一、填空题（本大题共 20 空，每空 1 分，共 20 分）。

1. 常用的五种分组密码工作模式是_____、_____、_____、输出反馈模式和_____。
2. 密码学的两个分支是_____和 _____。其中前者是对信息进行编码以保护信息的一门学问，后者是研究分析破译密码的学问。
3. 在密码学中，我们把没有加密的信息称为_____，加密后的信息称为_____。
4. *n* 级 *m*-序列的周期为_____。
5. AES 算法的分组长度是可变的，可以指定为_____位、_____位和_____位。
6. 最早提出可以证明其是完美安全的密码体制是_____。
7. 分组密码主要采用_____原则和_____原则来抵抗攻击者对其进行统计分析。
8. 密码的强度是破译密码所用算法的计算复杂性来决定的，而算法的计算复杂性由它的_____、_____来度量。
9. 一般地，反馈移位寄存器由两部分组成_____和_____。
10. 设$\{a_i\} \in G(p(x))$，$\{a_i\}$为 *m*-序列的充要条件是_____。

二、单项选择题（共 10 小题，每小题 2 分，共 20 分）。

1. _____算法抵抗频率分析攻击能力最强，而对已知明文攻击最弱。

   A、维吉利亚密码　B、仿射密码　C、希尔密码　D、转轮密码
2. DES 算法采用的是_____网络结构。

   A、Feistel　　B、RSA　　C、SP　　D、OFB
3. 一个密码体制的安全性_____由决定。

   A、加密算法　B、解密算法　C、加密算法和解密算法　D、密钥
4. 如果一个密码体制的加密密钥与解密密钥相同，则称其为_____。

   A、对称密码体制　　B、非对称密码体制

   C、双钥密码体制　　D、公钥密码体制
5. 在 DES 算法中，每个 S 盒的输入长度为 6 位，输出长度为_____位。

   A、2　　B、4　　C、6　　D、8

6. 使用有效资源对一个密码系统进行分析而未能破译，则该密码是_____的。

A、无条件安全　　B、不可破译　　C、计算上安全　　D、不安全

7. SM4 是一种分组密码算法，其分组长度和密钥长度分别为_____。

A、64 位和 128 位　　B、128 位和 128 位

C、128 位和 256 位　　D、256 位和 256 位

8. Golomb 对伪随机周期序列提出了 3 个随机性公设，其中，在序列的一个周期内，长为 i 的游程占游程总数的_____。

A、$\frac{i}{2}$　　B、$\frac{1}{2^i}$　　C、$\frac{1}{2^{i-1}}$　　D、$\frac{1}{2^i-1}$

9. 设 DES 加密算法中的一个 S 盒为：

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

若给定输入为 110100，则该 S 盒的输出为_____。

A、4　　B、12　　C、 9　　D、7

10. 在 AES 加密算法中，当明文分组长度为 192 比特，密钥长度为 128 比特时，其迭代轮数为_____。

A、10　　B、12　　C、14　　D、16

三、简答题（共 3 个小题，每小题 10 分，共 30 分）

1、简述根据密码分析者可获取的信息量不同，密码分析者常采用的几种攻击方式。并说明什么是 Kerckhoffs 原则？

2、设一个 4 级线性反馈移位寄存器(LFSR)的递推关系式为$a_{n+1} = a_n \oplus a_{n-3}$

(1) 给出该 LFSR 特征多项式；

(2) 设初始状态$(a_1,a_2,a_3,a_4)=(1,1,0,1)$，写出输出序列及序列周期。

(3) 列出序列的游程。

3、画图说明分组密码的输出反馈模式，并阐述该模式的特点。

四、计算题（共 3 小题，每小题 10 分，共 30 分）

1、已设英文字母 A，B，C，…，Z 分别编码为 0, 1, 2, …, 25。已知单表仿射加密变换为

$$c=19m+7 \bmod 26$$

其中 m 表示明文，c 表示密文，试对明文 HELP 进行加密和解密 (写出计算过程)。

2、试用 B-M 算法求生成序列 1101011 的最短线性反馈移位寄存器。

3、在 $GF(2)[x]/m(x)$ 中，$m(x)=x^8+x^6+x^5+x+1$，把其中的任意元素 $b_7x^7+b_6x^6+\cdots+b_1x+b_0$ 与 1 字节数据 $\underline{b}=b_7b_6...b_1b_0$（可用两位十六进制数表示）等同看待，试给出相应的计算 $Xtime(\underline{b})$ 的公式，并计算 $0x6b\cdot 0x55$。