**开发文档**

1. 简介

该组件包含S-DES加密算法加解密组件、暴力破解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。而暴力破解组件则是基于加密组件，通过蛮力法枚举所有可能的结果并检验是否符合要求。用户界面组件用于实现用户操作并显示结果。

1. 安装和配置

首先在命名空间中导入窗口类、EncryptCreator类、DecryptCreator类与ForcelyAttack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EncryptCreator类中的encrypt函数、DecryptCreator类中的decrypt函数、ForcelyAttack类中的run和find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. 类介绍

**3.1 S\_DES**

S\_DES 是程序的启动类，采用 main 方法实例化 Window 类并设置窗口标题和边界。

**3.2 Window**

Window 类用于创建图形用户界面（GUI），继承自 JFrame，实现了 ActionListener 接口。主要功能包括：

1.开始和结束程序时显示窗口。

2.提供文本框让用户输入明文、密文和密钥。

3.提供按钮来执行加密、解密和暴力破解操作。

4.显示结果和信息的文本区域。

**3.3 ForcelyAttack**

ForcelyAttack 类实现了暴力破解功能，主要方法包括：

run(String pin, String cin): 接受明文和密文，尝试找到可能的密钥并返回结果。

find(): 查找重复的密钥，如果仅找到一个，则返回最终密钥；如果找到多个，列出所有共享密钥；如果没有找到，返回无法破解的提示。

**3.4 EncryptCreator**

EncryptCreator 类用于加密操作，接受明文和密钥，并通过调用 encrypt 方法来生成密文。主要功能包括：

初始化密钥和明文的转换。

执行加密操作，返回加密结果。

**3.5 DecryptCreator**

DecryptCreator 类用于解密操作，接受密文和密钥，并通过调用 decrypt 方法来恢复明文。主要功能包括：

初始化密钥和密文的转换。

执行解密操作，返回解密结果。

1. 方法介绍

**4.1 Window 类方法**

init(): 初始化 GUI 组件。

actionPerformed(ActionEvent e): 处理按钮点击事件。

methodE(String strP, String strK): 处理加密操作。

methodD(String strC, String strK): 处理解密操作。

methodBF(String strP,String strC): 处理暴力破解操作。

**4.2 ForcelyAttack 类方法**

run(String pin, String cin): 返回可能的密钥。

find(): 查找解密后的密钥。

**4.3 EncryptCreator 类方法**

encrypt(): 返回加密后的密文。

**4.4 DecryptCreator 类方法**

decrypt(): 返回解密后的明文。

1. 实例代码
2. EncryptCreator encryptCreator = new EncryptCreator(plaintext,key);

cipertext = encryptCreator.encrypt();

1. DecryptCreator drcryptCreator = new DecryptCreator(ciphertext,key);

Plaintext = decryptCreator.decrypt();

3 ForcelyAttack forcelyAttack = new ForcelyAttack();

possibleKeys = forcelyAttack.run(plaintext,ciphertext);

actuallyResults = forcelyAttack.find();

4. Window window = new Window();

win.setTitle(title);

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

1. 类说明

EncryptCreator类的构造函数中会调用Init函数，完成对各个置换盒参数的初始化，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。

DecryptCreator类的构造函数中会调用Init函数，完成对各个置换盒参数的初始化，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。

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