S-AES开发手册

文件和文件函数结构如下

SAES.java：实现S-AES基本功能的主要函数文件，包含以下数据和函数：

S\_BOX：S盒

INVS\_BOX：逆S盒

G\_Mult：galois乘法盒

encrypt：基本加密框架函数

decrypt：基本解密框架函数

keyExpansion：密钥扩展

reBox：替换盒

roundConstant：轮常数

xorStrings：字符串异或

addRoundKey：加轮密钥

subBytes：长字节替换

shiftRows：行移位

mixColumn：列混淆

invShiftRows：逆行移位

invSubBytes：长字节逆替换

invMixCoiumns：逆列混淆

hexToBinary：16进制转2进制

SAESGUI\_1.java:实现2进制加密

包括gui构建部分：SAES\_GUI（）和主函数

SAESGUI\_2.java:实现字符加密

包括gui构建部分SAESGUI\_2（）、initComponents（），

主函数，

加密函数encrypt，解密函数decrypt

字符转二进制StrToBin，二进制转字符BinToStr

DoubleSAESGUI.java:实现双重加密

包括gui构建部分DoubleSAESGUI（）、initComponents（），

主函数，

加密函数doubleEncrypt，解密函数doubleDecrypt

MeetInTheMiddleAttack.java:实现中间相遇攻击

包括gui构建部分MeetInTheMiddleAttack，

主函数

按钮事件actionPerformed

攻击操作performAttack

TripleSAESGUI.java：实现三重加密

包括gui构建部分DoubleSAESGUI（）、initComponents（），

Main函数

加密函数tripleEncrypt，解密函数tripleDecrypt

CBCModeEncryptionGUI.java:实现cbc模式加解密

包括gui构建部分CBCModeEncryptionGUI（）、initComponents（），

Main函数

按钮事件actionPerformed

加密函数performCBCEncryption，解密函数performCBCDecryption

分块函数splitToBlocks，16进制异或函数xorHex