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：单表代换辅助工具

团队名称：无 （单人作品）

团队人员：胡鑫

2025 年 6 月 7 日

基本信息表

作品题目：**单表代换辅助工具**

作品内容摘要：该作品是一个基于 Python 的 Tkinter 库开发的图形化单表代换密码处理工具。该工具具备加密、解密和自动破译等功能，界面包含加密、解密两个主要页面。用户可以在加密页面输入明文，编辑或加载密钥后进行加密操作，并保存加密结果和密钥；在解密页面输入密文，同样能编辑、加载密钥实现解密，还可通过加载词典辅助自动破译。工具支持对输入文本进行频率统计、双字母组合分析和词典匹配，根据分析结果生成破译建议，方便用户对密码进行破解。

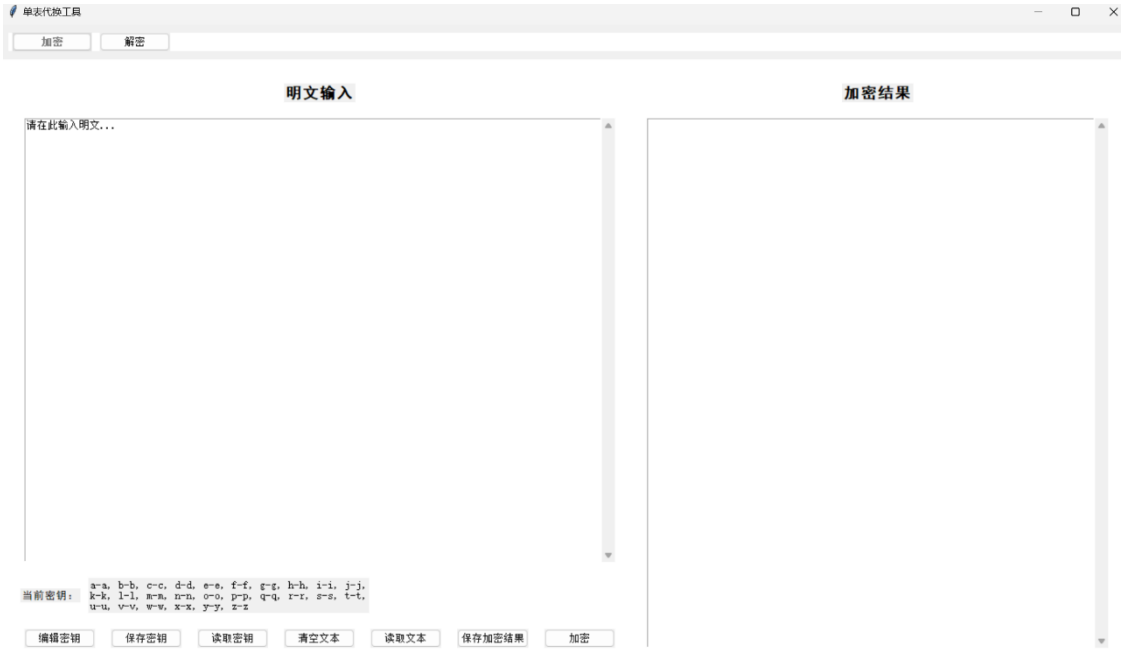
关键词（五个）：单表代换密码、加密解密、自动破译、频率分析、词典匹配

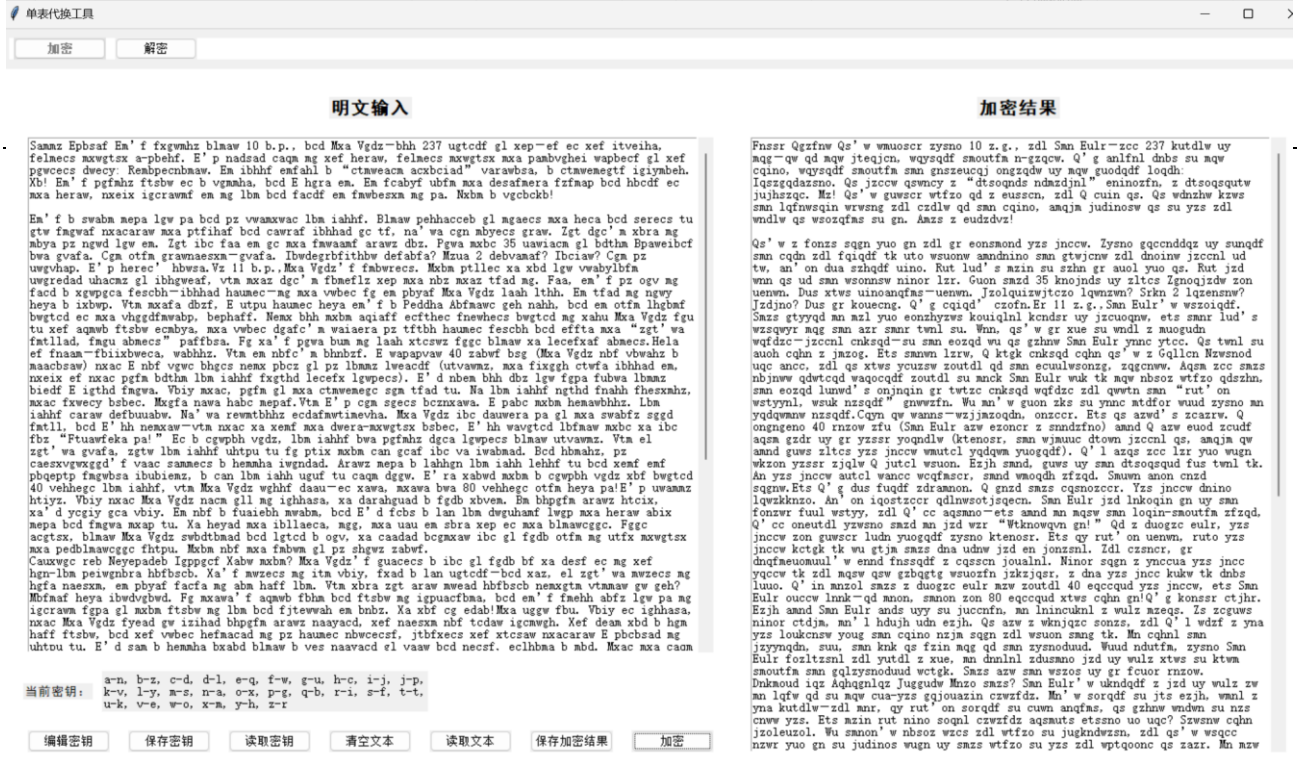
团队成员（按在作品中的贡献大小排序）：

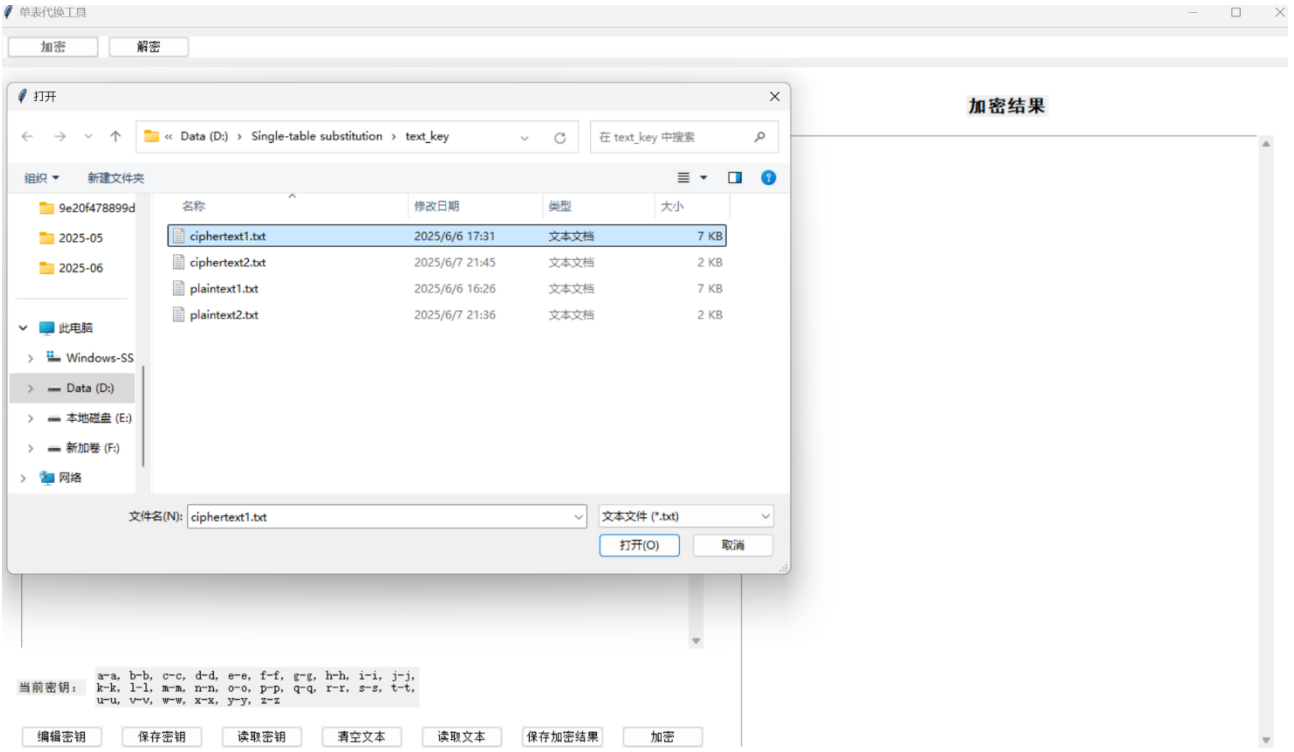
序号	姓名	学号	任务分工
1	胡鑫	PB23071384	全部
2			
3			

1.作品功能与性能说明

作品包括加密解密功能，且支持从 txt 文件中直接读取，也支持保存加密解密的结果。除此之外，密钥也支持读取与保存。在解密功能处统计了密文的字母频率以及最多的双字母组合从而给出意见，同时结合搜寻字典的方法，利用退火算法按照用户已经设定的部分密钥来生成其余密钥计算此合成密钥解密后的含有的字典内的单词数量，在经过多次迭代之后会使用出含有单词数最多的那一条合成密钥。







2.设计与实现方案

本单表代换工具旨在为用户提供一个图形化界面，实现单表代换密码的加密、解密以及自动破译功能。使用 Python 的 Tkinter 库构建用户界面，结合模拟退火算法进行自动破译，并利用词典匹配和频率分析评估密钥质

量。对于实现方案简单介绍一下各层代码：

- **主窗口初始化**：在 __init__ 中初始化主窗口，设置窗口标题、大小等属性。
- **加密页面**：create_encrypt_page 创建加密页面，包含明文输入框、密钥显示框、加密按钮等。
- **解密页面**：create_decrypt_page 创建解密页面，包含密文输入框、密钥显示框、解密按钮和自动破译按钮等。
- **加密功能**：perform_encryption 根据用户输入的明文和密钥进行加密操作。
- **解密功能**：perform_decryption 根据用户输入的密文和密钥进行解密操作。
- **重复破译功能**：break_cipher 使用模拟退火算法进行重复破译。
- **加载词典**：load_dictionary 从文件中加载词典。
- **保存密钥和文本**：save_key、save_encrypted_text 和 save_decrypted_text 分别用于保存密钥、加密文本和解密文本到文件。

2.1 实现原理

其余功能比较简单，主要介绍模拟退火算法的实现。

模拟退火算法是一种通用概率演算法，常用于在一个大的搜寻空间内找寻命题的最优解。该算法模拟固体退火过程，从一个较高的初始温度开始，逐步降低温度，在每个温度下进行多次状态转移，以一定的概率接受较差的解，从而避免陷入局部最优解。

- 代码中的实现原理：首先设定初始温度 temperature 为 100，冷却率 cooling_rate 为 0.999。
- 调用 generate_initial_key 生成一个初始密钥 initial_key，并将其赋值给 current_key。
- **评估初始密钥质量**：使用 evaluate_key_dictionary 评估当前密钥的质量，得到 current_score。
- **生成新密钥**：在每次循环中，调用 swap_mapping 对当前密钥进行随机扰动，生成一个新的密钥 new_key。
- **评估新密钥质量**：使用 evaluate_key_dictionary 评估新密钥的质量，得到 new_score。

- **判断是否接受新解**：如果新密钥的质量 new_score 优于当前密钥的质量 current_score，则直接接受新密钥；否则，调用 acceptance_probability 计算接受新解的概率，并与一个随机数进行比较，如果概率大于随机数，则接受新密钥。
- **更新当前密钥和得分**：如果接受新密钥，则将 current_key 更新为 new_key，将 current_score 更新为 new_score。
- **降低温度**：每次循环结束后，将温度 temperature 乘以冷却率 cooling_rate，逐渐降低温度。
- **记录最终密钥**：当温度降低到一定程度（小于 0.1）时，循环结束，将最终的密钥 current_key 赋值给 final_key。

其中的初始温度 temperaturey 以及冷却率 cooling_rate 、字典内的单词都可人为修改，在默认的设置（设定初始温度 temperature 为 100，冷却率 cooling_rate 为 0.999）中，在大约 6900 次会让温度下降到临界值，因此只能迭代 6900 次，如果需要提高迭代次数可以设置更高的温度或者更低的冷却率。由于探讨如何设置初始温度 temperaturey 以及冷却率 cooling_rate 、字典内的单词能让解密效果最大化十分困难，这里仅仅做了最简单的设置，单词也仅仅挑选了 29 个常见的英语组合。

2.2 参考文献

关于退火算法的论文：Kirkpatrick, S., Gelatt, C. D., Jr., & Vecchi, M. P. (1983, May 13). Optimization by Simulated Annealing. *Science*, 220(4598), 671-680.

2.3 运行结果

以提供的密文（ ciphertext2）为例，在根据对原文频率分析，将出现频率最大的两个字母 z，d 设置固定的密钥对 e-z,t-z 后，根据字典匹配评分的退火算法重复迭代后的解密结果让解密后出现了很多与字典匹配的单词，解密后的文本明显出现一部分英文的特征，接下来可以通过用户猜测固定其它的密钥对来进一步进行解密

3.系统测试与结果

3.1 测试方案

利用网上找到的两篇英文文章（一篇短文，一篇长文），通过随机密钥的生成将它们加密并保存各种的密文以及密钥。在解密界面用对应密钥解密后可以出现原文。同时可以观察在重复破译模式下，先通过频率分析把频率第一、第二高的字母设定相应的固定字母对：e-（），t-（）后解密出来的情况。

3.2 功能测试

加密解密功能测试都良好，能够读取密钥进行加密或者解密功能，不过注意固定密钥的输入记得为英文输入法，否则可能会发生 bug，同时注意固定的密钥对中不要有重复的密钥映射，否则会清空密钥。

3.3 性能测试

在各种测试中未发生卡顿。

3.4 测试数据与结果

在对长文本的加密文本进行破译过程中，当对高频率的字母设置固定密钥对（e-j,t-d）后，发现第一次重复迭代后的文本出现了很明显的英文特征，如英文单词“after”已经出现。

4.应用前景

可对单表代换密码进行辅助破译

5.结论

退火算法中初始温度 temperaturey 以及冷却率 cooling_rate 、字典内的单词等因素不知道如何设置让效果最佳，这需要大量的经验来进行设置，但是在粗糙的设置之下，在重复破译时仍可使解密的文本出现明显的英文化特征，如果设定更好的词典来锁定更多的英文特征，说不定会让效果更好。