一、项目概述

本项目实现了一个简化的AES多重加密程序，支持多种加解密模式，包括单次加密、ASCII加密、二重加密、三重加密等。项目中采用Java语言编写，界面使用Swing实现。

二、项目结构

1. jiami: 包含单次加密算法实现，包括基本的加密和ASCII加密功能。

2. jiemi: 包含单次解密算法实现。

3. double\_encryption: 实现二重加密和解密的功能。

4. triple\_encryption: 实现三重加密和解密的功能。

5. encryption\_model: 主界面，提供用户交互界面。

6. 中间相遇攻击和CBC测试: 完成相关测试。

三、主要组件及接口文档

1. jiami 类

●`String encrypt(String mingwen\_str, String key\_str)`

描述: 使用指定的密钥对明文进行加密。

参数:

- `mingwen\_str`: 明文字符串，必须为16位二进制字符串。

- `key\_str`: 密钥字符串，必须为16位二进制字符串。

返回: 加密后的密文字符串。

●`String asciiToBinary(String input)`

描述: 将ASCII字符串转换为二进制字符串。

参数:

- `input`: 需要转换的ASCII字符串。

返回: 对应的二进制字符串。

●`String binaryToAscii(String binaryInput)`

描述: 将二进制字符串转换为ASCII字符串。

参数:

- `binaryInput`: 需要转换的二进制字符串。

返回: 对应的ASCII字符串。

●`String encrypt\_ascii(String mingwen\_str, String key\_str)`

描述: 将明文进行ASCII编码后加密。

参数:

- `mingwen\_str`: 明文字符串。

- `key\_str`: 密钥字符串。

返回: 加密后的密文字符串。

1. jiemi 类

●String decrypt(String ciphertext\_str, String key\_str)`

描述: 使用指定的密钥对密文进行解密。

参数:

- `ciphertext\_str`: 密文字符串，必须为16位二进制字符串。

- `key\_str`: 密钥字符串，必须为16位二进制字符串。

返回: 解密后的明文字符串。

●`String decrypt\_ascii(String miwen\_str, String key\_str)`

描述: 对ASCII编码的密文进行解密。

参数:

- `miwen\_str`: ASCII编码的密文字符串。

- `key\_str`: 密钥字符串。

返回: 解密后的明文字符串。

1. double\_encryption 类

●`String double\_encrypt(String mingwen\_str, String key\_str)`

描述: 实现二重加密。

参数:

- `mingwen\_str`: 明文字符串。

- `key\_str`: 包含两个16位密钥的字符串（32-bits）。

返回: 二重加密后的密文字符串。

●`String double\_decrypt(String miwen\_str, String key\_str)`

描述: 实现二重解密。

参数:

- `miwen\_str`: 密文字符串。

- `key\_str`: 包含两个16位密钥的字符串（32-bits）。

返回: 解密后的明文字符串。

1. triple\_encryption 类

●`String triple\_encrypt(String mingwen\_str, String key\_str)`

描述: 实现三重加密。

参数:

- `mingwen\_str`: 明文字符串。

- `key\_str`: 包含三个16位密钥的字符串（48-bits）。

返回: 三重加密后的密文字符串。

●`String triple\_decrypt(String miwen\_str, String key\_str)`

描述: 实现三重解密。

参数:

- `miwen\_str`: 密文字符串。

- `key\_str`: 包含三个16位密钥的字符串（32-bits）。

返回: 解密后的明文字符串。

1. encryption\_model 类

●`public static void main(String[] args)`

描述: 主程序入口，启动图形界面。

该方法负责创建并展示主界面，处理用户输入和选择的加解密模式。

1. mid-meet-test 类
2. cbc 类

四、使用说明

1. 启动程序，输入相关数据。

2. 选择加解密模式（单次加密、ASCII加密、二重加密、三重加密和测试等）。

3. 点击“加密或测试”按钮进行加密或测试，点击“解密”按钮进行解密。

4. 加密或解密结果将在结果区域显示。

五、注意事项

明文长度应符合加密算法的要求，必要时进行填充。

六、结论

本项目实现了基本的AES加密解密功能，并提供了良好的用户交互界面，便于用户进行操作。通过简单的接口，方便了各个加密解密算法的扩展和维护。