开发人员：姜美辰 王钰涵 黄子芮

手册撰写人员：姜美辰 王钰涵 黄子芮

单位：重庆大学大数据与软件学院

联系方式：[1446915231@qq.com](mailto:2507568524@qq.com)

1.引言

1.1 关于本手册

​ 本手册旨在为S-DES算法实现程序提供全面的开发与使用指南。内容涵盖安装、配置、操作说明、实现原理以及测试等方面，旨在帮助开发者准确掌握该程序的使用方法与技术细节，更好地理解和应用S-DES算法。

1.2 目标与范围

编写S-DES（Simplified Data Encryption Standard）开发手册的主要目的是为了确保开发和使用S-DES算法实现程序的顺利进行，提供清晰的文档和指南，以支持用户、开发团队和维护人员，旨在提高程序的可维护性、可用性和用户体验的同时促进团队内部的知识共享和合作。主要包括以下目标：​

* 提供使用指南：详细说明了如何安装、配置、编译和使用S\_DES算法实现程序，以确保用户能够正确地运行和使用该工具
* 解释算法原理：解释了Simple DES算法的原理和工作流程​
* 提供实现细节：涵盖了程序的实现细节，包括程序结构、数据处理流程、密钥生成和用户界面设计等方面​
* 提供常见问题解答：提供了部分常见问题与故障排除，可以帮助用户解决可能遇到的问题
* 支持维护与更新：可以帮助开发团队理解项目的历史和设计决策，从而更好地管理和维护代码

2.项目概述

2.1项目描述

S\_DES算法实现程序是一个用于演示和理解Simplified Data Encryption Standard（S-DES）算法的工具。它提供了8bit二进制数据（或ASCⅡ编码字符串）和10位密钥的加密、解密和暴力破解密钥的功能，支持用户交互。

2.2功能特性

* 加密解密功能
* 支持8bit二进制数据和ASCⅡ编码字符串输入输出
* 支持10位密钥的输入和随机生成
* 提供对已知明文密文对进行密钥的单线程或多线程暴力破解的功能
* 提供图形用户界面支持

2.3技术栈

* 编程语言：Java

3.安装与配置

3.1环境要求

* 操作系统：Windows 10/11
* Java JDK：11及以上

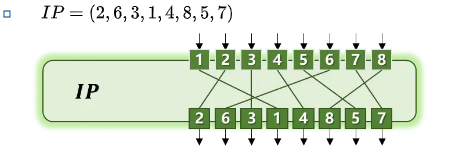
3.2构建与编译

* 编译代码：使用IntelliJ IDEA或其他支持JAVA语言的软件编译运行代码

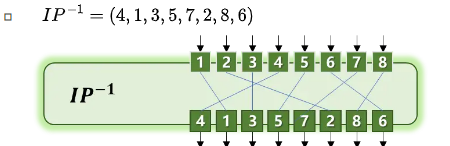
1. 程序结构与主要函数

4.1 函数文件functions.java

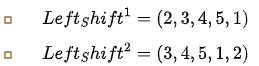
* 置换函数：根据输入的置换表对位串进行重新排列。函数通过遍历置换表中的索引，从输入位串中按顺序提取相应位置的位，形成新的位串。  
   初始置换盒：



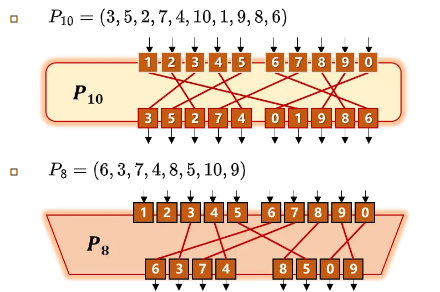
最终置换盒：



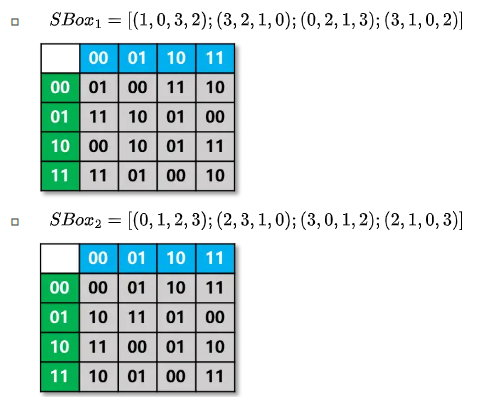
* 左移函数：对密钥进行左移操作。使用不同的左移表分别在第一轮和第二轮生成密钥时对分开的左半部分和右半部分进行不同位数的循环左移。

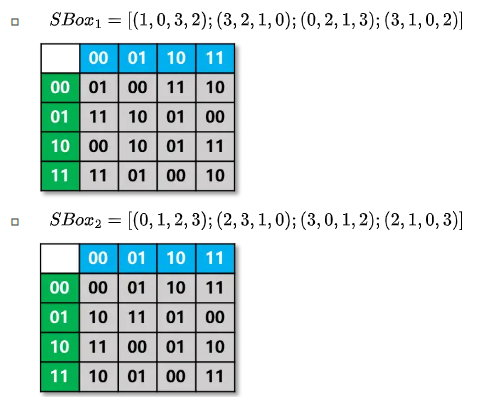


* 生成密钥：通过置换和左移操作生成两个子密钥K1和K2。首先对10位的密钥进行置换，将其分为左右两部分，然后对每部分分别进行左移操作，合并后通过置换生成K1。同理，再进行一次左移操作生成 K2。

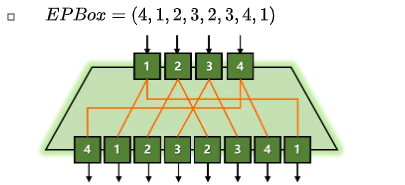


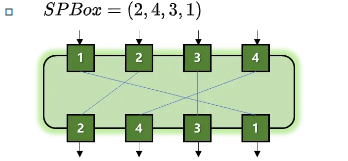
* S盒替换：将输入通过S盒进行替换，返回S盒的输出值。通过将输入的前后两位作为行和列的索引，查找 S盒中的值，并将该值转换为二进制格式。





* 轮函数：首先通过FEPBox对右半部分进行扩展置换，然后与子密钥进行异或操作，再通过S盒替换得到新的位串，最后通过置换SPBox 得到结果。





* 加密函数：先对明文使用初始置换 ()，然后使用轮函数F进行两轮操作，第一轮中，使用第一个子密钥K1对右半部分进行轮函数F操作，并将结果与左半部分进行异或操作，交换左右部分；在第二轮中，使用子密钥K2进行类似的操作。最终结果通过逆置换 () 得到密文。
* 解密函数：首先生成密钥K1和K2，然后以K2和K1的顺序进行两轮轮函数F操作，得到解密后的密文。

4.2 主页面文件MainPage.java

4.2.1 普通加解密

* 整体使用SpringLayout布局，使用add方法将输入框、标签、按钮等组件依次添加到窗口中，并通过JRadioButton提供了两个互斥的加密和解密的操作选项。
* 通过输入框获取10bits的密钥、8bits的明文或密文，也可以通过generateRandomKey()进一步调用functions类的generateKeys方法随机生成密钥，并通过validateInput()方法检验输入格式是否为二进制，长度是否符合要求。
* ActionListener 捕捉到按钮触发的加密或解密事件，并根据用户选择的操作调用并执行functions类中对应的函数。

4.2.2 ASCII码加解密

* 整体使用SpringLayout布局，使用add方法将输入框、标签、按钮等组件依次添加到窗口中，并通过JRadioButton提供了两个互斥的加密和解密的操作选项。
* 通过输入框获取10bits的密钥、1bytes的明文或密文，也可以通过generateRandomKey()方法随机生成密钥，并通过validateInput()方法检验输入格式是否符合要求。
* 加密函数将输入的 ASCII 字符会先转换为8位的二进制形式，并与普通加密相同，使用functions类中加密函数进行加密，将结果的8为二进制密文转化为ASCII字符，解密函数同理。
* ActionListener 捕捉到按钮触发的加密或解密事件，并根据用户选择的操作调用执行对应的函数。

4.2.3 暴力破解

* 整体使用GridBagLayout布局，组织了明文、密文的输入框，结果显示区域，破解时间输出框，以及用于选择线程模式的单选按钮。
* 通过输入框获取8bits的明文与对应的密文，并通过单选按钮让用户选择单线程破解模式或多线程破解模式。单线程破解逐一遍历所有可能的密钥，逐个解密并检查解密结果是否与明文匹配，多线程破解使用了Java的ExecutorService 和线程池来并发执行密钥遍历任务，使得每个线程负责处理一部分密钥空间，提高了破解速度。
* 用户点击执行后，程序遍历所有可能的密钥组合，尝试解密密文，并将解密后的结果与输入的明文进行比对。如果匹配，则认为找到的密钥是可能的正确密钥，并输出到JTextArea。
* 程序通过在操作开始和结束添加时间戳，计算了破解过程所花费的时间，并将结果输出到timeField中。

1. 安装指南

5.1 安装JDK

请确保您的电脑上具有JDK-11或其他兼容版本，若没有的话请进行安装与配置。

5.2 启动系统

请在IntelliJ IDEA或其他支持JAVA语言的软件平台上运行项目。

5.3 导入程序

请下载本程序的压缩包并解压，在您选择的软件平台中打开该项目，检查程序文件没有缺失后可直接运行并使用。