课程设计（论文）

课程名称： C语言程序设计

学院： 装备工程学院

姓名： 李乔琦

学号： 2111020123

指导老师： 张东阳

目录

[一、绪论 3](#_Toc103783023)

[（一）、研究的目的和意义 3](#_Toc103783024)

[（二）、国内外研究现状 3](#_Toc103783025)

[（三）、研究的思路与方法 3](#_Toc103783026)

[二、系统分析与设计 3](#_Toc103783027)

[（一）、系统分析 3](#_Toc103783028)

[（二）、系统设计 4](#_Toc103783029)

[（三）、结论 6](#_Toc103783030)

[三、本课程学习的总结 6](#_Toc103783031)

[四、参考文献 7](#_Toc103783032)

**维吉尼亚密码加密程序设计**

一、绪论

（一）、研究的目的和意义

随着经济全球化和信息化的发展，以互联网为平台的信息基础设施，对整个社会的正常运行和发展起着关键的作用，网络信息对社会的发展有重要的支撑作用。但网络空间面临的威胁也与日俱增，所以加强网络空间安全已经成为国家安全战略的重要组成部分。

密码是使用特定变换对数据等信息进行保护或安全认证的物项技术。使用密码对信息进行加密保护和安全认证，目的是有效地保证网络空间中的信息安全，对维护网络空间安全，维护信息安全，保护机密敏感信息具有重要的意义。

（二）、国内外研究现状

现代公钥密码的安全性基于数学上的困难问题，有坚实理论基础，包括信息论、计算复杂性理论、数论、概率论等，已经成为一门学科。现代密码学的任务已经不局限于传统密码的保密通信，而是含义更广的信息安全，其中包括保密通信、数据加密、身份认证、数字签名、密钥协商、秘密分享等重要的功能。

21 世纪初，我国研究并推出了系列商用密码算法，包括祖冲之序列密码算法、SM2 公钥密码算法、SM3 密码杂凑算法、SM4 分组密码算法、SM9 标识密码算法，其逐渐成为国际密码精准。如今，密码学的应用已经深入人们生活的各个方面，如数字证书、网上银行、身份证、社保卡和税务管理等，密码技术在其中发挥了关键作用。

近年来，其他相关学科的快速发展，促使密码学中出现了新的密码技术，如 DNA 密码、混沌密码和量子密码等。整个密码学的发展是由简单到复杂的逐步完善过程，这也符合历史发展规律和人类对容观事物的认识规律。同时，密码学的发展也促进了数学、计算机科学、信息通信等学科的发展;反之，其他学科的发展也促进密码学的发展。正是不同学科发展过程中的相互推动、联系、判透，使得人类对事物有了更深的认识。

（三）、研究的思路与方法

思路：本报告在了解密码学及其密码学在当今的国内外的发展趋势的基础上，使用维吉尼亚密码来了解密码的加密、解密过程并得出一定心得体会。

方法：利用C++设计维吉尼亚密码的解密与加密程序并即进行调试得出正确结果。

二、系统分析与设计

（一）、系统分析

采用维吉尼亚密码进行加密，运用凯撒密码体制根据题目要求将a—z分别对应1—26，设明文空间为C，密钥空间为K，密钥长度为d，密文空间为P，由题意，从而得到加密函数Ci=E(K,Pi)=(Pi+Ki mod d)(mod26)与解密密函数Pi=D(K,Ci)=(Ci-Ki mod d)(mod26)，运用加密解密函数，进行程序的编写。

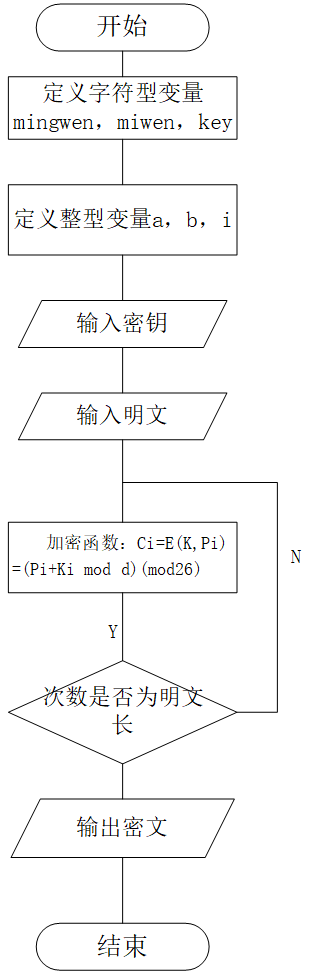
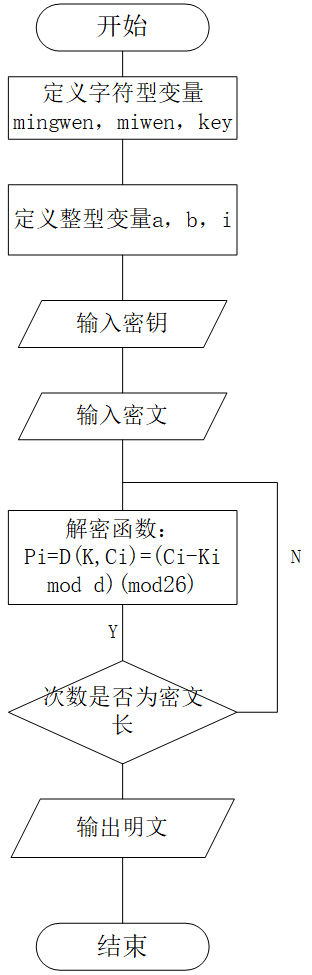
（二）、系统设计

1、系统流程图设计

加密函数：Ci=E(K,Pi)=(Pi+Ki mod d)(mod26)

解密函数：pi=D(K,Ci)=(Ci-Ki mod d)(mod26)

流程图如下：



2、程序设计

**加密程序的代码如下：**

#include <iostream>

#include <string.h>

using namespace std;

char mingwen[100],miwen[100],key[100];

int a,b,i;

int main()

{

    cout<<"密钥"<<endl;

    gets(key);

    a=strlen(key);

    cout<<"明文"<<endl;

    gets(mingwen);

    b=strlen(mingwen);

    for (i=0;i<b;i++)

       miwen[i]=((mingwen[i]-'a'+1)+(key[i%a]-'a'+1))%26+'a'-1;

    cout<<"密文"<<endl;

    puts(miwen);

    return 0;

}

**解密程序代码如下**

#include <iostream>

#include <string.h>

using namespace std;

char mingwen[100],miwen[100],key[100];

int a,b,i;

int main()

{

    cout<<"密钥"<<endl;

    gets(key);

    a=strlen(key);

    cout<<"密文"<<endl;

    gets(miwen);

    b=strlen(miwen);

    for (i=0;i<b;i++)

        mingwen[i]=((miwen[i]-'a'+1)-(key[i%a]-'a'+1)+26)%26+'a'-1;

    cout<<"明文"<<endl;

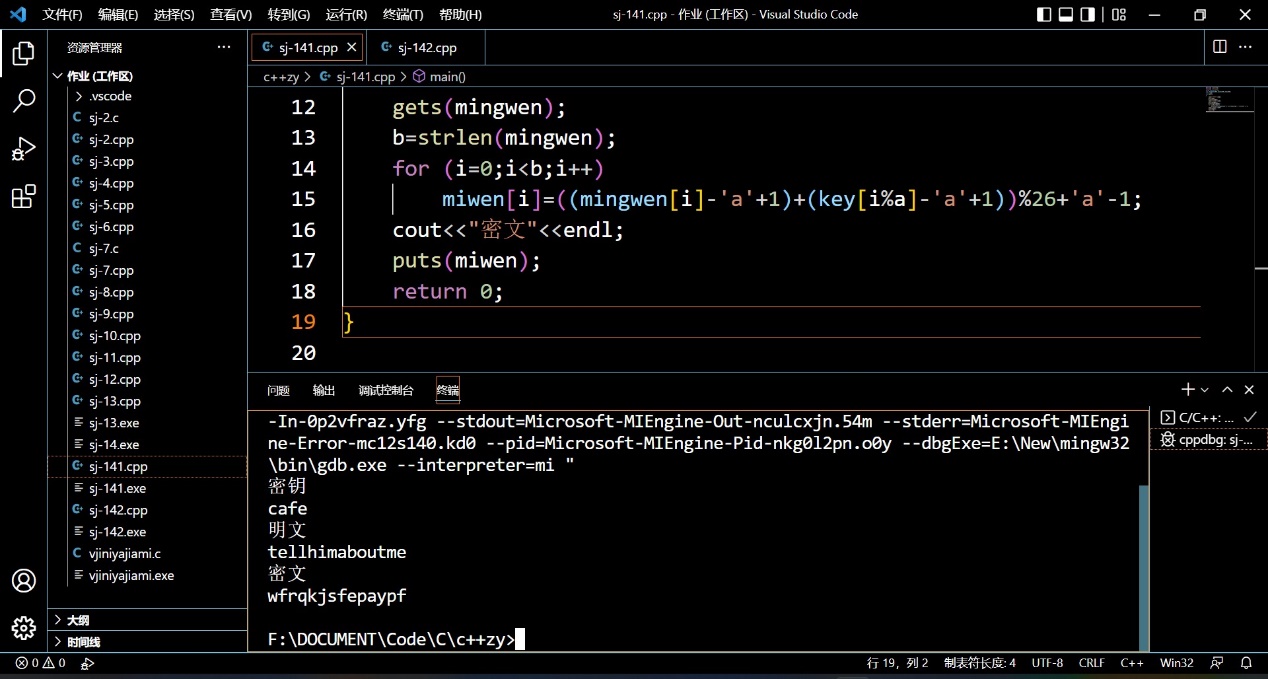
    puts(mingwen);

    return 0;

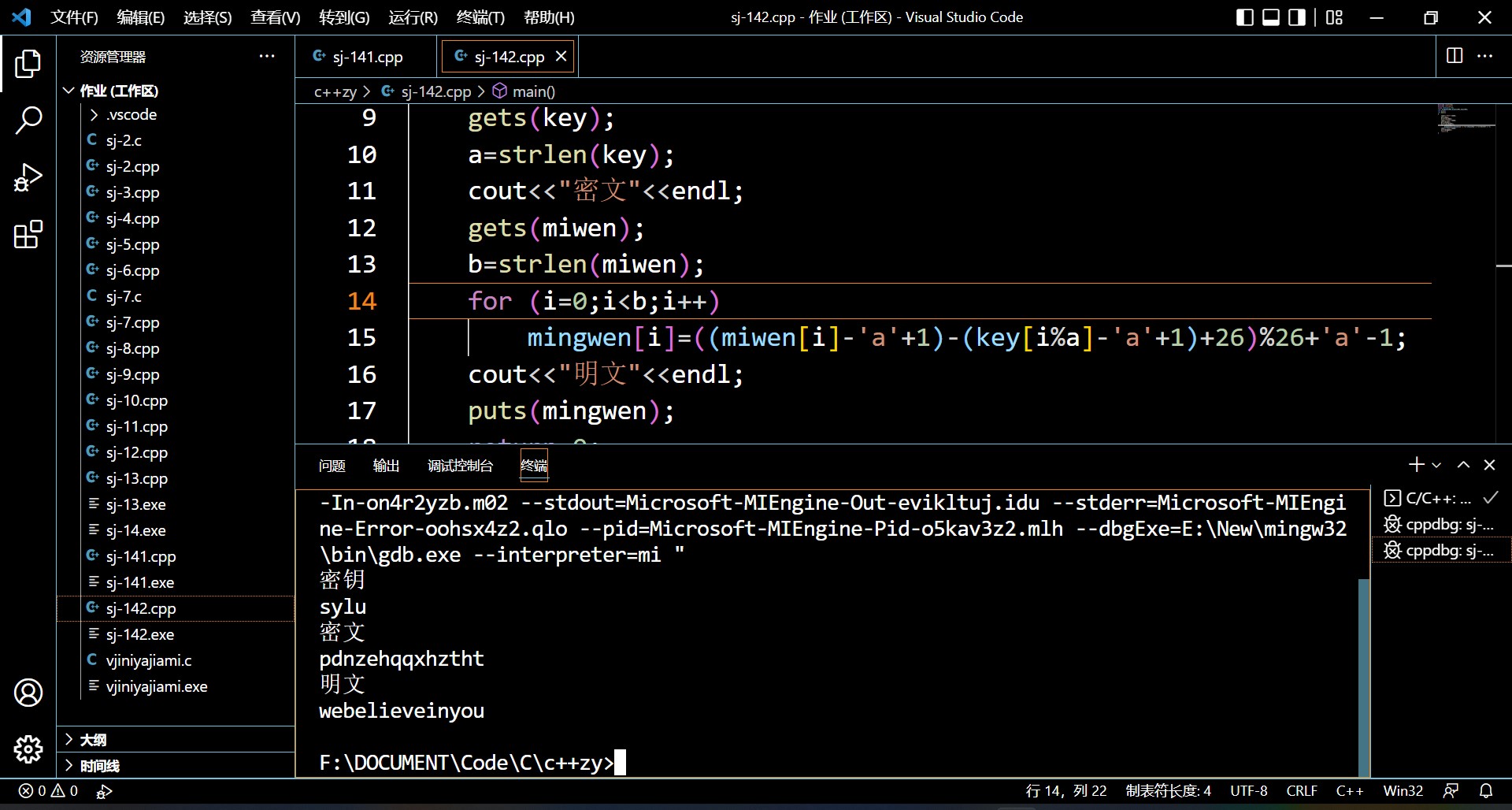
}

3、程序的运行与调试

加密程序的运行如图



解密程序的运行如图



4、数据测试结果分析

从运行的结果来看，一切正常，程序依照维吉尼亚密码分别对密文和明文进行加密和解密，加密和解密的结果也正常，符合预期的设计。

（三）、结论

维吉尼亚密码是古典密码中的一种多表代换密码，一种比较简单的，但保密性和安全性相对也较强的密码，从其加密和解密的算法可以看出，密钥越长，保密性就越好，安全性就越高，所以为提高破译的难度和时间，可以使用长长的密钥对明文进行加密。

三、本课程学习的总结

因为疫情，我们不得不进行线上学习。通过学习，令我收获颇丰。从开始还不会c语言，对c语言只有初步的认识，到后来明白了什么是程序设计，计算机及人工智能等信息技术的重要性，以及C语言的重要地位，再到后来能比较熟练地使用Dev-C++等C语言开发工具进行比较基础的程序设计，在到现在能非常熟练的使用开发工具进行稍微复杂的C语言程序设计，并且能够较好较快地完成张老师留下的课外设计作业。在张老师“能力驱动课程教学模式”的培养下，通过自身努力的学习，使我的C语言程序设计水平有较大的提高。

C语言是用好计算机的一项重要的工具，同时也算是一门手艺，在张老师的悉心教导之下，虽然还有个别问题还需要自己在努力一下，但还是可以较好地使用这门工具解决问题，应用这门手艺提高能力，同时也十分期待大二时张老师的单片机课程，相信到那时，我的C语言程序设计水平会有一个更大的飞跃。

经过这么些年的学习，我个人认为，学习就像开车子，首先你要想开车，会开车，之后车子要能开，要有油，车况要好，车子上的设备要都能用，你要用着顺手，才可以开车上路。对于我们来说首先要想学习，要想学好，之后要掌握一定的学习方法，这些是自己主观的意识，只能自己去搞，对于“车”来说，保证学习环境的良好和学生的生活，以及设施设备有的就对学生开放，就像车上不只能用油门刹车，还可以用空调，导航，中控大屏等，不要怕损失，不要怕责任。然后作为学习的人，也应该主动的去适应环境，主动的去适应工具，因为工具和环境不可能去适应你。

最后十分感谢张老师的辛苦付出，没有张老师的教学，就没有我程序设计水平的提高，然后感谢家里的支持，给我提供了良好的硬件设备，其次感谢同学们对我的帮助，最后感谢自己的努力有了一定的收获。希望这门课程以一个不错的成绩结束，也希望通过这门课程的学习，将张老师的“能力驱动课程教学模式”运用于今后的学习之路使自己的学习方法进步，学习能力提高。

四、参考文献

[1]、张东阳，张馨宸，岳明凯.基于算法的C/C++程序设计.沈阳：沈阳理工大学，2019

[2]、李子臣.密码学——基础理论与应用.北京：电子工业出版社，2019

[3]、https://www.csdn.net/tags/NtDaQg5sNDY4MjEtYmxvZwO0O0OO0O0O.html