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 $f(a_1,a_2,a_3)=a_1\oplus a_2a_3$，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$\{a_i\}$为 m 序列的充要条件是_____

6. 已知$\{a_i\}$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. $x_1\oplus x_2\oplus x_4x_5$　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. $\Phi(x)$，满足 $A(x)=\Phi(x)/p(x)$　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{a_i}的生成函数为 $A(x)=\Phi(x)/p(x)$，$p(x)$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。　（　）

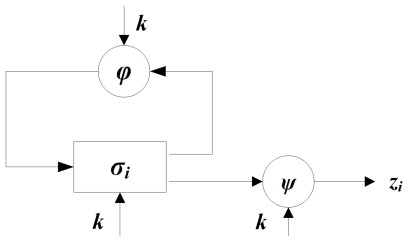
9. m 序列生成器产生的非 0 序列之间互相是移位关系。　(　)

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　(　)

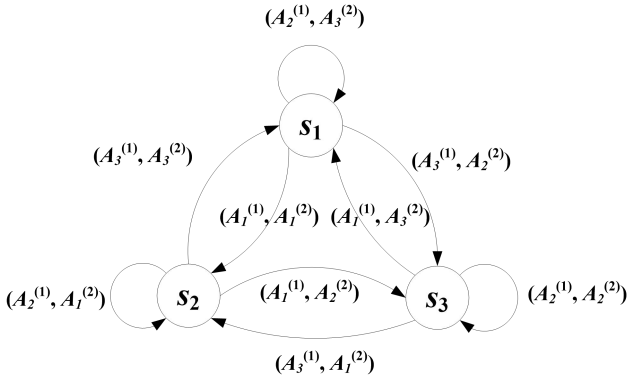
四、简答与计算：

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 $t(t>4n)$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$\{a_i\}\in G(p(x))$，$\{a_i\}$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$\{a_i\}\in G(p(x))$，同时也满足$\{a_i\}\in G(q(x))$，已知 $p(x)=x^7+x^5+x^3+x^2+1$，$q(x)=x^4+x^3+x^2+1$，试证$\{a_i\}$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	$\mathbf{a^{10}}$	d_n	$f_n(x)$	l_n	**m**	$f_m(x)$
0						
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						