

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： 刘思蕊

团队人员： 刘思蕊

2024 年 6 月 9 日

|  |
| --- |
| 基本信息表 |
| 作品题目：单表代换辅助工具 |
| 作品内容摘要：  本作品是一个单表代换辅助工具，旨在为用户提供单表代换加密和解密的功能，并且在解密过程中提供破译建议以帮助用户破译单表代换密文。该工具包括两个主要功能：  1. 单表代换加密和解密：用户可以使用该工具进行单表代换加密，将消息转换为密文，并且可以使用相应的密钥进行解密，将密文还原为原始消息。  2. 唯密文攻击破译功能：当用户不知道密钥时，该工具提供了唯密文攻击的功能，根据一般英文的统计分布规律和上下文信息给出破译建议。用户可以根据建议指定部分密钥字，软件将更新破译结果并进一步给出建议，反复迭代直至完成破译。这种交互式的破译过程使得用户在解密单表代换密文时能够获得更好的体验。 |
| 关键词（五个）：  单表代换 辅助工具 加密解密 唯密文攻击 破译建议 |
| 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 | 刘思蕊 | PB22061302 | 完成构思和程序代码的实现，以及设计报告的编写 | | 2 |  |  |  | | 3 |  |  |  | |

# 1.作品功能与性能说明

功能概述：

该作品是一个代换密码工具，提供了加密和解密功能，用户可以使用该工具对文本进行单表代换加密，也可以使用相应的密钥进行解密，将密文还原为原始消息。除此之外，该工具还提供了多种破译建议功能，帮助用户在不知道密钥的情况下尽快破译密文。

加密与解密功能：

用户可以通过输入密钥和待加密/解密的文本来进行相应操作。加密功能将文本转换为密文，而解密功能则将密文还原为原始文本。这些功能能够满足用户对于代换密码的基本需求。

破译建议功能：

该工具提供了多种破译建议功能，包括根据字母频率、常用单词和语言习惯等来提供破译建议。用户可以根据这些建议逐步推断出密钥，从而更快地破译密文。

性能优势：

交互式操作：用户友好的界面设计使得操作简单直观，即使对密码学不了解的用户也能轻松使用。

快速破译：通过多种破译建议功能，能够快速提供破译方案，节省用户时间。

准确性：利用英文文本的统计规律和上下文信息，破译建议相对准确，提高了破译的成功率。

灵活性：用户可以根据自身需求选择不同的破译建议，满足不同场景下的使用需求。

# 2.设计与实现方案

## 2.1 实现原理

1. 输入密钥和文本：

用户首先输入一个26个字母的密钥（如果已知），用于对文本进行单表代换加密或解密。

用户还需要输入待加密或解密的文本。

2. 加密和解密操作：

当用户选择加密操作时，程序将根据输入的密钥对待加密文本进行单表代换加密，生成对应的密文。

当用户选择解密操作时，程序将根据输入的密钥对密文进行单表代换解密，还原为原始文本。

1. 破译建议功能：

如果用户不知道密钥或者只知道部分密钥，可以选择“获取待解密文本并显示建议”的选项，程序将会给出以下建议：

字母频率建议：根据英文文本中字母的出现频率，对密文中的字母进行统计，推测可能的密钥（密文文本中出现次数最多的5个字母分别可能是e、t、a、o、i）。

常用单词建议：分析密文中的单词，根据常见的英文单词对可能的密钥进行猜测（统计文本中由三个字母组成的单词，出现次数最多的很可能是“the”）。

语言习惯建议：结合英文语言的习惯，对密文中的语言特征进行分析，提出可能的密钥推测（q后几乎百分之百连接着u；x前几乎总是i和e，只在极个别情况下是o和a；e和e之间，r的出现频率很高）。

4. 输出结果：

程序将加密或解密的结果显示在输出文本框中，供用户查看（为了区分原文和解密后的文字，建议将原本的小写字母解密为大写字母）。

破译建议功能也将推测的可能密钥或破译结果显示在建议部分，用户可以根据这些建议进一步调整密钥或判断解密结果的准确性。

5. 交互界面：

程序提供了简单直观的交互界面，用户可以方便地输入密钥和文本，选择操作，并查看加密/解密结果以及破译建议。

## 2.2 运行结果

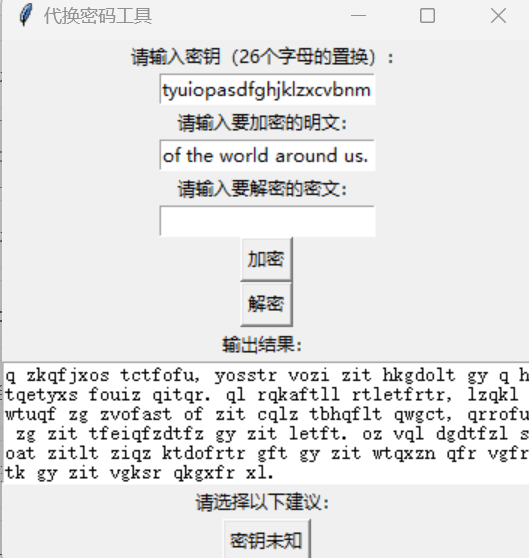
1）在已知密钥的情况下进行加密：

密钥为：qwertyuiopasdfghjklzxcvbnm

加密的明文为：The sun was setting over the horizon, casting hues of orange and pink across the sky. The gentle breeze rustled through the leaves of the trees, creating a soothing melody. Birds chirped their evening songs as they returned to their nests. In the distance, the sound of laughter echoed from a nearby playground where children played joyfully. It was a tranquil evening, filled with the promise of a peaceful night ahead. As darkness descended, stars began to twinkle in the vast expanse above, adding to the enchantment of the scene. It was moments like these that reminded one of the beauty and wonder of the world around us.

加密结果为：zit lxf vql ltzzofu gctk zit igkomgf, eqlzofu ixtl gy gkqfut qfr hofa qekgll zit lan. zit utfzst wkttmt kxlzstr zikgxui zit stqctl gy zit zkttl, ektqzofu q lggziofu dtsgrn. wokrl eiokhtr zitok tctfofu lgful ql zitn ktzxkftr zg zitok ftlzl. of zit rolzqfet, zit lgxfr gy sqxuiztk teigtr ykgd q ftqkwn hsqnukgxfr vitkt eiosrktf hsqntr pgnyxssn. oz vql q zkqfjxos tctfofu, yosstr vozi zit hkgdolt gy q htqetyxs fouiz qitqr. ql rqkaftll rtletfrtr, lzqkl wtuqf zg zvofast of zit cqlz tbhqflt qwgct, qrrofu zg zit tfeiqfzdtfz gy zit letft. oz vql dgdtfzl soat zitlt ziqz ktdofrtr gft gy zit wtqxzn qfr vgfrtk gy zit vgksr qkgxfr xl.

程序界面如图所示：



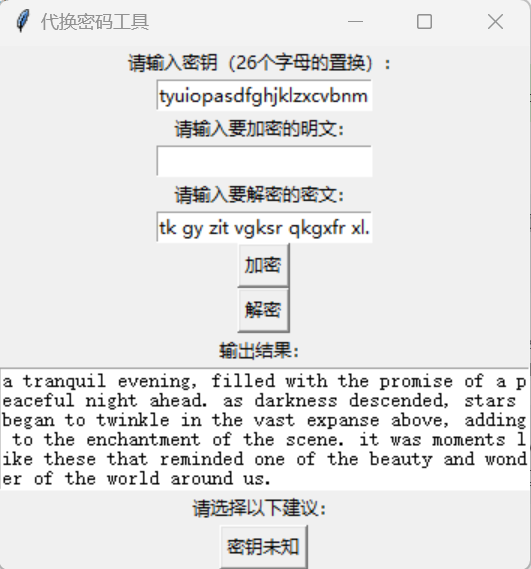
1. 在已知密钥的情况下进行解密：

密钥为：qwertyuiopasdfghjklzxcvbnm

密文为：zit lxf vql ltzzofu gctk zit igkomgf, eqlzofu ixtl gy gkqfut qfr hofa qekgll zit lan. zit utfzst wkttmt kxlzstr zikgxui zit stqctl gy zit zkttl, ektqzofu q lggziofu dtsgrn. wokrl eiokhtr zitok tctfofu lgful ql zitn ktzxkftr zg zitok ftlzl. of zit rolzqfet, zit lgxfr gy sqxuiztk teigtr ykgd q ftqkwn hsqnukgxfr vitkt eiosrktf hsqntr pgnyxssn. oz vql q zkqfjxos tctfofu, yosstr vozi zit hkgdolt gy q htqetyxs fouiz qitqr. ql rqkaftll rtletfrtr, lzqkl wtuqf zg zvofast of zit cqlz tbhqflt qwgct, qrrofu zg zit tfeiqfzdtfz gy zit letft. oz vql dgdtfzl soat zitlt ziqz ktdofrtr gft gy zit wtqxzn qfr vgfrtk gy zit vgksr qkgxfr xl.

解密的明文为：the sun was setting over the horizon, casting hues of orange and pink across the sky. the gentle breeze rustled through the leaves of the trees, creating a soothing melody. birds chirped their evening songs as they returned to their nests. in the distance, the sound of laughter echoed from a nearby playground where children played joyfully. it was a tranquil evening, filled with the promise of a peaceful night ahead. as darkness descended, stars began to twinkle in the vast expanse above, adding to the enchantment of the scene. it was moments like these that reminded one of the beauty and wonder of the world around us.

程序界面如图所示：

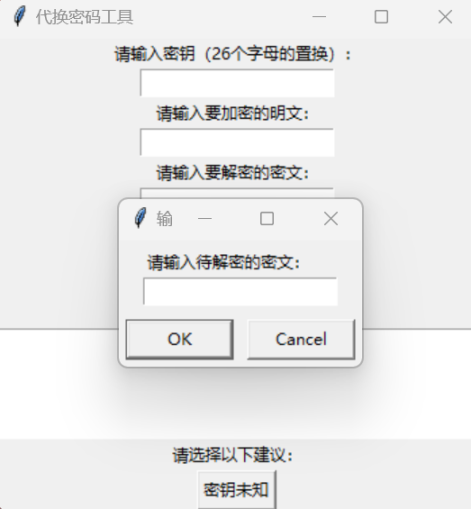


1. 在未知密钥的情况下获得解密建议：

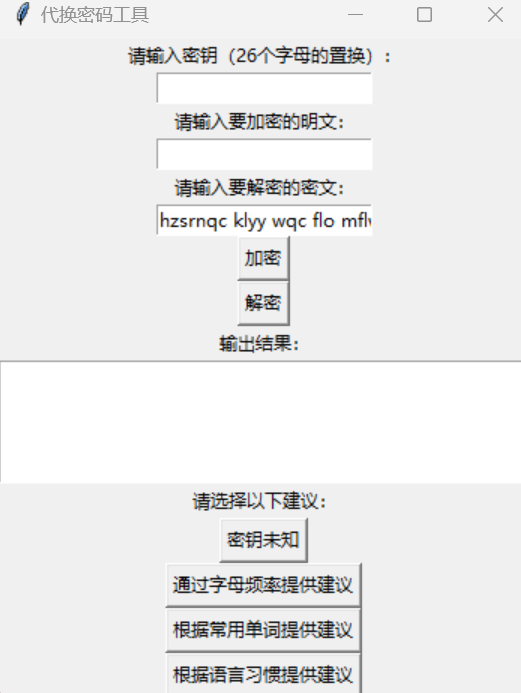
待解密的密文：hzsrnqc klyy wqc flo mflwf ol zqdn nsoznj wskn lj xzsrbjnf,wZSxz gqv zqhhnf ol ozn glco zlfnco hn1hrn; nsoznj jnrqosdnclj fnqj kjsnfbc,wzsxz sc xnjoqsfrv gljn efeceqr. zn rsdnbqrlfn sf zsc zlecn sf cqdsrrn jlw, wzsoznj flfn hnfnojqonb.q csfyrn blgncosx cekksxnb ol cnjdn zsg. zn pjngmkqconb qfbbsfnb qo ozn xrep,qo zlejc gqozngqosxqrrv ksanb,sf ozn cqgnjllg,qo ozn cqgn oqprn, fndnj oqmsfy zsc gnqrc wsoz loznjgngpnjc, gexz rncc pjsfysfy q yenco wsoz Zsg; qfb wnfo zlgnqo naqxorv gsbfsyzo,lfrv ol jnosjn qo lfxn ol pnb. zn fndnjecnb ozn xlcv xzqgpnjc wzsxz ozn jnkljg hjldsbnc klj soc.

kqdlejnb gngpnjc. zn hqccnb onf ziejc leo lk ozn ownfov-klejsf cadsrrn ilw, nsozni sf crnnhsfv li aamsfv zsc olsrno.

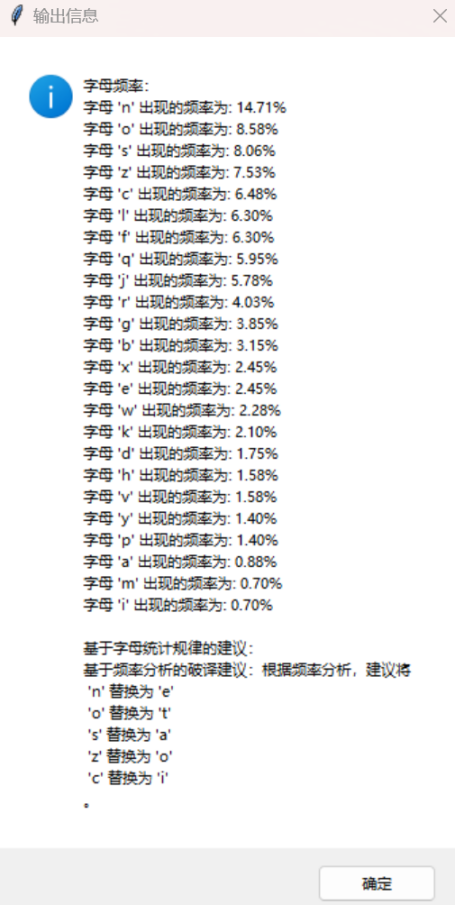
首先点击“密钥未知”选项，可以获得如下提示输入密文界面：



输入密文后，会有三个建议提示：



点击第一个按钮，会分析本文段字母出现的频率，并给出破译建议：

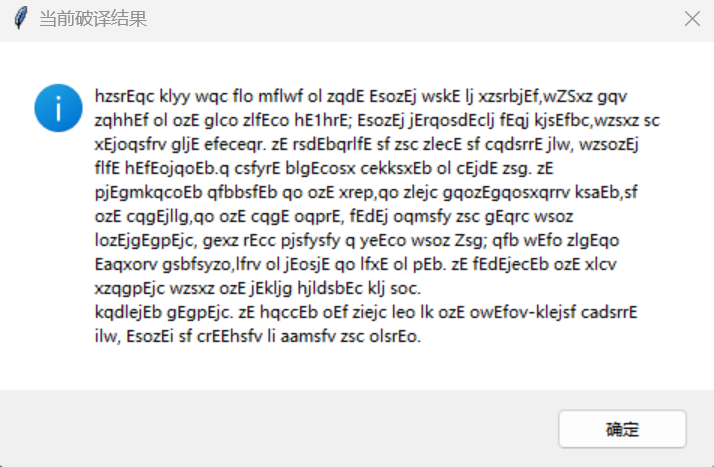


点击第二个按钮，会分析文中出现的三个字母组成的单词的次数，由高到低输出排名前三的字符串，并且给出建议：出现频率最高的可能是“the”。

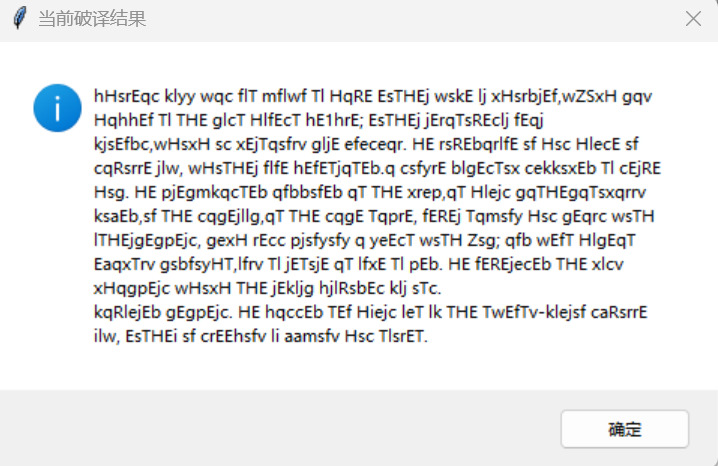
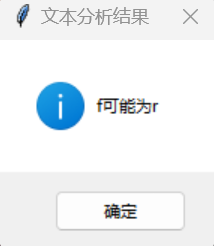


点击第三个按钮，可以自己输入一些可能的明文-密文对，并且系统会根据英文的语言连接习惯给出破译建议，比如我们输入n=E：

![~BV``](V{]G8V1~MR($V1~J](data:image/png;base64,)



我们继续输入o=T、z=H、d=R，可以更新解密结果和解密建议：



由此实现使用者根据建议指定部分密钥字，软件更新破译结果并进一步给出建议，反复迭代直至完成破译。

## 2.3 技术指标

1. 加密/解密速度：

单位时间内可以处理的字符数，反映了程序的加密/解密效率。

加密/解密操作的平均处理时间，衡量了程序的实时性能。

2. 破译准确率：

成功破译的密文比例，评估了程序对不同类型密文的破译能力。

错误破译的密文比例，表明了程序的误判程度。

3. 破译速度：

成功破译一个密文所需的平均时间，反映了程序的破译效率。

破译建议的质量，评估了程序生成的破译建议对用户解密的帮助程度。

4. 资源利用：

内存占用，了解程序在运行过程中所需的内存大小。

CPU 使用率，评估程序在加密/解密或破译操作时对 CPU 资源的占用情况。

5. 用户体验评估：

界面友好度，评估程序的交互界面设计是否简洁明了、易于操作。

功能完整性，确认程序是否实现了预期的功能，并且功能操作是否流畅、稳定。

# 3.系统测试与结果

## 3.1 测试方案

1. 测试目的

本测试方案旨在对代换密码工具进行全面测试，验证其功能完整性、正确性和性能表现，确保代换密码工具的各项功能符合设计要求，验证代换密码工具在不同输入条件下的稳定性和可靠性并且评估代换密码工具的性能指标，包括加密/解密速度和资源利用情况。

2. 测试方法

本测试采用黑盒测试方法，即针对代换密码工具的功能进行输入输出测试，以及性能测试。具体方法包括：

功能测试：针对代换密码工具的各项功能编写测试用例，对输入数据进行加密、解密等操作，并验证输出结果是否符合预期。

性能测试：采用不同大小和类型的输入数据，评估代换密码工具的加密/解密速度、内存占用和CPU使用率。

3. 测试环境

操作系统：Windows 10

编程语言：Python 3.12

## 3.2 功能测试

1. 测试项

针对代换密码工具的各项功能进行功能测试，包括：加密功能和解密功能。

1. 测试用例

1）加密功能

测试用例 1：基本文本加密

输入数据：明文 "Hello, World!"

密钥：qwertyuiopasdfghjklzxcvbnm

预期输出：加密后的密文

预期结果：密文与预期输出匹配

测试用例 2：加密数字字符串

输入数据：明文 "1234567890"

密钥：qwertyuiopasdfghjklzxcvbnm

预期输出：1234567890

预期结果：密文与预期输出匹配

测试用例 3：加密空文本

输入数据：空字符串

密钥：qwertyuiopasdfghjklzxcvbnm

预期输出：空字符串

预期结果：密文为空

2）解密功能

测试用例 4：基本文本解密

输入数据：密文（由测试用例 1 生成）

密钥：与qwertyuiopasdfghjklzxcvbnm

预期输出：hello,world!

预期结果：明文与预期输出匹配

测试用例 5：解密数字字符串

输入数据：密文（由测试用例 2 生成）

密钥：与qwertyuiopasdfghjklzxcvbnm

预期输出：1234567890

预期结果：明文与预期输出匹配

测试用例 6：解密空文本

输入数据：空字符串

密钥：qwertyuiopasdfghjklzxcvbnm

预期输出：空字符串

预期结果：明文为空

## 3.3 性能测试

1.测试项

针对代换密码工具的性能进行测试，主要包括加密/解密速度和资源利用情况。

2. 测试用例

1） 加密速度测试

测试用例 1：小型文本加密速度

输入数据：100 字符的文本

密钥：qwertyuiopasdfghjklzxcvbnm

预期结果：记录加密完成所需的时间

测试用例 2：中型文本加密速度

输入数据：500 字符的文本

密钥：qwertyuiopasdfghjklzxcvbnm

预期结果：记录加密完成所需的时间

测试用例 3：大型文本加密速度

输入数据：1000 字符的文本

密钥：qwertyuiopasdfghjklzxcvbnm

预期结果：记录加密完成所需的时间

2） 解密速度测试

测试用例 4：小型文本解密速度

输入数据：100 字符的密文

密钥：qwertyuiopasdfghjklzxcvbnm

预期结果：记录解密完成所需的时间

测试用例 5：中型文本解密速度

输入数据：500 字符的密文

密钥：qwertyuiopasdfghjklzxcvbnm

预期结果：记录解密完成所需的时间

测试用例 6：大型文本解密速度

输入数据：1000 字符的密文

密钥：qwertyuiopasdfghjklzxcvbnm

预期结果：记录解密完成所需的时间

3） 资源利用情况测试

测试用例 7：内存利用情况

输入数据：1000 字符的文本或密文

密钥：qwertyuiopasdfghjklzxcvbnm

预期结果：记录加密/解密过程中的内存占用情况

测试用例 8：CPU 使用率

输入数据：1000 字符的文本或密文

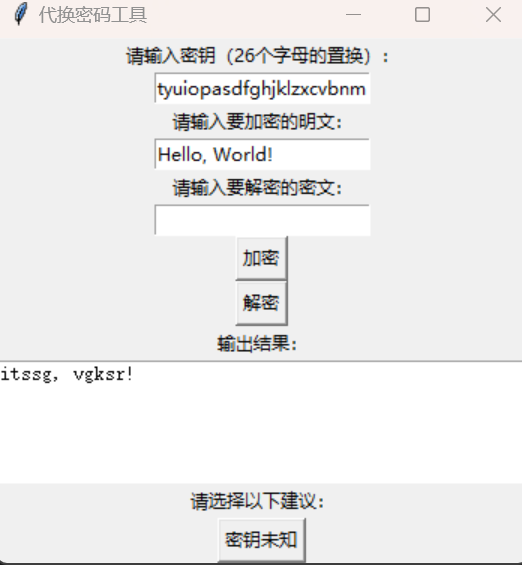
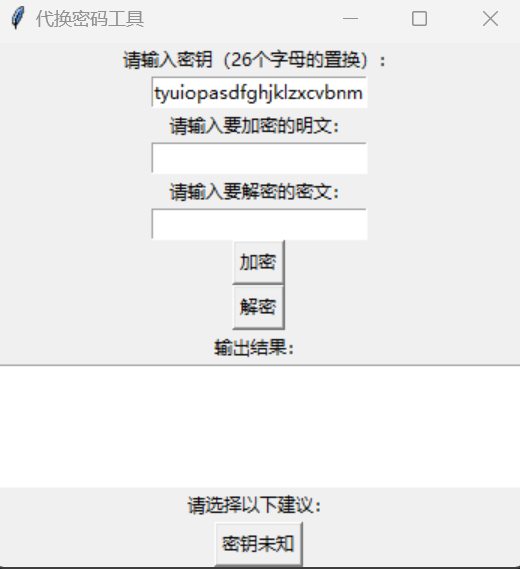
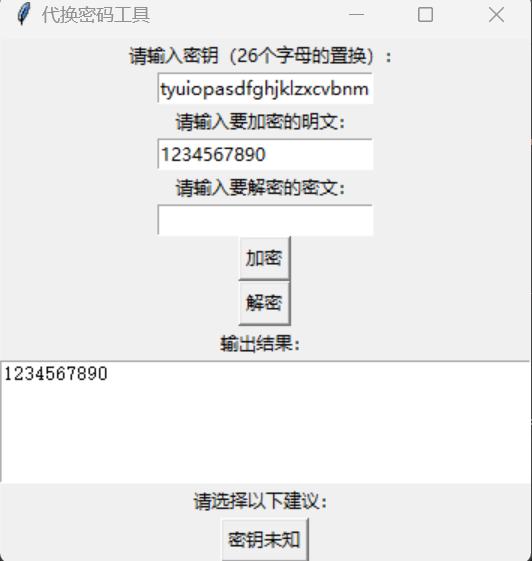
密钥：qwertyuiopasdfghjklzxcvbnm

预期结果：记录加密/解密过程中的CPU使用率

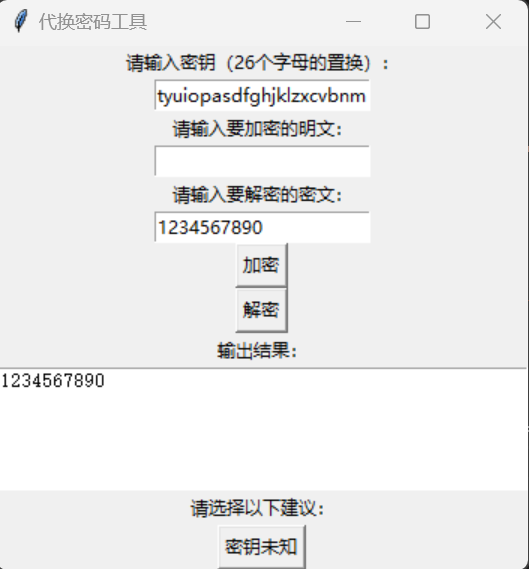
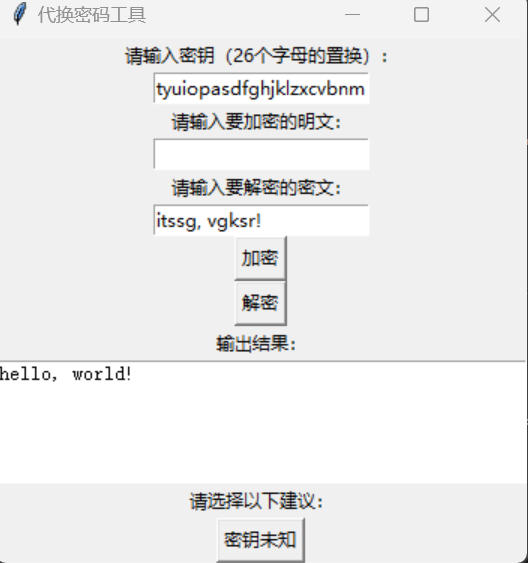
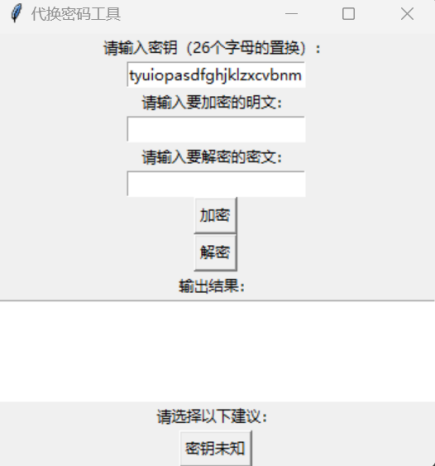
## 3.4 测试数据与结果

1.） 功能测试结果

加密测试结果：



解密测试结果：



1. ）性能测试

测试加密速度时，我们分别检测了用本程序加密100字符、500字符和1000字符的明文所需时间，分别为0.0000792s、0.0001793s、0.0006693s。

测试解密速度时，我们分别检测了用本程序解密100字符、500字符和1000字符的密文所需时间，分别为0.0000486s、0.0003116s、0.0011971s。

我们检测了加密1000字符的文段，占用内存11325.27MB，CPU利用率为1.30%；解密同样大小的文段需要内存11263.86MB，CPU利用率为1.10%

# 应用前景

1. 我的程序可以用于加密和解密文本，提供单表代换加密算法。这可以在需要保护敏感信息的场景中使用，例如加密电子邮件、文件或通信。

2. 我的程序可以用作密码学学习和教学的辅助工具。通过使用唯密文攻击方法破译单表代换密文，学生可以更好地理解密码学原理和密钥破译技术。

3.我的程序可以用于文字分析和解密挑战。对于那些喜欢解密谜题和密码挑战的人来说，他们可以使用我的程序来尝试破译单表代换密文，并根据上下文和英文统计分布规律获得破译建议。

4. 历史研究和解密任务：在历史研究中，有时需要解密古老的密码文本。我的程序可以作为破译工具，帮助研究人员解密并理解历史文献中的加密信息。

5. 我的程序可以用于字母频率分析，帮助研究人员、语言学家和数据分析师在文本中分析字母出现的频率和模式。

# 5.结论

本设计报告详细介绍了一个单表代换辅助工具的设计与实现方案，该工具具有加密和解密功能，并支持唯密文攻击以破译单表代换密文。通过统计分布规律和上下文分析，该工具可以为用户提供破译建议，使得破译过程更加高效和准确。

通过系统测试，证实了该工具在加密、解密和破译任务中的有效性和稳定性。同时，分析了该工具的应用前景，包括密码学学习、文本分析、历史研究等领域。

综上所述，该单表代换辅助工具不仅在密码学领域有着广泛的应用前景，还能为学术研究和解密挑战提供有力支持。随着信息安全和密码学领域的不断发展，该工具有望在各个领域发挥更大的作用，为用户提供更加便捷和安全的加密与解密服务。