目录

[一、概述 1](#_Toc181892607)

[二、环境要求 1](#_Toc181892608)

[三、功能说明 1](#_Toc181892609)

[四、主要函数说明 2](#_Toc181892610)

[五、用户界面设计 3](#_Toc181892611)

[六、安装与运行 3](#_Toc181892612)

一、概述

该程序是一个基于简化版高级加密标准(S-AES)的加密/解密工具，支持对二进制数据和字符串的加密与解密操作。当输入为字符串时，程序会将其转换为二进制数据进行加密，并使用ASCII编码输出加密结果。解密时，ASCII编码的密文将转换为二进制，再解密为原始字符串。

二、环境要求

编程语言:Python3.x

库依赖:

tkinter：用于构建图形用户界面(GUI)

操作系统支持：Windows、Linux（理论可行）、macOS（理论可行）

三、功能说明

S-AES：

加密流程：

1.用户在输入框中输入明文（16位二进制/2位以上字符串）。

2.输入16位的二进制密钥。

3.如果输入是字符串，将其转换为二进制形式，再执行S-AES加密。

4.将加密结果显示在结果框中。

解密流程：

1.用户在输入框中输入密文（16位二进制/2位以上字符串）。

2.输入与加密时相同的16位二进制密钥。

3.解密密文，若输入为字符串，则解密后还原为原始文本，显示在结果框中。

多重加密：

加密流程：

1.用户在输入框中输入明文（16位二进制/2位以上字符串）。

2.输入32/48位的二进制密钥。

3.按照输入的密钥长度选择二重加密/三重加密。

4.如果输入是字符串，将其转换为二进制形式，再执行S-AES加密。

5.将加密结果显示在结果框中。

解密流程：

1.用户在输入框中输入密文（16位二进制/2位以上字符串）。

2.输入与加密时相同的32/48位二进制密钥。

3.按照输入的密钥长度选择二重解密/三重解密。

4.解密密文，若输入为字符串，则解密后还原为原始文本，显示在结果框中。

四、主要函数说明

1.key\_expansion(key,n)

功能：密钥扩展。

参数：

key：16位二进制，是密钥。

n：整数，是第n次密钥扩展的声明。

返回：密钥扩展后的新密钥new\_key。

2.KEY3(key)

功能：扩展两次密钥。

参数：

key：16位二进制，原始密钥。

返回：密钥扩展完之后的新密钥KEY1、KEY2.

3.left\_shift(bits,shifts)

功能：对输入的bit串进行左移操作。

参数：

bits：bit串，如[1,0,1,0]。

shifts：整数，左移位数。

返回：bit串左移后的新bit串。

4.s\_box(bits,sbox)

功能：根据4位bit串前两位为行，后两位为列返回S盒的值。

参数：

bits：4位bit串，如[1,0,1,0]。

sbox：选择哪个S盒。

返回：S盒的值转换为二进制的4位bit串。

5.add\_round\_key(state,key)

功能：16位字符串异或操作。

参数：

state：16位二进制字符串。

key：16位二进制字符串。

返回：16位二进制字符串。

6.byte\_substitution(state)

功能：字节替换，将原字节用作索引值找到对应S盒值替换。

参数：

state：4位16进制字符的字符串，如[0,3,7,11]。

返回：4位16进制字符的字符串。

7.shift\_rows(state)

功能：行移位，16进制的字符串，第二行进行移位。

参数：

state：4位16进制字符的字符串。

返回：4位16进制字符的字符串。

8.mix\_columns(state)

功能：使用的运算方法进行列混淆。

参数：

state：4位16进制字符的字符串。

返回：4位16进制字符的字符串。

9.ascii\_to\_binary(s)和binary\_to\_ascii(b)

功能:字符串与二进制的相互转换。

参数:

s：输入字符串。

b：输入二进制字符串。

返回:转换后的结果。

五、用户界面设计

程序的用户界面采用tkinter库构建，界面简洁明了，包含以下元素：

输入框:用户可以输入字符串或二进制数据。

密钥框:用于输入二进制密钥。

加密按钮:点击后对输入数据进行加密。

解密按钮:点击后对输入数据进行解密。

结果框:显示加密或解密后的结果。

六、安装与运行

安装步骤：

1.安装Python:请确保已安装Python3.x。

2.安装依赖库:

在终端/命令行中执行以下命令安装所需的库：

pipinstalltkinter

运行步骤：

2.在终端/命令行中，进入程序所在目录并执行：

pythonS-DESv3.py

3.GUI界面将打开，用户可以输入明文和密钥进行加密或解密。