开发手册

1.项目结构

该项目的核心类是 SDES 类，包含了 SDES 加密和解密的所有实现。关键组件包括：

密钥生成 (generateKey)：生成两个子密钥 K1 和 K2。

功能 fK：实现了 Feistel 结构中的轮函数，包括扩展置换、S盒替换和置换操作。

置换和左移操作：包括多个置换表（如 P10、P8 等）和左移操作。

2.关键方法说明

2.1 generateKey(String key, int round)

通过10位密钥生成两个8位子密钥。

参数：

key：10位的二进制字符串密钥。

round：子密钥的生成轮数（1 或 2），分别用于生成 K1 和 K2。

返回值：

返回8位子密钥。

2.2 fk(String input, String key)

Feistel结构中的功能函数，接收左右两部分数据，执行S盒替换、XOR操作等。

参数：

input：8位输入，包含左右两部分（分别为4位）。

key：用于加密/解密的8位子密钥。

返回值：

返回处理后的8位字符串。

2.3 permute(String input, int[] permutation)

根据置换表对输入字符串进行置换。

参数：

input：输入的字符串。

permutation：置换表数组。

返回值：

返回置换后的字符串。

2.4 SBoxes(String input)

S盒操作，将8位输入分成两部分，每4位通过对应的S盒转换为2位输出。

参数：

input：8位输入字符串。

返回值：

4位的S盒替换后的输出。

2.5 leftXOR(String left, String right)

实现两部分二进制字符串的异或（XOR）操作。

参数：

left：左半部分的二进制字符串。

right：右半部分的二进制字符串。

返回值：

返回XOR操作的结果。

2.6 swap(String input)

将左右两部分数据互换。

参数：

input：8位字符串。

返回值：

左右两部分互换后的字符串。

2.7 leftShift(String input, int round)

根据轮次对输入数据进行循环左移操作。

参数：

input：需要左移的字符串。

round：指定第几轮操作。

返回值：

返回左移后的字符串。

3. 接口文档

3.1 外部接口

|  |  |  |  |
| --- | --- | --- | --- |
| 方法名 | 描述 | 参数 | 返回值 |
| encrypt | 加密明文，返回密文 | plaintext：8位明文  key：10位密钥 | 8位密文 |
| decrypt | 解密密文，返回明文 | ciphertext：8位密文  key：10位密钥 | 8位明文 |

3.2 内部接口

|  |  |  |  |
| --- | --- | --- | --- |
| 方法名 | 描述 | 参数 | 返回值 |
| generateKey | 生成8位子密钥 | key：10位密钥  round：1或2 | 8位子密钥 |
| fk | Feistel轮函数 | input：8位输入  key：8位子密钥 | 8位输出 |
| permute | 置换操作 | input：输入字符串  permutation：置换表 | 置换后的字符串 |
| SBoxes | S盒替换操作 | input：8位输入 | 4位输出 |
| leftXOR | 二进制字符串的异或操作 | left：左半部分  right：右半部分 | 异或结果 |
| swap | 左右部分互换 | input：8位输入 | 左右互换后的字符串 |
| leftShift | 循环左移操作 | input：待移位字符串  round：轮次 | 左移后的字符串 |

4. 注意事项

密钥格式：密钥必须为10位二进制字符串，如 "1010000010"。

明文和密文格式：明文和密文都必须为8位二进制字符串，如 "10101010"。

子密钥的生成：通过两个轮次生成两个8位的子密钥，分别用于加密的两轮操作。

5. 测试方法

准备工作：确保输入的明文和密钥符合二进制格式要求。

加密过程：调用 encrypt 方法并查看生成的密文。

解密过程：使用加密得到的密文，调用 decrypt 方法验证解密后的明文与原明文一致