S-AES 算法加密解密程序用户指南

1. 简介

Simplified Advanced Encryption Standard (S-AES) 是一种简化版本的高级加密标准（AES）算法，用于加密和解密数据。本程序提供了一个基于 S-AES 算法的加解密功能。

2. 功能概述

本程序提供以下四个主要功能:

（1） 对二进制文本进行加解密操作。

（2） 对 Ascii 编码下的字符文本进行加解密操作。

（3） 通过双重加密和三重加密的方式对文本进行加解密操作。

（4） 使用密码分组链(CBC)模式对较长的明文消息进行加解密操作。

3. 使用方法

运行 GUI 界面里的 choose()函数，可以展示 UI 界面，下面进行功能展示。

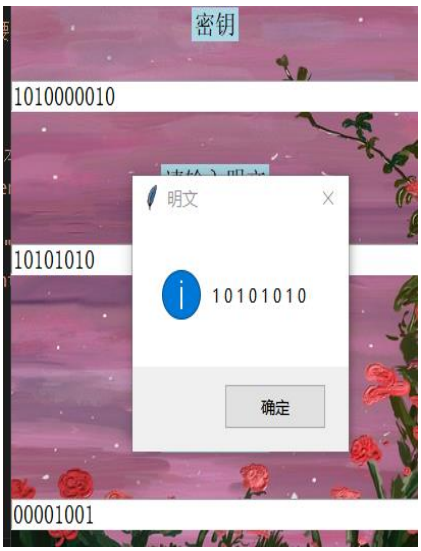
3.1 选择需要加解密的文本格式

用户根据需要进行加解密的文本格式选择该程序对应的功能，可以进行二进制加解密、Ascii 编码字节文本加解密、多重加解密算法、CBC 密码链模式加密。

3.2 加密（以二进制文本加解密为例）

步骤一：用户输入在通讯过程中使用到的密钥。
步骤二：输入相应格式的文本（此文二进制文本）进行加密。
步骤三：点击加密按钮弹出 messagebox 可以获取加密后的文本。
步骤四：输入相应格式的本文（此为二进制文本）进行解密。
步骤五：点击解密按钮弹出 messagebox 可以获取解密之后的文本。
步骤六：点击返回可以返回选择页面。

加解密过程如下图所示：



3.3 多重加密（包括双重加密和三重加密）

步骤一：用户输入两个密钥用于多重加密。
步骤二：输入需要加密的明文（输入明文通过“,”将字符串分解为需要加密的 16-bit 的字符）。
步骤三：点击加密按钮后会弹出 messagebox 并提示加密后的信息。
步骤四：输入相应格式的本文进行解密。
步骤五：点击解密按钮弹出 messagebox 可以获取解密之后的文本。
步骤六：点击返回可以返回二级选择页面。

4. 加解密参数

密钥：S-DES 算法使用一个 16 位密钥。确保输入正确的密钥以保证加密解密的一致性。

二进制文本：二进制文本需要保证输入的文本符合二进制格式。

字符文本：字符文本需要保证输入的文本符合 ASCⅡ码规定。

多重加密：在加密时需要使用两个密钥 16-bit 的密钥进行加解密操作。（注意两次输入密钥的先后顺序）

CBC：给定 16-bit 密钥和初始化向量后，输入符合规定的明文即可进行加解密操作。

5. 注意事项

（1） 确保密钥的安全性，不要将密钥泄露给其他人。

（2） 在使用加解密功能时，需要保证输入的文本符合相对应的格式，不然可能导致结果乱码或者无法加解密。

（3） 在对文本内容进行解密时，应使用本程序生成的密文，否则可能导致解密

出的明文部分信息丢失的情况。

（4） S-AES 算法通过简化密钥长度和加密轮数方便理解，但是加密能力有所不足，易被破解，不宜用于保密等级高的信息传输。