Chapter 1

古典密码

Exercise 1

对一个英文 txt 文档实现凯撒加密，编译后的可执行程序名为 caesar.exe，比如要对 1.txt 文件进行加密，执行”caesar -e 1.txt 1e.txt”, 其中-e 表示加密，1.txt 是要加密的文件，1e.txt 是指定的加密后将信息写入的文件。如果要对 1e.txt 解密，执行”caesar -d 1e.txt 1.txt”，其中-d 表示解密，1e.txt 是要解密的文件，1.txt 是解密后的文件。程序在 gitee 上有初始仓库，在要求时间前发送 pull request。程序编写完后写一个报告，报告内容包括，摘要，目标、设计、测试、总结，此报告上传到 gitee 上，上传的报告必需是 pdf 格式！

项目参考初始仓库`https://gitee.com/buuer/caesarcipher`

提交的仓库中，要将文件 message.txt 中的内容进行加密，密文以文本方式存储在 ciphers.txt 中，同时将 ciphers.txt 进行解密，解密后得到的明文以文本方式存储在 decode.txt 中。

说明

- 首先要考虑一个正常的 txt 文档中，除了包括字母，还要由标点符号，而算法只能处理字母，所以输入的 txt 文档要进行预处理，以某种规则去掉不能处理的字符，然后进行加密。**为了便于统一评判，我们要求在预处理时，将大写字母转换为小写字母，其他字符都不变，加密时只对小写字母进行加密。**
- 由于对原始文档进行了预处理，所以解密后的文档与原始文档不是完全一样的。
- 提交的文档为 PDF 格式。
- 建议对所有学生的此实验报告进行认真打磨，反复修改，直到符合要求，通过这个过程使得学生掌握此类文档的书写要求，掌握基本科技类文档的写作技能，在此课程的后续文档编写中，学生能够顺利输出合乎规范的文档。
- 在 gitee 上创建项目：caesarcipher，并且将学生做为观察者加入，项目描述为：“对一个纯英文的 txt 文件，利用凯撒加密方法进行加解密，由于其只能处理字母，所以要对 txt 文件进行

预处理，然后进行加解密，解密后的文件与原始的不同，这是正确的，而且由于预处理时有信息丢失，所以也不可能还原到原始文件。”, 学生做为观察者的原因时限制学生权限，以免其误操作修改项目中原始文件，学生完成后，向指导教师发起 pull requet，教师可以去其仓库下载其实验内容，实验内容除了代码，可执行程序，还需包含实验报告。

Exercise 2

对一个中文 txt 文档，利用古典加密的思想，设计一个加密方式对其进行加密，可以参考凯撒加密的方法，编译后的可执行程序名为 hancipher.exe，比如要对 1.txt 文件进行加密，执行”hancipher -e 1.txt 1e.txt”, 其中-e 表示加密，1.txt 是要加密的文件，1e.txt 是指定的加密后将信息写入的文件。如果要对 1e.txt 解密，执行”hancipher -d 1e.txt 1.txt”，其中-d 表示解密，1e.txt 是要解密的文件，1.txt 是解密后的文件。程序在 gitee 上有初始仓库，在要求时间前发送 pull request。**此练习不需要写报告**，但是需要在源代码中有清晰和足够的中文注释，并在项目的 readme.txt 文件中写出你所采用的加解密基本原理。

项目参考初始仓库`https://gitee.com/buuer/hancipher`

提交的仓库中，要将文件 plain.txt 中的内容进行加密，密文以文本方式存储在 ciphers.txt 中，同时将 ciphers.txt 进行解密，解密后得到的明文以文本方式存储在 decode.txt 中。