网络安全技术课程实验报告

**实验一**



**实验名称：\_\_\_\_\_\_\_ 基于DES加密的TCP聊天程序\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**姓名：\_\_\_\_\_\_\_\_\_\_\_\_卢天鉴\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**学号：\_\_\_\_\_\_\_\_\_\_\_\_1911445\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**专业：\_\_\_\_\_\_\_\_\_\_计算机科学与技术\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**提交日期：\_\_\_\_\_\_\_\_2022/3/18\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

## 一、实验目的

①理解DES加解密原理。

②理解TCP协议的工作原理。

③掌握linux下基于socket的编程方法。

## 二、实验要求及要点

①利用socket编写一个TCP聊天程序。

②通信内容经过DES加密与解密。

## 三、实验内容

## 1.具体过程：

DES加密解密设计实现:

首先定义封装DES操作的类CDesOperate，类的私有成员包括生成的16轮迭代密钥，初始密钥，以及加密解密流程中用到的四个函数。公有成员包括构造函数，析构函数，以及根据上述的四个函数封装的加密函数与解密函数，方便调用。

2.结果截图：

3.遇到问题及解决方法：

4.参考资料：

## 四、个人总结

本次实验主要训练了在LINUX系统下的网络套接字编程，了解学习了DES加密的算法和核心思想。