现代密码学作业

第五讲

第一节

1 设4级线性移位寄存器的反馈函数为$f(b_4,b_3,b_2,b_1)=b_4\oplus b_1$，初始状态$(b_4b_3b_2b_1)=(1000)$，写出该移位寄存器的输出.

2 设$n=4$，$f(b_4,b_3,b_2,b_1)=b_4\oplus(b_2\ \&\ b_3)\oplus b_1\oplus 1$，初态为$(b_4b_3b_2b_1)=(1011)$，试求此非线性移位寄存器的输出序列及周期.

3 设RC4每次输出的字符为0-3中的数，初始密钥为123，设a-z分别对应0-25，计算“ok”的加解密过程。

4试构造一个输出小m序列的5级LFSR。

第一节

5 （选做）调研GM/T 0005-2012随机性检测规范，对你熟悉的随机数生成函数进行伪随机性测试