流密码 (序列密码) 作业

1. 设一个4级反馈移位寄存器的反馈函数为 $f(a_1, a_2, a_3, a_4) = a_1 \oplus a_4 \oplus 1 \oplus a_2 a_3$, 其初始状态为 $(a_1, a_2, a_3, a_4) = (1, 1, 0, 1)$, 求此非线性反馈移位寄存器的输出序列及周期。
2. 对一个3阶线性反馈移位寄存器 (LFSR), 如果其反馈函数为

$$a_{t+3} = f(a_t, a_{t+1}, a_{t+2}) = a_t + a_{t+2} \bmod 2, \ t = 0, 1, 2, \cdots$$

   (1) 求由初始状态 $(a_0, a_1, a_2) = (0, 0, 1)$ 产生的序列。
   (2) 求由初试状态 $(a_0, a_1, a_2) = (1, 1, 0)$ 产生的序列。
   (3) 这两个序列有什么关系?
3. 对基于线性反馈移位寄存器 (LFSR) 的流密码进行已知明文攻击。假设敌手已经知道明文为1001 0010 0110 1101 1001 0010 0110, 通过窃听通信信道得到相对应的密文为1011 1100 0011 0001 0010 1011 0001。
   (1) 该密钥流产生器所使用的LFSR的阶数是多少?
   (2) 该LFSR的初始状态是什么?
   (3) 该LFSR的反馈函数是什么?
4. 敌手对一个基于 (LFSR) 的流密码执行一个攻击。在这个密码系统中, 为了处理字母, 26个大写字母中的每一个以及数字0, 1, 2, 3, 4, 5分别以如下的规则表示为5比特的向量。

   A↔0 = 00000_2

   .....

   Z ↔25 = 11001_2

   0↔26 = 11010_2

   .....

   5↔31 = 11111_2

   如果敌手已经知道该密码系统的如下特征:

   —该LFSR的阶数为 $m = 6$。

   —每一个明文消息都以WPI开头。

   在通信信道中敌手窃听到如下的消息 (第四位字符为数字0): J5A0EDJ2B

   (1) 该LFSR的初始状态是什么?
   (2) 该LFSR的反馈函数是什么?
   (3) 请解密密文J5A0EDJ2B。
   (4) 上面对该密码系统执行了什么类型的攻击?