该套题是通院董应宽老师在14年给学生的练习题，当前打印店售卖的也是这套题，虽然年份较老，但是确实是能找到的少数来自老师的题目。

第一章 绪论

一、填空：

1. 保密学包括两个重要的分支，分别是_____和_____
2. 信息系统产生安全问题的外因是_____内因是_____
3. 对于信息系统的被动攻击分为哪两类_____和_____
4. 一个黑客在信道上截获一段密文后试图破译该密文，这属于哪类威胁_____，该黑客进一步将密文的几个比特改变后转发给收方，这又属于哪类威胁_____
5. 在信息系统的自然威胁中电磁辐射会导致什么问题_____
6. 攻击者在用户A的主机上种植了盗号木马，并盗取了用户A和用户B的会话密钥，则攻击者使用该密钥以A的身份与B通信的攻击属于哪一类_____
7. 攻击者对某服务器发送大量的虚假链接请求，导致该服务器不能向合法用户提供正常服务，这在主动攻击中属于哪一类_____
8. 人为威胁的主要来源是_____和_____
9. 信息系统安全中包含哪5种安全业务_____
10. 不可否认业务是指哪两种情况_____和_____
11. 为保证通信链接的真实性，通信连接不能被第三方介入，以假冒其中的一方而进行非授权的传输或接受，这需要系统提供哪类安全业务？_____
12. 认证业务可以保证_____的真实性和_____的真实性
13. 在收方双方通信时，对发送的消息经常填充一些随机的报文，而在双方通信完毕保持静默的时候，仍然在信道上随机的传送一些消息，这样可提供哪种安全业务_____
14. 在保密系统中，授权用户可以使用授权密钥通过对密文解密来读取消息，而非授权用户则无法读取，那么该系统提供了哪种安全业务_____
15. 在信息系统的安全模型中，通信双方共享的秘密信息应采用什么方式传递才是安全的？_____
16. 在TCP/IP协议模型中，传输层的两个协议中_____协议是面向连接的，

_____协议是面向无连接的

17. 网络加密的基本方式包括_____和_____

18. 位于两个不同网络中的用户要实现端端安全通信，则可以在 OSI 的哪些层实现_____

19. 一个密码体制由哪些要素组成_____

20. 在保密通信系统中的基尔霍夫原则是指_____

21. 密码系统有哪些攻击类型?

22. 在密码系统的攻击类型当中，攻击者精心挑选了一段消息，并获得了被攻击者加密的相应密文，则他可以进行哪种攻击？_____

23. 在保密通信系统中，有两个安全的信道，一个是用来安全的传送消息的，另一个是用来传送_____

二、选择：每一项有 1 个或多个选项是正确的

1. 下面属被动攻击的有_____

A. 搭线窃听　B. 对文件或程序非法复制

C. 木马　　D. 对资源的非授权使用

2. 将密钥及加密算法封装在硬件芯片中的处理模型属于_____

A. 黑盒密码　B. 白盒密码　C. 灰盒密码　D. 可信计算

3. 敌手通过分析某个用户的通信频率来判断该用户的行为，这种攻击属于_____

A 内容获取　B 重放　C 业务流分析　D 篡改

4. 下列哪些类恶意程序需要主程序：

A 逻辑炸弹，B 特洛伊木马，　C 病毒，　D 蠕虫

5. 下面的安全业务中，那个业务能够保证一个数据不被非授权读取？

A.保密性业务 B.认证性业务 C. 完整性业务 D.不可否认性　E.访问控制

6. 分组密码的差分分析属于_____

A 选择明文攻击，B 选择密文攻击，C 已知明文攻击, D. 惟密文攻击

7. 在选择明文攻击时，除了需要知道加密算法和部分截获的密文以外，还需要知道_____

A. 不需要知道其它信息；　　B. 一些明密文对

C. 自己选择的明文消息及由密钥产生的相应密文；

D. 自己选择的密文消息及相应的被解密的明文。

8. 用户的数据要从一个网络传输到另一个网络，则为了实现端到端加密，最低可以在哪一层加密_____

A. 物理层　B. 链路层 C. 网络层　D. 应用层

9. 下面属于用户的隐私的是____

A 浏览网站的习惯　B 姓名和身份　C 保存的工作单位的机密文档

D. 所在的区域　E 用户是否在某个团队活动区域的附近

10. 下面复杂度属多项式时间复杂度的是

A　$O(1)$　B　$O(2^{3n})$　C $O(2n^3)$　D　$O(n)$

三、判断：(正确的划"√"，错误的划"×"，以下同)

1. 某一野战部队通过网络来传送作战指令，那么只要采用安全的密码算法加密，并且保护好密钥就达到保密要求了　（　）

2. 为了安全的通信，在会话开始前发方随机选择一个安全的密钥通过网络发送给收方，用于对会话的加密　(　)

3. bob 设计了一个密码算法，但该算法仅需至少 3 天时间就可破译，那么 bob 设计的算法达不到计算安全。　（　）

4. 一次一密密码系统是无条件安全的　（　）

5. 安全的杂凑算法都是计算上安全的　（　）

6. 在保密通信系统中接受者是指所有能够接收到密文的人　(　)

7. 惟密文攻击时只需要知道算法和密文就行了，不需要知道其它信息　（　）

8. 实现端到端加密一定不能在链路层进行　(　)

9. 链路加密可以保护位于不同路由器的两个用户之间通信的机密性。　(　)

10. 设计密码算法的目标是使其达到完善保密性　(　)

四、简答与计算：

1. 简述安全威胁的分类。

2. 消息的安全传输模型中安全通道的作用是什么，与普通的信道有何区别？

3. 在网络中要实现两个实体之间安全的消息传输需要考虑哪 4 个要素？
4. 什么是无条件安全和计算安全?
5. 已知敌手截获了 128 比特的密文，该密文是用 128 比特的密钥对 128 比特的明文加密得到的，请问如果敌手有无限大的计算能力，那么能否破译该密文，为什么？
6. 两种网络加密方式的区别是什么？

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。　（　）

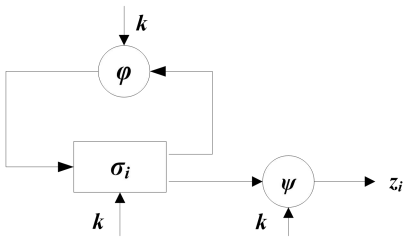
9. m 序列生成器产生的非 0 序列之间互相是移位关系。　(　)

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　(　)

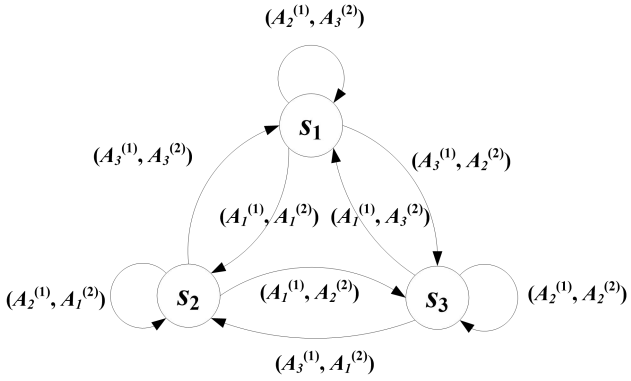
四、简答与计算：

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						

第三章

一、填空：

1. 分组密码中的代换是一种从明文空间到密文空间的一一映射，如果明密文的长度均为 n 比特则不同的可逆代换有多少个_____

2. 从易于实现、提高速度和节省软硬件资源的角度看，加解密算法应具有什么样的特性____

3. 一般情况下，一个 n bit 代换结构其密钥量是_____bit

4. 扩散的目的是_____混淆的目的是_____

5. 就代换和置换两类组件而言，采用_____变换能够达到扩散目的，采用_____变换能实现混淆

6. 乘积密码指顺序地执行两个或多个基本密码系统，如果采用相同的基本密码系统，则这样的乘积密码称为_____，其典型结构是_____

7. 在 Feistel 网络结构的密码中，加解密极其相似，加密和解密算法的唯一不同之处在于_____。

8. DES 的密钥长度_____分组长度_____输出密文长度_____加密轮数_____

9. DES 解密时子密钥的产生有两种方式，对于存储空间受限的环境，采用哪种方式更合适_____

10. DES 的初始置换和扩展置换如表所示，则长为 64 比特的明文分组其第 1、9、17、47 个比特在置换后分别位于哪个位置_____，DES 加密某轮的右 32 比特中第 1、28 比特在经过扩展置换后的位置是_____

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

（a）初始置换

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

（b）扩展置换 E

11. DES 密码的 S 盒定义如下表，如果输入是 101011，则输出是_____

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

12. EDE 的密钥长度_____分组长度_____输出密文长度_____加密轮数_____

13. DES 加密每一轮的子密钥的长度是_____，EDE 加密中一共有____个不同的子密钥

14. 在四种攻击中，差分密码分析属于_____ 线性密码分析属于_____

15. 已知一个 3 轮特征: $\alpha_0, \alpha_1, \alpha_2, \alpha_3$，则 3 轮特征概率为_____

α_0	L_0'= 4008000016	R_0'=0400000016	
α_1	L_1'= 0400000016	R_1'=0000000016	p_1=1/4
α_2	L_2'= 0000000016	R_2'=0400000016	p_2=1
α_3	L_3'= 0400000016	R_3'=4008000016	p_3=1/4

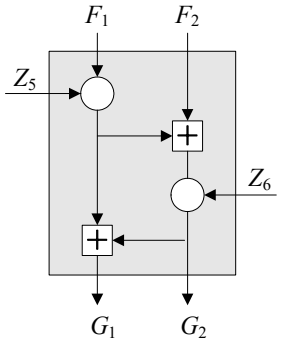
16. CFB-8 的一个比特的密文错误，会导致____个比特的错误传播？在 CFB-12 中，如果一个密文的倒数第二个比特发生了错误，则会导致_____个分组的错误传播。(注意，不包括发生密文错误的分组)

17. 在 IDEA 中，0^2=_____，2^{15}*8=_____，$2^{15}+2^{15}$=_____，2^{15} *2^{15}=_____

18. IDEA 的密钥长度___分组长度____输出密文长度_____加密迭代轮数_____子密钥个数___

19. IDEA 中 8 的乘法逆元是多少_____，加法逆元是多少_____

20. 如图乘加结构，则解密时 Z_5 对应的解密子密钥可表示为_____



MA结构

21. AES 的最小的密钥长度_____分组长度_____输出密文长度_____加密迭代轮数_____

22. 12 轮 AES 算法中，如果密钥长度 k，分组长度为 b，子密钥一共需要_____个比特

23. $(x^4+x+1) \bmod m(x)=x^8+x^4+x^3+x+1$ 的逆元是_____

24. AES 的状态在明文输入时第 n 个字节放在状态阵列的位置(i,j)上，则第 13 个字节所对应的状态阵列的位置(i,j)=_____

二、选择：每一项有 1 个或多个选项是正确的

1. 从古典密码的角度看，分组密码属于_____

A. 单表代换密码　B. 多表代换密码　C. 单表置换密码　D. 多表置换密码

2. 分组密码可以用于实现下述那些功能_____

A. 加密，　B. 产生伪随机数，　C. 产生密钥流序列　D. 产生 MAC　E. 数字签名

3. 实现扩散的方法是_____

A. 置换　B. 代换　C. 先置换再代换　D. 先代换再置换

4. 下面这些密码算法中，属于 Feistel 结构密码的有_____

A. AES　　B. IDEA　　C. RSA　　D. DES

5. 利用 DES 的取反特性进行的攻击，应属于哪一类密码攻击_____

A. 惟密文攻击　B. 已知明文攻击　C. 选择明文攻击　D. 选择密文攻击

6. 下列算法中，哪一个是现行国际分组加密标准_____

A. DES　B. RSA　C.IDEA　D.AES

7. 下列运行模式中，哪一种模式的错误传播最小？_____哪一种模式可将分组密码转换为自同步流密码_____，哪些模式可实现随机读取_____

A. ECB　B.CBC　C.CFB　D.OFB　E. CTR

8. 如上题，AES 状态阵列的第(2,5)位置上的元素对应明文的第_____个字节

A. 22　B. 7　C. 13　D. 10

三、判断：(正确的划"√"，错误的划"×"，以下同)

1. 分组密码用于加密时，其明文和对应密文的长度可以相同，也可以不同。　(　)

2. CFB 运行模式下的分组密码可以等效为一个同步流密码。　(　)

3. OFB 只需要 DES 的加密算法。　(　)

4. 在 AES 的解密算法中，所有密钥都要先进行逆向列混合，再进行轮密钥加　(　)

5. DES 算法是一种多轮迭代密码　(　)

四、简答与计算：

1. 分组密码在设计时，为什么会要求其加解密算法相似？

2. 试描述 Feistel 密码的结构

3.在 Feistel 密码中，如果第 i 轮的输入是 L_{i-1}，R_{i-1}，输出是 L_i，R_i，试用输出表示输入，其中轮函数设为 $F(R_{i-1}, K_i)$

4. 试画出 S 盒的结构，并说明其工作原理，即如何由输入得到输出

5. 已知 DES 满足取反特性，试说明在对 DES 进行选择明文攻击时工作量会减少一半。

6. 一个用单重 DES 加密的密文 C，密钥为 k，如何用 EDE 算法解密？

7. 两个密钥的二重 DES 的中途相遇攻击是如何实现的？

8. 三个密钥的三重 DES 算法结构，如何用该算法解密一重 DES 产生的密文

9. 什么是 ECB 模式，为什么不适合于加密长消息，如果明文长度不是分组的整数倍怎么办?

10. 画出 CBC 模式的逻辑图，并回答其初始向量 IV 为什么要保密?

11. 试分析一下 CBC、CFB、OFB 运行模式的错误传播情况。

12. CFB 和 OFB 哪一个适合有扰信道，为什么？试画出逻辑图

13. 什么是 CTR 模式？为什么可以并行计算和对密文进行随机存取？

14. Rijndael 算法是建立在 GF(2^8)有限域上的，且模多项式为 $m(x)=x^8+x^4+x^3+x+1$，试计算

$(x^6+x^2+x+1)\times(x^4+x+1) \bmod m(x)$，该计算用 x 乘来表示时，试给出计算过程。

15. 系数在 GF(2^8) 的 mod x^4+1 的乘法 $a(x)$ = '01'x^2, $c(x)$='03'x^3+'01'x^2+'01'x+'02' 试计算 $a(x)\times c(x)$。

16. CFB-64 和 CBC 的区别是什么？

17. 某攻击者要破译所截获的某 n 个密文分组，采用穷搜索攻击，试分析以下两种攻击的区别

1) 假设攻击者控制加密机，搜索所有可能的明文并加密，看是否等于截获的密文，从而实现对密文的破译。

2) 已知一些明密文对，搜索所有可能的密钥，然后再用该密钥对密文解密。

18. 以 DES 为例，试分析迭代密码中基本函数的子密钥相同和不同的区别。

五、证明题：

1. 已知 DES 满足取反特性，试证 EDE、3 个密钥的 3DES 都具有取反特性。

2. 试说明 AES 的轮结构中行移位和字节代换的顺序可以互换。

3. 试证明：在 Feistel 结构密码中解密过程第 1 轮的输出等于加密过程最后一轮输入左右两半交换值。

六、综合题

某人要做一个密码芯片，该芯片要实现以下功能：对数据流加密、MAC 认证、产生随机数。为节省硬件资源，如果仅有一重及多重 DES 可用，试分析分别采用何种模式、标准或结构能够实现这些功能

第四章

一、填空：

1. RSA 密码算法的安全性是基于_____困难性构建的

2. A 给 B 发送消息时用公钥加密算法进行加密，则加密时使用的密钥是公开钥还是秘密钥？_____该密钥由谁产生？_____

3. A 的密钥对为 PK_A,SK_A, B 的密钥对为 PK_B,SK_B，公钥密码算法记为 $f(\ )$，若 A 给 B 发送一个既加密又认证的消息 m，则密文 C 可表示为_____

4. 蒙哥马利模乘是为了避免求模运算中的_____运算而提出的

5. RSA 中最耗时运算是_____

6. 在 RSA 算法中为保证算法的安全性，对两个大素数 p，q 有什么要求_____和_____

7. 已知一超递增背包向量 A=(1, 3, 5, 11, 21, 44, 87, 175, 349, 701)，现在背包容积为 s＝452，试求该背包的解_____

8. ECC 算法的安全性是基于_____困难问题构建的。

9. 椭圆曲线 $y^2=x^3+x$-2 mod 5 的判别式是_____？

10. 160 比特的 ECC 的安全性相当于_____比特 RSA 算法的安全性；211 比特相当于_____比特 RSA 算法的安全性

二、选择：每一项有 1 个或多个选项是正确的

1. 用户 A 向 B 传输消息 m，采用公钥密码来实现 m 的保密性和认证性，则下列正确的是_____

A 先用 A 的私钥签名，再用 B 的公钥加密　　B 先用 B 的公钥签名，再用 A 的私钥加密

C. 先用 A 的私钥签名，再用 A 的公钥加密　　D 先用 A 的私钥加密，再用 B 的公钥签名

2. A 给 B 发送消息，并对消息进行认证，记 A 的密钥对为(PK_A, SK_A)，B 的密钥对为(PK_B, SK_B)，则 A 用密钥_____对消息加密，B 用密钥_____对消息解密，即可完成。

A. PK_B, SK_B　　B. PK_A, SK_A　　C. SK_B, PK_B　　D. SK_A, PK_A

3. 对公钥密码的可能字攻击属于_____

A 惟密文攻击　B 已知明文攻击　C 选择明文攻击　D 选择密文攻击

4. 基于有限域上离散对数困难性问题构建的体制有_____

A. RSA　B. Rabin　C. ECC　D. NTRU　E. 背包　F. ElGamal 体制

5. 椭圆曲线群 $E_3(1, 2)$上有多少个元素_____　A. 1 个　B. 2 个　C. 3 个　D. 4 个

6. 下列算法中可实现抗抵赖功能的是_____

A. AES　B. MD5　C. ElGamal 签名　D. DH 密钥交换协议

7. 用数字签名算法对所要传送的消息进行签名，并连同消息一起传送给接收方，这种做法可实现

——

A. 对消息来源的认证 B.消息完整性认证 C. 发方身份认证 D. 消息的保密性

8. 公钥密码算法的安全性最强的是下面哪一个

A. 适应性选择密文攻击下不可区分安全(IND-CCA2)

B. 非适应性选择密文攻击下不可区分安全(IND-CCA2)

C. 语义安全的

D. 单向性

三、判断：(正确的划"√"，错误的划"×"，以下同)

1. Millar-Rabin 素性检验算法是一种确定性检验算法 ( )

2. 公钥密码算法也是一种分组加密算法 ( )

3. 对于一个安全的公钥密码算法而言，已知公钥密码算法和加密密钥，求解密密钥在计算上是不可行的 ( )

4. 现有的典型公钥密码算法都是计算上安全的 ( )

5. 可以证明 Rabin 密码体制的安全性与大数分解困难问题等价 ( )

6. 椭圆曲线上的无穷远点为 O=(0,0)。 （ ）

四、简答与计算：

1. 试用扩展欧几里德算法求解 38 mod 103 的逆元

2. 利用蒙哥马利算法求 509 mod 101

3. 已知 RSA 的公钥为 n＝23×29，设加密指数 e＝13，试用扩展欧几里德算法求解私钥 d，并分别完成对消息 456 和 1000 的 RSA 加解密运算过程。

4. 试描述背包密码体制的密钥产生、加密和解密算法

5. 什么是陷门单向函数？

6. 试给出公钥加密体制同时提供加密和认证的过程。

7. 试述公钥密码的可能字攻击及对抗方法

8. 试描述 RSA 算法的密钥产生、加密、解密过程

9. 为了提高 RSA 算法解密速度，假设用户知道 $n=pq$ 的分解，则如何用中国剩余定理进行 RSA 解密，试给出其过程。

10. 试给出 a^{19} mod n 的快速指数算法的运算表达式

11. 已知一系统采用公共模进行公钥加密，攻击者截获了两个密文 c_1 和 c_2，公私钥对分别是（e_1,d_1）和（e_2,d_2）现在攻击者可以判断对应的明文相同，试问如何恢复明文 m

12. RSA 容易受到低指数攻击，试描述该类攻击。

13. 试述针对 RSA 的重复加密攻击。

14. 试述 Rabin 密码体制的密钥产生，加密，解密的过程；如何解决其解密不唯一的问题？

15. 已知一椭圆曲线 $E_7(1,1)$，则单位元是什么，该曲线上 P=(x,y)的逆元是什么，设该曲线上的两个点 P＝(2，2)，Q＝(0,6)，试计算 3P，P+Q

16. 试给出椭圆曲线群 $E_5(1,1)$上的所有点。

17. 如何将明文 m 转化为椭圆曲线上的一个点，如何再从该点中正确提取出 m？

18. 试述基于有限域 GF(p)上离散对数困难问题的 DH 密钥交换算法和 ElGaml 加密算法。

19. 试述基于椭圆曲线 $E_p(a,b)$的 DH 密钥交换算法和 ElGaml 加密算法。

20. 试给出 19P mod p 的快速倍点运算表达式，其中 P 是某椭圆曲线群 $E_p(a,b)$上的一个生成元。

21. 什么是基于身份的密码算法，用户的私钥由谁产生，有什么优点？

22. 试述双线性映射和 BDH 假设

五、证明题：

1. 证明. |p-q|的差值充分小时，n 能够被快速分解

2. 试证：RSA 中的解密算法能够正确恢复明文.

3. 对于 RSA 算法中两个大素数 p，q，试分析如果 2p 与 3q 的差值很小，也能被快速分解。

4. 试证，椭圆曲线群上的 DDH 问题是容易的

六、综合题

采用 KEM+DEM 的混合机制对消息 m 进行加密和认证，假设公钥密码算法是 RSA 算法，数字签名算法也采用 RSA 算法，H( )为 hash 函数，AES 为对称加密算法。请给出加密过程。

第五章

一、填空：

1. 消息认证中认证符的产生有哪两大类_____和_____

2. 消息认证码和杂凑函数的算法都是公开的，其根本区别是_____

3. MAC 与加密算法的区别在于_____

4. 某 MAC 算法输出长度为 64bit，认证密钥为 160bit，则对 MAC 的穷搜索攻击至少需要____轮

5. 采用先 hash 再对称加密的方法对消息进行认证，设密钥为 k，hash 函数为 H，加密算法为 E，认证的消息为 M，则在考虑和不考虑消息保密性的条件下，认证消息分别可表示为_____

6. 杂凑函数的单向性是指_____ 强单向散列函数是指_____

7. 已知杂凑函数的数出值为 m 比特，则第 I 类生日攻击的复杂度为_____，第 II 类生日攻击的复杂度为____

8. MD5 算法的分组长度为_____输出长度为_____，轮数为_____所以用穷搜索攻击寻找具有给定消息摘要的消息的复杂度为_____以大于 0.5 的概率用穷搜索攻击找出具有相同消息摘要的两个不同消息的复杂度为_____

9. SHA 算法的分组长度为_____输出长度为_____，轮数为_____所以用穷搜索攻击寻找具有给定消息摘要的消息的复杂度为_____以大于 0.5 的概率用穷搜索攻击找出具有相同消息摘要的两个不同消息的复杂度为_____

10. 假设消息的长度为 x，则 MD5、SHA-1、SHA-3 对消息的填充算法分别是_____

11. MD5 以 little-endian 方式存储数据，那么十六进制数 20347AB1 的实际存储是_____

12. HMAC 需要调用_____次 hash 运算，其输出长度由_____决定。

13. 对于一个长度为 n 的 MAC 码算法 $C_K(M)$，随机选取两个消息 M、M'，当 $Pr[C_K(M)=C_K(M')]$=____时，$C_K(M)$是均匀分布的。

二、选择：每一项有 1 个或多个选项是正确的

1. 以下哪些属性是消息认证能够完成的(　).

A.真实性；B.完整性；C.时间性和顺序性；D 不可否认性；E 保密性

2. 设杂凑函数 H( )的输出长度为 m 比特，已知 H(x)，找到 y≠x 满足 H(y)=H(x)的复杂度_____，若找到 y≠x 满足 H(y)=H(x)的概率大于 0.5 则复杂度为_____

A. $O(2^m)$　B. $O(2^{m-1})$　C. $O(2^{m/2})$　D. $O(2^m-1)$

3. $E_K[M||H(M)]$提供了哪些安全服务_____

A. 保密性　B. 完整性　C. 认证性　D. 不可否认性

4. $M||SK(H(M))$提供了哪些安全服务_____，其中 SK 是签名私钥

A. 保密性　B. 完整性　C. 认证性　D. 不可否认性

5. $E_K(M||(H(M||S)))$的安全性和下列哪个相当

A. HMAC　　B. $E_K[M||H(M)]$　　C. $E_{K1}[M||C_{K2}(M)]$　　D. $M||SK(H(M))$

6. SHA-3 标准算法是_____. A. MD5　　B. Keccak　　C. HMAC　　D. Sponge

7. 杂凑函数的单向性是指_____

A. 已知 h，求使得 $H(x)=h$ 的 x 在计算上是不可行的

B. 已知 x，找出 $y(y\neq x)$使得 $H(y)=H(x)$在计算上是不可行的

C. 找出任意两个不同的输入 x、y，使得 $H(y)=H(x)$在计算上是不可行的

8. 下面哪种对消息的认证方式所能提供的安全服务最多_____

A. HMAC(M)　　B. $E_K[M||H(M)]$　　C. $E_{K1}[M||C_{K2}(M)]$　　D. $E_K[M||SK(H(M))]$

三、判断：(正确的划"√"，错误的划"×"，以下同)

1. 采用消息认证码 MAC 认证消息可以实现消息完整性认证和消息源认证　　(　　)

2. 杂凑码是消息中所有比特的函数，因此提供了一定的错误检测能力　　(　　)

3. 带密钥的杂凑函数可以作为一种消息认证码　　(　　)

4. 数据认证算法采用 DES-CBC 模式，所以算法是可逆的　　(　　)

5. MD5 算法已经被破译，因此用于构造 HMAC 时也是不安全的　　(　　)

四、简答与计算：

1. 什么是第 I 类生日攻击和第 II 类攻击

2. 采用数据认证算法对消息进行认证，如果消息为 100bit，则应该怎样对消息填充？

3. 数据认证算法和 DES 的 CBC 模式的区别是什么？

4. 对消息认证码的攻击和对对称密钥算法的攻击在难度上有什么区别？

5. 试分析先加密再认证的 MAC 认证方式是否有被替换的可能，为什么，对安全有危害吗？

（一般没有危害，因为消息源认证是在双方共享密钥的条件下进行的，如果替换为别的密钥，收方可以检测出来，这和先加密再签名的问题不同）

6. 简述用杂凑函数来实现消息认证的三大类基本方式

7. Alice 要给 Bob 发送消息 M，为同时提供对 M 的保密性和认证性保护，试分别给出用消息认证码的实现方法和使用先 hash 再对称加密的实现方法表达式，并比较这两种方法的优劣。

8. 试分析加密密钥和认证密钥分开在安全性上的不同

9. HMAC 算法如何进行预计算？

10. 试描述迭代型杂凑函数的一般结构以及 SHA-3 算法的 sponge 结构

五、证明题：

1. 试证：对于基于 DES-CBC 的数据认证算法，如果仅将第一个分组 D_1 取反，密钥 k 取反，则最后输出的 MAC 也取反。

六、综合题

1. A 要向 B 发送消息 M, 设共享密钥为 k，消息认证码算法记为 $C_k(\quad)$，试回答下列问题：
   (1) 若仅关心 M 的认证性，则 A 发送的消息可表示为？
   (2) 若同时关心保密性和认证性，该怎么办？
   (3) 如果采用的消息认证算法为数据认证算法标准，试述该算法的过程
2. 某用户 A 想要给用户 B 发送一个消息 m，如果要对消息 m 的保密性与认证性进行保护，有四种方法，采用数据认证算法、先 hash 再加密、先签名再加密、HMAC
   (1) 请分别给出这几种方法下认证消息 m 的表达式。所需符号和算法自行定义和选取。
   (2) 其中安全性最强的和最弱的分别是哪一种方法，为什么

第六章

一、填空：

1. 通信双方 A 和 B 通信，则可能发生哪两种形式的抵赖或欺骗？

2. 数字签名能够抵抗不可否认性攻击的原因是_____

3．基于公钥加密的数字签名方式中，加密的消息应该是_____

4. 直接方式的数字签名的公共弱点是_____

5. 在具有仲裁方式的数字签名中，以下方式可以提供消息的保密性、_____、_____

① X→A：$ID_X \| E_{SKX}[ID_X \| E_{PKY}[E_{SKX}[M]]]$

② A→Y：$E_{SKA}[ID_X \| E_{PKY}[E_{SKX}[M]] \| T]$

6. 在如下有仲裁签名过程中如下： 消息①中的两个 *IDx* 的作用_____

① X→A：$ID_X \| E_{SKX}[ID_X \| E_{PKY}[E_{SKX}[M]]]$

② A→Y：$E_{SKA}[ID_X \| E_{PKY}[E_{SKX}[M]] \| T]$

二、选择：每一项有 1 个或多个选项是正确的

1. 为防止通信双方之间互相抵赖，可采用以下哪种技术进行认证?（ ）

A. MAC B. HMAC C. 先 hash 再加密， D. 数字签名

2. 数字签名可以提供的安全属性有_____

A. 保密性 B. 认证性 C. 完整性 D.不可否认性

3. DSA 使用的散列算法是：_____ A．MD4 B．SHA-1 C．MD5 D．SHA-3

4. 假设发方 A 的密钥对为(*pka*, *ska*)，收方 B 的密钥对为(*pkb*, *skb*)，下面哪一种签名能够防止签名的收方假冒攻击_____

A. m||Sig_{ska}(H(m)) B. m||ID_B||Sig_{ska}(H(m)) C. E_{pkb}(m||Sig_{ska}(H(m))) D. m||Sig_{ska}(H(m||ID_B))

三、判断：(正确的划"√"，错误的划"×"，以下同)

1. 数字签名的验证可由第三方来完成 （ ）

2. 基于对称加密算法可以实现对消息的数字签名 ( )

3. GQ 签名体制是基于有限域上离散对数困难问题构建的的 ( )

四、简答与计算：

1. 试描述 RSA 签名算法的体制参数、签名算法和验证算法?

2. 试述 DSA 数字签名算法，包括密钥产生、签名算法和验证算法，并给出验证过程正确性证明

3. 已知一离散对数签名的密钥产生和签名算法，试给出验证方程，并证明其正确性。

4. 已知 schnorr 签名的密钥产生和签名算法，试给出验证方程，并证明其正确性。

5. 已知 Guillou-Quisquater 签名体制的密钥产生和签名算法，试给出验证方程，并证明其正确性。

五、证明题：

1.试证 DSA 签名中两次使用相同的会话密钥 k，是不安全的

2.试分析以下构造完成了 ElGamal 签名的一个伪造

伪造 1：随机选择 e，令 $r=g^e y \bmod p$, $s=-r$,则(r, s)是消息 $m=es$ 的签名，其中(x,y)是签名者的公私钥对；

伪造 2：随机选择 e,v，令 $r=g^e y^v \bmod p$, $s=-rv^{-1} \bmod p-1$，则(r, s)是消息 $m=es$ 的签名，其中(x,y)是签名者的公私钥对。

3 试证 ElGamal 签名中两次使用相同的会话密钥 k，则不安全的。

第七章

一、填空：

1. 两个用户通信时在建立密钥的过程中需要考虑的核心问题是_____和_____

2. 保证消息实时性常用_____和_____两种方法。

3. 单向认证中只关心保密性的认证方式是_____

4. 一次口令认证协议 S/KEY 中，如果当前系统存储的当前用户口令信息为(ID_u, $hash^c(Pwd)$，c)，其中 Pwd 是用户口令，则用户口令还能使用多少次_____

4. 交互式证明与数学证明的区别是什么_____

5. 交互式证明系统必须满足两个基本要求_____和_____

6. 完成以下协议：

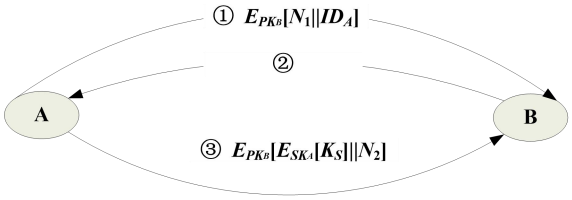
① P 随机选 r ($0<r<n$)，计算 $a \equiv r^2 \bmod n$，将 a 发送给 V。

② V 随机选 $e \in \{0,1\}$，将 e 发送给 P。

③ P 计算 $b \equiv ry^e \bmod n$，即 $e=0$ 时，$b=r$；$e=1$ 时，$b=ry \bmod n$。将 b 发送给 V。

④ 若 $b^2 =$ _____$\bmod n$，V 接受 P 的证明。

7. 具有保密性和认证性的密钥分配如图：试给出消息②的表示_____



具有保密性和认证性的密钥分配

二、选择：每一项有 1 个或多个选项是正确的

1. 在下面的认证类型中，发送方想要同接收方协商一个会话密钥，这属于_____

A. 身份认证　B. 密钥建立认证　C. 数据源认证　D. 消息完整性认证

2. 目前一些公司或机构中，员工上下班签到采用指纹系统进行认证，这属于_____

A. 身份证实　B. 身份识别　C. 零知识认证　D. 消息源认证

3. 下面可用于身份认证的选项是_____

A. 口令　B. 密钥　C. IC 卡　D. 指纹　E. 公钥

4. 下面哪一项技术针对抗等待重放攻击(　　)

A. 要求网络中各方以 KDC 的时钟为基准定期检查并调整自己的时钟

B. 使用一次性随机数的握手协议

C. 基于可信第三方认证

D. 获取旧会话密钥

三、判断：(正确的划"√"，错误的划"×"，以下同)

1. 数据源认证就是对发送方的身份进行认证。 ( )

2. 数据完整性认证也包括对数据新鲜性的认证。 ( )

3. 身份证实和身份识别的本质区别在于申请认证者是否首先出示自己的身份 ( )

面向链接的协议可以用时戳法实现新鲜性

4. 可采用询问-应答方式实现无连接应用过程的实时性认证？ （ ）

5. 询问-应答可用于防止重放攻击？ （ ）

6. 在身份的零知识证明协议中，其安全性与协议运行的轮数有关 ( )

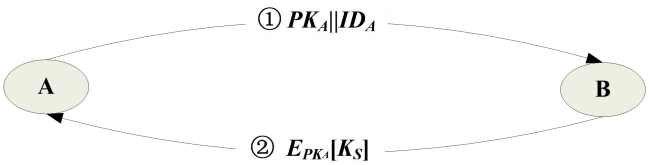
四、简答与计算：

1. Daolev-Yao 威胁模型的两点贡献是什么

2. 消息的新鲜性和主体的活现性的含义是相同的吗？为什么？

3．试给出无中心的单钥密钥分配的过程，并回答为什么不适合在大规模网络中应用

4. 试问对于如下的简单密钥分配协议的中间人攻击如何实现



简单使用公钥加密算法建立会话密钥

5．试述有限域 GF(p)上的 DH 密钥交换协议及其中间人攻击，为防止中间人攻击应采取什么办法，如果在椭圆曲线群上实现 DH 密钥交换中间人攻击又如何

6．实体认证中身份证实和身份识别的区别是什么？

7. NS 协议如下

① A→KDC：$ID_A \| ID_B \| N_1$

② KDC→A：$E_{KA}[K_S \| ID_B \| N_1 \| E_{KB}[K_S \| ID_A]]$

③ A→B：$E_{KB}[K_S \| ID_A]$

④ B→A：$E_{KS}[N_2]$

⑤ A→B：$E_{KS}[f(N_2)]$

请问基于旧会话密钥的重放可在第几步怎么进行?

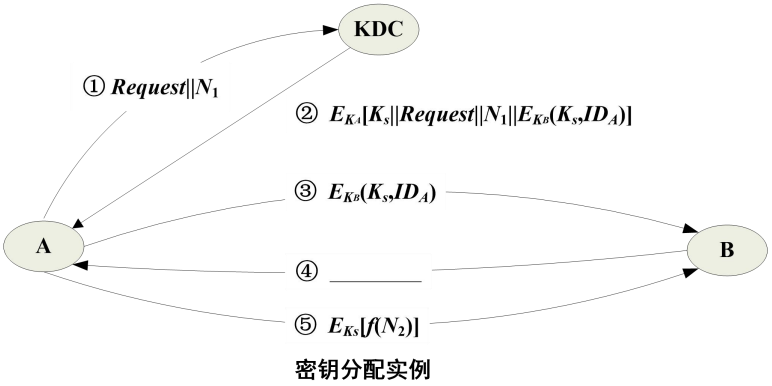
五、证明题：

六、综合题：

1. 如下图所示的密钥分发过程，

(1) 为什么消息②要插入消息①？　　(2) N_1 和 N_2 作用是什么？

(3) 试写出消息④的表达式。　　(4) 第③至⑤步的功能是什么？



密钥分配实例

2. NS 协议如下

① A→KDC：$ID_A \parallel ID_B \parallel N_1$

② KDC→A：$E_{KA}[K_S \parallel ID_B \parallel N_1 \parallel E_{KB}[K_S \parallel ID_A]]$

③ A→B：$E_{KB}[K_S \parallel ID_A]$

④ B→A：$E_{KS}[N_2]$

⑤ A→B：$E_{KS}[f(N_2)]$

请问基于旧会话密钥的重放可在第几步怎么进行?

3. 已知一改进的 NS 协议

① A→B：$ID_A \parallel N_A$

② B→KDC：$ID_B \parallel N_B \parallel E_{KB}[ID_A \parallel N_A \parallel T_B]$

③ KDC→A：$E_{KA}[ID_B \parallel N_A \parallel K_S \parallel T_B] \parallel E_{KB}[ID_A \parallel K_S \parallel T_B] \parallel N_B$

④ A→B：$E_{KB}[ID_A \parallel K_S \parallel T_B] \parallel E_{KS}[N_B]$

TB 是 B 建议的证书(会话密钥)截止时间，用于截止时间前再次发起会话时 K_S 是否可用的判别时间

N_A 和 N_B 的作用是什么？再次发起通信时如何认证？票据为_____