课程实践要求

一. 组织形式

1. 单人完成
2. 编程语言及环境：不限
3. 测试环境：pc 机/windows/无.net 等特殊支持；或自己准备
4. 时间节点
   a) 12 月 17 日之前完成
   b) 12 月 18-30 日，课堂汇报（自愿或随机抽查，提前一节课通知）
   c) 12 月 30 日 24:00 前，提交终稿

二. 题目 1：分组密码的轮数对雪崩效应的影响

1. 编写 DES 或 AES 加密/解密算法，算法中迭代轮数可自由设定。

2. 针对不同的迭代轮数，测试并统计当明文改变 1 个比特，或密钥改变 1 个比特时，密文的变化。

a）至少测试 3 种不同的迭代轮数

b）统计时，应当考虑到在不同密钥、不同明文基础上，改变 1 比特时，密文所发生的变化

c）统计结果应以图的形式直观表示出来

三. 题目 2：设计一个检查用户口令的随机性的工具

1. 设计一个口令随机性的评价标准

2. 设计算法实现该测试，输入一个用户设定的口令，输出评价结果。评价结果可以是一个分数，可以是个图，也可以是……，只要能直观地表达出该口令的好坏。

四、提交终稿内容

只提交设计报告，pdf 格式。内容至少包括：

a) 程序执行界面
b) 设计思路和关键技术
c) 实验结果及其分析
d) 创新点（不超过 400 字）

五、评分标准（满分 30）：

a）题目完成情况（每题 10 分）

b）文档质量（对照本科毕业论文要求）（10 分）

c）课堂汇报（最高 5 分，但总分不超过 30）