**一.实验目标**

理解网络安全协议的功能和作用，提升学生对网络安全协议实现意识，增进学生分析网络安全协议、设计协议的能力，促进学生的团队合作意识和分组编程能力，实现具有一定功能的网络安全协议。

**二.实验要求**

在《计算机网络安全》课程实验的基础上，综合利用网络安全课程上基础实验的内容，编程实践一个具有一定功能的网络安全协议。具体可从如下三个实验中选择一个分组完成，具体要求：

1. 在实现RC4、DES、AES、SHA、RSA、DH算法的基础上，完成对基本算法的封装；
2. 三至四人分组完成：具有三个或以上设备，在Kerberos认证、安全网络通信、双重签名、简易区块链等三个内容中选择一个完成编程和展示；
3. 除了实现程序并展示外，还需完成程序的报告展示，并按照论文格式要求完成对实验开发及功能的完整描述。

**三.实验内容**

Kerberos认证包括：访问者、认证服务器、票据授权服务器、服务器共四方。访问者项认证服务器发送申请，并认证身份信息；认证服务器基于内部存储的用户名-密码，对访问者身份认证、发送认证票据；访问者获得认证票据后，向票据授权服务器提交具体服务申请；票据服务器认证访问者票据，并根据内部存储的权限信息发出服务票据或拒绝票据；如果访问者获得服务票据，服务者将服务票据发给服务器，服务器认证票据后，对访问者提供服务。

**四.实验分析**

根据实验内容将程序分为 AS,TGS,Client,Server\_v 4部分。

AS:处理Client发送的消息，根据IDc获取Kc，根据IDtgs获取Ktgs，生成随机密钥Kc\_tgs用Ktgs加密一个TGT（Kc\_tgs,IDc,ADc,IDtgs,TS2,LF2）向客户端发送用Kc加密的IDtgs,TS2,LF2,TGT。

TGS：处理Cilent发送的消息，用自己的密钥Ktgs解密TGT获取Kc\_tgs,用Kc\_tgs解密Auth根据TGT的信息和Auth信息进行对Client验证，如果身份符合，生成随机密钥Kc\_v并用Kv加密生成Ticket(Kc\_v,IDc,ADc,IDv,TS4,LF4)，向Client发送用Kc\_tgs加密的消息Kc\_v，IDv,TS4,Ticket。

Client：客户端向AS发送消息IDc || IDtgs || TS1,获取AS发送消息用用户密码解密获得Kc\_tgs,TGT。再连接TGS向TGS发送Auth||TGT，Auth是用Kc\_tgs加密的IDc || ADc || TS3。

获取TGS发送的消息用Kc\_tgs解密获得Kc\_v，Ticket，IDv，TS4将Ticket和Auth发送给Server根据Server返回的消息确定是否验证成果。其中Auth是用Kc\_v加密的IDc,ADc，TS5。

Server：获取Client发送的消息，用自身密钥解密Ticket，用解密得到的Kc\_v解密获得Client的认证信息，验证成功向Client发送消息，否则断开连接。

**五.实验结构流程图**

## Client：



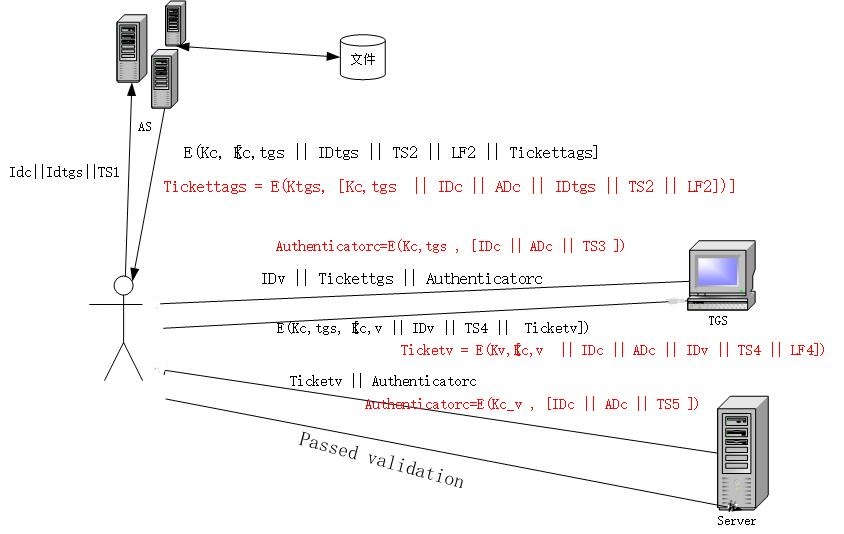
## TGS：



## 服务端：



**整体结构体**



**六.具体实现(个人)**

根据实验的需要，本次实验采用面对对象的方式对实验进行分模块处理。

**1.SOCKET模块**

基于ip和端口建立客户端和服务端并返回sock方便其他模块调用。

**2.User模块**

将Client功能封装到User类中，通过不同的函数处理实现Client功能。

**3.TGS模块**

将TGS功能封装到TGS类中，通过不同函数处理TGS功能。

**4.SERVER模块**

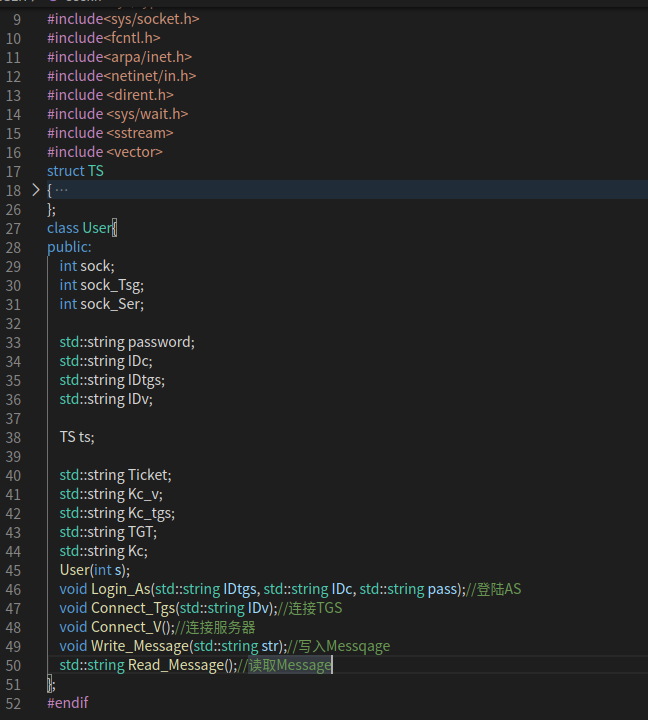
将SERVER功能封装到SERVER类中，通过不同函数处理SERVER功能。

**5.功能模块**

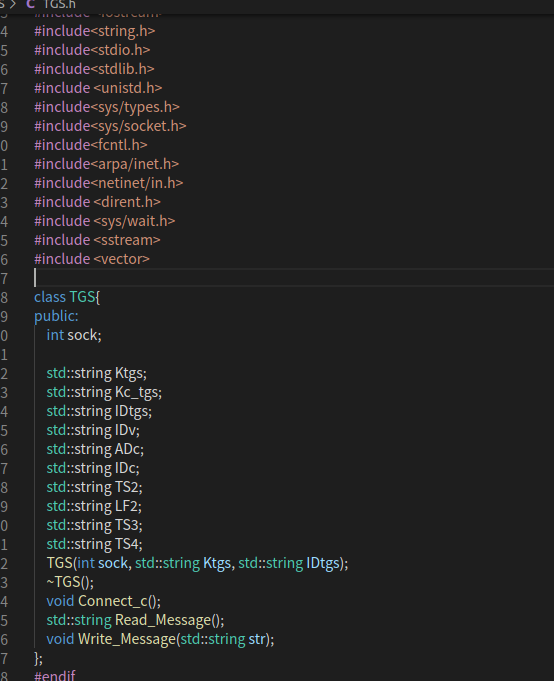
将每个模块用到的功能写到funcion.h中方便其他模块调用函数。

**七.成果展示**

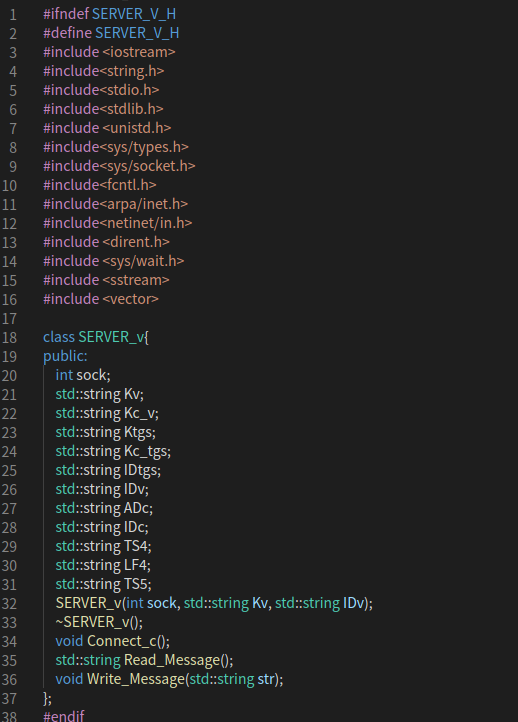
1. **User类**



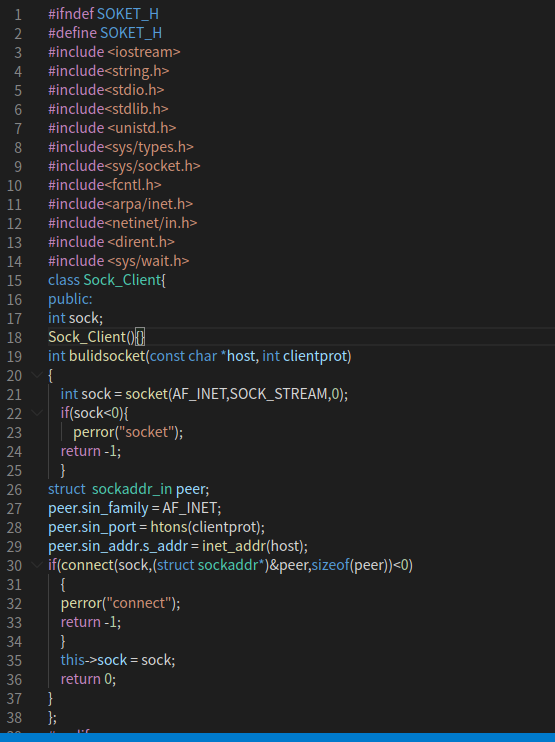
1. **TGS类**



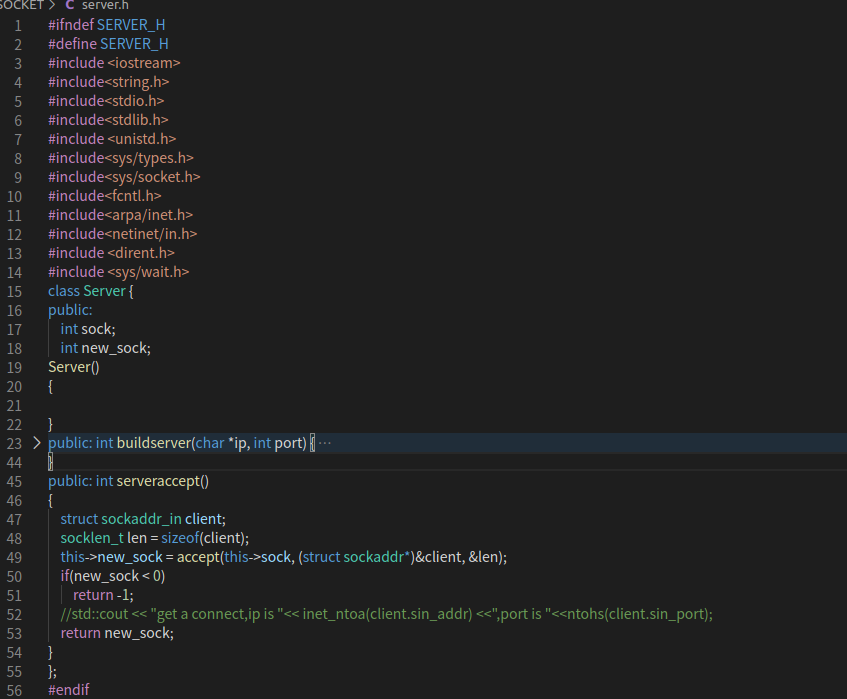
1. **SERVER类**



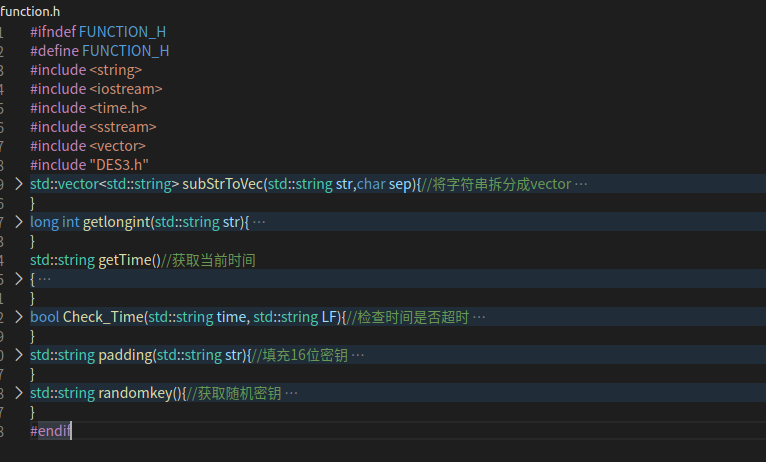
1. **Socket客户端类**



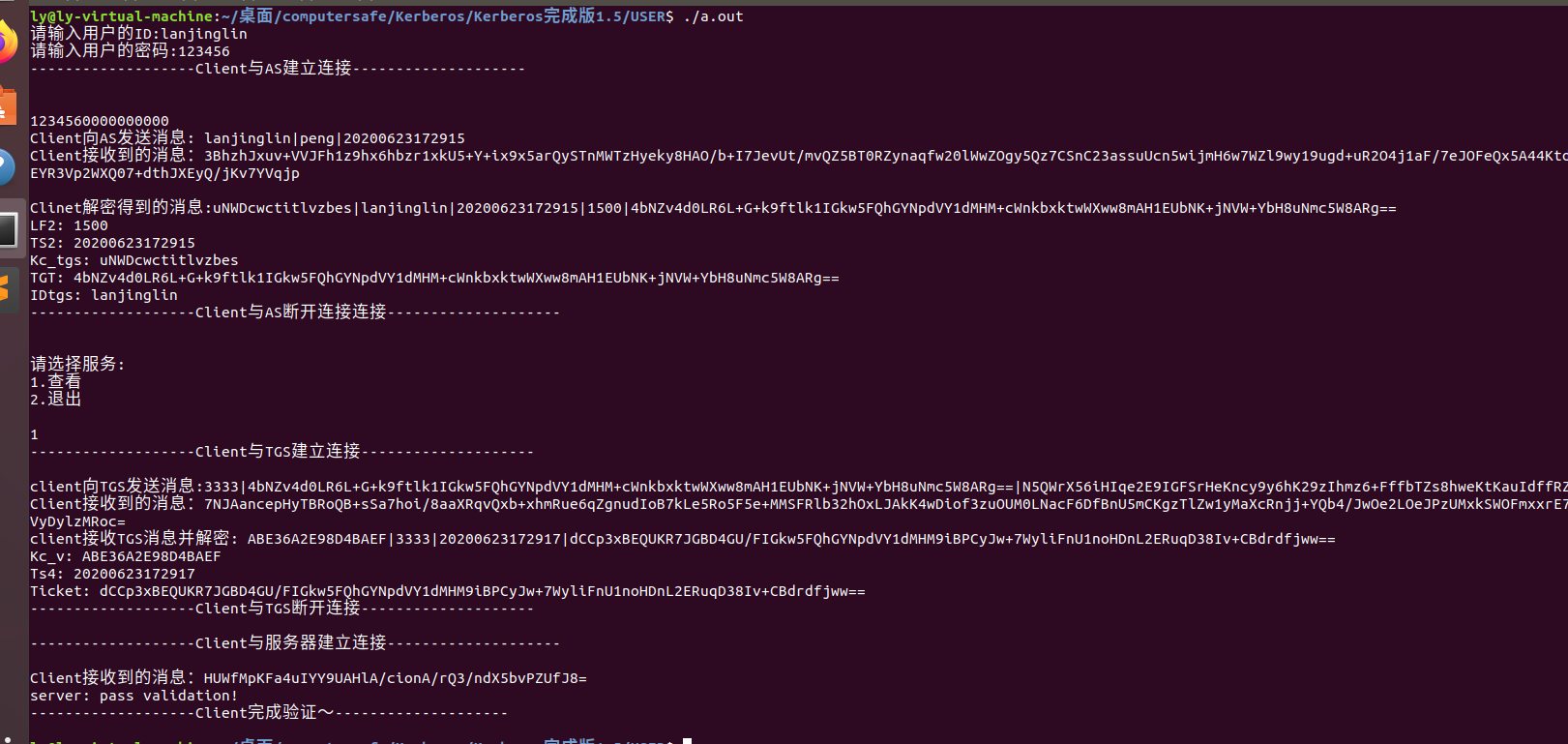
1. **Socket服务端类**



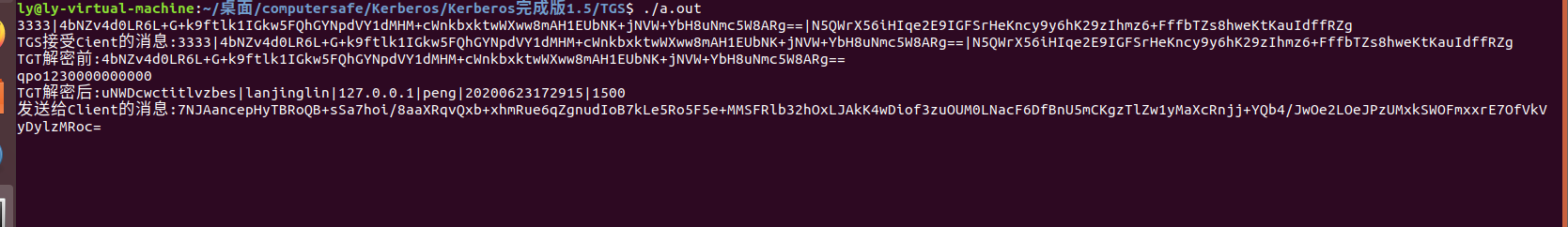
1. **Function.h**



Client运行截图



TGS运行截图



SERVER运行截图

