2025 年春季学期《密码学导论》作品设计报告

题目：单表代换辅助工具

姓名：孟昭明

学号：PB23331866

github：https://github.com/Troymzm/crypt-system

2025 年 3 月 17 日

中国科学技术大学网络空间安全学院

基本信息表

编号： 单人作品题目 1

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：

本作品为一个基于 Python 语言构建的单表代换密码辅助工具，主要功能包括加密明文、解密密文、加载密文进行分析、显示当前密文、频率分析、单词分析、更新字母映射、清除字母映射以及显示当前破译结果。主程序文件 main.py 提供了用户交互界面，通过菜单选项让用户选择不同的功能。工具通过调用 util.py 中的 SubstitutionCipher 类实现具体的加密、解密和分析操作，在分析的过程中使用了字母频率分析和单词模式匹配等密码学方法。项目还包含一个示例密文文件 sample.txt，用于加载和分析密文。

关键词（五个）：

单表代换密码、Python、加密与解密、频率分析、单词模式匹配

1.作品功能与性能说明

本项目是一个单表代换密码辅助工具，主要功能包括：

1. 加密明文：使用给定的 26 个小写字母密钥对明文进行加密。通过 SubstitutionCipher 类的 encrypt 方法实现。
2. 解密密文：使用给定的 26 个小写字母密钥对密文进行解密。通过 SubstitutionCipher 类的 decrypt 方法实现。
3. 加载密文进行分析:从文件或用户输入加载密文，并进行初始处理。通过 SubstitutionCipher 类的 load_ciphertext 方法实现。
4. 显示当前密文:显示当前加载的密文。
5. 频率分析:基于字母频率提供映射建议。通过 SubstitutionCipher 类的 analyze_frequency 和 suggest_mapping 方法实现。
6. 单词分析:基于单词模式提供映射建议。通过 SubstitutionCipher 类的 extract_words 和 suggest_patterns 方法实现。
7. 更新字母映射：更新密文字母到明文字母的映射关系。通过 SubstitutionCipher 类的 update_mapping 方法实现。
8. 清除字母映射:清除当前的字母映射关系。通过 SubstitutionCipher 类的 clear_mapping 方法实现。
9. 显示当前破译结果：显示当前的密钥映射和破译状态。通过 SubstitutionCipher 类的 get_current_key 和 display_current_state 方法实现。

2.设计与实现方案

本项目是基于 Python 语言设计的。

2.1 实现原理

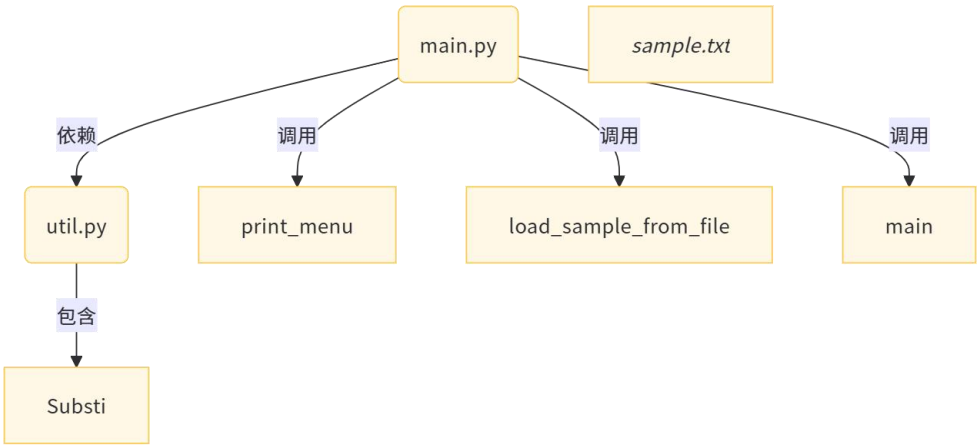

图 1：框图

2.2 运行结果

```
PS E:\code\crypt system> & D:/anaconda/python.exe "e:/code/crypt system/main.py"
**************************************************
        单表代换密码辅助工具
**************************************************
0: 退出系统
1: 加密明文
2: 解密密文
3: 加载密文进行分析
4: 显示当前密文
5: 频率分析
6: 单词分析
7: 更新字母映射
8: 清除字母映射
9: 显示当前破译结果
**************************************************
请选择功能：
```

图 2：运行结果图

2.3 技术指标

1. 加密和解密性能：时间复杂度为 O(n)，其中 n 是明文或密文的长度。每个字符只需查找一次映射关系，性能较高。

2. 频率分析性能：时间复杂度为 O(n)，其中 n 是密文的长度。通过一次遍历计算每个字母的频率，性能较高。

3. 单词提取和分析性能：单词提取的时间复杂度为 O(n)，其中 n 是密文的长度。通过正则表达式匹配单词，性能较高。单词模式分析的时间复杂度取决于单词的数量和长度。对于常见单词的匹配和模式生成，性能较高。

4. 映射更新和清除性能：映射更新和清除操作的时间复杂度为 O(1)，因为只需对字典进行插入或删除操作，性能较高。

5. 当前破译状态显示性能：显示当前破译状态的时间复杂度为 O(n)，其中 n 是密文的长度。通过一次遍历生成当前破译状态，性能较高。

3.系统测试与结果

3.1 测试方案

1. 测试单表代换加解密功能
2. 测试加载密文功能模块
3. 测试通过频率分析及单词模式匹配等方法破译示例密码

3.2 测试数据

1. 加密及解密的密钥为“qwertyuiopasdfghjklzxcvbnm”
2. 加密内容为“HELLO WORLD! THIS IS A SECRET MESSAGE.”
3. 测试需要破译的密文来自 sample.txt

3.3 测试过程及结果

3.3.1 加解密模块测试

加密过程：

```
请选择功能: 1
请输入要加密的明文: HELLO WORLD! THIS IS A SECRET MESSAGE.
请输入26个小写字母的密钥(按字母表顺序对应): qwertyuiopasdfghjklzxcvbnm
加密结果: itssg vgksr! ziol ol q ltektz dtllqut.
按回车键继续...
```

图 3：加密过程运行结果图

解密过程：

```
请选择功能: 2
请输入要解密的密文: itssg vgksr! ziol ol q ltektz dtllqut.
请输入26个小写字母的密钥(按字母表顺序对应): qwertyuiopasdfghjklzxcvbnm
解密结果: HELLO WORLD! THIS IS A SECRET MESSAGE.
```

图 4：解密过程运行结果图

3.3.2 加载密文模块测试

从文件导入：

```
请选择功能: 3
1: 使用示例密文
2: 输入自定义密文
请选择: 1
已加载示例密文
按回车键继续...
请选择功能: 4
当前密文: hzsrnqc klyy wqc flo mflwf ol zqdn nsoznj wskn lj xzsrbjnf,wzsxz gqv zqhhnf ol o
zn glco zlfnco hnlhrn;nsoznj jnrqosdnc lj fnqj kjsnfbc,wzsxz sc xnjoqsfrv gljn efeceqr.zn
rsdnb qrlfn sf zsc zlecn sf cqdsrrn jlw,wzsoznj flfn hnfnojqonb.q csfyrn blgncosx cekksxnb
 ol cnjdn zsg.zn pjnqmkqconb qfb bsfnb qo ozn xrep,qo zlejc gqozngqosxqrrv ksanb,sf ozn cq
gn jllg,qo ozn cqgn oqprn,fndnj oqmsfy zsc gnqrc wsoz loznj gngpnjc,gexz rncc pjsfysfy q y
enco wsoz zsg;qfb wnfo zlgn qo naqxorv gsbfsyzo,lfrv ol jnosjn qo lfxn ol pnb.zn fndnj ecn
b ozn xlcv xzqgpnjc wzsxz ozn jnkljg hjldsbnc klj soc kqdlejnb gngpnjc.zn hqccnb onf zlejc
 leo lk ozn ownfov-klej sf cqdsrrn jlw,nsoznj sf crnnhsfy lj gqmsfy zsc olsrno.
按回车键继续...
```

图 5：文件导入加载密文过程运行结果图

自定义密文：

```
请选择功能: 3
1: 使用示例密文
2: 输入自定义密文
请选择: 2
请输入密文: itssg vgksr! ziol ol q ltektz dtllqut.
已加载自定义密文
按回车键继续...
请选择功能: 4
当前密文: itssg vgksr! ziol ol q ltektz dtllqut.
按回车键继续...
```

图 6：自定义加载密文过程运行结果图

3.3.3 破译示例密码过程

3.3.3.1 使用频率分析建议

```
请选择功能: 5
基于频率分析建议:
建议: 'n' 可能对应 'E', 频率: 14.69%
建议: 'o' 可能对应 'T', 频率: 8.57%
建议: 's' 可能对应 'A', 频率: 8.04%
建议: 'z' 可能对应 'O', 频率: 7.52%
建议: 'l' 可能对应 'I', 频率: 6.64%
建议: 'q' 可能对应 'N', 频率: 6.47%
建议: 'c' 可能对应 'S', 频率: 6.47%
建议: 'j' 可能对应 'H', 频率: 6.29%
建议: 'f' 可能对应 'R', 频率: 6.29%
建议: 'r' 可能对应 'D', 频率: 4.02%
按回车键继续...
```

图 7：频率分析密文运行结果图

3.3.3.2 根据频率分析建议，设置映射：密文'n'-> 明文'E'

```
请输入密文字母: n
请输入对应明文字母: e
已更新映射: n -> E
按回车键继续...9
请选择功能: 9
当前密钥映射: ____________E____________
当前破译状态:
hzsrEqc klyy wqc flo mflwf ol zqdE EsozEj wskE lj xzsrbjEf,wzsxz gqv zqhhEf ol ozE glco zl
fEco hElhrE;EsozEj jErqosdEc lj fEqj kjsEfbc,wzsxz sc xEjoqsfrv gljE efeceqr.zE rsdEb qrlf
E sf zsc zlecE sf cqdsrrE jlw,wzsozEj flfE hEfEojqoEb.q csfyrE blgEcosx cekksxEb ol cEjdE
zsg.zE pjEqmkqcoEb qfb bsfEb qo ozE xrep,qo zlejc gqozEgqosxqrrv ksaEb,sf ozE cqgE jllg,qo
 ozE cqgE oqprE,fEdEj oqmsfy zsc gEqrc wsoz lozEj gEgpEjc,gexz rEcc pjsfysfy q yeEco wsoz
zsg;qfb wEfo zlgE qo Eaqxorv gsbfsyzo,lfrv ol jEosjE qo lfxE ol pEb.zE fEdEj ecEb ozE xlcv
 xzqgpEjc wzsxz ozE jEkljg hjldsbEc klj soc kqdlejEb gEgpEjc.zE hqccEb oEf zlejc leo lk oz
E owEfov-klej sf cqdsrrE jlw,EsozEj sf crEEhsfy lj gqmsfy zsc olsrEo.
```

图 8：设置解密映射运行结果图

同以上方法根据频率分析建议设置映射 o->T

3.3.3.3 使用单词模式匹配分析建议

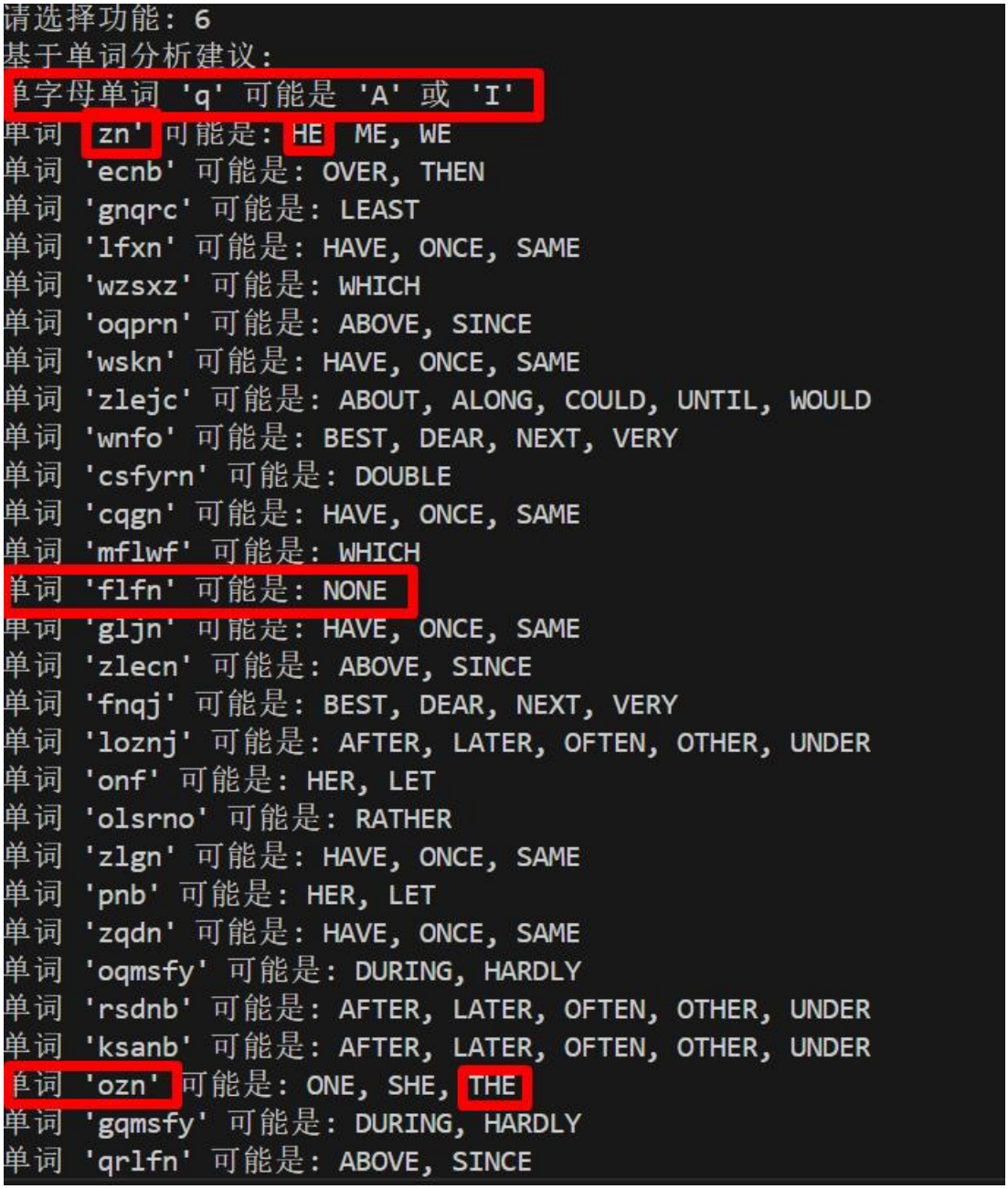

图 9：单词模式匹配分析建议运行结果图

结合我们自身的英语知识，可以选择图 9 中画红色框中的建议，并应用（设置对应的解密映射）

3.3.3.4 在已经设置过一些解密映射后继续使用单词模式匹配给出分析建议

```
Hsg.HE pjEAmkAcTEb ANb bsNEb AT THE xrep,AT Hlejc gATHEgATsxArrv ksaEb,sN THE cAgE jllg,AT
 THE cAgE TAprE,NEdEj TAmsNy Hsc gEArc wsTH lTHEj gEgpEjc,gexH rEcc pjsNysNy A yeEcT wsTH
Hsg;ANb wENT HlgE AT EaAxTrv gsbNsyHT,lNrv Tl jETsjE AT lNxE Tl pEb.HE NEdEj ecEb THE xlcv
 xHAgpEjc wHsxH THE jEkljg hjldsbEc klj sTc kAdlejEb gEgpEjc.HE hAccEb TEN Hlejc leT lk TH
E TwENTv-klej sN cAdsrrE jlw,EsTHEj sN crEEhsNy lj gAmsNy Hsc TlsrET.
按回车键继续...
请选择功能: 6
基于单词分析建议:
单词 'lfrv' 可能是: ONLY
单词 'wqc' 可能是: DAY, MAY, WAS
单词 'ecnb' 可能是: OVER
单词 'lfxn' 可能是: ONCE
单词 'wzsxz' 可能是: WHICH
单词 'gqv' 可能是: DAY, MAY, WAS
单词 'klj' 可能是: OUR, YOU
单词 'cqgn' 可能是: SAME
单词 'glco' 可能是: JUST, MOST
单词 'gexz' 可能是: MUCH, SUCH, WISH
单词 'flfn' 可能是: NONE
单词 'sf' 可能是: IN, ON
单词 'xlcv' 可能是: YOUR
单词 'klej' 可能是: YOUR
单词 'loznj' 可能是: OTHER
单词 'leo' 可能是: BUT, OUT
单词 'xrep' 可能是: YOUR
单词 'jlw' 可能是: OUR, YOU
单词 'zsc' 可能是: HIS, HOW
单词 'zqdn' 可能是: HAVE
单词 'qfb' 可能是: AND, ANY
单词 'ol' 可能是: TO
单词 'flo' 可能是: NOT
单词 'zsg' 可能是: HIS, HOW
按回车键继续...
```

图 10：继续使用单词模式匹配分析建议运行结果图

在不断交互后我们可以得到如下的破译结果

```
PHILEAS FOGG WAS NOT KNOWN TO HAVE EITHER WIFE OR CHILDREN,WHICH MAY HAPPEN T
O THE MOST HONEST PEOPLE;EITHER RELATIVES OR NEAR FRIENDS,WHICH IS CERTAINLY
MORE UNUSUAL.HE LIVED ALONE IN HIS HOUSE IN SAVILLE ROW,WHITHER NONE PENETRAT
ED.A SINGLE DOMESTIC SUFFICED TO SERVE HIM.HE BREAKFASTED AND DINED AT THE CL
UB,AT HOURS MATHEMATICALLY FIXED,IN THE SAME ROOM,AT THE SAME TABLE,NEVER TAK
ING HIS MEALS WITH OTHER MEMBERS,MUCH LESS BRINGING A GUEST WITH HIM;AND WENT
 HOME AT EXACTLY MIDNIGHT,ONLY TO RETIRE AT ONCE TO BED.HE NEVER USED THE COS
Y CHAMBERS WHICH THE REFORM PROVIDES FOR ITS FAVOURED MEMBERS.HE PASSED TEN H
OURS OUT OF THE TWENTY-FOURIN SAVILLE ROW,EITHER IN SLEEPING OR MAKING HIS TO
ILET.
```

图 11：示例密文破译结果图

把这段文字复制粘贴至浏览器上搜索可知破译结果无误

4.应用前景

4.1 应用前景

1. 密码分析研究：本工具可以用于研究和分析单表代换密码的破译方法，探索更高效的频率分析和单词模式分析技术。

2. 安全测试：本工具可以用于测试单表代换密码的安全性，评估其在不同应用场景下的可靠性。通过模拟攻击和破译过程，发现潜在的安全漏洞。

4.2 开发方向

1. 扩展功能：该工具仅支持单表代换密码，对于更复杂的密码算法（如多表代换密码、维吉尼亚密码等）不适用。需要扩展功能以支持更多类型的密码算法。

2. GUI 开发：当前的用户界面为命令行界面，交互性和用户体验较差。可以考虑开发图形用户界面（GUI），提高用户体验和操作便捷性。

3. 完善项目文档：当前项目缺乏详细的使用文档和测试用例，未来开发中可以需要编写详细的使用说明和单元测试，确保代码的可靠性和可维护性。

5. 结论

通过对单表代换密码辅助工具的设计与实现，本项目成功地完成了一个基于 Python 的密码学辅助工具的开发。本工具成功实现了单表代换密码的加密与解密功能，并通过加载密文文件和用户输入的方式，支持对密文的分析与破译。频率分析和单词模式匹配功能为用户提供了直观的破译建议，极大地简化了人工破译的复杂性。通过交互式界面，用户可以方便地更新字母映射、清除映射以及查看当前破译状态，为密文的破译提供了有力支持。未来，随着功能的进一步扩展和优化，本工具有望在密码学研究、教学以及信息安全领域发挥更大的作用。

注：本项目开源于 github 上，可访问 https://github.com/Troymzm/crypt-system 获取源码