# 用户手册

1.引言  
1.1编写目的

 编写用户手册的目的是充分叙述“S-AES算法实现”软件能实现的功能，以使用户了解软件的使用范围及使用方法。  
1.2参考资料

1. [美]William Stallings.《密码编码学于网络安全—原理与实践(第8版)》[M].陈晶等译.北京：电子工业出版社，2021：附录D：简化AES.  
   2. 软件概述  
   2.1功能

#### 2.1.1基本测试

根据S-AES算法编写和调试程序，提供GUI解密支持用户交互。

#### 2.1.2交叉测试

设有A和B两组位同学(选择相同的密钥K)；则A、B组同学编写的程序对明文P进行加密得到相同的密文C；或者B组同学接收到A组程序加密的密文C，使用B组程序进行解密可得到与A相同的P。

#### 2.1.3扩展功能

考虑到向实用性扩展，加密算法的数据输入可以是ASII编码字符串(分组为2 Bytes)，对应的输出也可以是ACII字符串(很可能是乱码)。

#### 2.1.4多重加密

##### 2.1.4.1 双重加密

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。

##### 2.1.4.2 中间相遇攻击

假设找到了使用相同密钥的明、密文对(一个或多个)，可使用中间相遇攻击的方法找到正确的密钥Key(K1+K2)。

##### 2.1.4.3 三重加密

将S-AES算法使用48bits(K1+K2+K3)的模式进行三重加解密。

#### 2.1.5工作模式

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。  
3. 运行环境  
3.1硬件

内存：最低 2G，建议4G

硬盘：1.5 GB硬盘空间+至少1 GB缓存空间

屏幕：1024x768最小屏幕分辨率  
3.2支持软件

操作系统：Microsoft Windows 10/8/7/Vista/2003/XP (32 or 64 bit)  
软件环境：IntelliJ IDEA Community Edition 2022.3.3

JDK14

4. 使用说明  
4.1输入  
4.1.1数据格式

S\_AES：16bit的数据和16bit的密钥

S\_AES\_AESII：ASII编码字符串(分组为2 Bytes)或16bit的数据和16bit的密钥

S\_AES\_2：16 bit的数据，32 bit的密钥

S\_AES\_pojie：16bit的数据（明文1、明文2、明文3、密文1、密文2、密文3）

S\_AES\_3：48bit的主密钥和16bit的加密信息或16bit的加密信息和解密信息

S\_AES：16bit的主密钥和48bit的加密信息或48bit的加密信息和解密信息  
4.2输出  
4.2.1数据格式

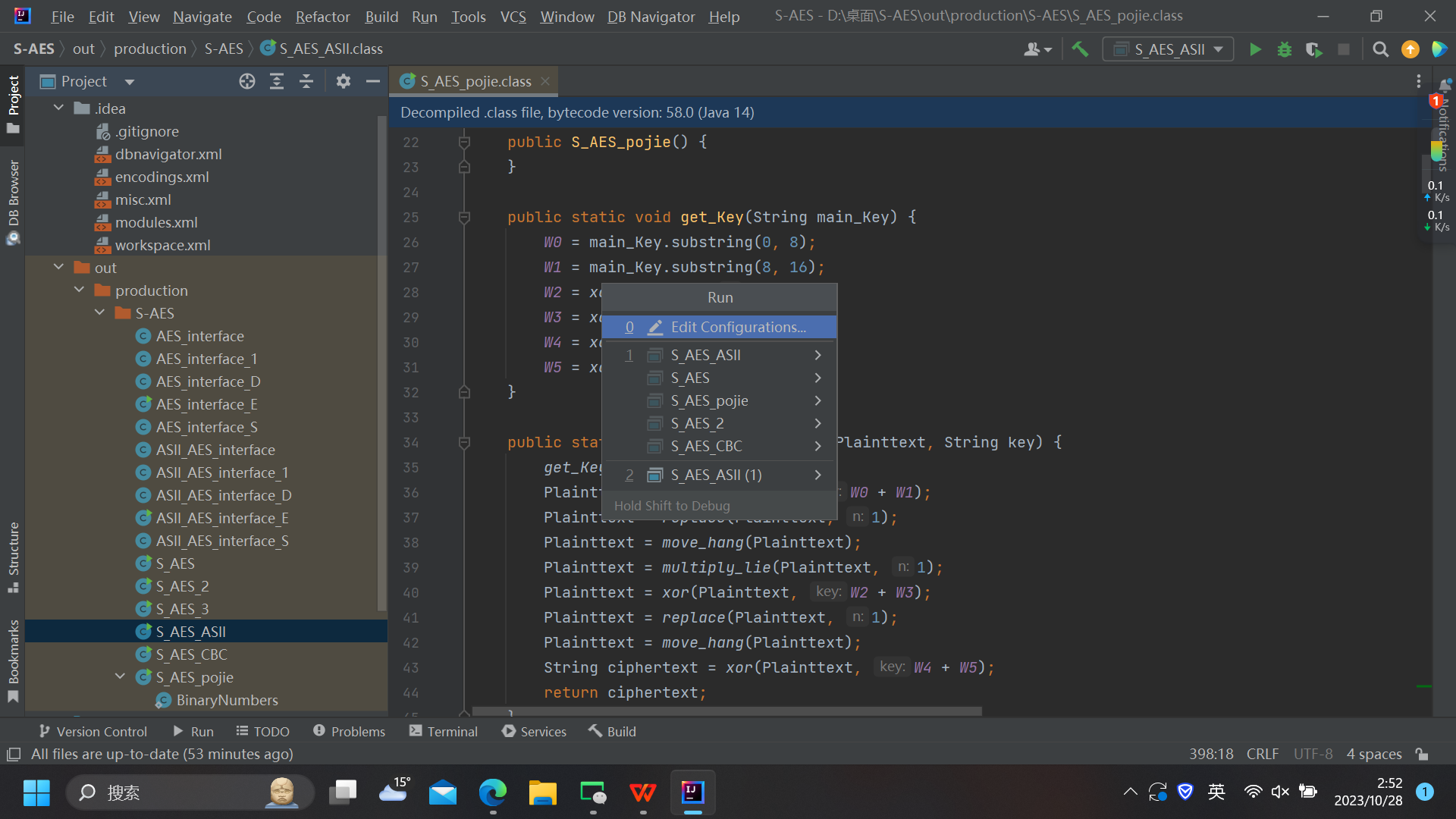
S\_AES：16bit的密文

S\_AES\_AESII：ACII字符串(很可能是乱码)或16bit的密文

S\_AES\_2：16bit的密文

S\_AES\_pojie：多组16bit的密钥K1和K2

S\_AES\_3：16bit的数据（明文或密文）

S\_AES：48bit的数据（明文或密文）  
5. 运行说明  
  
6. 程序文件（或命令文件）和数据文件一览表  
