S-DES 算法用户手册

目录

1. 简介

S-DES（Simplified Data Encryption Standard）是一种简化版的数据加密标准，用于保护数据的机密性。它使用了较小的密钥空间和较少的轮次，适用于教育和演示目的，但不适用于真正的安全通信。本用户手册将介绍如何使用 S-DES 算法进行加密和解密。

2. S-DES 算法概述

（1）S-DES 算法主要包括以下几个部分：

初始置换（Initial Permutation）
轮函数（Round Function）
密钥生成（Key Generation）
轮密钥（Round Keys）
轮次（Rounds）
最终置换（Final Permutation）

（2）分组长度：8-bit

（3）密钥长度：10-bit

（4）算法描述：

加密算法：$C = IP^{-1}(f_{k_2}(SW(f_{k_1}(IP(P)))))$

解密算法：$P = IP^{-1}(f_{k_1}(SW(f_{k_2}(IP(C)))))$

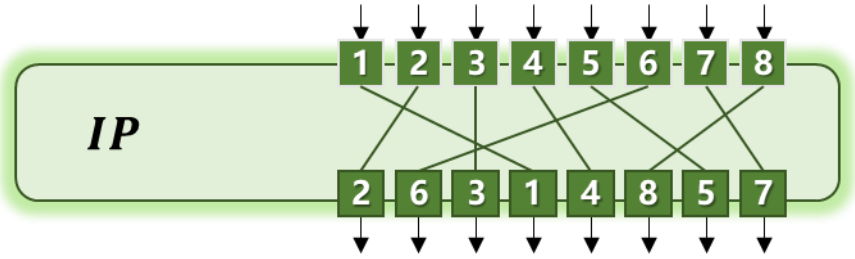
密钥扩展：$k_i = P_8(Shift^i(P_{10}(K))), (i = 1, 2)$

3. 加密和解密流程

3.1 加密流程

（1）输入明文（8 位二进制）。
（2）进行初始置换（Initial Permutation）。

- IP=(2,6,3,1,4,8,5,7)

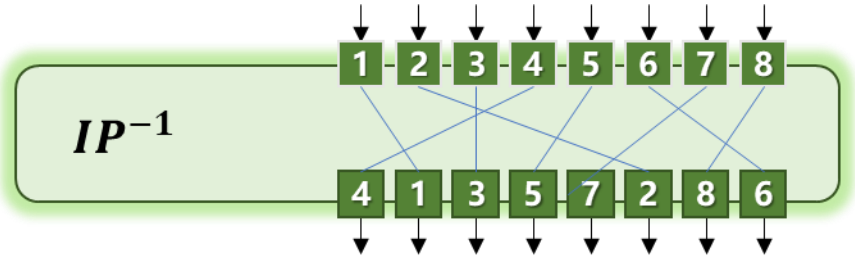


（3）将输入分为左半部分（L0，4 位）和右半部分（R0，4 位）。
（4）使用轮函数和轮密钥执行 2 轮的 Feistel 网络运算。

（5）最后一轮结束后，将左右两部分进行交换，得到 R2L2。

（6）进行最终置换（Final Permutation）。

- IP^{-1}=(4,1,3,5,7,2,8,6)



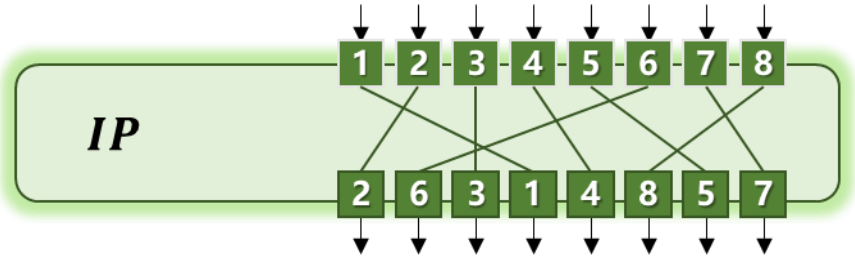
（7）输出密文（8 位二进制）。

3.2 解密流程

（1）输入密文（8 位二进制）。

（2）进行初始置换（Initial Permutation）。

IP=(2,6,3,1,4,8,5,7)



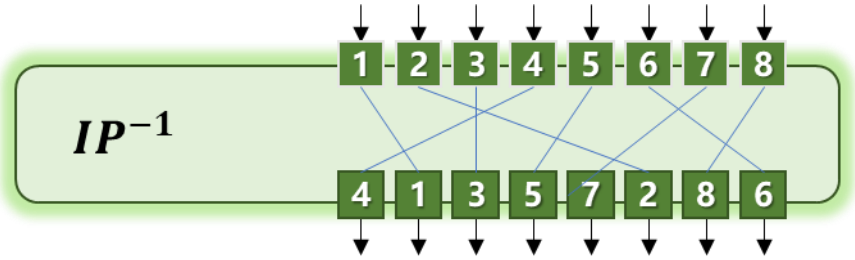
（3）将输入分为左半部分（L0，4 位）和右半部分（R0，4 位）。

（4）使用轮函数和轮密钥执行 2 轮的 Feistel 网络运算，但是轮秘钥的顺序与加密相反。

（5）最后一轮结束后，将左右两部分进行交换，得到 R2L2。

（6）进行最终置换（Final Permutation）。

IP^{-1}=(4,1,3,5,7,2,8,6)

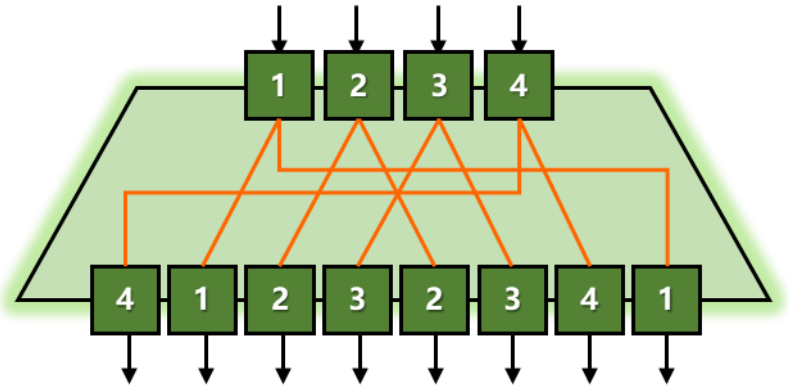


（7）输出明文（8 位二进制）。

3.3 轮函数

（1）对置换后的右半部分进行扩展置换（E-P），将其扩展为 8 位。

- EPBox=(4,1,2,3,2,3,4,1)



（2）将扩展后的结果与轮密钥 K_i 进行异或运算。

（3）再将异或的结果拆分成 2 个 4 位的块。

（4）将这 2 个块分别通过 S 盒代替（$SBox_1$ 和 $SBox_2$）

- $SBox_1$=[(1, 0, 3, 2) ; (3, 2, 1, 0) ; (0, 2, 1, 3) ; (3, 1, 0, 2)]

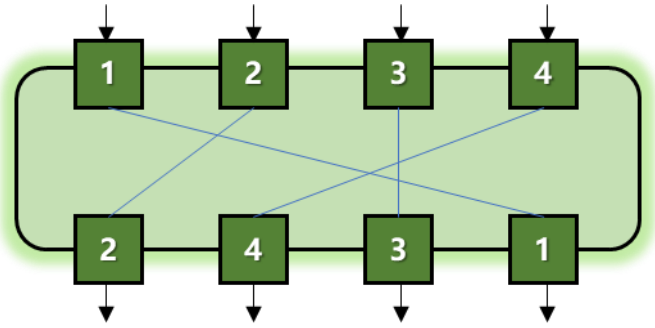
	00	01	10	11
00	01	00	11	10
01	11	10	01	00
10	00	10	01	11
11	11	01	00	10

- $SBox_2$=[(0, 1, 2, 3) ; (2, 3, 1, 0) ; (3, 0, 1, 2) ; (2, 1, 0, 3)]

	00	01	10	11
00	00	01	10	11
01	10	11	01	00
10	11	00	01	10
11	10	01	00	11

（5）然后再通过 SPBox 进行 P4 置换

- SPBox=(2, 4, 3, 1)



（6）最后将 P4 置换后的结果与左半部分（L_{i-1}）进行异或，得到 F 函数输出的结果。

3.4 实用性扩展

加密算法的数据输入扩展为可以是 ASCII 编码字符串(分组为 1 Byte)，对应地输出也可以是 ASCII 字符串。

（1）将明文密文中的 ASCII 编码字符串划分为单个的 ASCII 编码字符

（2）再将其转化为对应的 8bits 的二进制

（3）再作为输入进行如上 3.1/3.2 的加解密步骤，

（4）经过加解密之后再将得到的 8bits 二进制转化为对应的 ASCII 字符串，即完成了对应的 ASCII 加解密的扩展。

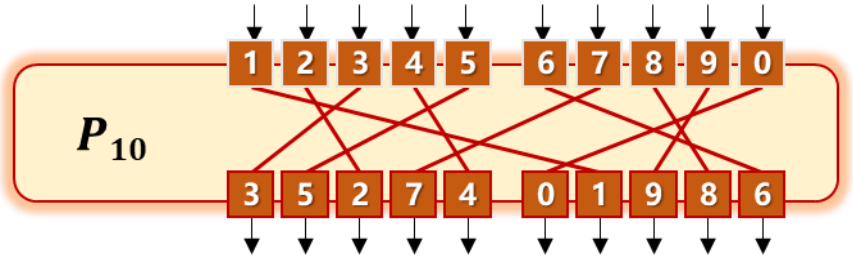
4. 密钥生成

S-DES 算法使用一个 10 位的密钥，密钥生成的过程如下：

（1）输入 10 位密钥。

（2）进行初始置换得到 Permutation-10。

- P_{10}=(3, 5, 2, 7, 4, 10, 1, 9, 8, 6)



（3）将 Permutation-10 分为左半部分（K1，5 位）和右半部分（K2，5 位）。

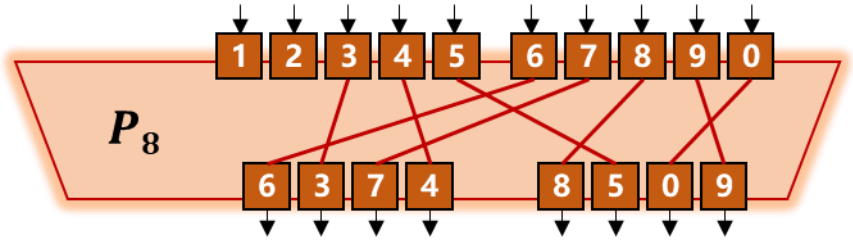
（4）分别对 K1 和 K2 执行循环左移 i 位操作，得到 K1+和 K2+。（i 为第 i 轮）

- $Left\_Shift^1$=(2, 3, 4, 5, 1)
- $Left\_Shift^2$=(3, 4, 5, 1, 2)

（5）合并 K1+和 K2+

（6）然后进行 Permutation-8 置换，得到轮秘钥 1 和轮秘钥 2。

- P_8=(6, 3, 7, 4, 8, 5, 10, 9)



5. 示例

下面是一个 S-DES 加密和解密的示例：

明文：10101010

密钥：1110001010

加密
初始置换得到：00110011
分成 L0=0011 和 R0=0011
K1=11100100
K2=10010010
轮函数运算：
第 1 轮：L1=R0=0011，R1=L0⊕f(R0,K1)=0011⊕0100=0111
第 2 轮：L2=R1=0111，R2=L1⊕f(R1,K2)=0011⊕0100=0111
最终置换得到密文：10101111
解密
密文：10101111
密钥：1110001010
初始置换得到:10101111
分成 L0=R0=0111
K1=10010010
K2=11100100
轮函数运算：
第 1 轮：L1=R0=0111，R1=L0⊕f(R0,K2)=0111⊕0100=0011
第 2 轮：L2=R1=0011，R2=L1⊕f(R1,K1)=0111⊕0100=0011
最终置换得到明文：10101010

6. 安全性考虑

S-DES 算法是一种非常简单的加密算法，不适用于真正的安全通信，因为它的密钥空间相对较小，容易受到暴力破解和差分密码攻击等攻击方式的威胁。因此，在实际应用中，不建议使用 S-DES 算法来保护敏感数据。

7. 结束语

本用户手册提供了关于 S-DES 算法的详细介绍和使用指南。请谨慎使用 S-DES 算法，并在需要更高安全性的情况下考虑使用更强大的加密算法。如果您需要更多信息或有任何问题，请咨询加密专家或安全专业人士。