# 实验六-流密码

## 【实验目的及要求】

1、 了解常用的流密码算法，并对其进行实现；

2、 了解常用的伪随机数生成算法，并对其进行实现。

## 【实验步骤】

（一）必做

（1） 编程实现 BBS 伪随机数生成算法；

（2） 编程实现 RC4 流密码算法；

（3） 编程实现梅森旋转算法；

（4） 编程实现 ZUC-128 算法。

**注：**关于（4）的介绍可见附件二。

（二）选做

1、难度：简易

（1）编程实现 ANSI X9.17 伪随机数发生器。

**注：**关于 (1) 的介绍可见附件一。

## 【实验报告】

1、 实验布置两周内，请同学们将实验报告提交至0J平台对应位置，逾期者酌情扣分。

2、 对于每个算法，报告中应含有函数调用关系图、测试样例及运行结果截图，并且记录自己本次实验的收获感想，和对实验不足之处的建议；部分算法需要流程图及伪代码。

3、 报告格式见课程附件二；且该格式仅供参考，同学们可酌情更改。

**4、 请注意：所有实验中，**并不是做困难难度的实验的难度系数一定高于难度为中等；**难度系数由实验自身难度和具体实现情况以及程度决定；**如果只能敷衍完成，同学们不如选择在更简单的选做题上创新。

## 【思考题】

思考 RC4 算法中什么样的密钥属于弱密钥。