S-DES 算法加密解密程序用户指南

1.简介

S-DES（Simplified Data Encryption Standard）是一种简化版的DES加密算法,主要用于教学目的。S-DES算法保留了DES算法的核心特性，但参数规模较小，以便更容易理解DES算法的工作原理和结构。

2.功能概述

本程序提供以下两个主要功能：

(1)加密：使用 S-DES 算法对输入的明文进行加密。

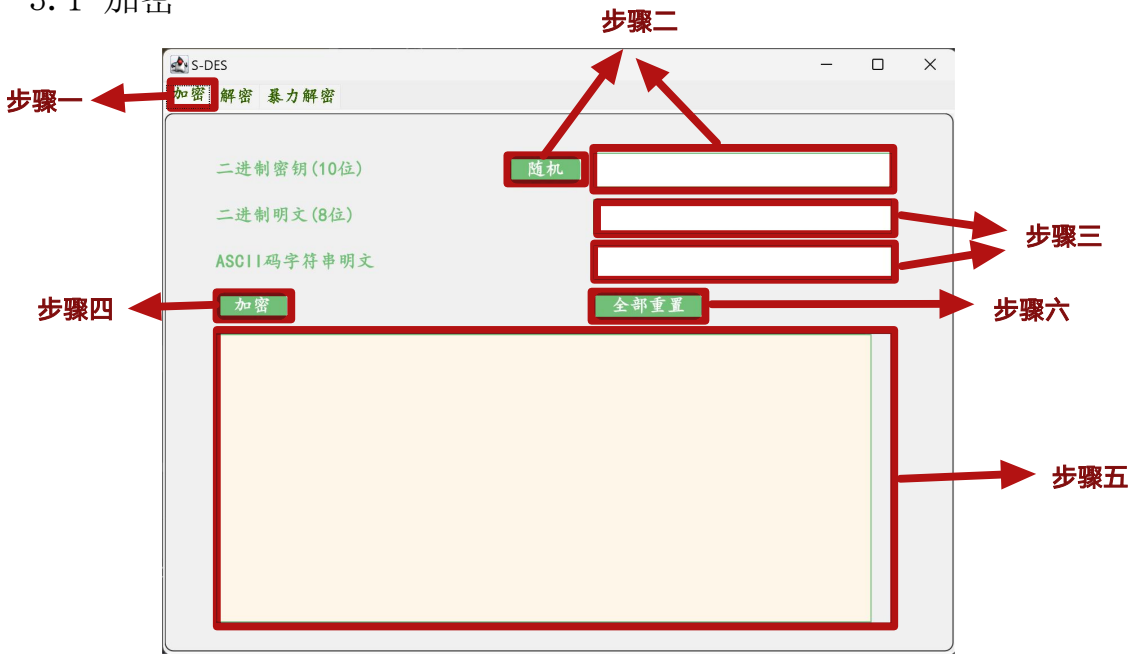
(2)解密：使用 S-DES 算法对输入的密文进行解密。

(3)暴力解密：使用S-DES算法对输入的一对明文和密文进行争对密钥的暴力解密。

3.使用方法

运行 UI 包下的 Main 类的 main 函数，显示运行界面，就能更具文字提示进行相应的功能。

3.1 加密



步骤 1：运行程序，点击加密页面。

步骤 2：输入加密参数密钥或随机生成密钥。

步骤 3：输入二进制明文或 ASCII 码字符串明文。

步骤 4：点击“加密”按钮。

步骤 5：加密结果将显示在文本框中，可以复制加密结果便于后续操作。

步骤 6：点击“全部重置”按钮即可清除输入框和文本框中的所有内容，进行下一次加密操作。

3.2 解密

步骤 1：运行程序，点击解密页面。

步骤 2：输入加密时输入的相同的参数密钥或随机生成密钥测试程序的解密功能。

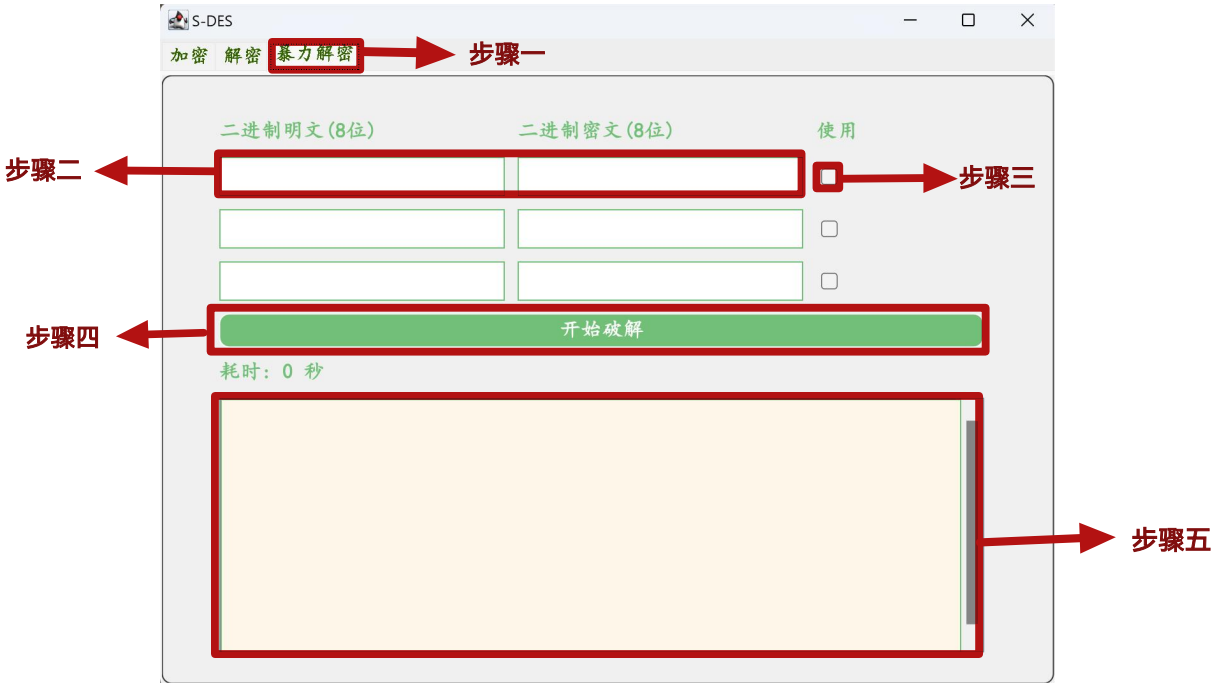
步骤 3：输入二进制密文或 ASCII 码字符串密文。

步骤 4：点击“解密”按钮。

步骤 5：解密结果将显示在文本框中，可以复制解密结果便于后续操作。

步骤 6：点击“全部重置”按钮即可清除输入框和文本框中的所有内容，进行下一次加密操作。

3.3 暴力解密



步骤 1：运行程序，点击暴力解密页面。

步骤 2：输入一对或多对二进制明文和二进制密文。

步骤 3：勾选使用。

步骤 4：点击“开始破解”按钮。

步骤 5：找出所有可能的密钥和验证过程以及破解所耗费的时间将在验证在文本框中显示，可以复制结果便于后续操作。

4. 加密解密参数

密钥：本 S-DES 算法加密解密程序支持 10 位的密钥，可以随机生成或者手动输入。

5. 常见问题

(1)、若输入正确位数的明文/密文和密钥，点击加密或解密按钮时却出现弹窗提示，说明同时输入了明文/密文和 ASCII 码字符串明文/密文。本程序可以实现 8bit 二进制密文和任意 bit 的 ASCII 字符的解密， 但是同时只支持一种形式的加密，否则会报错。

(2)、加密空字符 ASCII 字符时解密结果会显示 16 进制。

6. 注意事项

(1)、不要将明文和密钥泄露出去以保证安全性。

(2)、本程序可以实现 8bit 二进制密文和任意 bit 的 ASCII 字符的解密， 但是同时只支持一种形式的加密，否则会报错。

(3)、对于十位二进制的密钥，可以选择随机生成或者手动输入，但是需要满足 10 位。

(4)、本程序支持用户提供一对或多对明密文对进行针对密钥的暴力解密，考虑到 密钥碰撞的原因，我们会遍历所有密钥空间，找出所有可能的密钥并进行验证。