

《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	18信安3-4班
实验地点	网安基地新珈楼 C203	指导教师	王张宜	时间	2020.11.24

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
2017301510027 李兆恒	S ₁	011011	011111				
2016301500207 肖亦晓	S ₃	011100	111100				
2016301500241 杨燊铨	S ₄	011110	010110				
2017301500191 吴润泽	S ₆	011110	011100				
2017301500330 陈 磊	S ₈	011010	010010				
2018302060248 张培铭	S ₁	101110	101111				
2018302070001 沈思源	S ₃	101100	101101				
2018302070131 谌金垚	S ₆	000100	100100				
2018302080167 王智超	S ₄	110011	110111				
2018302110381 李江旭	S ₂	100010	110010				
2018302180056 鲁震豪	S ₆	000101	000001				
2018302180057 王晨旭	S ₇	110100	111100				
2018302180059 梅润元	S ₂	101110	111110				
2018302180060 吴逸豪	S ₂	000000	010000				
2018302180062 翁 斌	S ₇	001101	001111				
2018302180063 袁浩天	S ₇	011011	011010				
2018302180064 张展鹏	S ₇	010111	010011				
2018302180068 陈亚楠	S ₆	000100	010100				
2018302180069 郭点点	S ₅	011110	111110				
2018302180070 程昊天	S ₃	110101	100101				
2018302180073 郭梦卓	S ₈	110111	010111				
2018302180077 郑津哲	S ₆	100101	000101				
2018302180079 王怡静	S ₈	100011	100010				
2018302180083 王丹君	S ₃	001010	000010				
2018302180084 倪迩畅	S ₄	011111	011110				
2018302180085 张思远	S ₇	000001	010001				
2018302180086 严诚逸	S ₄	101111	101101				
2018302180087 李宁馨	S ₇	101001	100001				
2018302180088 周渴一	S ₃	111100	111110				
2018302180091 盛威龙	S ₂	111100	101100				
2018302180097 易子嘉	S ₇	000000	000010				
2018302180098 陈映江	S ₇	001011	001111				
2018302180099 郭瑞华	S ₈	101100	101110				
2018302180151 邱振芳	S ₁	100011	100010				
2018302180154 许 可	S ₃	011101	011111				
2018302180160 唐炜钦	S ₈	100101	100100				

2018302180163 李金峰	S ₂	111000	111001				
2018302180166 梅荣新	S ₅	000000	010000				
2018302180168 徐搏鸿	S ₇	011100	011000				
2018302180169 叶嘉昕	S ₅	000010	001010				
2018302180174 汪 毓	S ₁	100010	101010				
2018302180176 蔡文颂	S ₅	111101	111001				
2018302180179 陈思涵	S ₆	100100	101100				
2018302180181 潘昱霏	S ₆	101110	101111				
2018302180183 曾一帆	S ₂	100010	000010				
2018302180184 林玉龙	S ₃	111001	110001				
	S ₇	001101	011101				
	S ₅	001000	101000				
	S ₄	110111	100111				
	S ₈	111101	011101				
	S ₆	101001	001001				
	S ₅	101001	101011				
	S ₄	111101	111001				
	S ₂	010001	000001				
	S ₅	011000	011100				
	S ₆	100000	000000				
	S ₁	111011	101011				
	S ₄	110100	110101				
	S ₇	010100	010110				
	S ₄	111101	011101				
	S ₁	000110	001110				
	S ₄	100001	100000				
	S ₅	100000	100001				
	S ₇	110010	111010				
	S ₈	100101	100001				
	S ₃	111100	101100				
	S ₄	100100	100101				
	S ₂	111001	101001				
	S ₈	000011	000111				
	S ₆	001010	011010				
例 1	S ₄	111111	111101	000010	1110	0010	1100
例 2	S ₂	101110	100110	001000	0001	1011	1010
例 3	S ₁	011010	010010	001000	1001	1010	0011