

《密码学》课程设计实验报告

实验序号：02

实验项目名称：分组密码 DES

学 号		姓 名		专业、班	13 信安
实验地点	计算机学院3楼信息安全实验室	指导教师	王张宜	时间	2016.4.13 8:30-11:30

一、 实验目的及要求

教学目的：

- (1) 掌握分组密码的基本概念；
- (2) 掌握 DES（3DES）密码算法；
- (3) 了解 DES（3DES）密码的安全性；
- (4) 掌握分组密码常用工作模式及其特点；
- (5) 熟悉分组密码的应用。

实验要求：

- (1) 复习掌握实验 1（古典密码）使用的置换、代替、XOR、迭代等技术；
- (2) 比较 DES 中代替技术与古典密码中的联系与区别；
- (3) 理解 S 盒、P 置换等部件的安全性准则；
- (4) 实现 DES 算法的编程与优化。

二、实验设备（环境）及要求

Windows 操作系统，高级语言开发环境

三、实验内容与步骤

1. DES 子密钥扩展算法的实现

输入：64 位密钥

子过程：

- (1) 置换选择 1（教材 图 3-3）
- (2) 循环左移（教材 表 3-1）
- (3) 置换选择 2（教材 图 3-4）

输出：16 个 48 位长的子密钥。

3. DES 加密过程完整实现

- ① 64 位密钥经子密钥产生算法产生出 16 个子密钥： K_1, K_2, \dots, K_{16} ，分别供第一次，第二次，...，第十六次加密迭代使用。
- ② 64 位明文首先经过初始置换 IP (Initial permutation)，将数据打乱重新排列并分成左右两半。左边 32 位构成 L_0 ，右边 32 位构成 R_0 。
- ③ 由加密函数 f 实现子密钥 K_1 对 R_0 的加密，结果为 32 位的数据组 $f(R_0, K_1)$ 。 $f(R_0, K_1)$ 再与 L_0 模 2 相加，又得到一个 32 位的数据组 $L_0 \oplus f(R_0, K_1)$ 。以 $L_0 \oplus f(R_0, K_1)$ 作为第二次加密迭代的 R_1 ，以 R_0 作为第二次加密迭代的 L_1 。至此，第一次加密迭代结束。
- ④ 第二次加密迭代至第十六次加密迭代分别用子密钥 K_2, \dots, K_{16} 进行，其过程与第一次加密迭代相同。
- ⑤ 第十六次加密迭代结束后，产生一个 64 位的数据组。以 R_{16} 作为其左边 32 位，以 L_{16} 作为其右边 32 位，两者合并再经过逆初始置换 IP^{-1} ，将数据重新排列，便得到 64 位密文。至此加密过程全部结束。

综上可将 DES 的加密过程用如下的数学公式描述：

$$\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \\ i = 1, 2, 3, \dots, 16 \end{cases} \quad (3-1)$$

4. DES 解密过程实现

由于 DES 的运算是对和运算，所以解密和加密可共用同一个运算，只是子密钥使用的顺序不同。

把 64 位密文当作明文输入，而且第一次解密迭代使用子密钥 K_{16} ，第二次解密迭代使用子密钥 K_{15}, \dots ，第十六次解密迭代使用子密钥 K_1 ，最后的输出便是 64 位明文。

解密过程可用如下的数学公式描述：

$$\begin{cases} R_{i-1} = L_i \\ L_{i-1} = R_i \oplus f(L_i, K_i) \\ i = 16, 15, 14, \dots, 1 \end{cases} \quad (3-2)$$

5. DES 的 S 盒密码学特性（重点）

通过编程实现或者手工计算，试验证 S 盒的以下准则：

- ① 输出不是输入的线性和仿射函数；
- ② 任意改变输入中的一位，输出至少有两位发生变化；
- ③ 对于任何 S 盒和任何输入 x ， $S(x)$ 和 $S(x \oplus 001100)$ 至少有两位不同，这里 x 是一个 6 位的二进制串；
- ④ 对于任何 S 盒和任何输入 x ，以及 $y, z \in GF(2)$ ， $S(x) \neq S(x \oplus 11yz00)$ ，这里 x 是一个 6 位的二进制串；
- ⑤ 保持输入中的 1 位不变，其余 5 位变化，输出中的 0 和 1 的个数接近相等。

例如，可通过如下步骤验证②、③两条：

设 S 盒的输入为 X，输出为 Y。（X 和 Y 都以二进制表示）

(1) 对于已知输入值 $X_1=110010$ 和 $X_2=100010$ ，分别求出对应的输出值 Y_1 和 Y_2 。

(2) 比较输出值 Y_1 和 Y_2 各位的异同，即按位计算 $Y_1 \oplus Y_2$ 。

根据上面得出的结果试说明 S 盒对于 DES 的安全性影响。

6.扩展思考

(1) Feistel 结构为什么可以保证算法的对合性？

(2) 第 16 轮为什么不做左右互换？

(3) 如果去掉初始置换和逆初始置换，对算法安全性有影响吗？（提示：算法所有的细节都是公开的）

(4) 证明 DES 解密算法是加密算法的逆，即 DES 的对合性。

(5) a. 设 X' 是对 X 按位取反的结果。证明如果明文和密钥都取反，则密文取反。即

$$\begin{aligned}\text{如果 } Y &= E(K, X) \\ \text{那么 } Y' &= E(K', X')\end{aligned}$$

提示：首先证明对任意两个相同长度的串 A 和 B ，有

$$(A \oplus B)' = A' \oplus B。$$

b. 假设对 DES 的穷举攻击需要搜索 2^{56} 个密钥的密钥空间。a 中的结论对此是否有影响？

(6) 证明 DES 中每个子密钥的前 24 位均来自于初始密钥的同一个子集，该子集有 28 位，而后 24 位来自于初始秘密钥的另外 28 位。

四、实验结果与数据处理

1. 程序优化要点

(1) 编程语言及编译器的选择

Java、C、汇编

(2) 程序优化的三个方向

A. 执行速度优化方案：

函数——>宏（消除函数调用和参数传递的时间开销）

循环结构——>顺序结构（消除循环控制变量的额外计算）

预计算——>造表（空间换取时间）

B. （编译后的）可执行程序的大小； C. 源代码的长度

五、分析与讨论

六、教师评语

成绩

签名：

日期：

DES S 盒题库

姓名	S 盒号码	输入 1	输入 2	输入差分	输出 1	输出 2	输出差分
2012302530064 李德卿	S ₁	011001	001001	010000			
2013301200259 刘富聪	S ₄	110100	110000	000100			
2013301650030 鲍家?	S ₂	011100	011101	000001			
2013302530001 郝世荣	S ₅	110010	110110	000100			
2013302530002 唐知行	S ₆	000011	001011	001000			
2013302530003 何瑶杰	S ₈	001000	101000	100000			
2013302530005 王斐	S ₆	000101	100101	100000			
2013302530006 左志恒	S ₅	000011	100011	100000			
2013302530007 汤净	S ₄	100011	110011	010000			
2013302530008 吴疆	S ₈	100001	100101	000100			
2013302530009 程晓曼	S ₂	000110	010110	010000			
2013302530010 常磊	S ₈	000101	000001	000100			
2013302530013 朱荣豪	S ₂	101110	101010	000100			
2013302530014 邓广鑫	S ₈	011011	011111	000100			
2013302530015 李典杰	S ₆	000101	000100	000001			
2013302530016 熊一繁	S ₅	011000	111000	100000			
2013302530017 曾然	S ₄	101111	111111	010000			
2013302530018 汪昕晨	S ₃	011110	010110	001000			
2013302530019 樊成阳	S ₃	111111	111101	000010			
2013302530020 何能斌	S ₄	010110	010100	000010			
2013302530021 龚玉凤	S ₆	011000	011010	000010			
2013302530022 冯文滨	S ₈	101000	101001	000001			
2013302530023 张浩天	S ₃	000110	001110	001000			
2013302530024 肖兴振	S ₂	111111	110111	001000			
2013302530025 方佳圆	S ₇	000011	001011	001000			
2013302530026 彭振峰	S ₆	100100	000100	100000			
2013302530027 黄伟杰	S ₄	010000	110000	100000			
2013302530028 李晓彤	S ₃	001111	001110	000001			
2013302530031 郭航	S ₅	000010	000110	000100			
2013302530032 王淦玉	S ₆	101011	101111	000100			
2013302530033 何勇	S ₁	000100	100100	100000			
2013302530034 陈尧麟	S ₅	001001	011001	010000			
2013302530035 吴继远	S ₈	001110	011110	010000			
2013302530036 涂子璇	S ₁	110100	110101	000001			
2013302530037 伍锡勋	S ₄	000100	100100	100000			
2013302530038 李葛东	S ₁	001101	000101	001000			
2013302530039 陈新	S ₇	011111	111111	100000			

2013302530040 卢鑫宇	S ₁	011100	011110	000010			
2013302530041 杨子涵	S ₈	001000	011000	010000			
2013302530042 张尧	S ₃	111000	101000	010000			
2013302530043 李聪聪	S ₅	101100	100100	001000			
2013302530044 张展齐	S ₈	110010	111010	001000			
2013302530045 吴哲琪	S ₁	000111	100111	100000			
2013302530046 赖登佑	S ₇	110101	110100	000001			
2013302530048 孙雅静	S ₂	000101	010101	010000			
2013302530049 张瑾	S ₂	110111	110101	000010			
2013302530050 蔡逸凡	S ₇	111011	011011	100000			
2013302530051 桑田	S ₅	101011	100011	001000			
2013302530052 廖庆文	S ₇	010110	010010	000100			
2013302530053 牛碧诺	S ₅	011001	010001	001000			
2013302530054 汪灿	S ₆	111001	111011	000010			
2013302530055 邹羽婷	S ₅	001101	000101	001000			
2013302530056 杨靖骁	S ₅	011111	011101	000010			
2013302530057 史鹿曼	S ₁	111110	110110	001000			
2013302530058 蔡婷婷	S ₁	010100	011100	001000			
2013302530059 梅珂嘉	S ₁	100110	100111	000001			
2013302530060 王戈扬	S ₃	110001	110101	000100			
2013302530061 王立洁	S ₄	111101	011101	100000			
2013302530062 李学礼	S ₈	100001	101001	001000			
2013302530063 方济海	S ₄	111010	111011	000001			
2013302530064 丁鸿宇	S ₅	000001	000101	000100			
2013302530065 陈思仪	S ₃	100000	101000	001000			
2013302530066 范坤昊	S ₁	111010	111011	000001			
2013302530067 张月丹	S ₆	010100	000100	010000			
2013302530068 焦杨	S ₄	111100	111000	000100			
2013302530069 白嘉宁	S ₅	010000	010001	000001			
2013308880015 朱近赤	S ₁	010001	010011	000010			
2013308880017 吴双可	S ₈	110110	100110	010000			
2013300110038 叶璐瑶	S ₈	000010	001010	001000			
2013302530070 马巍	S ₂	001110	101110	100000			
2013302530071 高云峰	S ₃	000111	000101	000010			
2013302530072 曾倩	S ₅	101111	100111	001000			
2013302530073 王宇	S ₂	110101	110100	000001			
2013302530074 李帅	S ₇	111111	110111	001000			
2013302530075 董树雨	S ₈	001000	011000	010000			
2013302530076 陆永芳	S ₆	110100	110000	000100			

2013302530077 魏晨	S ₆	010110	000110	010000			
2013302530078 盛祥荣	S ₈	000110	010110	010000			
2013302530079 李文泽	S ₇	110001	010001	100000			
2013302530080 朱莉纬	S ₇	111111	111110	000001			
2013302530081 付欣淙	S ₅	001000	101000	100000			
2013302530082 田雨	S ₇	110100	110101	000001			
2013302530083 程正	S ₂	110011	110010	000001			
2013302530085 宗希	S ₃	100101	100001	000100			
2013302530086 陈越	S ₁	101010	100010	001000			
2013302530087 文一字	S ₃	000100	001100	001000			
2013302530088 赵知非	S ₁	011001	011000	000001			
2013302530089 訾璐	S ₄	101110	100110	001000			
2013302530090 颜珍妮	S ₄	000110	100110	100000			
2013302530091 林秀	S ₃	110011	110001	000010			
2013302530093 张彦君	S ₂	001111	011111	010000			
2013302530095 汪路琪	S ₄	000000	100000	100000			
2013302530096 齐燕	S ₅	101001	101101	000100			
2013302530097 李莹	S ₃	111110	110110	001000			
2013302530098 李志洋	S ₅	101100	101110	000010			
2013302530099 方众	S ₅	100010	100000	000010			
2013302530100 韦业鑫	S ₂	011011	010011	001000			
2013302530101 孟小钰	S ₇	000101	000111	000010			
2013302530102 冯亦龙	S ₅	100111	110111	010000			
2013302530103 刘鑫瑞	S ₈	011000	011010	000010			
2013302530104 李凯伦	S ₇	000111	001111	001000			
2013302530105 陈鑫	S ₃	000000	000001	000001			
2013302530106 陈杰	S ₈	110000	110100	000100			
2013302530107 王思锦	S ₅	100011	110011	010000			
2013302530108 孟诣卓	S ₆	011111	111111	100000			
2013302530109 周晓丽	S ₂	000111	100111	100000			
2013302530110 赵菁	S ₂	111111	101111	010000			
2013302530111 鲁闻达	S ₁	111010	011010	100000			
2013302530112 秦楠楠	S ₄	001111	101111	100000			
2013302530113 朱佳明	S ₇	011111	010111	001000			
2013302530114 李子希	S ₄	001111	011111	010000			
2013302530115 张琴	S ₆	011110	011111	000001			
2013302530116 杨帆	S ₁	001111	001101	000010			
2013302530118 陈雨龙	S ₁	100000	100100	000100			
2013302530119 钱梦洁	S ₈	011110	011100	000010			

2013302530120 全权	S_5	010010	110010	100000			
2013302530121 王天奇	S_1	111001	111000	000001			
2013302530122 郑思言	S_3	001000	101000	100000			
2013302530123 鹿岩	S_2	010011	010010	000001			
2013302530124 崔博武	S_6	111110	111111	000001			
2013302530125 曹?琰	S_1	111110	110110	001000			
2013302530126 张浩?	S_4	101111	101011	000100			
2013302530127 李想	S_6	011111	111111	100000			
2013302530128 王涛	S_5	011101	010101	001000			
2013302530129 程秋平	S_4	101000	101010	000010			
2013302530130 王佩琪	S_5	111100	111000	000100			
2013302530132 徐著	S_6	010011	010001	000010			
2013302530133 董斯山	S_6	110011	110010	000001			
2013302530134 薛圣浩	S_3	010110	010010	000100			
2013302530135 毛涛	S_8	111110	111100	000010			
2013302530136 吴荀	S_4	010110	010111	000001			
2013302530137 张尧	S_8	010011	010010	000001			
2013302530138 朱星滔	S_8	110100	110101	000001			
2013326660031 罗杰	S_5	011110	111110	100000			