S-DES加密算法测试文档

1. 基本测试
   1. GUI解密交互界面（实现）

图形用户界面, 应用程序, Word

描述已自动生成

* 1. 8bit的数据加解密功能（实现）

使用密钥0111010100对明文10100101加密并解密



基本测试通过

1. 交叉测试

A，B组同时使用密钥1111100000对明文10101010进行加密

A组测试结果：

图形用户界面, 文本, 应用程序

描述已自动生成

B组测试结果：

图形用户界面, 文本, 应用程序

描述已自动生成

交叉测试通过

1. 扩展功能测试
   1. 实用性扩展，数据输入可以是ASII编码字符串(分组为1 Byte)，对应地输出也可以是ACII字符串(很可能是乱码)

使用密钥1000100110对字符串encrypt加密并解密

图形用户界面, 文本, 应用程序

描述已自动生成

扩展功能通过

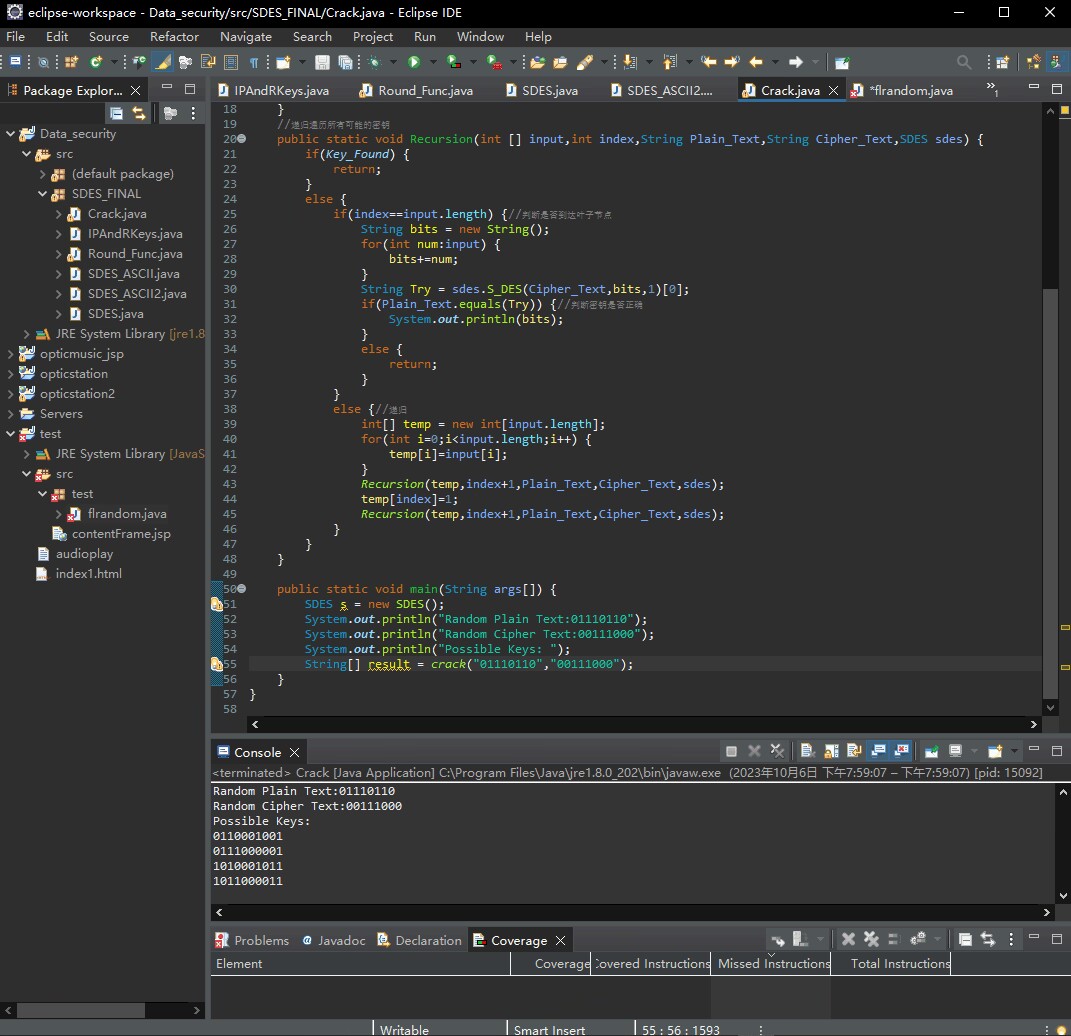
1. 暴力破解测试
   1. 破解过程：

电脑萤幕画面

描述已自动生成

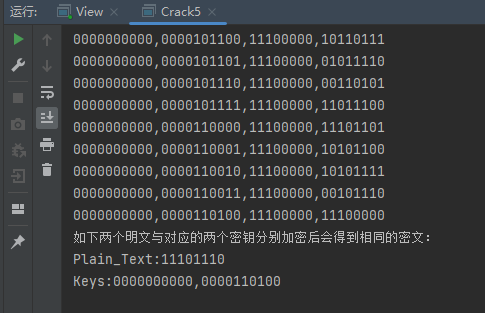
在已知一对明文与密文的情况下，成功破解SDES算法获得第一个密钥用时为8ms。

1. 封闭测试
2. 随机选择的一个明密文对，是不是有不止一个密钥Key



从结果来看，同时获得四个密钥可以使得加密的明文与密文相同

1. 对应明文空间任意给定的明文分组P，是否会出现选择不同的密钥加密得到相同密文Cn的情况？



从结果来看，对于明文11101110，当密钥为0000000000或者0000110100时，加密得到的密文均为11100000。由此得到结论，对于给定的明文分组，可能存在不同的密钥使得加密结果相同