网络安全技术课程实验报告

**实验一**



**实验名称：\_\_\_\_\_\_\_实验1 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

DES（Data Encryption Standard）算法是一种用56位有效密钥来加密64位数据的对称分组加密算法，该算法流程清晰，已经得到了广泛的应用，算是应用密码学中较为基础的加密算法。TCP（传输控制协议）是一种面向链接的、可靠的传输层协议。TCP协议在网络层IP协议的基础上，向应用层用户进程提供可靠的、全双工的数据流传输。

本章训练的目的如下。

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

## 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。