目录

[一、概述 1](#_Toc180355731)

[二、环境要求 1](#_Toc180355732)

[三、功能说明 1](#_Toc180355733)

[四、用户界面设计 2](#_Toc180355735)

[五、安装与运行 2](#_Toc180355736)

[六、注意事项 3](#_Toc180355737)

一、概述

该程序是一个基于S-AES算法的工具，支持对二进制数据和二位字符串的加密与解密操作。同时支持将S-AES算法通过双重加密进行扩展，分组长度仍然是16 bits，但密钥长度为32 bits。将S-AES算法通过三重加密进行扩展，使用48bits(K1+K2+K3)的模式进行三重加解密。基于S-AES算法，使用密码分组链(CBC)模式对较长的明文消息进行加密。

二、环境要求

编程语言:Python3.9

库依赖:

tkinter：用于构建图形用户界面(GUI)

操作系统支持：Windows、Linux、macOS

三、功能说明

加密流程：

1.用户在输入框中输入明文（可以是二位字符串或16位二进制数据）。

2.输入16位的二进制密钥。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。

3.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（ASCII字符串或16位二进制数据）。

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。

攻击解密流程：

1. 用户输入明文与密文对。
2. 通过中间相遇攻击的方式找到正确的密钥。
3. 将结果显示在结果框。

四、用户界面设计

程序的用户界面采用tkinter库构建，包含以下元素：

1.S-AES

明文输入框：用户可以输入二进制数据。

密钥输入框：用于输入位的二进制密钥。

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。

2.ASCII

明文输入框：用户可以输入二进制数据。

密钥输入框：用于输入位的二进制密钥。

ASCII加密按钮：点击后对输入数据进行加密。

ASCII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。

3.双重

明文输入框：用户可以输入二进制数据。

密钥输入框：用于输入位的二进制密钥。

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。

4.三重

明文输入框：用户可以输入二进制数据。

密钥输入框：用于输入位的二进制密钥。

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。

1. Attacked

明文输入框：用户可以输入二进制数据。

密文输入框：用于输入位的二进制密钥。

解密按钮：点击后对输入数据进行解密。

密钥对结果框：显示攻击解密后的结果

六、安装与运行

安装步骤：

1.安装Python:请确保已安装Python3.9

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：

pip install tkinter

运行步骤：

2.在终端/命令行中，进入程序所在目录并执行：

python S-AES.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。

七、注意事项

密钥格式要求:密钥必须为相应位数的二进制数，任何非二进制格式输入都会触发错误。

输入数据:支持相应位数的二进制数据或二位字符串作为输入。如果是字符串，加密时会先将其转换为二进制。

加密输出:加密后的结果为ASCII编码的字符串，便于传输和显示。

解密过程:在解密时，ASCII格式的密文会被解码为二进制，再进行解密。