用户指南

1.引言

1.1 编写目的

此次用户手册是面向想要使用 S-AES 算法进行加密的和使用我们的系统的用户。

1.2 项目背景

项目背景 S-AES 算法参考于《密码编码学与网络安全--原理与实践第八版》的附录五。

2. 软件概述

2.1 目标

通过编程实现 S-AES 加、解密程序以及多重加密，CBC 加密模式和中间相遇攻击。

2.2 功能

a.能够实现对于数字和 ASCII 码的加密

b.能够实现多重加密和 CBC 加密模式，三重加密采用的是加密解密加密的加密方式

c.能够对二重加密实施中间相遇攻击解密

3. 运行环境

Windows 系统以及 pycharm、Visual Studio Code 开发工具

4. 使用说明

以下为使用图例：

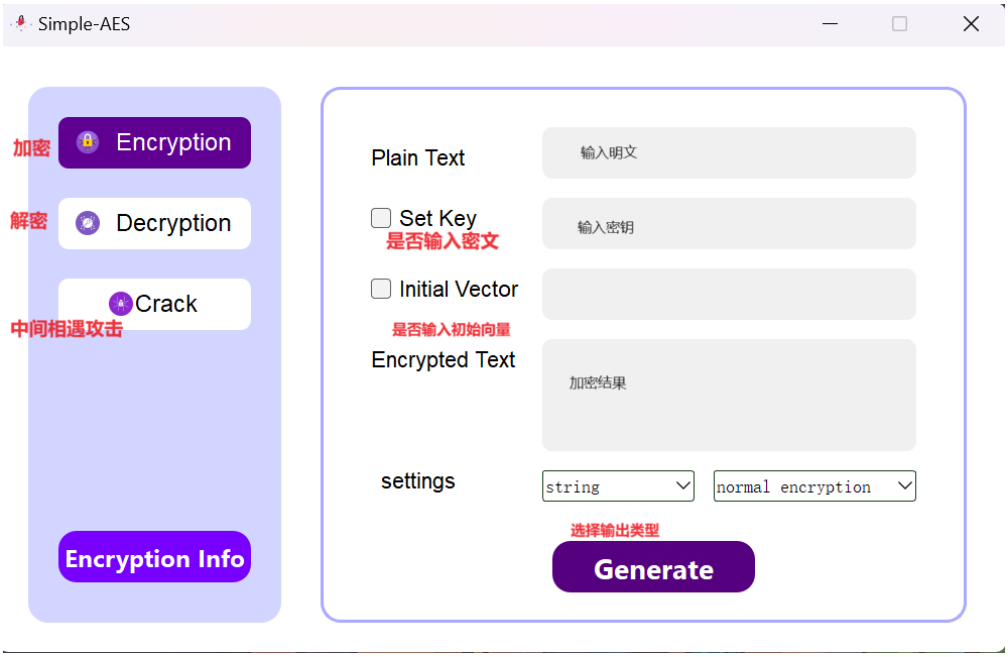

图 1 加解密输入框及输出类型选择

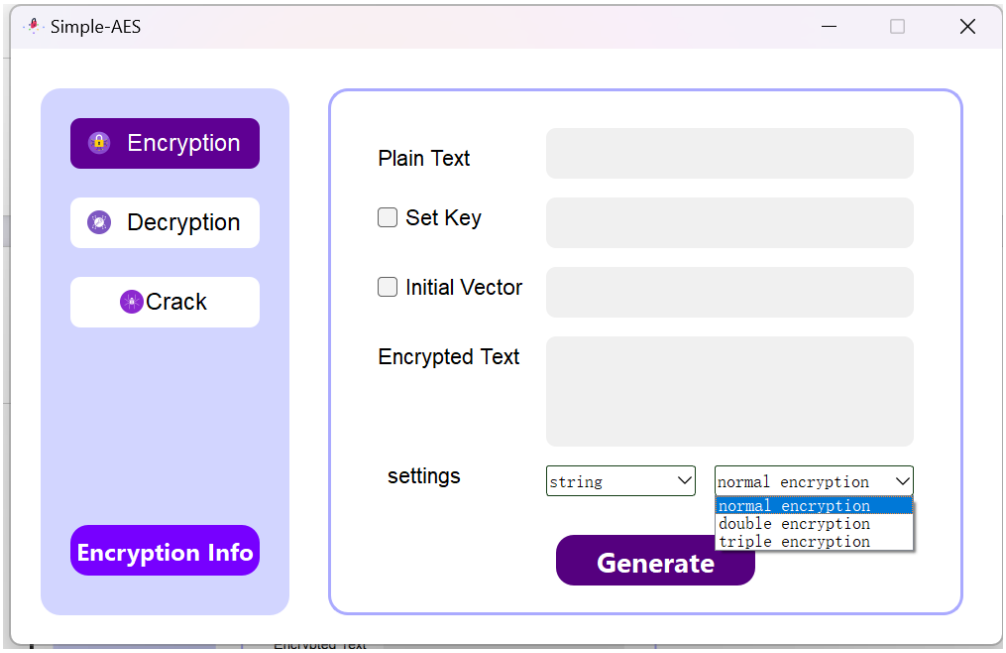

图 2 选择加密类型

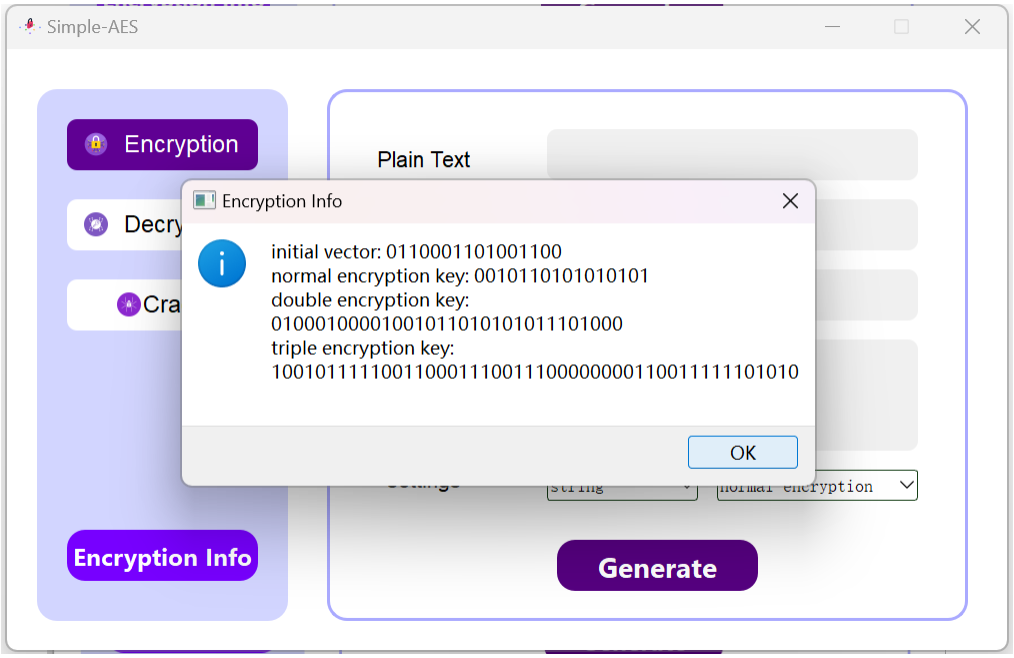

图 3 默认值设置内容

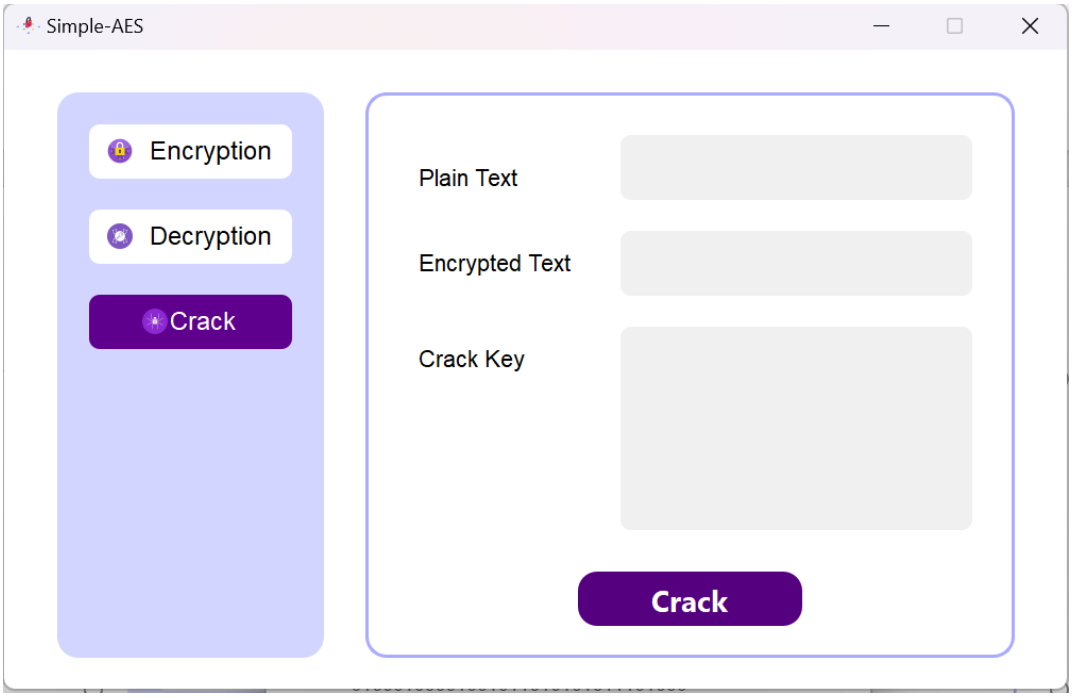

图 4 中间相遇攻击输入界面

4.2 输入

输入支持为字符或者字符两种格式，支持普通加密，双重加密，三重加密，中间相遇攻击，CBC 加密。

4.2.1 数据格式

普通加密：输入密钥和明文为16位以内的整数或者字符

普通解密：输入密钥和密文为16位以内的整数或者字符

二重加密：输入密钥为32位，明文为16位内的整数或者字符

二重解密：输入密钥为32位，密文为16位内的整数或者字符

中间相遇攻击：输入明文密文为16位以内的整数

三重加密：输入密钥为48位和密文为16位内的整数或者字符

三重解密：输入密钥为48位和密文为16位内的整数或者字符

CBC加密：输入多个明文组，输入16bit密钥和初始向量

CBC解密：输入多个密文组，输入16bit密钥和初始向量

4.3 输出

输出根据输入的字符或者字符两种格式进行输出，支持普通解密，双重加密解密，三重加密解密，中间相遇攻击，CBC加密解密。

4.3.1 数据格式

普通加密：输出密文为16位以内的整数或者字符

普通解密：输出明文为16位以内的整数或者字符

二重加密：输出密文为16位以内的整数或者字符

二重解密：输明文为16位以内的整数或者字符

中间相遇攻击：输出密钥16位以内的整数

三重加密：输出密文为16位以内的整数或者字符

三重解密：输出明文为16位以内的整数或者字符

CBC加密：输出多个密文组

CBC解密：输出多个明文组

4.4 出错和恢复

a. 请报告出错信息给管理人员；

b. 用户应采取的措施为重启恢复、再启动尝试