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。

文本

描述已自动生成

定义使用的静态数组

初始置换IP，逆初始置换IP，按位取值或赋值，置换计算，E盒，压缩S盒，等分变换等等。

：

文本

描述已自动生成

文本

描述已自动生成

DES密钥生成:

DES密钥是一个64bit的分组，但是其中8bit是用于奇偶校验的，所以密钥的有效位只有56bit，由这56bit生成16轮子密钥。

密钥生成，首先将有效的56bit进行置换选择，将结果等分为28bit的两个部分，再根据所在的迭代轮数进行循环左移，左移后将两个部分合并为56位的密钥，从中选取48位作为此轮迭代的最终密钥，共生成16个48位的密钥。每一个密钥，分为两个24位的部分放在一个ULONG32的二维数组中保存。

文本

描述已自动生成

DES加密运算:

DES的加密运算也分为16轮迭代。

首先将明文分为64bit的数据块，不够64位的用0补齐。每一轮中，对每一个64bit的数据块，首先进行初始换位，并将数据分为32bit的两部分：

经过初始置换并且分组之后，将进行DES加密算法的核心部分。

首先，保持左部不变，将右部由32位扩展成为48位，分别存在两个ULONG32类型的变量里，每个占24bit。再将右部扩展成为48位之后，与该轮的密钥进行异或操作，由于48位分在一个ULONG32数组中的两个元素中，故要进行两次异或。在异或操作完成之后，对新的48位进行压缩操作，即S盒。

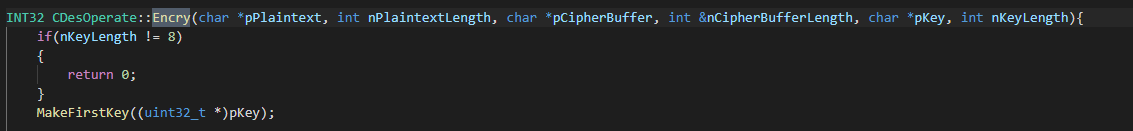
将其每取6位，进行一次操作。8个6bit的数据存在ULONG rexpbuf[8]中，然后进行数据压缩操作，每一个6位经过运算之后输出4位，故最终输出的是32位的压缩后的数据。

再把左右部分进行异或作为右半部分，最原始的右边作为左半部分，即将完成一轮完整的加密操作。最后进行逆初始置换，完成一轮完整的加密操作。

封装DES加密函数：

将上述运算整合在一起，可以封装成一个加密函数，以便于调用，其中pPlaintext为明文部分，nPlaintextLength为明文长度，pCipherBuffer为准备存放密文的缓冲区，nCipherBufferLength为密文长度，pKey为密钥，nKeyLength为密钥长度。

首先检查初始密钥长度，若正确，则创建16轮迭代的密钥。

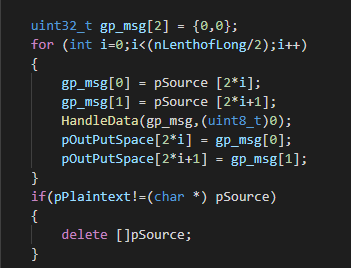


由于加解密均要以32bit为单位进行操作，故需要计算相关参数，以确定加密的循环次数以及密文缓冲区是否够用，确定后将需要加密的明文格式化到新分配的缓冲区内。

文本

描述已自动生成

开始对明文进行加密，加密后将之前分配的缓冲区从内存中删除。



TCP聊天程序设计:

服务端：

文本

描述已自动生成

先设定服务端地址，然后绑定套接字，进行监听，等待来自客户端的请求链接。

客户端：

客户端同服务端类似，先设定地址，然后与正在监听的服务端进行链接。聊天调用加密聊天函数，设置密钥为lutianjian。

文本

描述已自动生成

加密聊天函数：

该函数在完成必要的错误检查后，调用fork()函数创建了一个子进程，如“if(nPid != 0)”满足，则代表当前进程为父进程，否则为子进程。父进程负责接收密文消息，解密并输出到屏幕；同时子进程负责从标准输入读取消息，加密并发送到指定套接字，两个进程完全并行，实现实时聊天的功能。

文本

描述已自动生成

2.结果截图：

文本

描述已自动生成

可以看到该程序是全双工的，互相可以发送聊天信息。

同时经过了DES加密。

3.遇到问题及解决方法：



这个问题出现了密钥长度问题，经过排查可以得到：

定义密钥时字符串长度为4的倍数 不然在解密的时候会出现报异常 字符串长度问题

## 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，同时对全双工的通信有着更深的理解。现代密码学的特征是算法可以公开。保密的关键是如何保护好自己的密钥，而解密的关键则是如何能破解得到密钥。系统的安全管理者，要根据本系统实际所使用的密钥长度与其所保护的信息的敏感程度、重要程度以及系统实际所处安全环境的恶劣程度，在留有足够的安全系数的条件下来确定其密钥和证书更换周期的长短。同时，将己废弃的密钥和证书放入黑库归档，以备后用。密钥更换周期的正确安全策略是系统能够安全运行的保障，是系统的安全管理者最重要、最核心的日常工作任务。