S-AES开发手册

文件和文件函数结构如下

S\_AES.java：包含S-AES功能、界面设计的主要函数文件，包含以下函数：

S-AES功能函数：

encryptCBC：CBC加密函数

decryptCBC：CBC解密函数

xorStrings16：16位异或函数

splitToBlocks：分块函数

encrypt：单次加密函数

keyExpansion：密钥扩展函数

xorStrings：字符异或函数

roundConstant：轮常数

SubNib：S盒替换函数

subBytes：长字节S盒替换函数

shiftRows：行移位函数

mixColumns：列混淆函数

addRoundKey：密钥加函数

decrypt：单次解密函数

invSubBytes：逆S盒替换函数

invShiftRows：逆行移位函数

invMixColumns：逆列混淆函数

convertStringToBin：字符转换二进制函数

convertBinToString：二进制转换字符函数

hexToBinary：十六进制转换二进制函数

douencrypt：双重加密函数

doudecrypt：双重解密函数

triencrypt：三重加密函数

tridecrypt：三重解密函数

zhongjian：中间碰撞攻击

S\_AES：GUI主体

f1：基本测试界面

f2：主界面

f3：双重加解密界面

f4：中间相遇攻击界面

f5：三重加解密界面

f6：工作模式界面

ActionListener：GUI/算法接口