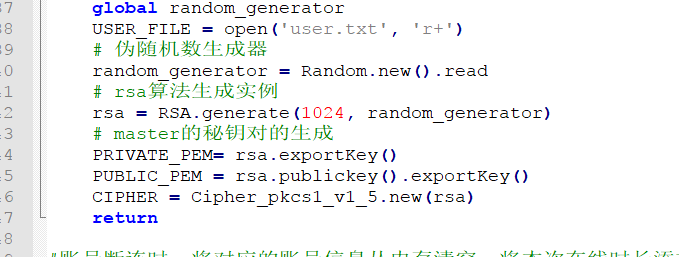
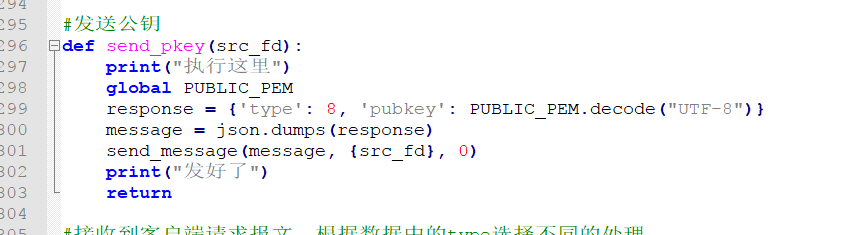
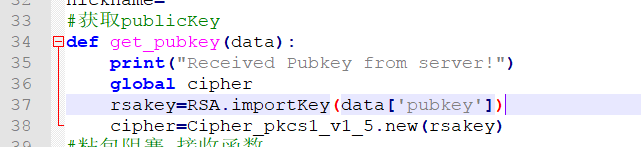


2.基本功能已经完善，如注册，登陆，存表，创建小组，加入小组以及私聊。但更多的情况并没有完全考虑，故需要不断的修订完善。(5.31)





3.(6.14)实现了第一次连接时的RSA非对称加密，防止被抓包获取密码，提高安全性。



4.（6.14）实现了普通聊天的AES对称加密。（增强信息的隐秘性）