一、实验项目描述

1． 编写 C 程序实现 DES 加、解密：

(1) 编程实现 基于自己的名字来构造 DES 密钥；

(2) 应用 (1) 获得的密钥将一幅灰度图 (BMP 格式) 进行加、解 密（注意：BMP 位图加密以后要求仍然保留位图的格式，意思只对 BMP 位图的像素值进行加密，格式不变化，可以是彩色图像！也可以采用感兴趣区域，先检测出来 BMP 图像中的重要区域，只对这个区域进行加解密处理！）；

(3) 应用 ECB 和 CBC 两种操作模式分别完成 (2)。

2． 对 DES 进行如下分析：

(1) 分析 DES 的雪崩性质

随机产生两个只有一位不同的明文，如：

00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

10000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

应用 1.(1) 中生密钥分别对其进行加密，给出在加密第 1 轮后的不同位数，第 2 轮后的不同位数， … ，以及第 16 轮后的不同位数。

(2) 分析 DES 的完整性性质：

假定输入的某一位固定不变 (随机确定) ，然后变动其它位 (随机的变动) ，将满足这一条件的 2^8 个明文进行 DES 加密，这些明文的加密密钥均一样 (即 1.(1) 生成的密钥) 。统计输出中每位为 0 或 1 频率。

(3) 差分分析

编写程序求出 DES 上8个 S 盒中任选一个 S 盒的差分分布表；

给出差分值的最大情况及其出现的位置。

(4) 用如下三种 S-盒替换 DES 中的 S-盒，然后应用这一变化后的 DES 去测试上述三种性质。

· 基于某个线性函数计算获得的 S-盒。

· 随机产生的 S-盒。

· 自行设计一种 S-盒(**选做**) 。

二、实验要求

1 ． 自行查阅分 析 BMP 灰度图像文 件的格式；

2 ． 实验中编写的程序需定义清晰、规范的接口 (可采用面向对象的结构，也可采用函数模快化结构) ；

3 ． 实验获得的数据结 果 (如频率统计结果等) 需用图 (Excel 图或 Matlab 图) 或表格(Word 表格)的形式给出。

4. 在自己设计的 S-盒中，如果用到了某些算术变换，自行构造即可，且可以自行做出一些假定和简化(但需在实验报告中显式给出) 。

三、实验 结果 (将来需体现在实验报告中)

本次实验的实验报告中应给出如下实验结果：

1． 实验实现时用到的数据结构；

2． 实验实现时的重要算法；

主要包括：

(1) DES 密钥生成算法；

(2) DES 加、解密算法的概要描述；

(3) 随机明文生成算法；

(4) S-盒的差分分布表计算算法；

(5) 基于某个线性函数计算的 S-盒生成算法；
(6) 随机产生的 S-盒生成算法；
(7) 自行设计一种 S-盒生成算法（**选做**）。
3．各种情况下的计算结果及分析。