**实验三 Simple DES加密算法实现**

**一、实验目的**

1. 熟练掌握Simple DES（SDES）算法的加密与解密原理，理解其核心思想与操作流程。

2. 通过编程实现SDES算法，熟悉现代密码算法的基本设计思想和实现方法。

**二、实验原理**

Simple DES（SDES）是一种简化的对称加密算法，基于DES算法的核心思想设计而成。SDES的操作基于固定长度的密钥和明文分组，主要包括以下过程：

1. **密钥生成**：

SDES使用一个10位的主密钥，通过置换和分组操作生成两个子密钥*K1*和*K2*。这两个子密钥分别在加密和解密过程中使用。

 主密钥经过P10置换（置换10位顺序），分为两部分。

 两部分分别左移一位，经过 P8置换生成*K1*。

 两部分再次左移两位，经过P8置换生成*K2*。

1. **加密过程**：

SDES的加密过程以8位明文为输入，结合子密钥*K1*和*K2*进行加密。主要步骤包括：

 初始置换（IP）：对明文进行固定的初始置换操作。

 轮函数（F函数）：结合子密钥进行复杂操作，包括扩展置换、S盒替换和P4置换。

 两轮加密：每轮加密使用一个子密钥，通过轮函数和交换操作完成。

 逆初始置换（IP−1）：对最终结果进行逆置换，生成密文。

1. **解密过程**：

解密过程与加密类似，但子密钥的使用顺序相反，即先使用*K2*，再使用*K1*。

**三、实验内容**

1. **密钥生成**：

 输入一个10位的主密钥，生成两个子密钥*K1*和*K2*。

 显示密钥生成过程的中间结果，例如P10、P8和左移操作结果。

1. **加密实现**：

 输入一个8位的明文字符串。

 实现SDES加密算法，完整展示初始置换、两轮加密和逆初始置换的过程。

 输出最终的密文结果。

1. **解密实现**：

 输入生成的密文。

 使用SDES解密算法，验证解密结果与原明文是否一致。

 显示解密过程的中间结果。

1. **功能验证**：

 验证不同密钥对相同明文的加密效果，分析密钥的重要性。

 比较明文中单个位的变化如何影响密文（雪崩效应）。

**四、实验报告要求**

实验报告正文部分格式及内容如下：

实验目的：给出本次实验所涉及并要求掌握的知识点。

实验内容：给出实验的具体内容。

实验代码：给出实验时所实现的核心代码，展示算法的实现过程。

实验结果：给出实验的实际运行结果，并分析实验结果，验证算法的正确性和效率。

实验总结与心得：总结实验过程，分析实验中出现的问题及解决方法，总结实验的心得体会，并提出实验的改进意见。