

作品类别： □软件设计 □硬件制作 □工程实践

**《密码学导论》课程大作业作品设计报告**

作品题目： 单表代换辅助工具

名字： 李博博

学号： PB22030771

2024年 6月 8日

|  |
| --- |
| 基本信息表 |
| 作品题目：单表代换辅助工具 |
| 作品内容摘要：   1. 辅助使用者对明文进行单表代换加密 2. 辅助收到密文且已知密钥的使用者进行解密 3. 利用频率关系辅助破译未知密钥的单表代换密文 |
| 关键词（五个）：  1.单表代换2.加密3.已知密钥解密4.未知密钥破译5.频率攻击 |
| 团队成员（按在作品中的贡献大小排序）：   |  |  |  |  | | --- | --- | --- | --- | | 序号 | 姓名 | 学号 | 任务分工 | | 1 | 李博博 | PB22030771 |  | | 2 |  |  |  | | 3 |  |  |  | |

# 1.作品功能与性能说明

功能1：对明文进行加密

功能2：对已知密钥的单表代换密文进行解密

功能3：对未知密钥的单表代换密文进行破译

# 2.设计与实现方案

功能1：输入明文和a到z字母所对应的密文，输出产生的密文

功能2：输入密文和a到z字母所对应的明文，输出产生的明文

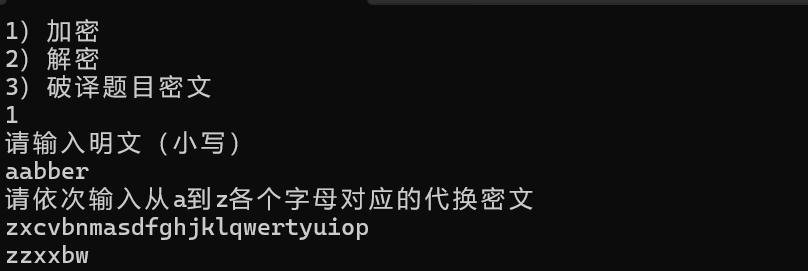
功能3：对待破译密钥进行频率分析，然后给出一个建议的明文破解方案，并提供手动调节的方式，通过手动调节细调可以得到明文

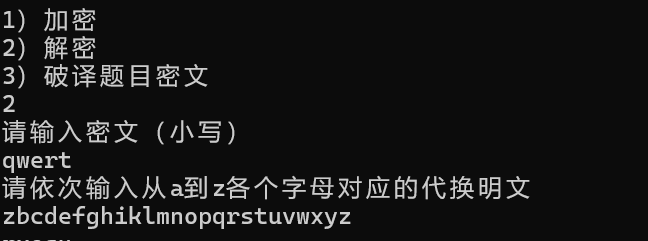
## 2.1 实现原理

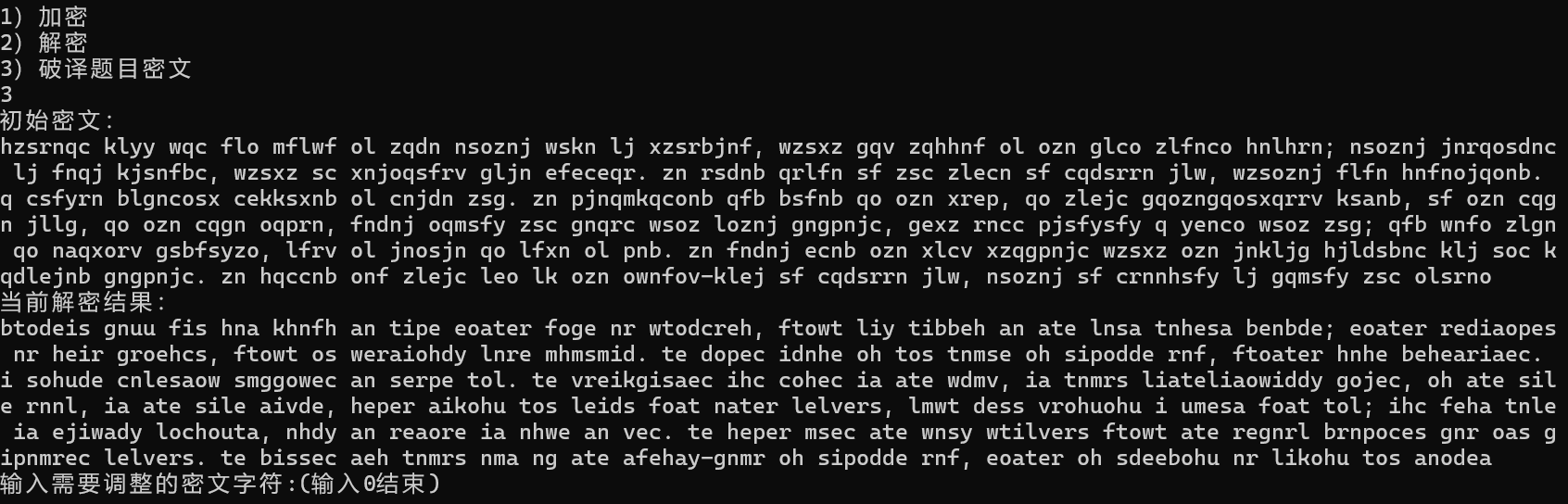
功能1,2：设置两个数组C（明文）M（密文）和密钥数组KEY，只需要检测字母然后在key中找到对应的字母替换放入另外一个数组即可

功能3：首先进行频率的统计，依据统计结果找到最适合的字母进行替换，给出建议的明文。然后进行手动替换字母，按0-可以结束调整

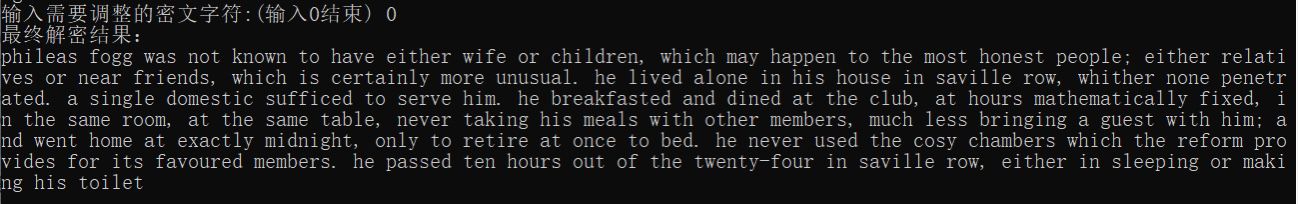
## 2.2 运行结果







经过调整可得



# 3.应用前景

**用于简单单表代换的辅助使用，能辅助破译未知密文**