用户操作指南

**1 引言**

**1.1 S-DES算法介绍**

为了更好地理解DES算法，美国圣克拉拉大学的Edward Schaefer教授于1996年开发了Simplfied DES方案，简称**S-DES**方案。它是一个供教学而非安全使用的加密算法，它与DES的特性和结构类似,但参数小，明文分组为8位，主密钥分组为10位，采用两轮选代。它是一种简化的数据加密标准，通过减少数据块和密钥的大小以及减少迭代次数来简化算法，主要用于教育和学术目的，以帮助理解和教学DES（Data Encryption Standard）算法的基本原理。

**1.2项目概述**

身处数字化时代，信息安全是保护个人隐私和敏感数据的核心。通过加密技术，如S-DES算法，可以有效地防止数据在传输过程中被未授权访问或篡改。在信息化社会中，信息安全是国家安全的基石，它关系着全国网民的切身利益，影响着国家安全和社会大局稳定。加强对个人信息，特别是隐私信息的保护力度，是适应大数据时代发展的必然要求，许多加密算法也因此应运而生。

本项目使用了S-DES算法来进行编写，利用其提供的加密、解密和生成密钥等功能进行数据传输和保护，也加入了暴力破解等功能来用于测试系统的安全性，评估系统的防御能力。同时项目进行过程中使用相同算法流程和转换单元(P-Box、S-Box等)，以保证算法和程序在异构的系统或平台上都可以正常运行。

**1.3应用场景**

S-DES算法的实现主要针对教育和研究目的，通过简化版的DES算法帮助学习者和教育者理解加密算法的内部工作原理。它适用于各种教学和实验环境，以及需要基本数据加密保护的场景。在安全评估中，S-DES可以用于测试系统的安全性，通过尝试所有可能的密码组合来评估系统的防御能力。尽管S-DES提供的安全性不如DES，但它仍然可以用于对数据进行基本的加密，特别是在数据量较小或安全要求不高的情况下。

**2 系统要求**

**2.1 环境配置**

2.1.1 开发工具

编程语言：Python

开发工具：Pycharm，VS Code，Anaconda

2.1.2 运行环境

操作系统：Windows

Python：使用Python语言结合Tkinter库来实现GUI交互

GUI接口：使用库构建GUI界面，包括输入密钥等用户交互组件，以及按钮触发事件。

**2.2 系统组成**

系统的开发和测试共由五个关卡组成，分别为基础测试、交叉测试、拓展功能、暴力破解和封闭测试。实现S-DES算法的加密和解密过程，支持8-bit数据输入和10-bit密钥输入，通过GUI接收用户输入的明文和密钥，并显示加密后的密文或解密后的明文，同时也支持ASCII编码字符串的加密和解密，增强了其实用性。系统可以通过暴力破解，尝试所有可能的密钥组合以找到正确的密钥，支持多线程以便在暴力破解中使用多线程来提高破解效率。

**2.3 功能实现**

①加解密功能：S-DES算法实现了数据的加密和解密功能，这是其核心功能之一。它采用了与DES算法相同的基本结构，包括替换（Substitution）和置换（Permutation）步骤。

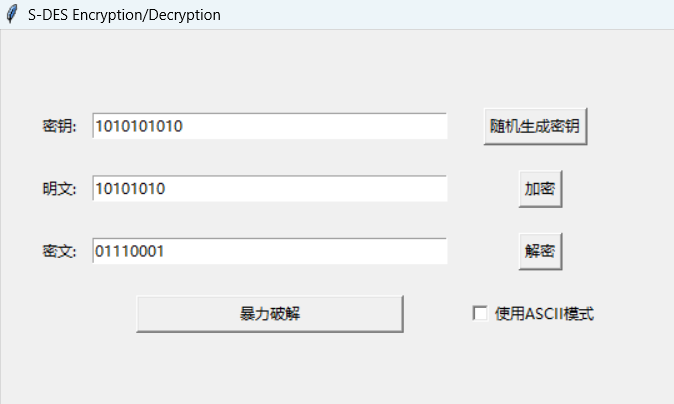
②暴力破解功能：系统同时包括了暴力破解功能，这使得它不仅可以用于加密，还可以用于安全分析，帮助测试和分析不同密钥组合的有效性。

③编程实现：系统的实现位于源代码文件夹中，这是整个算法的具体实现部分。它被设计为一种易于理解和实现的方式，可以帮助学习者更好地理解DES算法的工作原理和潜在的安全问题，在实际使用过程中提供一定程度安全性的加密方案。

**3 系统功能介绍**

**3.1 基础加密及解密**

①加密：在输入框中输入10bit的密钥和8bit的明文，可以输出同为8bit的密文，密钥也可以通过点击右上方的“随机生成密钥”按钮随机生成。



②解密：在输入框中输入10bit的密钥和8bit的密文，可以输出同为8bit的明文。



**3.2 ASCII字符串加密及解密**

在界面的右下角选择使用ASCII模式，表示使用ASCII编码字符串进行解密加密。

①加密：输入的明文为字符串，对应的加密输出也同样可以是ASCII字符串（也有可能输出乱码，不属于错误输出）。



②解密：输入的密文为字符串，对应的解密输出也同样可以是ASCII字符串（也有可能输出乱码，不属于错误输出）。



**4 系统评估**

**4.1 性能评估**

性能评估通过交叉测试及封闭性测试来实现，在交叉测试中，考虑到是**算法标准**，所有人在编写程序的时候需要使用相同算法流程和转换单元(P-Box、S-Box等)，以保证算法和程序在异构的系统或平台上都可以正常运行。

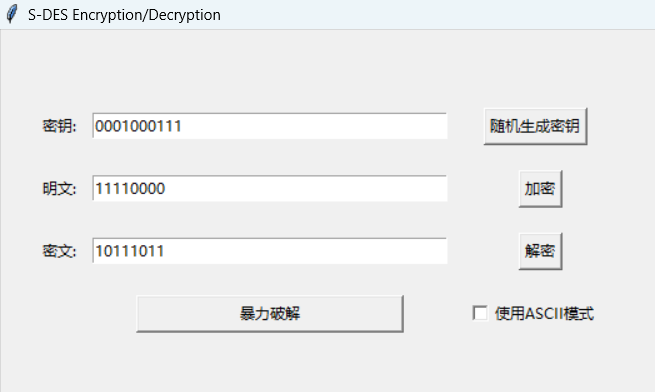
交叉测试界面：

①二进制：

A方解密结果：密钥：0001000111

密文：10111011

求得明文：11110000



B方加密结果：密钥：0001000111

明文：11110000

求得密文：10111011



②ASCII编码字符串：

A方解密结果：密钥：1100110100

密文：ùÂg

求得明文：CQU



B方加密结果：密钥：1100110100

明文：CQU

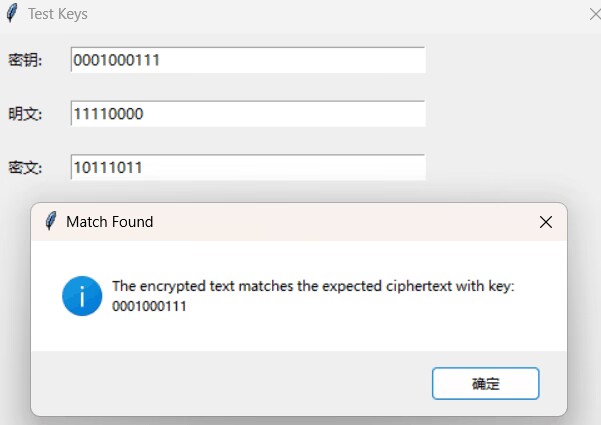
求得密文：ùÂg

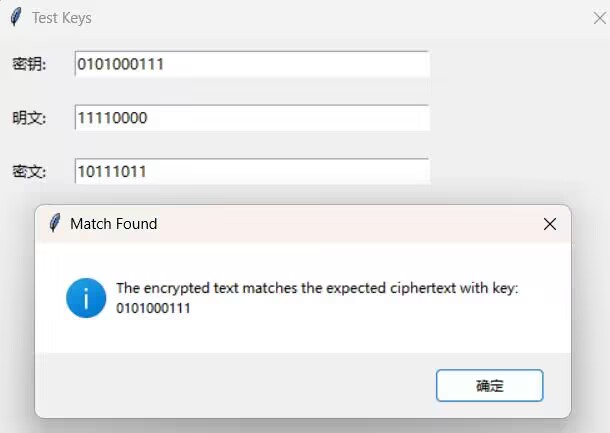


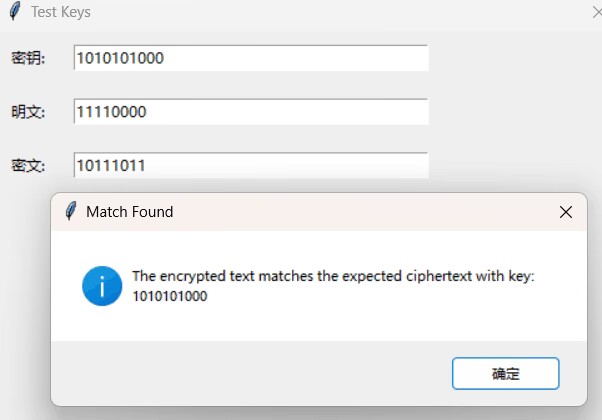
封闭性测试证明了通常情况下对于一个给定的明文-密文对，只存在一个密钥Key 能够得到相应的密文C，同时它也证明了S-DES算法实现安全性评估的相关要素。在理论上，对于不同的密钥K和相同的明文分组P，应该得到不同的密文C。这是因为加密算法的设计目的是确保不同密钥产生不同的密文，以增加破解的难度。然而，在一些特殊情况下，可能会出现不同密钥K产生相同密文C的情况，这通常是由于加密算法的缺陷或弱点所致。在现代密码学中，这种情况被视为严重的安全漏洞，因此加密算法的设计和评估都致力于防止这种情况的发生。

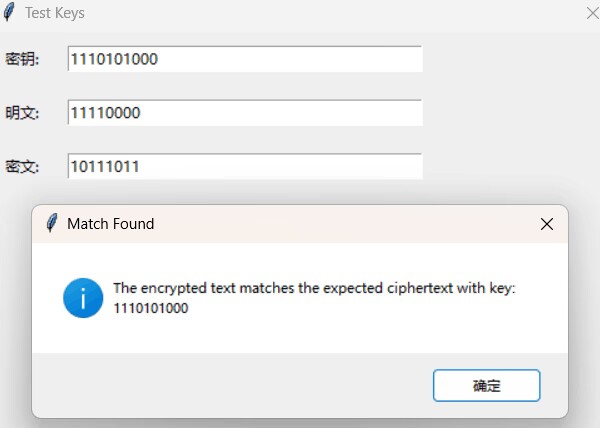
封闭测试界面：

①二进制：

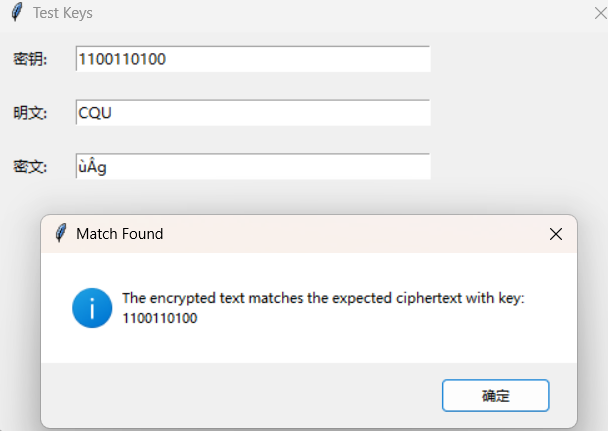


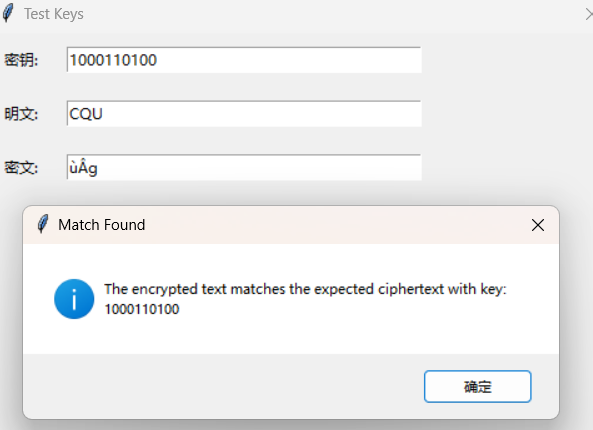






②ASCII编码字符串：

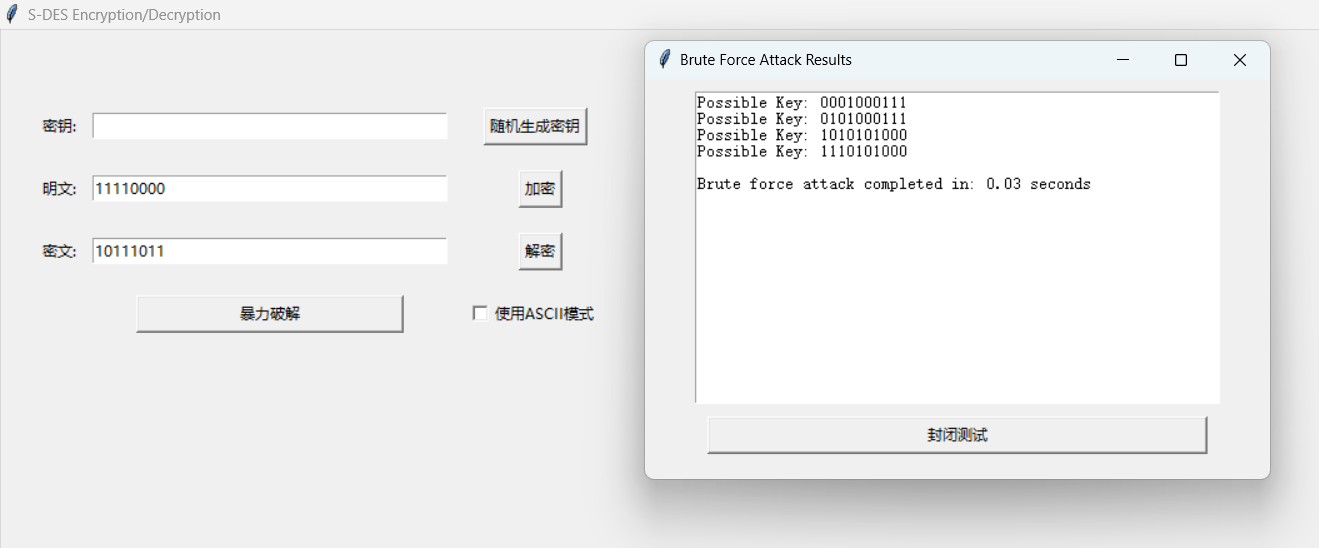




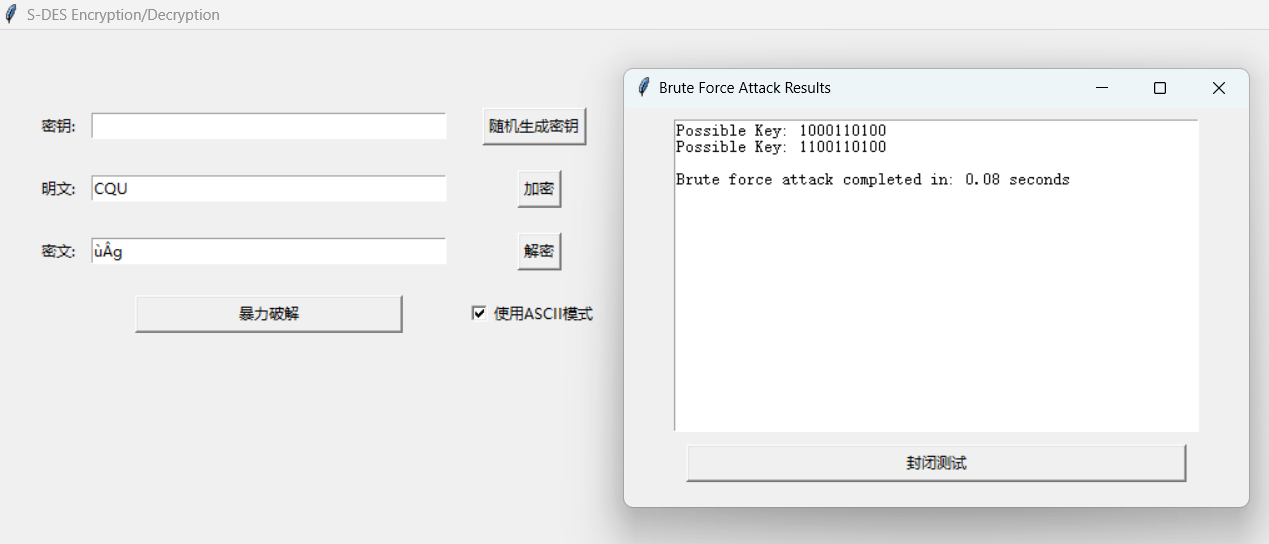
**4.2 安全性评估**

安全性评估主要通过系统的暴力破解测试来实现，在用户界面的下面存在暴力破解按钮，可以进入暴力破解。通过尝试所有可能的密钥组合，暴力破解可以帮助开发者评估所使用密钥的强度，了解其在实际应用中的安全性。通过暴力破解的结果，开发者可以识别出潜在的弱点，从而改进加密算法或建议使用更复杂的密钥生成策略。

①二进制：



②ASCII编码字符串：



**5 结论**

开发人员通过多次安全性评估和用户界面测试，不断调整和完善，实现了基本的S-DES算法系统的加密、解密功能，通过交叉测试、暴力破解测试和封闭测试证明了系统一定的安全性和高效性。

**6 附录**

**6.1 参考资料**

William Stallings.密码编码学与网络安全原理和实践[M].北京：电子工业出版社，2015

**6.2 术语解释**

对称加密算法：加密和解密使用相同密钥的加密算法。

密钥长度：密钥的位数，本项目中为10-bit。

分组长度：数据被分割成固定长度的块，本项目中为8-bit。

初始置换（IP）：加密前对数据块进行的第一次置换。

最终置换（IP^{-1}）：解密后对数据块进行的最后一次置换。

密钥扩展：将原始密钥扩展为多个子密钥的过程。

轮函数（F）：加密过程中对数据块进行的一系列变换。

S-Box：一种非线性替换函数，用于将输入的比特转换为输出的比特。

P-Box：置换盒，用于重新排列数据比特的顺序。

SW：交换函数，用于交换数据块的某些部分。

左移位：对数据或密钥进行的循环左移操作。

ASCII编码：一种字符编码标准，用于将字符转换为数字代码。

暴力破解：尝试所有可能的密钥组合以找到正确的密钥。

多线程：同时执行多个线程以提高程序的执行效率。

GUI：图形用户界面（Graphical User Interface），指通过图形方式显示的用户界面，用户可以通过图形元素进行交互操作。