Manual of myTLS

杨乙　21307130076　信息安全

项目结构

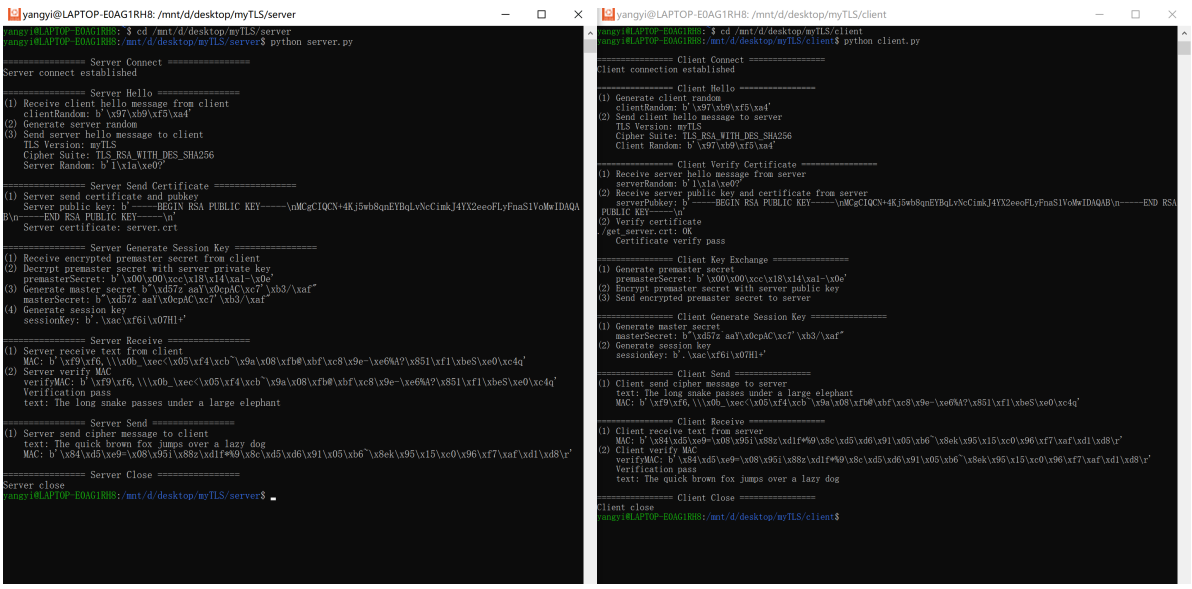
```
.
├── ca
│   ├── ca.crt
│   └── ca.key
│
├── client
│   ├── get_server.crt      # 运行时候生成
│   └── client.py
│
└── server
    ├── server.crt
    ├── server.key
    └── server.py
```

运行方法

先在一个终端定位到 `server` 文件夹，执行命令 `python server.py`

再在另一个终端定位到 `client` 文件夹，执行命令 `python client.py`

运行结果



注意事项

- **请在 Linux 环境下运行**（因为代码 `client.py` 使用 `os.system()` 运行的 `openssl` 命令只能在 Linux 环境下运行）
- 先运行 `server.py`，再运行 `client.py`
- 可能需要安装的第三方库（以指令的形式给出）：

```
pip install rsa
pip install hkdf
pip install pyDes
```

完成情况

基础部分：

- 客户端和服务器连接
- 产生会话密钥
- 加密和解密
- MAC和验证

额外部分：

- 服务器证书验证
- 双向传输

加密算法

密码交换	信息加密	MAC 生成与校验
RSA	DES	SHA256