**密码学与网络安全实验1**

**学号： 姓名： 专业：网络工程 实验日期：**

1. **实验目的**

* 实现Vigenere密码
* 实现凯撒密码
* 实现playfair密码
* 实现希尔密码

1. **实验内容与要求**

* 根据Vigenere密码原理，利用所掌握的语言实现Vigenere密码加密解密过程，增加界面模块。
* 根据凯撒密码原理，利用所掌握的语言实现凯撒密码加密解密过程，增加界面模块。
* 根据playfair密码原理，利用所掌握的语言实现playfair密码加密解密过程，增加界面模块。
* 根据希尔密码原理，利用所掌握的语言实现希尔密码加密解密过程，增加界面模块。

1. **实验重点和难点**

* 实验重点：实现Vigenere加密解密；实现凯撒加密解密；实现playfair加密解密；实现希尔加密解密；
* 实验难点：增加界面模块。

1. **实验过程**

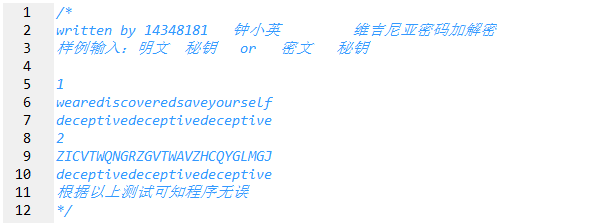
(这次的我一共做了四个古典密码，分别是Caesar，Playfair，Hill和Vigenere密码，其中Caesar和Playfair是用Python2.7写的，有图形界面；Hill和Vigenere是用C++写的。)

* 实现Vigenere加密解密。
* 实验原理
* 加密过程很简单，就是给定密钥字母x和明文字母y，密文字母是位于x行和y列的那个字母。这样就决定了加密一条消息需要与消息一样长的密钥字符串，通常，密钥字符串是密钥词的重复。  
    
  以《密码编码学与网络安全——原理与实践》中的例子来作为本文的例子。比如密钥词是deceptive，消息是“we are discovered save yourself”，那么加密过程如下：  
  deceptivedeceptivedeceptive（密钥字符串）  
  wearediscoveredsaveyourself（消息）  
  ZICVTWQNGRZGVTWAVZHCQYGLMGJ（密文）
* 实验步骤

黑框框主界面代码



测试样例：



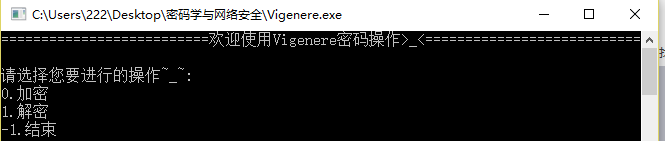


图1-1主界面

* 加密操作

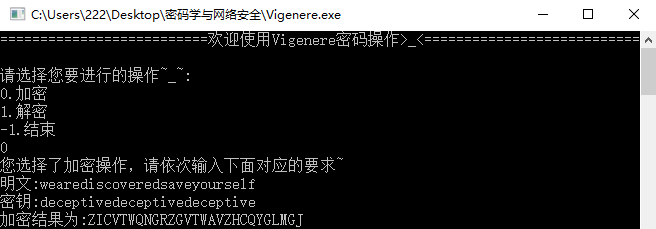


图1-2加密操作界面

* 解密操作



图1-3解密操作界面

* 结束操作



图1-4结束操作界面

* 实现凯撒加密解密。
* 实验原理
* 实验步骤

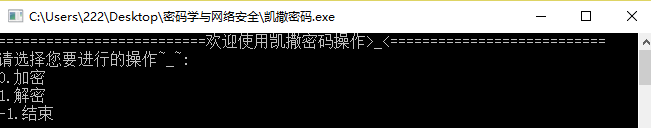


图1-1主界面

* 加密操作

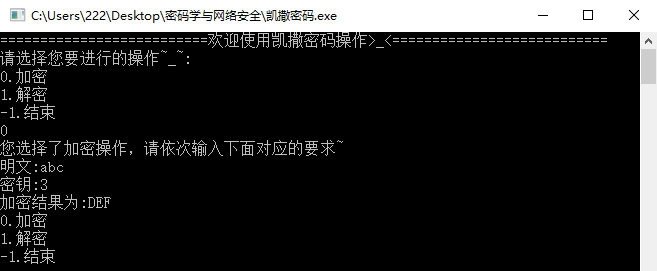


图1-2加密操作界面

* 解密操作

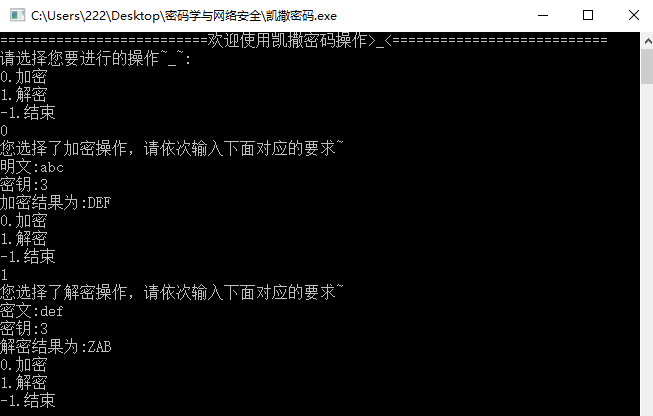


图1-3解密操作界面

* 结束操作

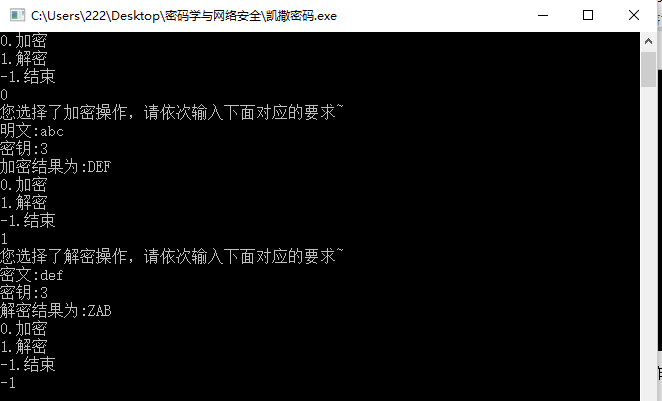


图1-4结束操作界面

1. **实验总结**

在理解四种密码学的基础上用自己所学的语言来实现，在这过程中遇到了许多问题，不过在同学的帮助下顺利解决，但因对希尔密码以及playfair密码理解不够透彻，导致写的代码不完善，到现在还未解决掉bug。至于可视化界面，正在努力学习中，谢谢老师给予我学习的机会，我会利用时间把这次的作业完善好，增加可视化界面！谢谢！