流密码 (序列密码) 作业答案

1. 设一个4级反馈移位寄存器的反馈函数为 $f(a_1, a_2, a_3, a_4) = a_1 \oplus a_4 \oplus 1 \oplus a_2a_3$, 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。
   解: 根据反馈函数可知该非线性反馈移位寄存器的输出序列为110111101111…
   该非线性反馈移位寄存器的周期为5。

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) 求由初始状态 $(a_0, a_1, a_2) = (1, 1, 0)$ 产生的序列。
   (3) 这两个序列有什么关系?
   解: (1) 初始状态 $(a_0, a_1, a_2) = (0, 0, 1)$ 产生的序列为0011101001110100…
   (2) 初始状态 $(a_0, a_1, a_2) = (1, 1, 0)$ 产生的序列为1101001110100111101…
   (3) 这两个序列是相互移位的版本。

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?
   解: (1) 由明文和对应的密文可知密钥序列为0010111001011100101110010111, 可知该序列的周期为7, 故该LFSR的阶数为3。
   (2) 该LFSR的初始状态为$(a_1, a_2, a_3) = (0, 0, 1)$。
   (3) 设反馈函数为$a_{t+3} = f(a_t, a_{t+1}, a_{t+2}) = c_3a_t + c_2a_{t+1} + c_1a_{t+2} \bmod 2,\ t \geq 1$,
   由$(a_4, a_5, a_6) = (0, 1, 1)$可得方程组
$$\begin{cases} a_4 \equiv (c_3a_1 + c_2a_2 + c_1a_3) \bmod 2 \\ a_5 \equiv (c_3a_2 + c_2a_3 + c_1a_4) \bmod 2 \\ a_6 \equiv (c_3a_3 + c_2a_4 + c_1a_5) \bmod 2 \end{cases}$$
   得$$\begin{pmatrix} c_3 \\ c_2 \\ c_1 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_3 & a_4 \\ a_3 & a_4 & a_5 \end{pmatrix}^{-1} \begin{pmatrix} a_4 \\ a_5 \\ a_6 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$
   故该LFSR的反馈多项式为$a_{t+3} = a_t + a_{t+1} \bmod 2,\ t \geq 1$。

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?

解: (1) 明文 WPI 对应的数字分别为 22, 15, 8, 根据编码规则可以明文 x = 10110 01111 01000;

同样的, 密文的前三个字符 J5A 对应的编码为 y = 01001 11111 00000;

从而密钥的前三个字符对应的二进制编码为 k = 11111 10000 01000;

故该 LFSR 的初试状态为 (1, 1, 1, 1, 1, 1)。

(2) 设反馈函数为$f(a_t, a_{t+1}, a_{t+2}, a_{t+3}, a_{t+4}, a_{t+5}) = c_6a_t + c_5a_{t+1} + c_4a_{t+2} + c_3a_{t+3} + c_2a_{t+4} + c_1a_{t+5} \bmod 2$, $t \geq 1$, 由密钥序列的前12位状态可得

$$\begin{pmatrix} c_6 \\ c_5 \\ c_4 \\ c_3 \\ c_2 \\ c_1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}^{-1} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

所以其反馈函数为 $f(a_t, a_{t+1}, a_{t+2}, a_{t+3}, a_{t+4}, a_{t+5}) = a_t + a_{t+1} \bmod 2$, $t \geq 1$。

(3) 根据编码规则可以密文 J5A0EDJ2B = 01001 11111 00000 11010 00100 00011 01001 11100 00001;

根据反馈函数可知密钥序列 k = 11111 10000 01000 01100 01010 01111 01000 11100 10010;

密文和密钥序列异或得到明文的二进制形式为 x = 10110 01111 01000 10110 01110 01100 00001 00000 10011, 所以明文为 WPIWOMBAT。

(4) 上面对该密码系统执行了已知明文攻击。