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：单表代换密码破译辅助工具

设计作者：沈恩祈 PB23151787

所属院系：网络空间安全学院

2025 年 6 月 4 日

基本信息表
作品题目：单表代换密码破译辅助工具
作品内容摘要：本文介绍了一款基于单表代换密码的工具设计与实现。该工具分为三个主要部分：主控制台、加密/解密功能模块以及辅助破译功能模块。通过 Python 编程语言和 Tkinter 图形界面库，实现了单表代换密码的加密、解密以及辅助破译等功能。本文详细阐述了该工具的设计思路、实现原理、功能测试以及应用前景，旨在为密码学教学与学习提供一个实用的辅助工具。
关键词（五个）： 单表代换密码；加密；解密；辅助破译；频率分析

1.作品功能与性能说明

功能

- **加密**：（1）根据用户提供的密钥对输入的明文进行加密。

  （2）由程序自动生成随机密钥帮助加密，并记录密钥
- **解密**：依据用户提供的密钥对输入的密文进行解密。

- **无密钥破译**：根据用户所提供的密文进行频率分析，并在频率基础上为用户提供最贴合的对应关系，并允许手动固定，进而迭代直到得出最优解

- **辅助功能**：
  - **频率统计**：对字母频率进行统计并自动绘图。
  - **迭代优化**：在固定某些对应的条件下，自主寻找最优解。
  - **词典匹配建议**：检查解密文本有效单词的占比，以此判断破译进度。
  - **导入导出功能**：方便用户留存加密、解密、破译得到的数据。

2.设计与实现方案

2.1 实现原理

（硬件框图、软件流程、相关描述等）

软件流程

1. **功能选择**：用户通过程序主界面选择自己所需功能
2. **数据输入**：在所选功能中输入明文（密文）、密钥，并选择相应功能。
3. **数据接收**：Flask 应用接收用户提交的数据。
4. **功能处理**：根据用户选择的功能，调用 Python 文件中的相应函数进行处理。
    - **加密 / 解密**：使用 do_encrypt 和 do_ decrypt 类进行加密和解密操作。
    - **频率分析**：使用 analyze_frequency 类计算字母频率并合理安排对应关系。
    - **辅助功能**：调用相应的辅助函数，如 evaluate_mapping、optimize_mapping 等。
5. **结果返回**：将处理结果返回给程序界面进行显示。

补充介绍：

(1) 单词的有效性以 nltk 库的英语单词词典为基准进行短单词有效性检查。

(2) 单个字母及二字节的常见频率排序由 letter.py 文件运行所得，其基本功能是读取布朗语料库内所有文章并进行统计。

2.2 参考文献

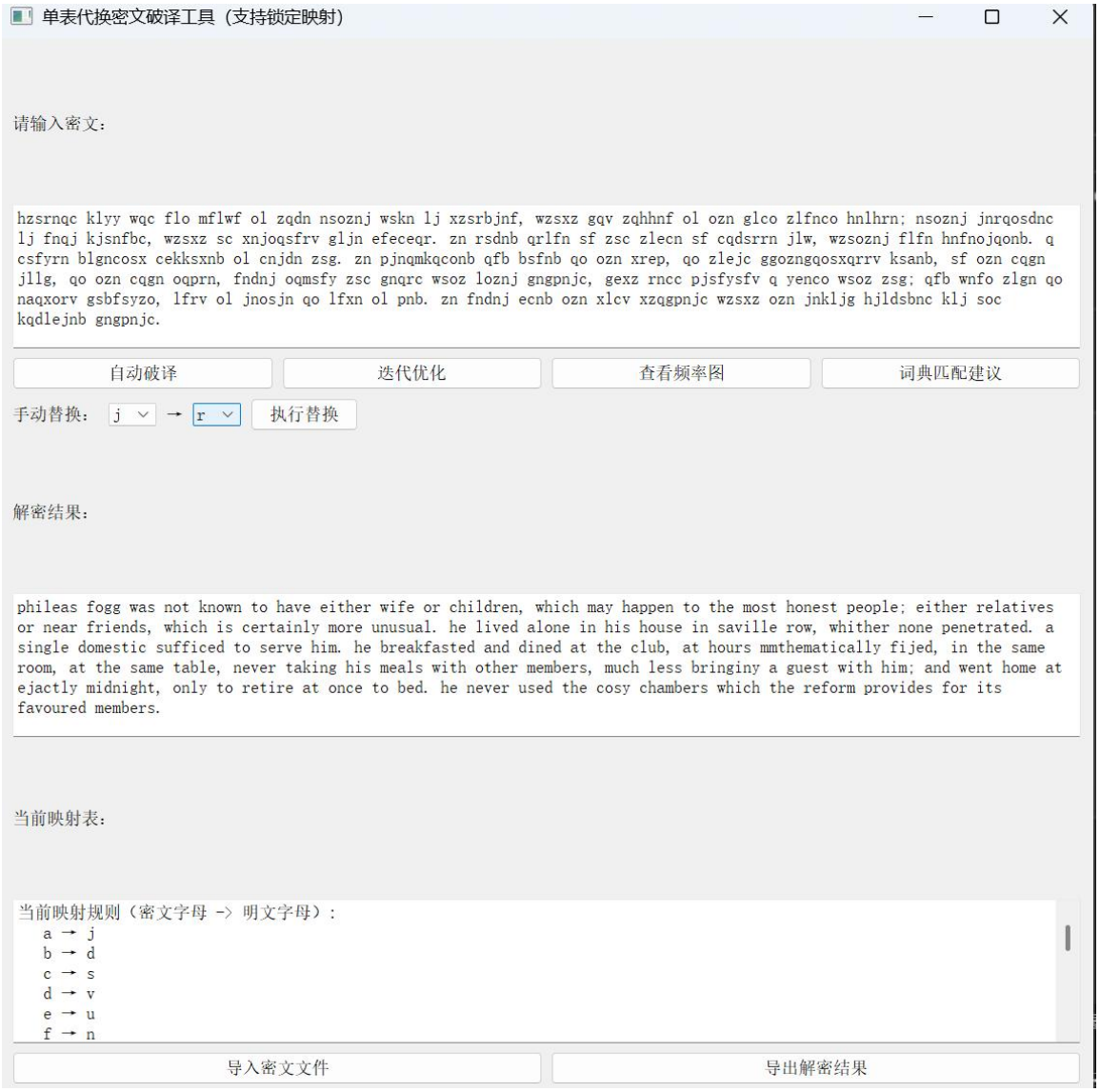
(1) Stallings, W. (2017). Cryptography and Network Security: Principles and Practice . Pearson.

(2) Schneier, B. (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C . Wiley.

(3) Paar, C., & Pelzl, J. (2010). Understanding Cryptography: A Textbook for Students and Practitioners . Springer.

(4) 密码学导论

2.3 运行结果



2.4 技术指标

编程语言：python；

引用库的介绍：

a. tkinter ：所有 Python 脚本都使用 tkinter 库来创建图形用户界面

b. os 和 sys ：在 main.py 中用于操作文件路径和调用外部脚本。

c. subprocess ：在 main.py 中用于启动外部 Python 脚本。

d. collections.Counter ：在功能二新.py 中用于统计字符频率。

e. matplotlib.pyplot ：在 功能二新.py 中用于绘制字符频率分布图。

f. nltk.corpus.words ：在 功能二新.py 中用于词典匹配。

g. re ：在 功能二新.py 中用于正则表达式操作。

h. json ：在 功能一新.py 中用于保存和加载密钥。

i. random ：在 功能一新.py 和 功能二新.py 中用于生成随机密钥和优化映射表。

3.系统测试与结果

3.1 测试方案

- **功能测试**：对加密、解密、频率分析和辅助功能进行测试，验证其功能的正确性和稳定性。
- **性能测试**：使用不同长度的文本进行测试，记录处理时间和运行结果，评估系统的性能以及可靠性。

3.2 功能测试

- **加密**：输入明文和密钥，验证加密结果是否正确。

结果：无论是手动输入密钥、外部导入密钥还是程序随机生成密钥，程序运行良好。并且当用户输入密钥不合法时，会弹出错误提示，具有一定的抗压性。

- **解密**：输入密文和密钥，验证解密结果是否正确。

结果：程序正常运行，解密结果正确且可成功导出。并且当用户输入密钥不合法时，会弹出错误提示，具有一定的抗压性。

- **频率分析**：输入文本，验证字母频率计算是否正确。

结果：对输入文本的概率分析正确。

- **辅助功能测试**：分别测试字典贴合度，密钥导入（输出），密文导入（输出）验证其功能的正确性。

结果：各项功能均能正常使用。

3.3 性能测试

- 使用 200 字节和 800 字节长度的文本进行测试，记录处理情况。

结果：
200 字节文本破译不确定度较大，建议的可靠性较低，需要用户多次尝试高频字符的固定，在该类情况下，单纯依赖程序推荐的固定关系破译难度较大。
800 字节文本破译较为稳定，初始状态下的破译程度较高，用户只需根据某些较为常见的单词固定低频字符即可，多次迭代后可轻松得到正确明文。

3.4 测试数据与结果

测试数据来源：ai 随机生成的英语语句。

测试结果：程序的加密解密等功能运行稳定。在密文破译的表现上，面对密文体积足够大时可以轻松破译，而面对密文内容较少时，程序则主要起到辅助的作用，检测用户的每一次固定操作，反馈当前破译结果的可靠性来辅助破译。对于题目中所举出的例子，该程序可较轻易地完成破译。

4. 应用前景

教育领域

- **密码学教学辅助工具**：在密码学课程中，该工具可以作为教学辅助工具，帮助学生直观地理解单表代换密码的加密、解密和破译过程。通过实际操作，学生可以更好地掌握密码学的基本概念和原理。
- **课程设计**：该工具可以作为密码学课程设计的参考项目，帮助学生设计和实现自己的密码学工具，培养学生的编程能力和创新思维。
- **实践操作**：学生可以通过实际操作加密和解密功能，了解信息安全的基本操作，为未来从事信息安全相关工作打下基础。

密码学研究

- **算法分析**：该工具可以用于密码学算法的研究，帮助研究人员分析单表代换密码的加密和破译效果，评估其安全性。
- **破译方法研究**：辅助破译功能模块提供了频率分析和映射优化等方法，研究人员可以利用这些方法研究更高效的破译算法，提高破译成功率。
- **算法改进**：研究人员可以基于该工具的实现，提出改进的单表代换密码算法，提高其安全性和效率。

未来方向：

- **未来扩展工具：**支持多表代换密码的加密和解密功能，进一步提高加密效果。
- **现代加密算法：**可以增加对现代加密算法（如 AES、RSA 等）的支持，使其成为一个**综合性**的密码学工具。
- **增强破译功能：**研发更复杂的破译算法可以研究和实现更复杂的破译算法，提高破译成功率。 尝试分布式破译，可以实现分布式破译功能，利用多台计算机的计算能力，提高破译效率。

5. 结论

- 本文设计并实现了一款单表代换密码辅助工具，通过 Python 编程语言和 Tkinter 图形界面库，实现了加密、解密和辅助破译等功能。测试结果表明，该工具功能完整、性能良好，具有较高的应用价值。本工具当前局限在于对统计数据质量的依赖，以及对过短密文的处理能力有限。程序算法虽能找到局部最优，但不保证总能找到全局最优解，即可能被无关单词误导做出错误判断。未来可进一步优化工具的性能，增加更多密码学算法的支持，以满足更广泛的应用需求。

代码地址：https://github.com/Yoloseq/about_cryptology.git