中国科学技术大学 University of Science and Technology of China | 网络空间安全学院 School of Cyber Science and Technology

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：综合古典密码加解密器

制作人员：王宇杰

2024 年 6 月 6 日

基本信息表

作品题目：综合古典密码加解密器

作品内容摘要：

本报告介绍了《密码学导论》课程大作业的作品“综合古典密码加解密器”的设计与实现过程。该作品采用 Python 编程语言，分别实现了单表代换密码、仿射密码和维吉尼亚密码的加密与解密功能。用户可以自由组合这些加密方式，进行串联加密。此外，还通过学习和应用 tkinter 库，设计了一个简洁实用的图形用户界面（GUI）。本报告详细描述了系统功能、性能测试、设计与实现方案、测试方案和运行结果，最后讨论了作品的应用前景。关键词包括：单表代换加密、维吉尼亚加密、仿射加密、组合串联、GUI。

关键词（五个）：单表代换加密，维吉尼亚加密，仿射加密，组合串联，GUI

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	王宇杰	PB22331841	各种加密实现的构思，具体代码的实现，代码的运行，改进与维护工作
2			
3			

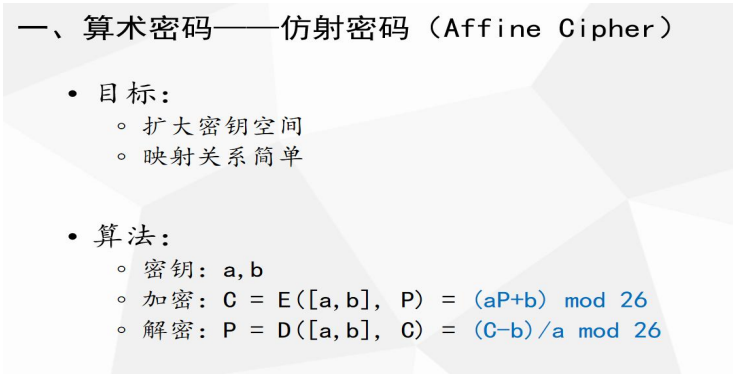
1.作品功能与性能说明

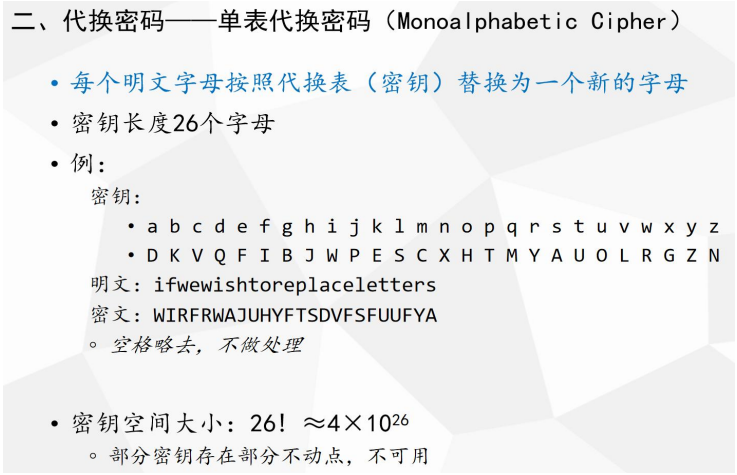
功能：用 python 实现了三种密码——单表代换密码，仿射密码，维吉尼亚密码的加密与解密；同时做了一点小改进，用户可以自由组合这三种加密方式，进行一次串联加密，如可以指定先仿射加密，再单表代换加密，最后维吉尼亚加密，一步到位，也能进行同一种加密方式不同密钥的组合；我也上网粗浅学习并制作了一个 GUI，还算简洁实用。

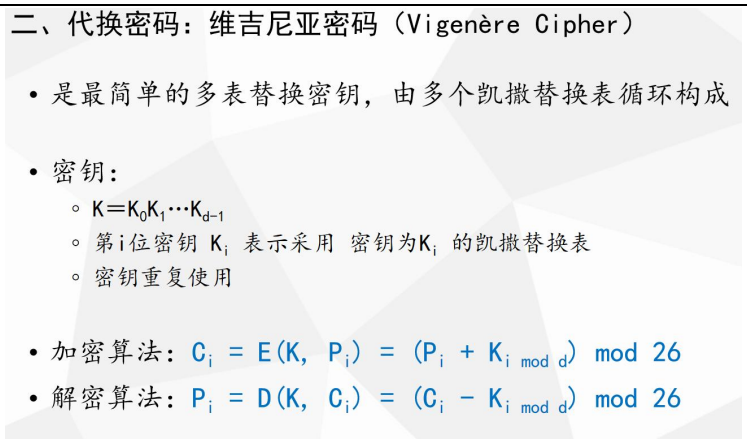
性能：以上三种密码的代码实现都比较固定，我自定义的组合加密消耗的时间大致是用户组合的密码实现之和，运行速度较快，运行稳定；能对输入的密钥进行检查，确保输入的合法。

2.设计与实现方案

2.1 实现原理







软件流程

需求：完成三种密码，并实现他们的串联

设计：先完成三种密码的单独实现，再用一个组合函数实现串联

实现：用了 python3.12 实现

测试通过

2.2 参考文献

csdn 上有关 tkinter 如何编辑一个 GUI，网址：

https://blog.csdn.net/muzihuaner/article/details/106248343

csdn 以及其他密码学网站上有关单表代换，维吉尼亚密码，仿射密码的实现，网址：

https://blog.csdn.net/Alpherkin/article/details/121021025

https://blog.sma11new.com/post/20191151848

上课 ppt 中有关单表代换，维吉尼亚密码，仿射密码的介绍

2.3 运行结果

实现了三种密码以及他们的串联

这个是用户界面：

2.4 技术指标

运行速度快，运行稳定；能对非法输入做出一定反应，避免系统崩溃；用户界面较为简洁实用，易于上手。

3.系统测试与结果

3.1 测试方案

1.测试环境

硬件：Intel Core i7, 16GB RAM

软件：Windows 10, Python 3.12

2.测试目的

验证加密算法的功能和性能

3.测试方法

功能测试：验证加密和解密操作的正确性

性能测试：评估加密和解密操作的执行时间

4.测试标准

功能测试标准：加密和解密正确

性能测试标准：加密和解密时间小于 1ms

3.2 功能测试

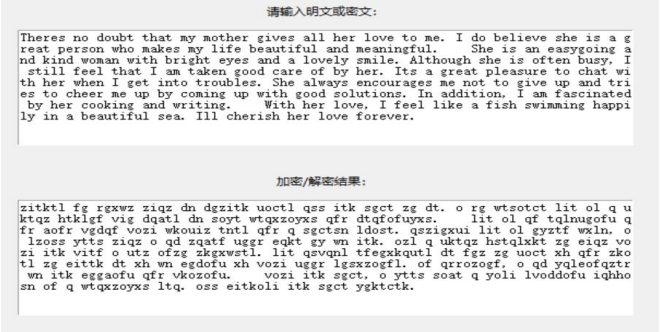
测试用例：

起始明文(网上随便找的小作文）Theres no doubt that my mother gives all her love to me. I do believe she is a great person who makes my life beautiful and meaningful. She is an easygoing and kind woman with bright eyes and a lovely smile. Although she is often busy, I still feel that I am taken good care of by her. Its a great pleasure to chat with her when I get into troubles. She always encourages me not to give up and tries to cheer me up by coming up with good solutions. In addition, I am fascinated by her cooking and writing. With her love, I feel like a fish swimming happily in a beautiful sea. Ill cherish her love forever.

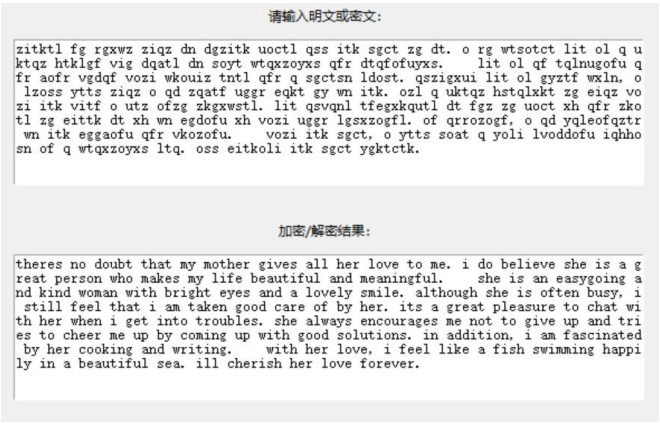
单个密码的加解密和组合密码的加解密均通过：

单表代换 密钥：qwertyuiopasdfghjklzxcvbnm

加密

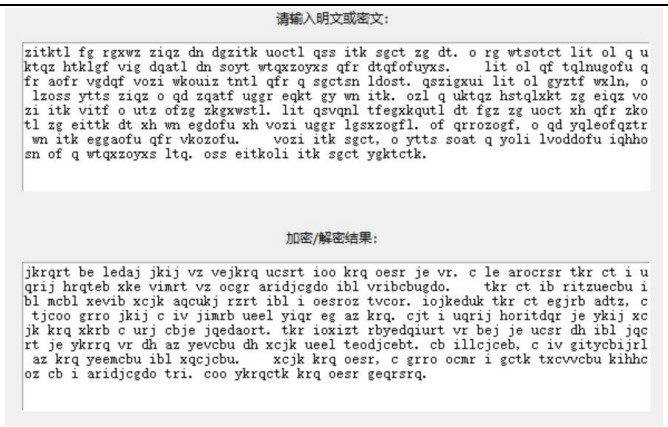


解密

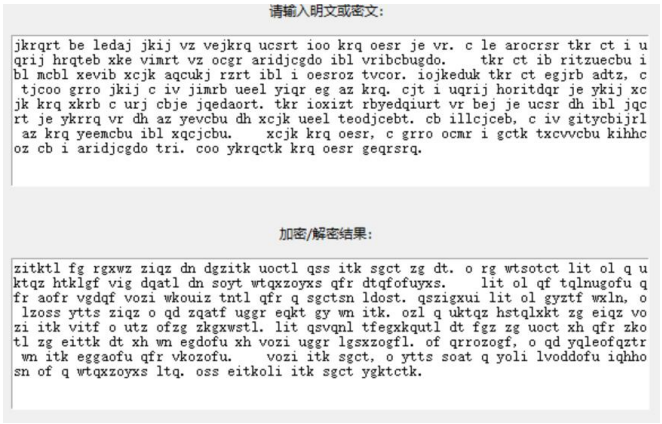


仿射密码 a=3，b=12

加密

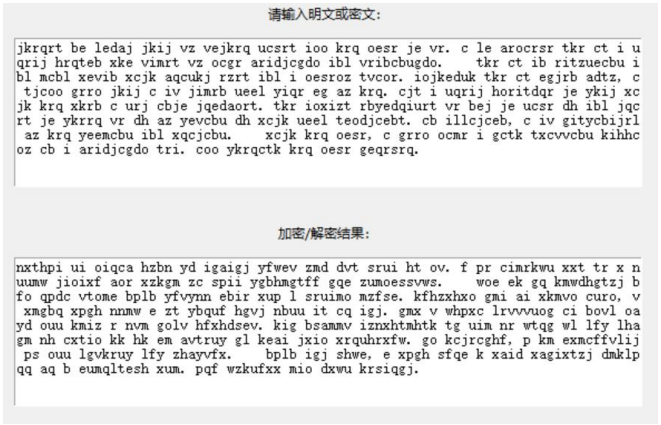


解密

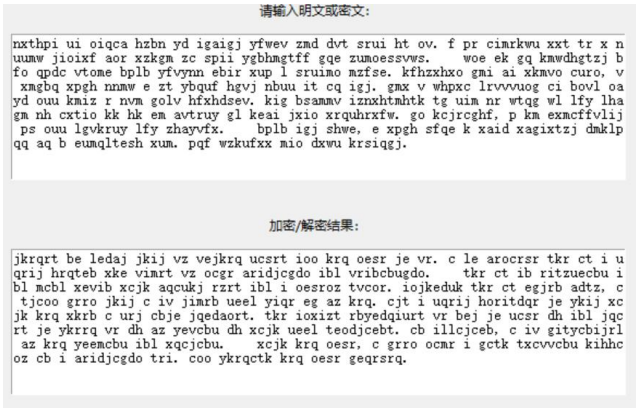


维吉尼亚密码 密钥：encrypted

加密

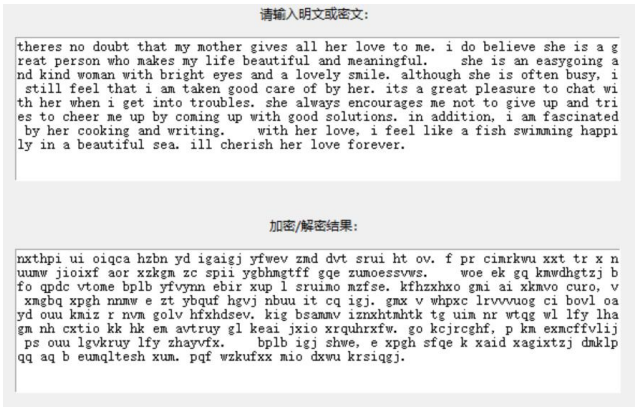


解密

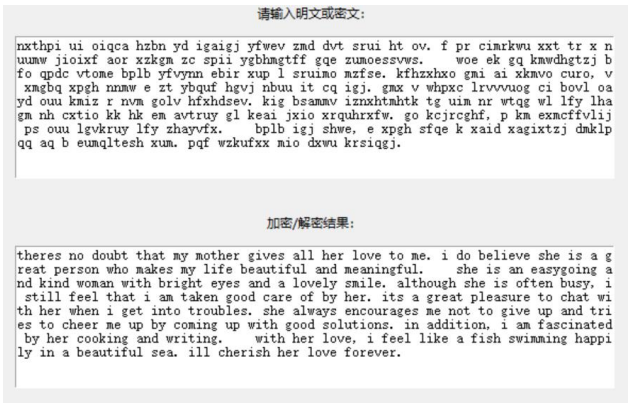


单表代换-仿射密码-维吉尼亚密码 密钥同上

组合加密



组合解密



比对可以看出串联加密和一次一次加密后的结果是一样的

同时对不合理输入会有反馈：

3.3 性能测试

还是上面那个实例：

单表代换加密用了 0.17000ms，解密用了 0.13380ms

仿射密码加密用了 0.37660ms，解密用了 0.49320ms

维吉尼亚密码加密用了 0.19340ms，解密用了 0.21250ms

组合加密用了 0.43360ms,解密用了 0.72950ms

3.4 测试数据与结果

	用例	预期结果	实际结果	是否通过
功能测试	见上	成功加密	成功加密	是
性能测试	见上	<1ms	均小于 1ms	是

功能和性能均符合预期

4.应用前景

可以用于古典密码的加解密，也可以用于古典密码的教学演示，未来如果还要添加新的古典密码种类或其他密码，可以直接加入这个大框架，让串联的种类变得更多。

5. 结论

综合古典密码加解密器成功实现了三种经典加密算法及其组合串联功能，通过功能和性能测试，验证了系统的正确性和高效性。系统运行稳定，能够对非法输入进行有效检查，确保输入的合法性。图形用户界面简洁实用，易于上手，为用户提供了良好的操作体验。未来，该系统可以扩展更多古典密码算法或其他类型的加密方式，进一步丰富功能和应用场景，具备较大的应用前景和教学价值。