**S-AES加密程序用户指南**

1. **概述**
   1. **系统简介**

本软件为基于S-AES加密算法的加密、解密及破解程序，该软利用S-AES算法实现了16bit明密文的转换、中间相遇攻击猜测密钥以及ASCII码加解密转换。

* 1. **系统运行环境**

该系统运行需要如下的软件环境

|  |  |
| --- | --- |
| 操作系统 | Windows 7（64bit）以上 |
|  |  |

1. **软件功能介绍与使用说明**
   1. **软件的功能**

本软件基于S-AES算法，可以实现16bit明密文的转换、中间相遇攻击猜测密钥以及ASCII码加解密转换。

* 1. **使用说明**

运行对应的程序后，会出现对应的界面。

* + 1. **基本测试界面**

1）运行/S\_AES/src/TEST1/SAESGUI\_1.java，会进入基本测试界面。

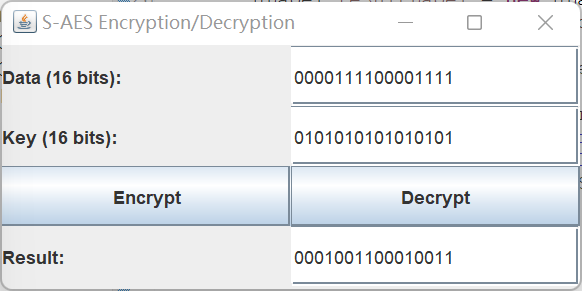


图1 基本测试界面

输入密钥和明/密文，点击encrypt/decrypt即可加/解密。

2）运行/S\_AES/src/TEST1/SAESGUI\_2.java，会进入基本测试界面。

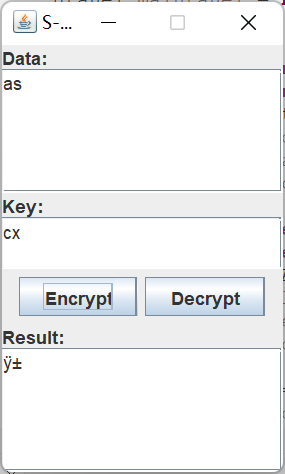


图2 支持符号输入的界面

输入密钥和明/密文，点击encrypt/decrypt即可加/解密。

* + 1. **双重加解密界面**

运行/S\_AES/src/TEST1/DoubleSAESGUI.java，进入双重加解密界面

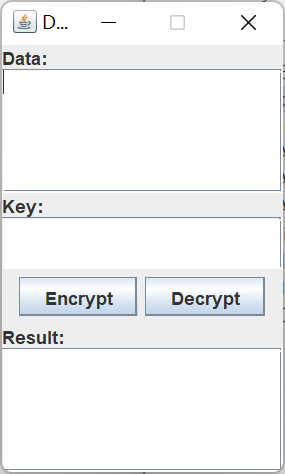


图3 双重加解密界面

输入密钥和明/密文，点击encrypt/decrypt即可加/解密。

* + 1. **中间相遇攻击界面**

运行/S\_AES/src/TEST1/MeetInTheMiddleAttack.java，进入中间相遇攻击界面。

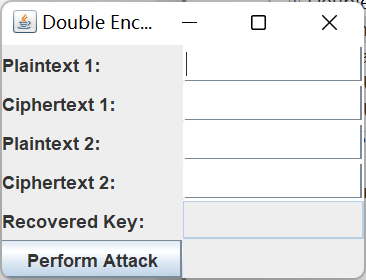


图4 中间相遇攻击界面

输入明文和密文，点击按钮即可开始破解。

* + 1. **三重加解密界面**

运行/S\_AES/src/TEST1/TripleSAESGUI.java，进入三重加解密界面。

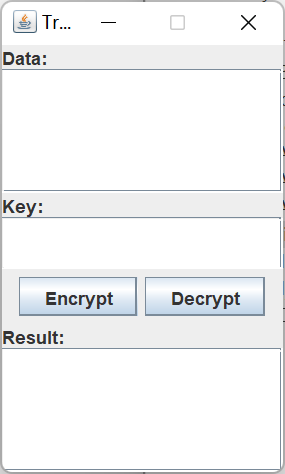


图5 三重加解密界面

输入密钥和明/密文，点击encrypt/decrypt即可加/解密。

* + 1. **工作模式界面**

运行 /S\_AES/src/TEST1/CBCModeEncryptionGUI.java，进入工作模式界面。

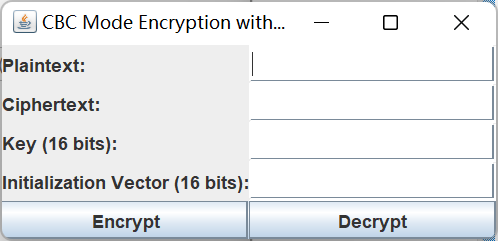


图6 工作模式界面

输入密钥和明/密文，点击encrypt/decrypt即可加/解密。

1. **相关说明**
   1. **开发环境**

软件开发环境如下所示

|  |  |
| --- | --- |
| 操作系统 | Windows 11（64bit） |
| 开发工具 | Eclipse IDE |
| 开发语言 | JAVA |

* 1. **测试环境**

与开发环境相同。