**S\_AES加密算法测试结果**

1. 基本测试
   1. 加密测试

明文：1001001101101001；密钥：0010110101010101



* 1. 解密测试

密文：0100111110000110；密钥：0010110101010101



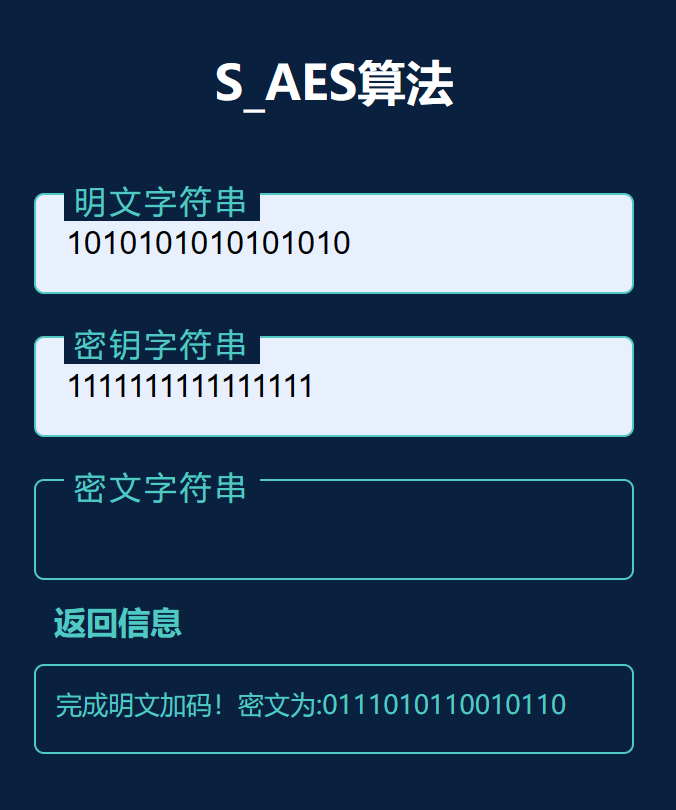
* 1. 结果

明文的加密与密文的解密都能成功实现，并且能够成功对应

1. 交叉测试
   1. 加密交叉测试

明文：1010101010101010；密钥1111111111111111





* 1. 解密交叉测试

密文：0111010110010110；密钥：1111111111111111





* 1. 结果

测试结果良好，能够与其他组获得相同结果

1. 扩展功能
   1. Ascii码加密



* 1. Ascii码解密



* 1. 结果

能够成功加解密ascii码

1. 多重加密
   1. 双重解密
      1. 双重加密

明文：0010110101010101；

密钥：01001111100001100111010110010110



* + 1. 双重解密

密文：1011110011100101；

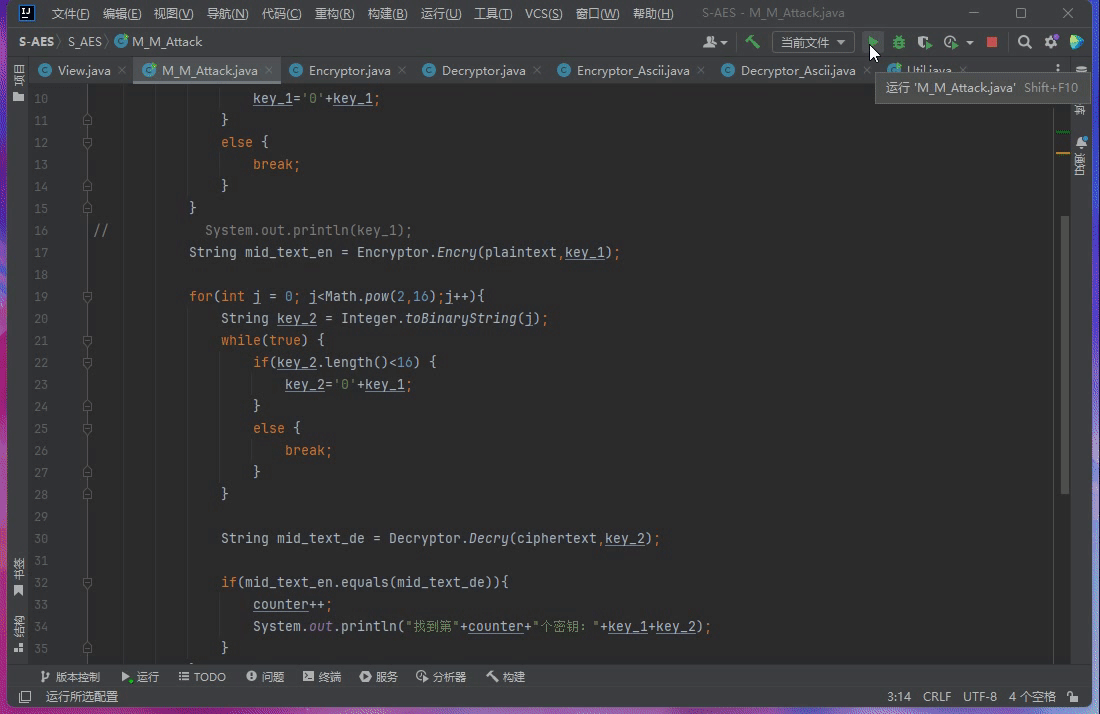
密钥：01001111100001100111010110010110



* + 1. 结果

成功进行双重加解密

* 1. 中间相遇攻击



* 1. 三重加密
     1. 三重加密

明文：0010110101010101；

密钥：

010011111000011001110101100101100010110101010101



* + 1. 三重解密

密文：1001011110110100；

密钥：

010011111000011001110101100101100010110101010101



* + 1. 结果

三重加解密成功

1. 工作模式
2. CBC加解密：

代码输出：

CBC加密过程

Plain\_text\_1:0111010101110000

Plain\_text\_2:0111010101110000

IV:1010101010101010

Cipher\_text\_1:1110101101101000

Cipher\_text\_2:0110111101101001

CBC解密过程

Cipher\_text\_1:1110101101101000

Cipher\_text\_2:0110111101101001

IV:1010101010101010

Plain\_text\_1:0111010101110000

Plain\_text\_2:0111010101110000

其中，令明文分组P1与P2相同，可见经过相同的密钥加密得到的密文分组C1与C2不相同；

1. 篡改密文后解密对比：

篡改前：

CBC解密过程

Cipher\_text\_1:1110101101101000

Cipher\_text\_2:0110111101101001

IV:1010101010101010

Plain\_text\_1:0111010101110000

Plain\_text\_2:0111010101110000

篡改后：

篡改密文后的解密过程

Cipher\_text\_1:0000101101101000

Cipher\_text\_2:0000111101101001

IV:1010101010101010

Plain\_text\_1:0010010101111101

Plain\_text\_2:1101010101110111

当密钥与IV常量相同时，对密文篡改后解密得到的结果与原始结果不同；

