

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： 单表代换破译辅助工具

团队名称： Team Jellaswill

团队人员： 邱健珏

2025年 6月 1日

|  |
| --- |
| 基本信息表 |
| 作品题目：单表代换破译辅助工具 |
| 作品内容摘要：  本作品是一个单表代换辅助工具，具备加密、解密、频率分析（包括字母、单词、二元组、三元组）以及多种辅助功能，如频率分级、短单词检查、元音检查和对比破译模式等。用户可通过网页界面输入明文或密文，选择相应功能并提交，即可查看处理结果。 |
| 关键词（五个）：  单表代换  加密解密  频率分析  破译辅助  Flask |
| 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 | 邱健珏 | PB23030847 | 算法设计  界面设计 | | 2 |  |  |  | | 3 |  |  |  | |

# 1.作品功能与性能说明

**功能**

* **加密**：根据用户提供的密钥对输入的明文进行加密。
* **解密**：依据用户提供的密钥对输入的密文进行解密。
* **频率分析**：支持对输入文本进行字母、单词、二元组和三元组的频率分析。
* **辅助功能**：
  + **频率分级**：对字母频率进行分级。
  + **短单词检查**：检查密文中短词解密后是否为有效英文单词。
  + **元音检查**：检查解密后文本中单词的元音情况。
  + **对比破译模式**：提供破译建议，如根据字母频率建议添加密钥等。

**性能**

该工具基于 Flask 框架开发，具备基本的稳定性和响应能力。在处理文本时，能快速计算各种频率并给出相应结果。

# 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. **用户交互**：用户通过网页界面输入明文 / 密文、密钥，并选择相应功能。
2. **数据接收**：Flask 应用接收用户提交的数据。
3. **功能处理**：根据用户选择的功能，调用 util.py 中的相应函数进行处理。
   * **加密 / 解密**：使用 encryptor 和 decryptor 类进行加密和解密操作。
   * **频率分析**：使用 FrequencyAnalyzer 类计算字母、单词、二元组和三元组的频率。
   * **辅助功能**：调用相应的辅助函数，如 suggest\_vowels、suggest\_by\_word\_frequency 等。
4. **结果返回**：将处理结果返回给网页界面进行显示。

**相关描述**

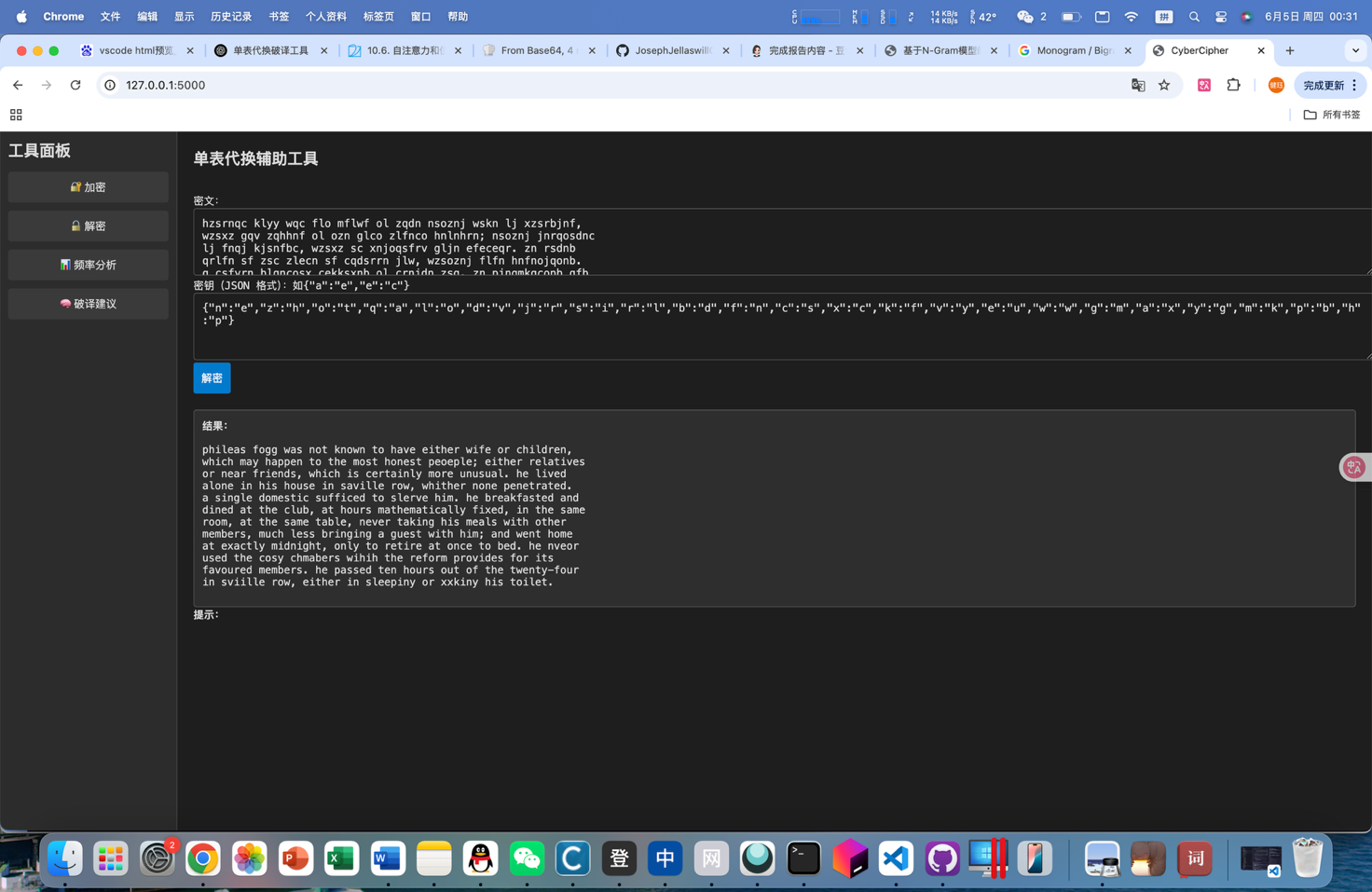
* **数据存储**：使用 Python 的字典存储密钥和频率信息。
* **文本处理**：使用正则表达式和 Python 的字符串处理函数对文本进行处理。
* **英语词典**：使用 nltk 库的英语单词词典进行短单词有效性检查。

## 2.2 参考文献

Kahn, David. The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet. Scribner, 1996.

密码学导论教材

## 2.3 运行结果



## 2.4 技术指标

编程语言：Python

Web 框架：Flask

依赖库：flask、nltk

# 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。
* **性能测试**：使用不同长度的文本进行测试，记录处理时间，评估系统的性能。

## 3.2 功能测试

* **加密测试**：输入明文和密钥，验证加密结果是否正确。
* **解密测试**：输入密文和密钥，验证解密结果是否正确。
* **频率分析测试**：输入文本，验证字母、单词、二元组和三元组的频率计算是否正确。
* **辅助功能测试**：分别测试频率分级、短单词检查、元音检查和对比破译模式，验证其功能的正确性。

## 3.3 性能测试

使用不同长度的文本进行测试，记录处理时间。测试结果表明，在运行在现代个人计算机中，运行效率没有太大问题。

## 3.4 测试数据与结果

* **测试数据**：使用 example/cipher.txt 中的密文。
* **测试结果**：各项功能均能正常运行，处理结果符合预期，成功在辅助下破解出example/key.json文件中的代换表

# 4.应用前景

本工具可应用于密码学教学、密码分析和简单的加密解密场景。在教学中，可帮助学生理解单表代换密码的原理和破译方法；在密码分析中，可辅助分析人员进行频率分析和破译工作；在简单的加密解密场景中，可方便用户进行加密和解密操作。

# 5.结论

本作品实现了单表代换辅助工具的基本功能，具备加密、解密、频率分析和多种辅助功能。通过测试，系统的功能和性能均符合预期。该工具具有一定的应用前景，可在密码学教学和密码分析等领域发挥作用。但在性能和功能方面仍有改进空间，如可进一步优化频率分析算法，增加更多的破译辅助功能等。