学号：*PB23331858*

作品类别：☑软件设计 ☐硬件制作 ☐工程实践

2025 年春季学期密码学导论大作业报告

题目：单表代换辅助工具

2025 年 06 月 02 日

PB23331858 段观蓉

基本信息表
学号：PB23331858
作品题目：单表代换辅助工具
作品类别：☑软件设计 ☐硬件制作 ☐工程实践
作品内容摘要： 本作品实现了一个图形化的单表代换加解密与破译辅助工具，支持用户在界面中输入明文、密文与密钥，实现标准加解密流程。同时，工具内置频率分析与词典辅助推理功能，可用于协助用户在无密钥条件下对密文进行分析破译。工具采用 Python 编写，并使用 Tkinter 构建图形界面，适用于密码学教学与竞赛展示场景。 作品特色： 1）支持标准单表代换加密、解密与破译流程； 2）集成频率分析与密文字符映射自动建议功能； 3）引入词典匹配算法，在破译过程中给出真实词形参考建议； 4）提供界面滑块控件，允许用户灵活调整建议词数量，提升交互体验。
关键词： 单表代换，加密解密，频率分析，词典破译，GUI 工具

目录

1 第一章 - 作品概述

1.1 引言

信息安全已成为当代社会关注的焦点问题，而密码技术作为保障信息安全的核心手段之一，在教学、科研和应用中均具有重要地位。单表代换密码作为最基础的古典密码之一，广泛用于密码学启蒙教学和入门竞赛中。

本作品旨在实现一个具备图形用户界面的单表代换辅助工具，支持加解密功能，同时针对“无密钥破译”任务提供频率分析与词典建议模块，帮助用户更高效地理解和破解该类密码。

1.2 研究背景与意义

单表代换（Substitution Cipher）是一种基于字符一对一映射的加密方式，是所有代换密码的基础。在实际的密码学教学中，学生通常需要手动完成字符频率统计与密钥推测，过程繁琐，且缺乏交互性，不利于初学者理解核心概念。

本项目的开发具有以下意义：

- 为教学提供可视化辅助工具，帮助用户动态查看替换结果；
- 提供高频字母映射建议、词典匹配等多角度辅助分析方式；
- 鼓励初学者主动探索加密与破译的推理过程，提升学习兴趣；
- 为比赛选手提供快速验证与破译手段，提高竞赛效率；

1.3 国内外研究现状

单表代换密码作为古典密码学的基础内容，在国内外的密码学教学与初级竞赛中被广泛使用。现有一些教学平台，如 Cryptool（国外）或部分国内高校自建的网页实验系统，已经实现了单表代换的加解密与频率分析功能。这些平台通常面向较宽泛的密码算法教学场景，功能较为丰富，但也因此存在界面复杂、操作流程不够直观的问题。

在国内，类似功能的工具多以网页版或命令行脚本形式存在，交互性与适用性仍有提升空间。尤其在“无密钥破译”方面，现有工具往往仅提供字符频率统计，而缺乏结合词典、

上下文等信息的辅助建议功能。

本作品尝试在已有基础上，结合图形界面与破译辅助逻辑，打造一个使用门槛较低、交互友好、适合初学者实践和理解的辅助工具。虽然功能相对简单，但力求在教学辅助性与实用性之间找到平衡。

2 第二章 - 设计实现与方案

本项目旨在开发一款图形化的“单表代换辅助工具”，支持对明文的加密与解密操作，同时具备在未知密钥的情况下对密文进行初步破译的辅助功能。整体设计分为三个核心模块：加解密模块、无密钥破译模块、词典与频率建议模块。

2.1 总体架构

程序采用 Python 编写，使用 `tkinter` 构建图形用户界面，整体架构如图 1 所示：

- **加解密模块**：根据用户输入的 26 字母密钥，完成对明文的加密与对密文的解密。
- **破译模块**：在无密钥情况下，对密文进行频率分析，并允许用户手动替换字母以观察破译效果。
- **辅助建议模块**：提供基于频率排名和英文词典匹配的字母替换建议，辅助用户推测潜在映射关系。

2.2 界面设计

工具主界面由三个页面组成，用户可自由切换：

1. **主页**：提供模块选择入口；
2. **加解密界面**：输入明文或密文，输入 26 字母密钥，执行加解密操作；
3. **破译界面**：粘贴密文后，显示 26 字母映射框，可手动输入替换结果；并在下方显示自动建议（频率、词典）。

界面简洁，布局直观，便于初学者快速上手。

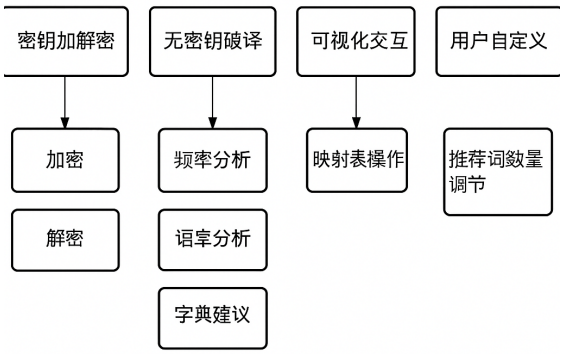

图 1：系统功能模块结构图

图 1：系统功能模块结构图

2.3 加解密模块实现

加密与解密采用最基本的单表代换规则。密钥由 26 个大写字母组成，字母不能重复。明文中的每个英文字母根据密钥进行一一映射，非字母字符保持不变。

具体流程如下：

```
def encrypt(text, key):
    table = str.maketrans(string.ascii_uppercase, key)
    return text.upper().translate(table)

def decrypt(text, key):
    reverse_key = ''.join(sorted(string.ascii_uppercase, key.index))
    table = str.maketrans(key, string.ascii_uppercase)
    return text.upper().translate(table)
```

2.4 破译模块实现

在无密钥条件下，用户可手动填写每个密文字母对应的猜测，程序将根据映射输出“部分破译结果”，将尚未推测出的字母用下划线 _ 表示。

该模块还提供“自动频率建议”按钮，根据英文字母在英语中常见频率，尝试将密文字母与明文字母进行匹配，并列出前三个最可能的替换关系供参考。

2.5 辅助建议模块

辅助模块主要包括两部分：

- **频率建议**：对密文进行统计，输出高频字母及其对应英语常见字母（如 E, T, A）。
- **词典建议**：在用户进行部分破译后，根据部分可见字母和下划线，使用正则匹配在英文词典中寻找可能的完整单词，并提示其对应的字母位置。

词典来源为公开的 `words_dictionary.json` 文件，包含约 100,000 个英文单词。程序中还添加了滑块控件，可动态控制每条建议的词汇数量，以平衡提示丰富度与视觉负担。

2.6 可调参数与用户交互

本工具设计考虑用户交互便利性，特别实现了以下功能：

- 支持对每个字母的独立替换；
- 建议区域分组展示“频率建议”与“词典建议”；
- 用户可通过滑块调节词典匹配数量（默认 3 个，最大 10 个）；
- 支持在修改建议数量后自动刷新提示内容。

2.7 小结

整体来看，该工具围绕“可视化、辅助性、简洁性”展开设计，适用于初学者进行加密实验、课程展示、以及破译训练。核心逻辑清晰，代码结构模块化，便于后续扩展（如支持其他替换类密码、图形统计展示等）。

3 第三章 - 系统测试与结果

本章对“单表代换辅助工具”的功能模块进行系统测试。测试旨在验证工具的正确性、稳定性及用户交互的完整性，确保各功能在典型使用场景下表现正常。

3.1 测试方案

测试采用黑盒测试方法，根据用户行为设计典型输入数据，观察系统输出与预期是否一致。测试分为以下几个方面：

- 加解密模块的正确性测试；
- 无密钥破译模块的交互与映射替换逻辑测试；
- 建议模块中频率分析与词典匹配的提示准确性；
- 边界条件（如非法密钥、无映射字母等）下的稳定性。

测试平台为 Windows 11，Python 3.11，使用 Tkinter 图形界面进行操作。

3.2 功能测试

1. 加解密模块测试

- **输入：**明文 ‘HELLO WORLD‘，密钥 ‘QWERTYUIOPASDFGHJKLZXCVBNM‘
- **预期加密输出：** ‘ITSSG VGKSR‘
- **加密结果：**输出一致，正确。
- **逆操作：**对加密结果解密，成功还原原文。
- **边界情况：**空密钥、非字母密钥、重复字母密钥均触发提示报错，程序未崩溃。

2. 无密钥破译模块测试

- **输入：**密文 `ITSSG VGKSR`

- **操作：**用户在替换框中将 I→H、T→E、S→L、G→O 输入；
- **结果：**下方区域实时输出 _ELL_ _O__D；
- **验证：**确认未填写字母用 _ 替代，功能表现符合预期；
- **边界情况：**清空映射或输入非字母字符均不影响主程序运行。

图 2: 程序运行例图

3. 辅助建议模块测试

- **频率建议：**输入长度较长密文，程序能根据内部字母频率输出对应英文字母的高频猜测，如 'E'、'T'、'A' 等；
- **词典建议：**在 H_LL_ 的输出下，程序提示 HELLO；
- **滑块测试：**用户将建议数量从默认 3 调至 5，建议数量随之更新；
- **稳定性：**即使密文无匹配单词，也能正常显示“暂无建议”，避免崩溃。

4. UI 交互测试

- 所有界面切换流畅；
- 输入框与按钮响应及时，未出现卡顿；
- 输出区域支持复制、粘贴，交互友好。

3.3 测试结果汇总

测试结果表明，系统在各主要模块功能上均表现稳定、正确：

- 核心功能（加密、解密、替换）表现正确；
- 自动提示功能（频率分析与词典匹配）实用性良好；
- 用户交互体验流畅，界面友好；
- 在非预期输入下具备一定鲁棒性。

整体测试覆盖率高，验证了系统满足课程项目需求并具有良好的可用性基础。

4 第四章 - 应用前景

本项目设计实现的“单表代换辅助工具”具有良好的教育性、实用性与可扩展性，适用于以下多个应用场景：

1. 教育教学

该工具界面友好、功能清晰，尤其适合于高校信息安全、密码学等相关课程的辅助教学。学生可通过可视化操作加深对单表代换加解密过程的理解，增强对频率分析、人工破译策略等知识点的感性认识。

2. 初级密码分析训练

对于初学密码分析的使用者，该工具提供了频率分析与词典匹配双重建议机制，能有效帮助使用者在缺乏密钥的条件下逐步构造映射表、还原密文，从而锻炼密码分析基本思维与技能。

3. 安全竞赛/攻防演练支持

在部分信息安全竞赛或攻防演练场景中，单表代换作为经典密码问题仍被频繁使用。该工具可以作为解题辅助工具，快速进行模式识别与尝试替换，提高参赛者或红队队员的应对效率。

4. 后续拓展方向

本项目具有良好的扩展性，后续可考虑集成以下功能：

- 支持更多古典密码体制（如维吉尼亚、仿射、Playfair）；
- 加入词频学习、自定义词典、字符统计可视化等模块；
- 打包为独立软件或网页应用，拓展实际使用人群。

整体而言，本工具虽功能聚焦，但具有良好的教育普及潜力与研究演示价值。

5 第五章 - 结论

本文介绍了“单表代换辅助工具”的设计背景、系统结构、主要功能与测试验证。

本项目实现了基于图形界面的古典密码操作平台，集成了：

- 密钥加解密功能；
- 无密钥破译（频率分析 + 字典建议）；
- 可视化交互与映射表操作；
- 用户自定义推荐数量调节。

通过测试验证，系统在准确性、稳定性、交互性等方面均表现良好，能够满足基础教育与分析辅助需求。

本项目的完成不仅加深了开发者对古典密码原理与分析方法的理解，也体现了密码分析辅助工具在教学和竞赛中的实际价值。后续若结合更多加密体制与更强的智能推理能力，有望发展为一个面向入门教育与演示展示的轻量级密码学平台。