第二章 流密码

一、填空：

1. 分组密码和流密码的根本区别在于\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. *n*-LFSR最大周期是\_\_\_\_\_\_\_\_\_\_

3. 已知一3-FSR，其反馈函数为*f*(*a*1,*a*2,*a*3)=*a*1⊕*a*2*a*3，且当前的状态(*a*3,*a*2,*a*1)=(101)，则其前两个状态分别是\_\_\_\_\_\_\_\_\_\_\_\_，输出序列的周期是\_\_\_\_\_\_\_\_\_\_\_\_

4. n级m序列的异相自相关函数值为\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

5. 序列{*ai*}为m序列的充要条件是\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

6. 已知{*ai*}为m序列，且在该序列中最大0游程为4，则该序列的周期是\_\_\_\_\_\_\_

7. 已知*p*(*x*)=*x*3+*x*+1, 则其产生的非0序列的异相自相关函数值是\_\_\_\_\_\_\_\_

8. n级M序列的周期是\_\_\_\_\_\_\_\_\_\_\_\_

9. 已知一钟控生成器由LFSR1控制LFSR2，极小多项式分别为*f*1(*x*)=1+*x*+*x*3和*f*2(*x*)=1+*x*2+*x*3，则产生序列的周期为\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_，线性复杂度为\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_。

10. 已知LFSR1为一10级m序列，LFSR2为以5级m序列，则构成的钟控序列的周期为\_\_\_\_\_\_,线性复杂度为\_\_\_\_\_\_\_\_\_\_\_\_\_\_

11. n级m序列中长为*i*的1游程有多少\_\_\_\_\_，长为n的1游程有多少\_\_\_\_\_，长为n的0游程有几个\_\_\_

12. 至少知道\_\_\_\_\_\_\_\_\_个连续的密钥流bit可以破译m序列

13. RC4算法的最大密钥长度是\_\_\_\_\_\_\_\_\_\_\_

14. 已知某一n级LFSR其非零状态的状态转移图为一个大圈，则其产生的非0序列的周期是\_\_\_\_\_\_\_\_

15. eSTREAM计划候选算法Grain v1的密钥长度\_\_\_\_\_\_是针对硬件还是软件开发的\_\_\_\_\_\_\_\_\_\_

二、选择：每一项有1个或多个选项是正确的

1. 下面哪些多项式可以作为非退化的5-LFSR的反馈函数(状态转移函数)\_\_\_\_\_

A. 1+*x*+*x*4 B. *x*1⊕*x*2⊕*x*4*x*5 C. 1+*x*+*x*5 D. *x*4+*x*5

2．对于一个n-LFSR，设其序列生成函数为*A*(*x*)，特征多项式*p*(*x*)，全0状态除外，则下面那个要素与其它要素不是一一对应的\_\_\_\_\_\_\_\_

A. *Ф*(*x*)，满足*A*(*x*)=*Ф*(*x*)/*p*(*x*) B. 初始状态 C. *p*(*x*) D. G(*p*(*x*))中的序列

3. 一个LFSR的极小多项式为*p*(*x*)，其所生产的序列也都能由特征多项式为*t*(*x*)的LFSR产生，则gcd(*p*(*x*),*t*(*x*))=\_\_\_\_\_\_\_\_\_

A. *p*(*x*) B. *t*(*x*) C. 1 D. 次数大于1的某个*g*(*x*)，且不等于*p*(*x*)和*t*(*x*)

4. 下面哪个选项不是Golomb对伪随机周期序列提出的随机性公设\_\_\_\_\_\_\_\_\_

A. 在一个周期内0和1个数至多差1 B. 长为*i*的游程占游程总数的1/2*i*

C. 异相自相关函数为常数 D. 任意比特的下一比特不可预测

5. 哪些组合通常作为密钥流产生器的状态转移函数和输出转移函数\_\_\_\_\_\_

A. 线性的*φ*和线性的*ψ* B. 线性的*φ*和非线性的*ψ*

C. 非线性的*φ*和线性的*ψ* D. 非线性的*φ*和非线性的*ψ*

三、判断：(正确的划”√”，错误的划”×”，以下同)

1. 在流密码中，只要被加密的明文长度小于密钥流序列的周期，就可以达到无条件安全了 （ ）

2. 只要LFSR产生的序列的周期足够大，就能够达到计算上安全的，可用于作为密钥流序列 （ ）

3. 流密码中如果第*i*个密钥比特与前*i*-1个明文有关则称为同步流密码 ( )

4. LFSR的初始状态对其产生序列的周期没有任何影响 ( )

5. 序列{*ai*}的生成函数为*A*(*x*)=*Ф*(*x*)/*p*(*x*)，*p*(*x*)的次数大于1，则必有*G*(*p*(*x*))中的一个序列，满足*A*(*x*)=*x*/*p*(*x*) ( )

6. LFSR产生的序列中有一条序列是m序列，则所有非0序列都是m序列（ ）

7. 钟控序列的线性复杂度是指产生钟控序列的密钥流产生器中包含的移位寄存器的总级数 （ ）

8. n级m序列中，存在两个0的n-1游程。 （ ）

9. m序列生成器产生的非0序列之间互相是移位关系。 ( )

10. 任何给定的GF(2)上的密钥流序列都可以用一个LFSR来生成 ( )

四、简答与计算：

1. 试画出二元加法同步流密码的结构.

2. 如图所示的用有限状态自动机描述的密钥流产生器，请问哪部分是驱动部分，哪部分是非线性组合部分？或者说目前普遍采用的密钥流产生器中，哪部分一般采用线性函数，哪部分采用非线性的？



3. 已知一有限状态自动机的状态转移图如图所示，则当初始状态为*s*1，且输入字符序列为*A*1(1)*A*2(1)*A*1(1)*A*3(1)*A*3(1)*A*1(1)时，输出的状态序列和输出符号序列分别是什么？



4. \*在线性反馈移位寄存器LFSR中，LFSR的结构图，特征多项式*p*(*x*)和递推式三者中任给一个，求另外两个，及产生序列的周期。

5. 已知一明文串为00011001，相应的密文串为10111110，密钥流序列由3级m序列生成，试破译之。

6. 使用一个n级m序列加密*t*(*t*>4*n*)比特消息U，如果敌手猜测出U的奇数位都是1，则敌手能否破译出该消息？如何破译？

7. 给出Geffe序列的结构，周期和线性复杂度

8. 给出钟控生成器的结构和周期

五、证明题：

1. 试证定理2-2和定理2-4

2. 试证定理2.6 设{*ai*}∈*G*(*p*(*x*))，{*ai*}为m序列的充要条件是*p*(*x*)为本原多项式

3. n次不可约多项式*p*(*x*)的周期为*r*，试证*A*(*x*)=1/*p*(*x*)的充要条件是0的n－1游程出现在一个周期的最后n-1bit

4. 已知序列{*ai*}∈G(*p*(*x*))，同时也满足{*ai*}∈G(*q*(*x*))，已知*p*(*x*)=*x*7+*x*5+*x*3+*x*2+1, *q*(*x*)= *x*4+*x*3+*x*2+1, 试证{*ai*}为m序列。

5. 试证，对于特征多项式一样，而仅初始条件不同的两个*m*输出序列，对应位相加后所得的新的序列也是m序列，并且这个新的m序列与前两个m序列的特征多项式相同，相互之间满足移位关系

6. 试证，m序列的异相自相关函数为-1/T，T是序列的周期。

六、综合题

1. 一个LFSR的特征多项式*p*(*x*)是不可约多项式，该LFSR的状态转移图由若干个圈组成，试问(1)这些圈中包含的状态数目与该线性反馈移位寄存器的特征多项式的周期有何关系，(2)共有多少个圈，并给出说明。

2. 已知一序列的前10比特为**0010001111**

(1) 试用B-M算法求出产生该序列极小多项式和线性复杂度

(2) 给出产生该序列的LFSR的递推式、结构图和周期

(3) 破译该序列最少需要知道多少连续的密钥流比特

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **n** | **a10** | ***dn*** | ***fn*(*x*)** | ***ln*** | **m** | ***fm*(*x*)** |
| **0** |  |  |  |  |  |  |
| **1** |  |  |  |  |  |  |
| **2** |  |  |  |  |  |  |
| **3** |  |  |  |  |  |  |
| **4** |  |  |  |  |  |  |
| **5** |  |  |  |  |  |  |
| **6** |  |  |  |  |  |  |
| **7** |  |  |  |  |  |  |
| **8** |  |  |  |  |  |  |
| **9** |  |  |  |  |  |  |
| **10** |  |  |  |  |  |  |