**开发文档**

1. 简介

该组件包含S-AES加密算法加解密组件及用户界面组件。其中加解密组件结构类似，都是通过实例化加解密构造器并传入参数，之后调用公有函数返回所需的内。用户界面组件用于实现用户操作并显示结果。

1. 设计思路

将明文和密钥均用字节或半字节形式表示，并存在每一位为0或1的int型数组中。再将该字节或半字节的值转化为十进制整数，便于进行之后的异或、S盒置换、列混淆中的乘法等各种运算。最后再将结果转化为16位字符串输出。

1. 安装和配置

首先在命名空间中导入窗口类、AESEncryptCreator类与AESDecryptCreator类，其次在主函数将Window类实例化并调用窗口类的构造函数，接着在窗口的事件监听器中实例化完成对应操作所需要的类，并分别调用AESEncryptCreator类中的encrypt函数和AESDecryptCreator类中的decrypt函数。在运行程序后，向文本框输入符合要求的内容并点击对应的执行按钮，即可在下方的主文本框中显示结果。

1. 接口列表

AESEncryptCreator类：参数为明文与密钥，无返回值，调用其encrypt函数后返回密文

DecryptCreator类：参数为密文和密钥，无返回值，调用其decrypt函数后返回明文

ForcelyAttack类： 无参数，无返回值，调用run函数后返回该明密文对被暴力破解后可能的密钥，调用find函数后返回通过程序运行以来所有输入的明密文对解得的结果。

Window类：无参数无返回值

1. 实例代码
2. AESEncryptCreator aESEncryptCreator= new AESEncryptCreator (plaintext,key);

cipertext = aESEncryptCreator.encrypt();

1. AESDecryptCreator aESDecryptCreator= new AESDecryptCreator (ciphertext,key);

Plaintext = aESDecryptCreator.decrypt();

3. Window window = new Window();

win.setTitle(title);

win.setBounds(x,y,width,height);

1. 类说明

AESEncryptCreator类的构造函数中会调用Init函数，完成对SBox和逆SBox盒参数的初始化，而encrypt函数中会按照加密步骤依次调用执行该操作所对应的函数，最终完成加密。其中mutiply4函数返回列混淆时矩阵对应元素与4 乘法的结果；ByteToHalfByte函数实现将密钥从按字节表示变为按半字节表示，利于后续的密钥扩展，和密钥相加；DtoB函数实现将十进制整数变四位二进制数组，便于之后的S盒置换时寻找变换后的元素，SboxFind函数最终实现S盒置换。

DecryptCreator类的构造函数中会调用Init函数，完成对SBox和逆SBox盒参数的初始化，而decrypt函数中会按照解密步骤依次调用执行该操作所对应的函数，最终完成解密。其中mutiply4函数返回列混淆时矩阵对应元素与4 乘法的结果；ByteToHalfByte函数实现将密钥从按字节表示变为按半字节表示，利于后续的密钥扩展，和密钥相加；DtoB函数实现将十进制整数变四位二进制数组，便于之后的S盒置换时寻找变换后的元素，SboxFind函数最终实现S盒置换。

调用Window类的setTitle函数并将窗口名称作为参数传入，再调用setBounds函数并将窗口位置及大小作为参数传入