**课程编号：** A0802260030

信息安全工程实践2

总结报告



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **姓名** | **黄能文** | **学号** | | **20184875** |
| **班级** | **软信1802** | **指导教师** | | **马毅** |
| **实验名称** | **信息安全工程实践2** | | | |
| **开设学期** | **2019-2020夏季学期** | | | |
| **开设时间** | **第1周——第2周** | | | |
| **报告日期** | **2020年7月23日** | | | |
| **评定成绩** |  | | **评定人** |  |
| **评定日期** |  |

**东北大学软件学院**

1. 实践目的与意义

熟悉并且能完成密码学与计算机的实际项目。不仅从理论上要了解密码学的各种加密解密，还要能使用计算机实现这个项目。最终达到学以致用的目的。

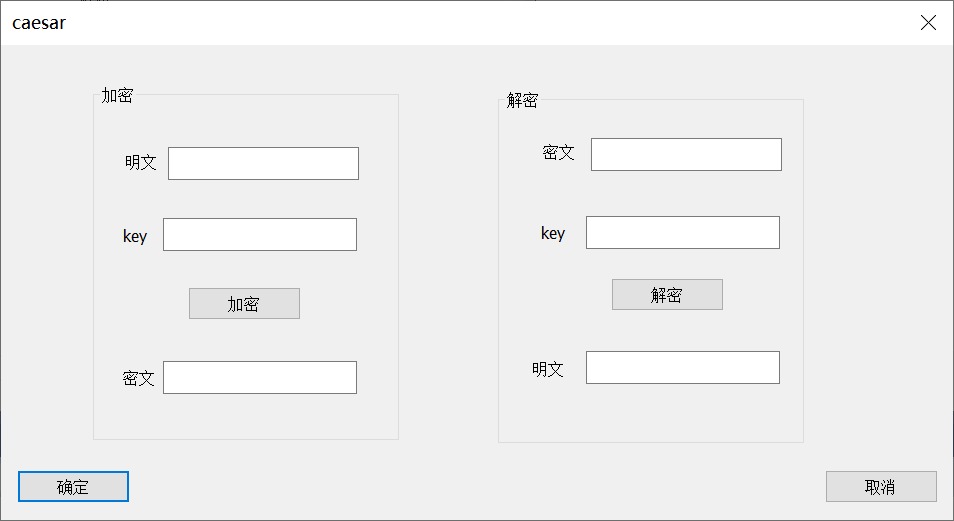
1. 实践环境

VS stdio，MFC，C语言

1. 系统设计

分8个部分，分别是：凯撒密码、维吉尼亚密码、playfair密码，列置换密码、RC4、DES、RSA、DH。每个部分都有自己的窗口。每个窗口包含待加密文本的输入框，密钥输入框，密文输出框和待解密文本输入框，密钥输入框和明文输出框及加密解密按钮。

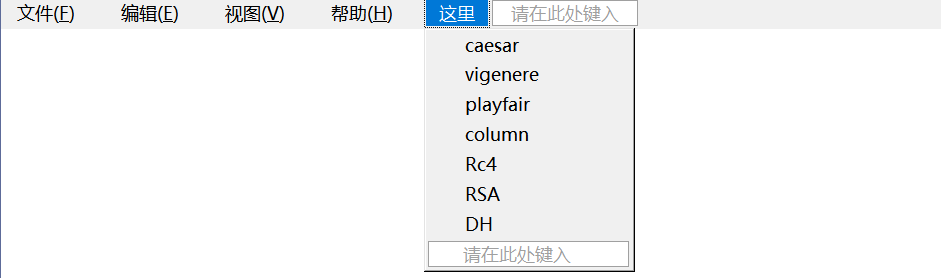
例图：



1. 系统实现

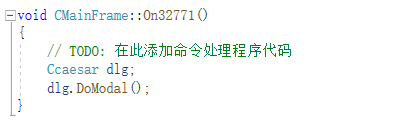
整体：

启动位置：

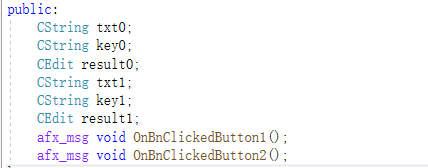


使用菜单来启动对话框，对话框包含对应功能

启动函数如下：

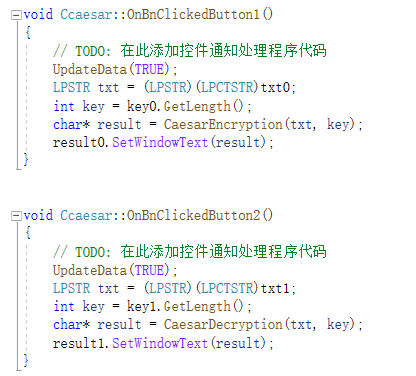


对话框功能实现的变量：



统一采用这六个变量，避免混淆。且功能函数封装良好，避免输入错误。

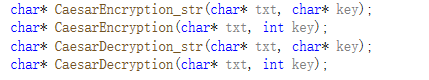
对话框按钮的功能实现：



得益于形式的统一，按钮点击函数也很统一，只需修改函数名就差不多了。

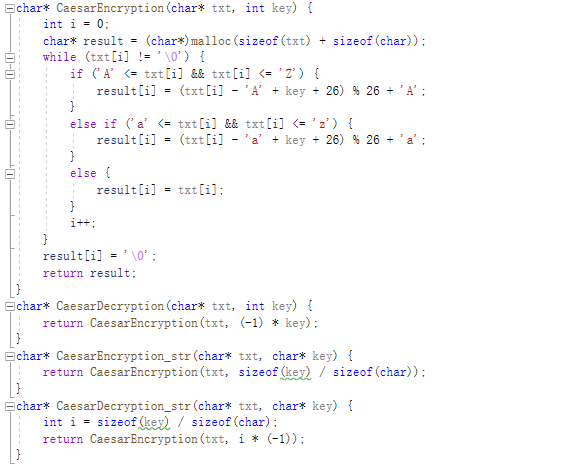
凯撒密码：

函数;



凯撒密码计算只需要int key 和文本就够了，其它几个都没什么区别。

实现：



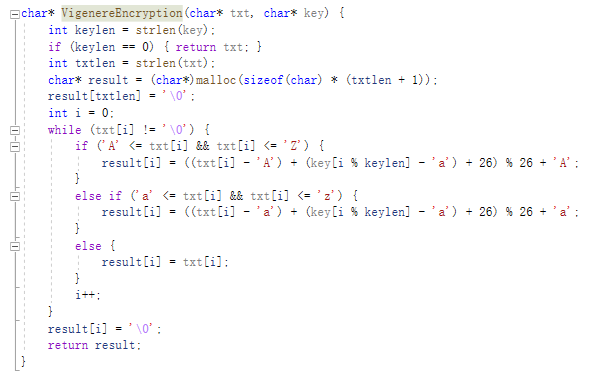
利用ascii码来使字符移位，区分大小写，为大小写都提供服务。解密函数只需要改变密钥，再使用加密函数，使文本循环一周就可以了。

维吉尼亚密码：

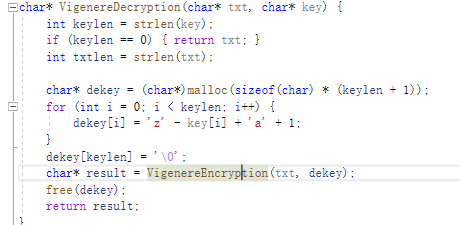
声明：



实现：



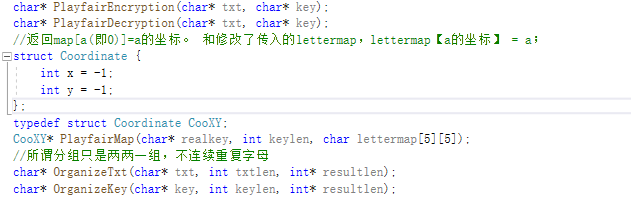
其实与凯撒类似，只不过。移位用的密钥是循环的数。



解密与凯撒同理

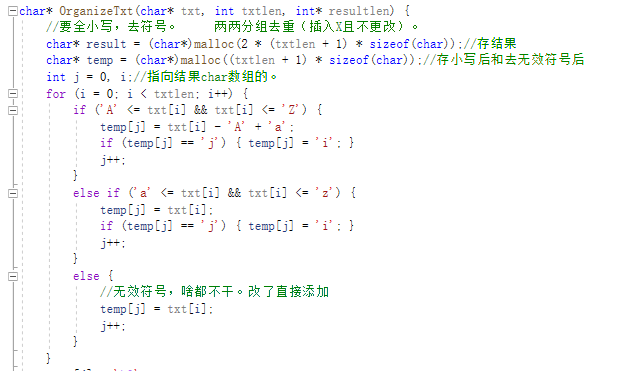
Playfair密码：

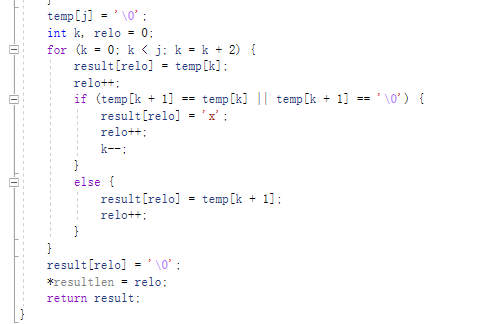
声明：



实现：

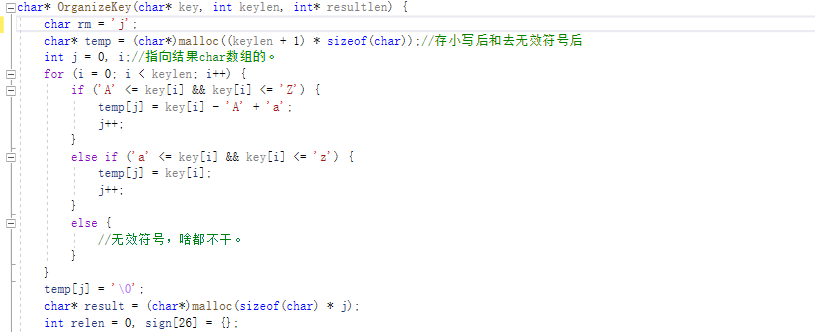
1.明文处理函数

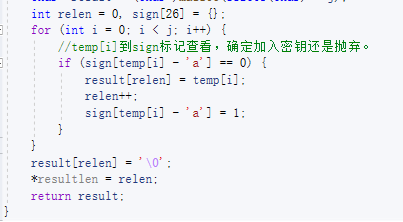




把明文两两分组处理，因为麻烦就干脆丢弃符号了。且统一用i替换j。

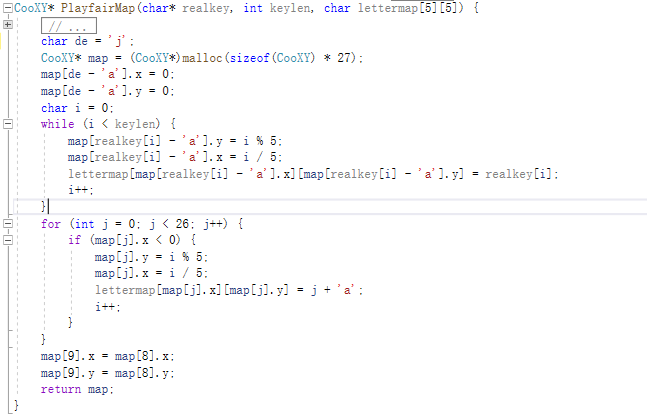
1. 密钥处理函数





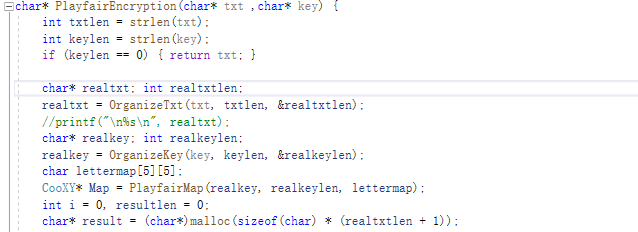
密钥去重和去无用字符。

1. 生成密钥图函数：

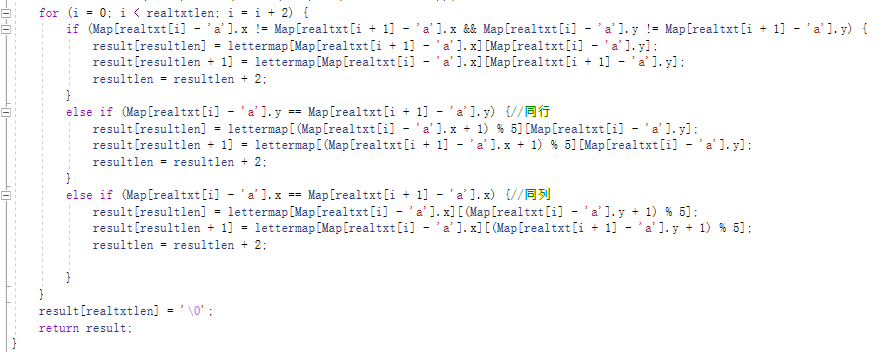


利用密钥生成图

1. 加密函数：

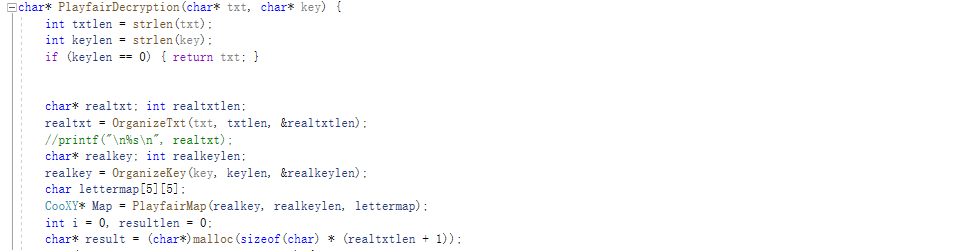


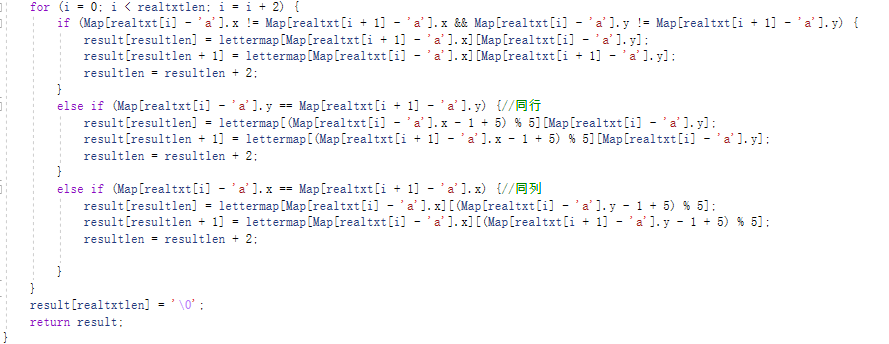
利用已有的函数准备



两两处理，3种形式

1. 解密函数：

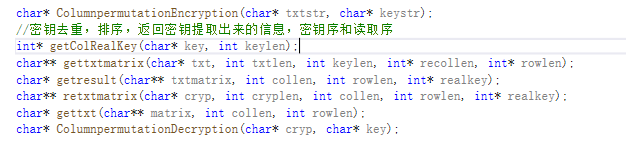




加密和解密的区别仅在于同行和同列的情况。

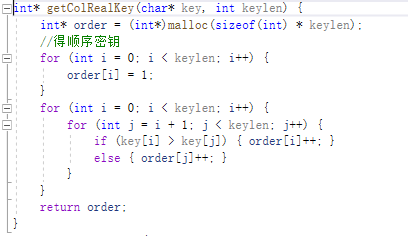
列置换：

声明：



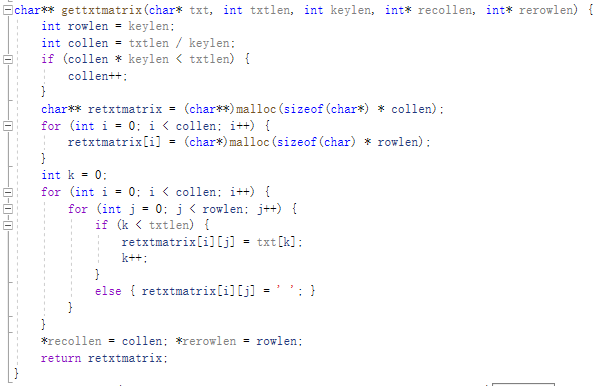
实现：

1. 获得数字形式的密钥：



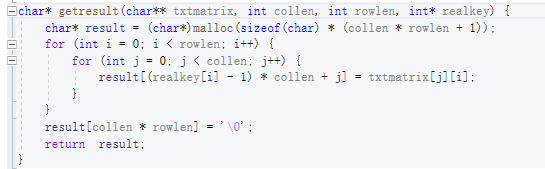
用比较得密钥顺序

1. 获得文本矩阵



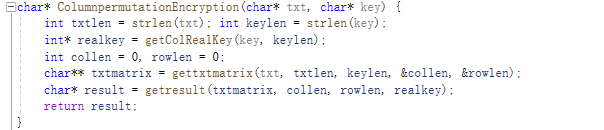
排列文本矩阵，空位补空格

1. 文本矩阵和数字密钥的处理：



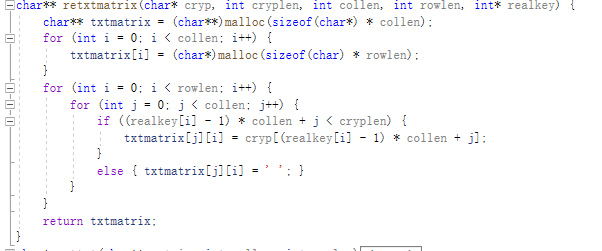
数字密钥和文本矩阵得密文

1. 整体作为一个加密函数：

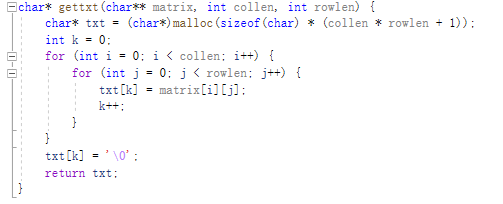


依次调用

1. 密文返回矩阵：

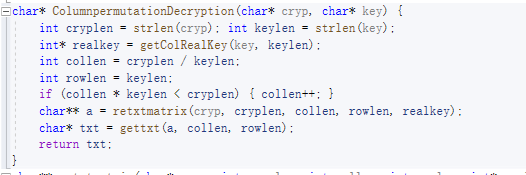


1. 矩阵返回明文：



逆操作

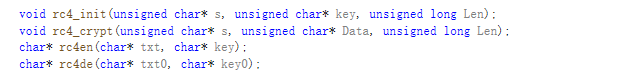
1. 整体的解密函数：



依次调用

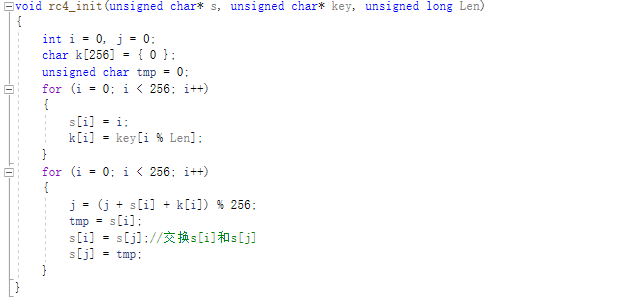
RC4

声明：

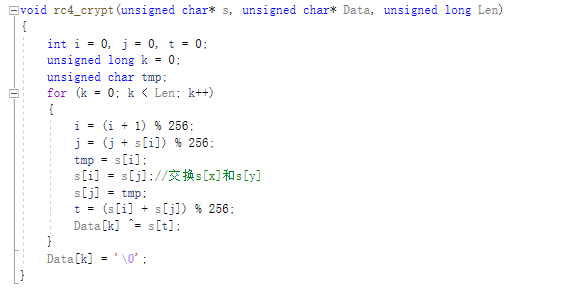


实现:

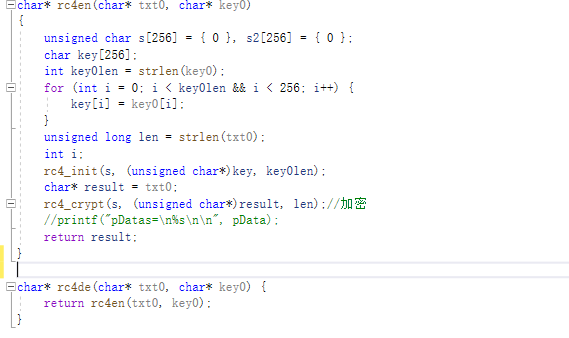
1. 初始化密钥流



1. 用密钥流加密函数



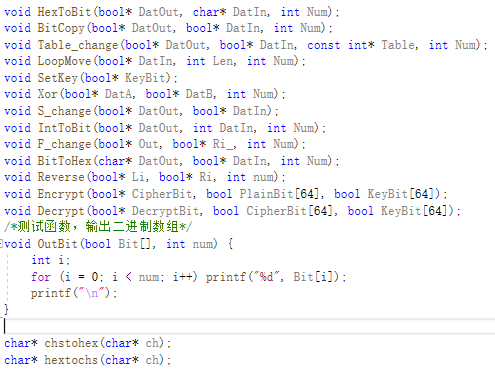
1. 加密和解密函数



DES

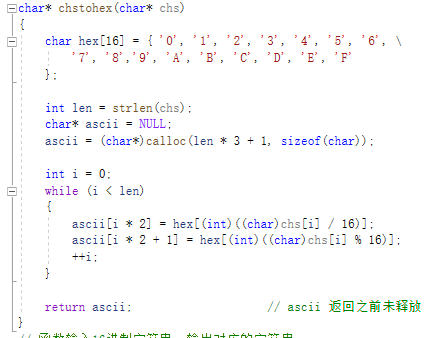
声明：



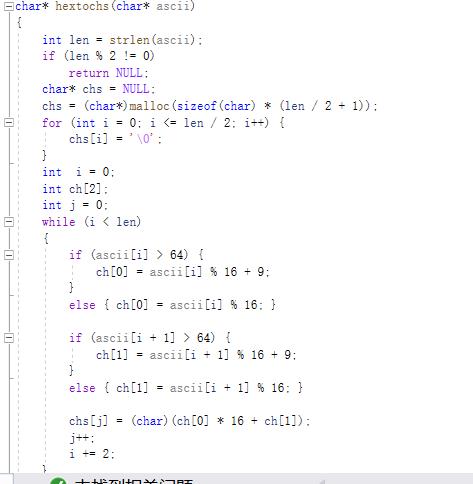


实现：

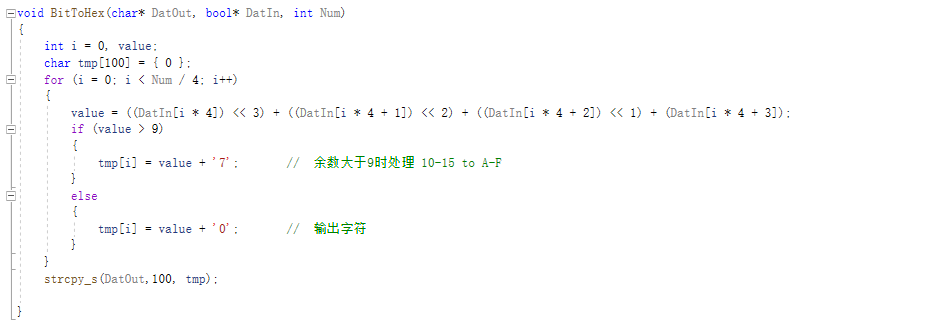
1. Ascii文本转16进制



1. 16进制转ascii文本



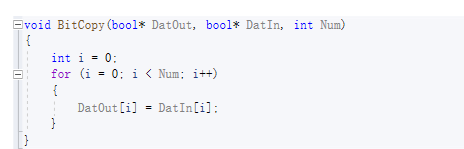
1. 2进制转16进制



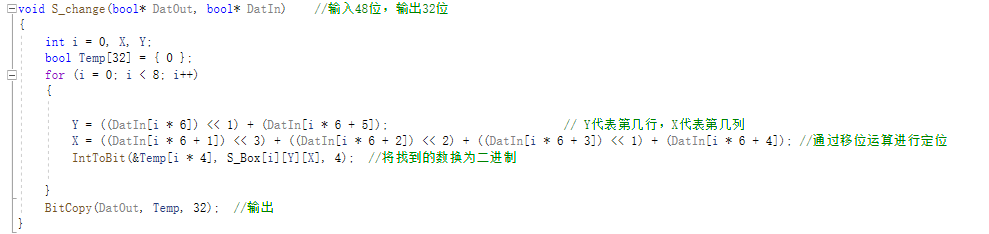
1. 16进制转2进制



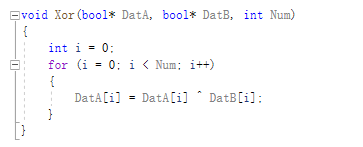
1. 2进制数组复制函数



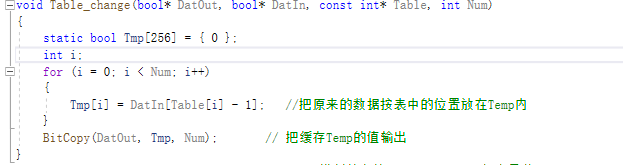
1. S变换



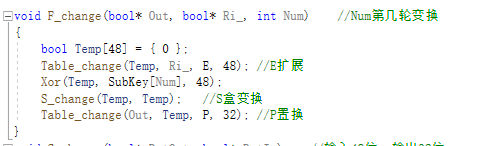
1. 异或函数



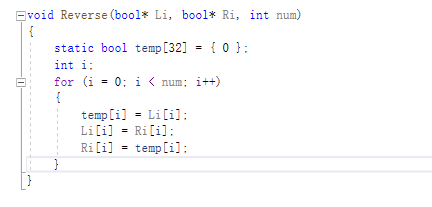
1. 按表调整位置



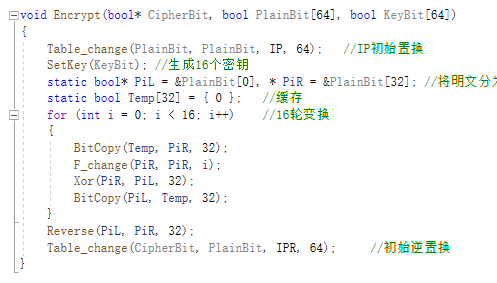
1. 交换



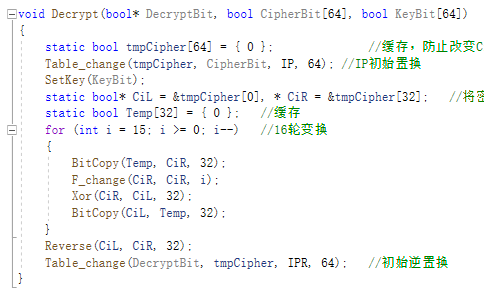
1. 左右互换



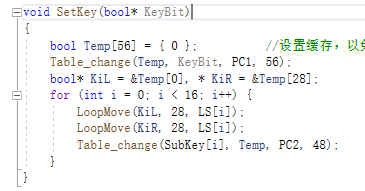
1. 以64位一组加密



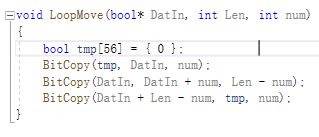
1. 以64位一组解密：



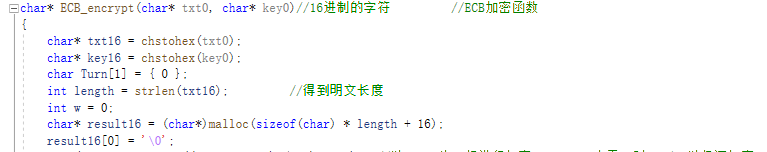
1. 2进制密钥生成

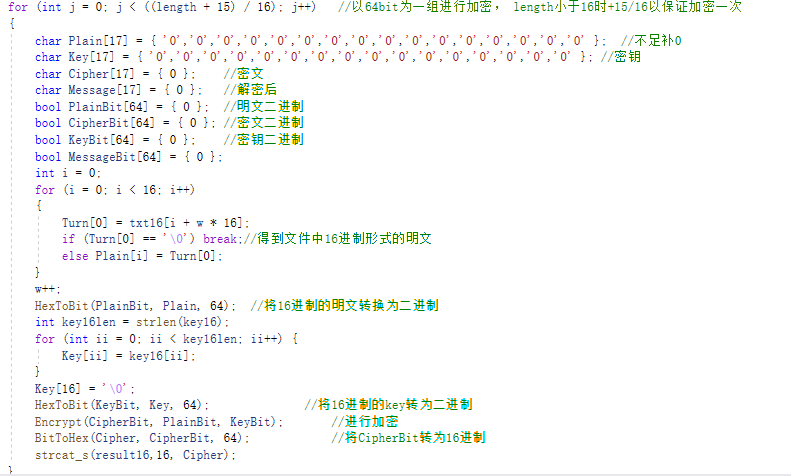


1. 2进制循环移位函数



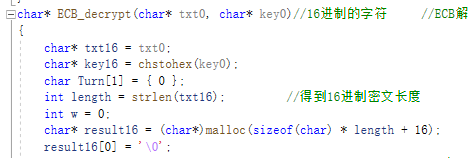
1. Ascii字符串明文，密钥。输出16进制密文函数

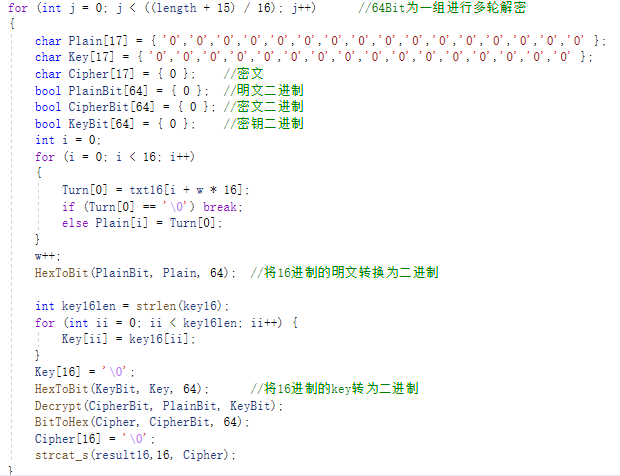






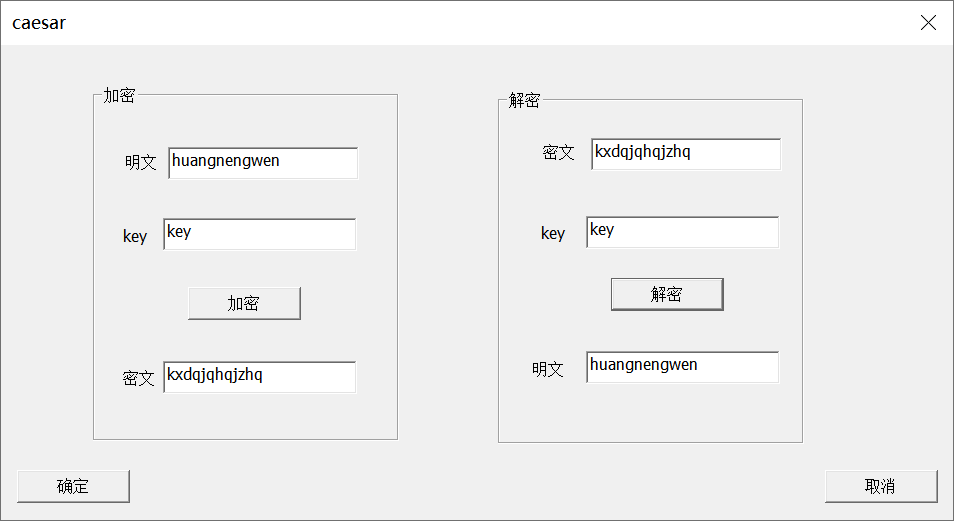
1. 16进制密文和ascii字符密钥输入，输出ascii明文





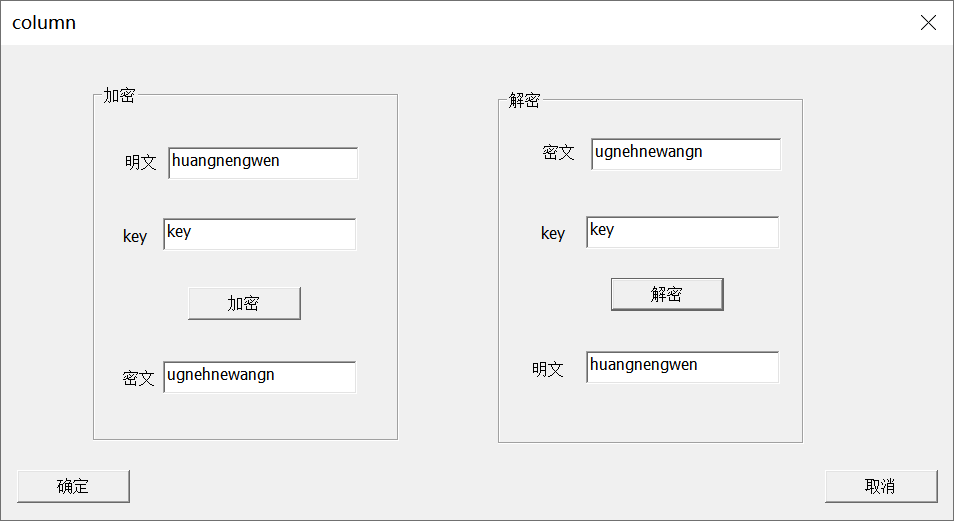


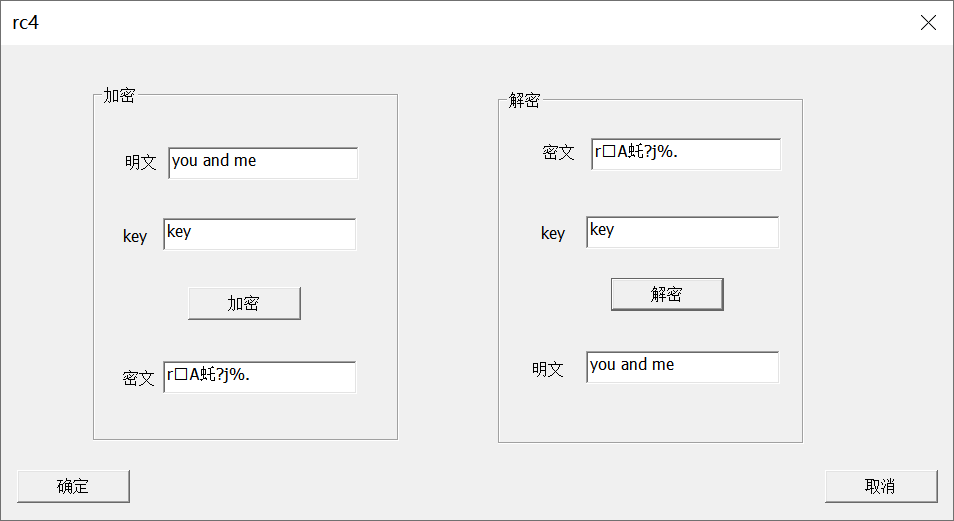
1. 系统测试









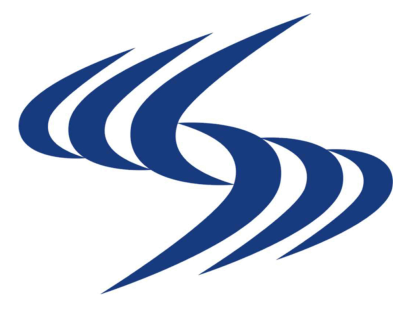


六、 结束语

**通过这次实践，我受益良多，重新回顾密码学的知识，更往前一步，将他做出来，做之前有很多的担心害怕，但做着做着就感受到进步的开心。而且对密码学的加密解密更加理解，精巧，重要性，不言而喻。**

**虽然实践结束了，但我感觉到我还需要练习，我深深的感受到我的能力不足，我希望我继续完成这个项目。**

**《信息安全程序实践2》成绩评定表**



|  |  |  |  |
| --- | --- | --- | --- |
| **评价内容** | **具 体 要 求** | **分值** | **得分** |
|
| **报告质量** | **实验报告格式规范，符合要求；报告内容充实、正确，实验目的归纳合理到位。** | **20** |  |
| **平时表现** | **课程设计过程中，无缺勤现象，态度积极，具有严谨的学习态度和认真、踏实、一丝不苟的科学作风。** | **10** |  |
| **提交材料及实践验收成绩** | **能够按照规范提交课程设计要求的所有材料（要求在以“学号-姓名”命名的文件夹中，包含实验报告电子版和实验源代码等），材料完备，格式内容等符合要求。能够按实验要求合理设计并开发出程序，功能完整性强，原理及实验结果分析准确，归纳总结充分。答辩认真，清晰，分工明确。** | **60** |  |
| **创新性** | **对完成选做实践项目过程中有创新性。** | **10** |  |
| **总 分** | | |  |