TLS1.3实现用户手册

0.Requirements

1）运行环境Python3

2）需要额外安装的库函数python 包，PyCrypto、 PyCryptodome、cryptography

2.0）安装命令 python3 -m pip install libname

2.0）在linux系统中，python3没有将包secrets默认包含进去，如在linux系统中测试，需要在手动将secrets包加入到/usr/lib/python3/site-pakages目录下。Secrets包下载路径：https://github.com/python/cpython/blob/3.7/Lib/secrets.py

3）（可选）需要安装最新的openssl（version 1.1.0），生成自己的公钥和私钥以及签名证书。

1.Usage

1）服务器端使用命令

python3 main.py

根据使用提出命令操作，建议先设置主机IP和端口号（默认:127.0.0.1 4443），即先选择3

# C:\Users\ERIC_H~1\AppData\Local\Temp\1543497045(1).png

根据提示输入IP 地址和端口号即可。再次选择时选择2即可。

2）客户机使用命令

Python3 main.py

根据提示选择1即可。之后便可以输入想加密传输的数据。发送以及接受的数据将在屏幕上，便可以加密交流。

2.Certificate (可选)

1）客户群和服务器需要使用openssl生成各自的私钥、公钥、签名证书。使用链接: <https://www.openssl.org/docs/manmaster/man>

2）客户端需要命名为:client.key client.csr client.crt

3）服务器端需命名为：server.key server.csr server.crt

4）需要在main.py的同级目录下新建文件夹.ssh，将其生成的文件拷贝到其目录下。

5）服务器端需要移除原始.ssh文件夹。