**密码学第六次作业**

1.【随机数发生器】

（1）大多数二进制随机数应用场景对随机数序列产生提出了两个不同且未必兼容的要求：和。

（2）真随机数发生器（TRNG）将作为输入以产生真随机序列。可能的随机源有：声音/图像输入，磁盘驱动等。

（3）常见的伪随机数发生器有生成伪随机比特流的伪随机数产生器（PRNG）和生成伪随机值的伪随机函数（PRF）。从接受输入和产生输出的角度，试简述二者的区别。

（4）PRF常用于消息认证。检验位输入位输出的函数是PRF的方式与检验PRNG类似：从位输入位输出的所有函数的集合中均匀选取一个函数，如果对于目前多项式时间的所有方法都无法区分二者（需要固定），那么就认为该函数是PRF。中共包含个函数。

（5）PRNG常用于加密消息。除特意构造的用于产生流密码的算法如曾在局域网中广泛使用的和我国学者自主设计的外，还可利用分组密码工作模式等方式构造。根据教材图8-4(a)，CTR模式的不变，值每次只加1却仍能产生随机序列，是因为所选用的分组密码往往具有良好的。

2.【线性同余算法】产生伪随机数的线性同余算法的表达式一般写作。为了方便讨论，一般取，即。对于参数和的选取，请回答下列问题：

（1）取，试证明的最大周期为4，并列出这时的所有可取值。

（2）有时候，选择的参数即使可提供全周期，也不一定能提供很好的随机性。试比较和提供的随机数序列，并回答：哪一个的随机性更好一些？

（3）【选做】试证明若为素数，给定使算法获得最大周期，则任取满足，有也使得算法获得最大周期。

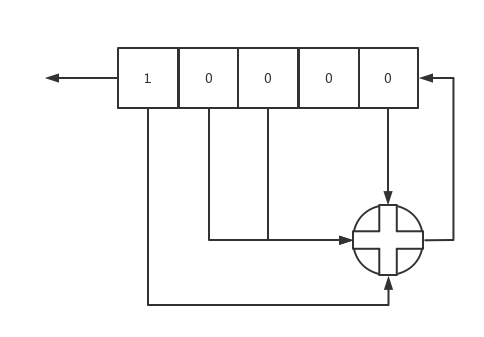
3.【线性反馈移位寄存器】

（1）线性反馈移位寄存器（LFSR）的反馈函数为对移位寄存器的某些位进行，并将结果填充到（选填高位或低位）。若位参与运算，我们记，否则记，则如果移位寄存器中的值为，有，这个递推关系对应到的特征多项式为。

（2）线性反馈移位寄存器（LFSR）中寄存器的个数称为LFSR的，一个级的LFSR最多只能存储种状态，这是由于当LFSR的初态为时，其反馈函数的返回值。

（3）LFSR最多存储的状态数称为其，在数值上等于其反馈函数特征多项式的。若该特征多项式为本原多项式，则其一定能取到最大周期，我们将这样的LFSR所生成的序列称为。

（4）下图所示LFSR的特征多项式为。填写下表，并简单记述从状态31推导状态30的过程。



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 时刻 | 状态 | | | | | 输出 |
| 1级 | 2级 | 3级 | 4级 | 5级 |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |
| 7 |  |  |  |  |  |  |
| ...... | | | | | | |
| 30 |  |  |  |  |  |  |
| 31 | 0 | 0 | 0 | 0 | 1 | 1 |

（5）【选做】从已知明文攻击角度：已知LFSR的级数，给定连续的位明密文，确定其反馈函数。

**注意：**

以上作业请使用**pdf**文档格式提交，于**2022年4月15日（星期六）23:59**之前在OJ系统上提交，并将作业命名为“**学号\_姓名\_密码学第六次作业**”。如“21371234\_张三\_密码学第六次作业”。