**实验二 随机数生成方法的设计与验证**

**实验目的：设计一种生成(伪)随机数的算法并验证其随机性。**

**实验设备：**PC机 一台/人

**实验原理：**1.真实的随机数难以产生。

1. 可以用迭代加密、同余运算等方法产生在可行的计 算时间难以预测的伪随机数。
2. 符合要求的(伪)随机数需要经过随机性和不可预测性的检验。

**实验内容及注意事项：**

参考循环加密、DES输出反馈方式、ANSI X.917伪随机数产生器

及Blum Blum Shub(BBS)产生器等方法或采用原创方法，设计一种

可以通过随机性检验的随机数生成算法。

**实验步骤：**

1. 设计随机数生成方法，并输出任意n个随机数。
2. 对设计的随机数生成方法进行随机性和不可预测性检验。
3. 分析结果，得出结论。

**注意：**

1. 不可直接调用已有的随机数生成算法(可以借鉴其思想+进行一定程度的改进)。
2. 随时数的验证数目至少有1000位。
3. 实验结束需要提交纸质实验报告(**关键部分手写**)，其中包括实 验的主要算法(可复制打印) 及电脑中实验结果的截屏。

4. 实验报告中要求有标题，主要的实验过程以及明确的实验结论。