第一章练习题

一、判断题

1.一个人可以通过执行一系列的步骤来完成一项任务构成协议。

2.通过执行协议必须完成某项任务或达成某项共识。

3.在公钥协议中，数字证书可离线担保实体确实是公钥的所有者。

4.对不同类型的安全协议，存在着不同的攻击，而且新的攻击方法在不断产生。

5.协议中使用的密码算法被认为是抽象的并且不能对密码分析免疫。

6.安全协议又称为密码协议。

7.密钥协商可以不需要任何的可信第三方来完成。

8.算法应用于协议中消息处理的环节，对不同的消息处理方式要求不同的算法。

9.当用户接收到的信息都是二进制串时，用户无法判断是否是经过加密等处理。

10.重放属于对安全协议攻击类型中的篡改。

二、填空题

1.协议运行环境中的角色是_____、攻击者、可信第三方。

2.电子商务协议最关注_____，即协议应保证交易的双方都不能通过损害对方的利益而得到其不应该得到的利益。

3.在重放中，攻击者介入协议运行，通过_____再重放的方式实现攻击。

4.当用户接收到的信息都是二进制串时，用户无法判断二进制串是否经过加密等处理，_____就是利用这一点使得用户将一个消息错误的解释成其他的消息。

5.抵抗类型攻击的方法有很多，有的使用每次改变消息元素的顺序，确保每次的加密密钥不同。或者在消息中添加_____或_____的类型信息。

6._____是攻击者选择或更改证书信息来攻击协议的运行。

7._____是指安全方案和协议的最基本组成构建或模块。

8.攻击者可以通过_____获取协议运行中所传输的消息。

9.可证明安全理论最成功的实际应用是_____。

10.理论上任何安全多方计算问题都可以通过_____协议来解决。

三、名词解释

1.协议

2.安全协议

3.攻击者

4.可信第三方

5.密码分析

四、简答题(第 1、2、3、4 题每题五分，第 5 题 8 分，第 6 题 10 分)

1. 安全协议的安全性质有哪些？

2.最常用最基本的安全协议分为哪几类？

3.安全协议的三大理论分析方法是哪些？

4.已知 A 和 B 已经共享一个密钥，并且分别选择随机数 Na 和 Nb。A,B 的协议过程如下：

（1）A->B:{Na}k

（2）A->B:{Nb}k，Na

（3）A->B:Nb

攻击者 C 通过反射攻击，成功完成两次协议的执行，请写出 C 对 A 的“信使攻击”过程。

5.试简要叙述协议的三层含义。

6.安全协议存在哪些安全缺陷及各自原理。

答案：

一、判断题

1.错 2.对 3.对 4.对 5.错 6.对 7.对 8 对 9.对 10.对

二、填空题

1.参与者 2.公平性 3.复制 4.类型攻击 5.认证数 消息域 6.证书操纵 7.极微本原 8.窃听 9. RO 模型方法论 10.电路计算

三、名词解释

1.协议是两个或两个以上的参与者采取一系列步骤以完成某项特定的任务。

2.安全协议是以密码学为基础的信息交换协议，其目的是在网络环境中提供各种安全服务。

3.攻击者就是协议过程中企图破坏协议安全性和正确性的人。

4.可信第三方是指在完成协议的过程中，值得信任的第三方，能帮助互不信任的双方完成协议。

5. 攻击者利用在协议运行中所获取的消息进行分析以获取有用的信息。

四、简答题

1.机密性、完整性、认证性、非否认性和公平性等。

2.密钥建立协议、认证协议、电子商务协议、安全多方计算协议。

3.安全多方计算、安全协议的形式化分析方法、安全协议的可证明安全理论性。

4.（1）A->C:{Na}k

（1’）C->A:{Na}k

（2’）A->C:{Na’}k,Na

（2）C->A:{Na’}k,Na

（3）A->C:Na’

（3’）C->A:Na’

5.(1)协议需要两个或两个以上的参与者。一个人可以通过执行一系列的步骤来完成一项任务，但它不构成协议。

（2）在参与者之间呈现为消息处理和消息交换交替进行一系列的步骤。

（3）通过执行协议必须能完成某项任务或达成某项共识。

6.（1）基本协议缺。在安全协议的设计中没有或很少防范攻击者而引发的协议缺陷。

（2）并行会话缺陷。当多个协议实例同时执行时，如果协议对并行会话攻击缺少防范，会导致攻击者通过交换适当的协议消息获得所需要的信息。

（3）口令/密钥猜测缺陷。这类缺陷产生的原因是用户往往从一些常用的词中选择其口令，从而导致攻击者能够进行口令猜测攻击；或者选取了不安全的伪随机数生成算法构成密钥，使攻击者能够恢复密钥。

(4)陈旧消息缺陷。协议设计中对消息的新鲜性没有充分考虑，从而使攻击者能够进行消息重放攻击。

(5）内部协议缺陷。协议的可达性存在问题，协议的参与者中至少有一方不能完成所有必需的动作而导致的缺陷。

（6）密码系统缺陷。协议中使用的密码算法导致协议不能完全满足所要求的机密性、认证性等需求而产生的缺陷。

第二章练习题

一、判断题

1. 密码系统的设计原则是：对合法的通信双方来说，加密和解密变换是复杂的；对密码分析员来说，由密文推导出明文是容易的。（ ）
2. 在对称密钥体制中，加密密钥和解密密钥是一样的或者彼此之间是容易相互确定的。（ ）
3. 在非对称密码体制中，加密密钥和解密密钥不同，从一个难以推出另一个，可将加密和解密能力分开。（ ）
4. Rabin 体制和 RSA 体制基于大数问题。（ ）
5. Hash 函数一般满足输入值可以为任意值，但输出字符串的长度固定。（ ）
6. 数字签名主要用于对消息进行签名，以防消息的伪造和篡改。（ ）
7. 公钥密码体制的安全性是指计算上的安全性。（ ）
8. 消息认证就是认证消息的完整性，当接收方收到发送方的消息时，接收方能够验证收到的消息是真实的和未被篡改的。（ ）
9. 椭圆曲线数字签名算法和 RSA 与 DSA 的功能相同，并且数字签名的产生与验证速度要比 RSA 和 DSA 慢。（ ）
10. 基于 ID 的和基于 PKI 的密码学系统都是对称的，主要不同点在于密钥的管理。（ ）

二、填空题

1. 一个加密方案包括三个集合____、____、_____。

2. 加密方案包括三个算法____、_____、_____。

3. 理论上不可攻破的密码系统通常称作_____。

4. 根据密钥的特点，将密钥体制分为_____和_____。

5. 随机数分为_____和_____。

6. 密码学意义上安全的伪随机序列要求满足以下两条特性：_____、_____。

7. 常用的分组密码算法：_____、_____和_____。

8. 数字证书是有权威机构 CA，又称_____。

9. _____采用共享密钥，是一种广泛使用的消息认证技术。

10.数字签名特征：_____。

三、名词解释

1.消息认证　2.分组密码　3.对称密码体制　4.非对称密码体制　5.随机数
6.语义安全性 7.加密方案不可延展性　8.DES 9.散列函数

四、简答题

1.请回答建立一个公开密钥密码系统的两个最基本条件是什么？。

2.消息认证码作为一种广泛使用的消息认证技术，可以保证消息在传输过程中保持了完整性，试述发送和接收的过程。

3.一个签名方案是一个五元组（P,A,K,S,V），试分析其满足的 4 个条件。

4.ElGamal 密码体制特点是什么？

5.Hash 函数 H 需要满足的基本要求有哪些？

6.密码学意义上安全的伪随机序列要求满足的特性是什么？

五、计算题

1．在 RAS 体制中，设 p=47,q=59,d=157。另两个字母为一块，一次加密一块，编码如下：另空白=00，A=01，B=02……,Z=26。明文“its all greek to me” 的密文是什么？

答案

一、判断

1．错 2.对 3.对 4.错　5.对　6.对 7.对 8.对 9.错 10.错

二、填空题

1.一个加密方案包括三个集合：密钥集、消息集、密文集。

2.密方案包括三个算法：密钥产生算法、加密算法、解密算法。

3.理论上不可攻破的密码系统通常称作一次一密系统。

4.根据密钥的特点，将密钥体制分为对称和非对称密码体制。

5.随机数分为真随机数和伪随机数。

6.密码学意义上安全的伪随机序列要求满足以下两条特性：不可以测性、随机性。

7.常用的分组密码算法：数据加密标准、高级数据加密标准和 IDEA 密码体制。

8.数字证书是有权威机构 CA，又称证书授权。

9.消息认证码采用共享密钥，是一种广泛使用的消息认证技术。

10.数字签名特征：任何人都可以利用签名者的公钥认证签名的有效性、签名是无法被伪造的。

三、名词解释

1.消息认证：消息认证就是认证消息的完整性，当接收方收到发送方的消息时，接收方能够验证收到的消息是真实的和未被篡改的。它包含两层含义：一是验证信息的发送者是真正的而不是冒充的，即数据起源认证；二是验证信息在传送过程中未被篡改、重放或延迟等。

2.分组密码: 将明文分成 m 个明文块 x = (x1，x2，…，xm)。每一组明文在密钥 k = (k1，k2，…，kt)的控制下变换成 n 个密文块 y = (y1，y2，…，ym)，每组明文用同一个密钥 k 加密。

3.对称密码体制:(私钥密码体制,秘密密钥密码体制)加密密钥和解密密钥相同,或实质上等同,即从一个容易推出另一个

4.非对称密码体制:（公钥密码体制）加密密钥和解密密钥不相同,从一个很难推出另一个.

5.随机数：随机数是较短的随机位序列，在密码学中非常重要，分为真随机数和伪随机数。随机序列主要应用于序列密码，序列密码的强度完全依赖于序列的随机性和不可预测性。

6.语义安全性：如果在给定密文的情况下能够有效计算得到的信息在未知密文的情况下也能够有效计算得到，则称该密文方案提供了语义安全性

7.加密方案不可延展性：如果未知明文的情况下。攻击者由一个已知密文构造其他的有效的密文在计算机上是不可行的，则称该加密方案具有不可延展性

8.DES：用 56 位密钥将 64 位的明文转换成 64 位的密文，其中密钥总长为 64 位，另外 8 位是奇偶校验位

9.散列函数：散列（HASH）函数 H 也称哈希函数或杂凑函数等，是典型的多到一的函数，其输入为一可变长 x（可以足够的长），输出一固定长的串 h（一般为 128 位、160 位，比输入的串短），该串 h 被称为输入 x 的 Hash 值，计作 h=H(x)。

四、简答题：

1 .请回答建立一个公开密钥密码系统的两个最基本条件。

第一，加密和解密变换必须是计算上容易的；第二，密码分析必须是计算上困难的。

2. 发送方 A 要发送消息 M 时，使用一个双方共享的密钥 k 产生一个短小的定长数据块，即消息校验码 MAC=Tk(M)，发送给接收方 B 时，将它附加在消息中。这个过程可以表示为 A → B ：M || Tk(M)接受方对收到的报文使用相同的密钥 k 执行相同的计算，得到新的 MAC。接受方将收到的 MAC 与计算得到的 MAC 进行比较，如果相匹配，那么可以保证报文在传输过程中维持了完整性

3.一个签名方案是一个五元组（P,A,K,S,V）,试分析其满足的 4 个条件。

签名方案是一个五元组（P,A,K,S,V）：

1）P 是所有可能的消息组成的有限集。

2）A 是所有可能的签名组成的有限集。

3）K 是所有可能的密钥组成的有限集。

4）对每一个 k∈K，有一个签名算法 Sk∈S 和一个相应的验证算法 Vk∈V。对每一个消息 x∈P 和每一个签名 y∈A，每一个签名算法 Sk：P→ A 和验证算法 Vk：P×A→{0,1}满足：当 y= Sk (x)时，Vk(x,y)=1，否则 Vk(x,y)=0。

4.ElGamal 密码体制特点

密文由明文和所选随机数 k 来定，因而是非确定性加密，一般称之为随机化加密，对同一明文由于不同时刻的随机数 k 不同而给出不同的密文。代价是使数据扩展一倍

5.Hash 函数 H 一般满足以下几个基本要求：

（1）输入 x 可以为任意长度；输出数据串长度固定；

（2）正向计算容易，即给定任何 x，容易算出 H(x)；反向计算困难，即给出一 Hash 值 h，很难找出一特定输入 x，使 h=H(x)；

（3）抗冲突性（抗碰撞性），包括两个含义，一是给出一消息 x，找出一消息 y 使 H(x)=H(y)是计算上不可行的（弱抗冲突），二是找出任意两条消息 x、y，使 H(x)=H(y)也是计算上不可行的（强抗冲突）。

6.密码学意义上安全的伪随机序列要求满足的特性是什么？

（1） 不可预测性（2）随机性

五、计算题

解：N=p*q=2773

Q(N)=(p-1)*(q-1)=2668

de=1mod2668

157e=1mod2668

157e=2668k+1

e=17

C(it)=092017 mod N=0948

C(s)=190017 mod N=2342

C(al)=011217 mod N=1084

C(l)=120017 mod N =1444

C(gr)=071817 mod N=2663

C(ee)=050517 mod N=0695

C(k)=110017mod N=0778

C(to)=201517 mod N=0774

C(m)=001317 mod N=0219

C(e)=0517 mod N=0508

密文是：094823421084144426630695077807740219 0508

一、填空题：

1._____就是把一个消息分成几块，单独的每一块看起来没有意义，但是所有的块集合起来能恢复出原消息。
2.秘密共享是一种将_____的密码技术。
3.秘密共享的目的是_____，已达到分散风险的目的。
4.在秘密共享方案中，最常见的就是_____。
5.在一个（m,n）门限方案中，m 为_____。
6.1979 年 Shamir 提出一个称为（m,n）门限方案的构造方法，此方案是把一个信息分成几部分，每部分叫做它的_____。
7.阈下信道属于_____算法。
8.在阈下信道方案中，签名者选择一个随机数，并通过_____生成一个新的随机数。
9._____试图使彼此互不信任的双方对一个随机位达成共识。
10.比特承诺方案具有两个重要性质：一是_____，二是约束性。

二、判断题

1.秘密分割协议中，如果一部分丢失，所持有人又不在，消息就丢掉了。（ ）
2.在（m,n）门限方案中，把信息分成 n 部分，其中 m 部分不能用来重构消息。（ ）
3.阈下信道有密钥保护，安全性很高。（ ）
4.在阈下信道方案中，签名者选择的数字是随机的。（ ）
5.在参数设置中，签名者随机取两个大素数 p 和 q，这两个数不必保密。（ ）
6.单向函数抛币协议中，通信双方达成共识的单向函数 f 对双方是保密的。（ ）
7.单项函数抛币协议中，其安全性取决于单向函数。（ ）
8.公开密钥密码抛币协议既可与公开密钥密码又可与对称密码一起工作，没任何限制。（ ）
9.在公开密钥密码抛币协议中不需要可信的第三方介入实际的协议。（ ）
10.不经意传输协议是一个双方协议。（ ）

三、名词解释

1.秘密分割

2.秘密共享
3.投币入井协议
4.（m，n）门限方案
5.阈下信道
6.不经意传输协议

四、计算题

1.已知（3，5）秘密共享，P=17，a_1=8，a_2=7，求秘密共享序列。

2.已知（3，5）秘密共享中，K_1=9，K_2=4，K_3=13，p=17，

即：$a\times1^2+b\times1+K=9 \bmod 17$

$a\times2^2+b\times2+K=4 \bmod 17$

$a\times3^2+b\times3+K=13 \bmod 17$

求 K。

五、简答题

1.秘密共享的目的是什么？

2.门限秘密共享有几个安全问题，各是什么？

3.（t,n）秘密共享中，怎样根据 t 和 n 的选择，权衡其安全性和可靠性？

4.比特承诺方案具有几个重要性质，各是什么?

5.举例说明构造比特承诺使用的单向函数。

6.假设 Alice 和 Bob 要离婚，讨论谁得到什么，并且俩人谁也不想见谁，在谁拥有车这个问题上有争议，最后他们决定抛硬币， 如果他们相互不信任，请问如何能在电话里抛硬币决定？ （采用单向函数的抛币协议 ）

答案：
一、填空题
1.秘密分割 2.秘密分割存储 3.阻止秘密过于集中 4.门限方案 5.门限值 6.共享
7.传统数字签名 8.单向函数 9.硬币抛掷游戏 10.隐蔽性
二、判断题
1.对 2.错 3.错 4.对 5.错 6.错 7.对 8.错 9.对 10.对
三、名词解释
1.秘密分割:秘密分割就是指把一个消息分成 n 块,单独的每一块看起来没意义，但所有的块集合起来就能恢复出原消息。

2.秘密共享：秘密共享是一种将秘密分割存储的密码技术，目的是阻止秘密过于集中，以达到分散风险和容忍入侵的目的，是信息安全和数据保密中的重要手段。

3.掷币入井协议：每个协议有一个点，在这个点上其中一方知道掷币结果，但不能改变它。然后，这一方能推迟向另一方泄露结果。这就称作掷币入井协议。

4.（m，n）门限方案：把一个信息分成 n 部分，每部分叫做它的“影子”或共享，它们中的任何 m 部分都能够用来重构消息，这就叫做（m，n）门限方案。

5.阈下信道：阈下信道是指在基于公钥密码技术的数字签名、认证等应用密码体制的输出密码数据中建立起来的一种隐蔽信道，除指定的接收者外，任何其他人均不知道密码数据中是否有阈下消息存在。

6.不经意传输协议：不经意传输协议，是一种可保护隐私的双方通信协议，能使通信双方以一种选择模糊化的方式传送消息。不经意传输协议是密码学的一个基本协议，他使得服务的接收方以不经意的方式得到服务发送方输入的某些消息，这样就可以报数接受者的隐私不被发送者所知道。

四、计算题：

1.已知（3，5）秘密共享，P=17，a_1=8，a_2=7，求秘密共享序列。

解： 构造 2 次随机多项式 $F(x) = K + a_1x + a_2x^2 \bmod p$

a1=8, a2=7 $F(x) = 11 + 8x + 7x2 \bmod 17$

秘密分割 $K_1 = F(1) = 7\times12 + 8\times1 + 11 \equiv 9 \bmod 17$

$K_2 = F(2) = 7\times22 + 8\times2 + 11 \equiv 4 \bmod 17$

$K_3 = F(3) = 7\times32 + 8\times3 + 11 \equiv 13 \bmod 17$

$K_4 = F(4) = 7\times42 + 8\times4 + 11 \equiv 2 \bmod 17$

$K_5 = F(5) = 7\times52 + 8\times5 + 11 \equiv 5 \bmod 17$

$(K_1, K_2, K_3, K_4, K_5) = (9, 4, 13, 2, 5)$

2.已知（3，5）秘密共享中，K_1=9，K_2=4，K_3=13，p=17，

即：$a\times1^2+b\times1+K=9 \bmod 17$

$a\times2^2+b\times2+K=4 \bmod 17$

$a\times3^2+b\times3+K=13 \bmod 17$

求 K。

解： 令 x=0

$l_1=(x_2-x)/(x_2-x_1)\times(x_3-x)/(x_3-x_1)=2/（2-1）\times3/（3-1）=3$

$l_2=(x_1-x)/(x_1-x_2)\times(x_3-x)/(x_3-x_2)=1/（1-2）\times3/（3-2）=-3$

$l_3=(x_1-x)/(x_1-x_3)\times(x_2-x)/(x_2-x_3)=1/（1-3）\times2/（2-3）=1$

$K=（K_1\times l_1+K_2\times l_2+K_3\times l_3）\bmod 17=11$

五、简答题：

1.答：秘密共享的目的是阻止秘密过于集中，以达到分散风险和容忍入侵的目的

2.答：两个，是机密性和强健性。

3.答：高 t，提供高安全性，低可靠性；低 t，提供低安全性，高可靠性

4.答：两个，一是隐蔽性，即接受者不能通过接受的箱子来确定承诺值 m；二是约束性，发送者能改变箱子中的承诺值 m。

5.答：哈希函数 ,公钥加密。

6.答：【1】Alice 选择一个随机数 x，她计算 y=f（x），这里 f（x）是单向函数；

【2】Alice 将 y 送给 Bob；

【3】Bob 猜测 x 是偶数或奇数，并将猜测结果发给 Alice；

【4】如果 Bob 的猜测正确，抛币结果为正面;如果 Bob 的猜测错误，则抛币的结果为反面。Alice 公布此次抛币的结果，并将 x 发送给 Bob；

【5】Bob 确信 y=f（x）。

一、名词解释

1.RFID	2.RFID 标签	3.RFID 中的主动干扰	4.RFID 标签读写器
5.时间戳	6.密钥传输协议	7.会话密钥的不可控性	8.密钥协商协议
9.密钥的完整性	10.密钥确认	11.未知密钥共享安全	12.前向安全

二、填空

1.无线网络协议 IEEE802.11 共有两种认证方式_____和_____。
2.根据 RFID 标签的能量来源，可以将其分为三大类：_____、____、____ 。
3.一个安全性的 RFID 系统应该解决_____、_____、____三个基本安全问题。
4.常用的保证新鲜值的机制有_____、_____、_____。
5.基于身份的可否认认证协议有_____和_____安全性质。
6.Kerberos 的认证服务任务被分配到_____和_____两个相对的独立服务器。它们同时连接并维护一个中央数据库存放用户口令、标识等重要信息。
7.有基本消息格式的基于 DH 交换的协议容易受到_____攻击。
8.在一个密钥建立协议中，其中的两个用户想用密码技术建立一个新的密钥用于保护他们的通信，这个密钥称为_____。
9.站对站（STS）协议在信息交换时添加了_____机制，从而为 DH 协议提供认证。
10.在密钥建立协议中，有许多机制可以用来使用户检测会话密钥是否被重放。我们现在常用的是_____机制来改进我们的协议。
11.随着电子商务的发展，隐私问题也越来越突出，它已经成为影响电子商务成长的关键之一。在隐私保护方面，除了法律与管理外，_____是解决隐私问题最有效、直接和廉价的手段。

三、判断

1.Hash—Lock 协议为了避免信息泄露和被追踪，它使用 metal ID 来代替真是标签的 ID。
2.读写器到标签之间的信道叫做后向信道，而标签到读写器之间的信道叫做前向信道。
3.半主动标签本身不带有电池，因此不能通过自身能量主动发送数据。
4.在 Hash 链协议中，当使用两个不同杂凑函数的 Tag 读写器发起认证时，Tag 总是发送不同的应答。
5.无线网络的工作模式可分为基础结构模式和自组织网络模式。
6.两个用户想用密码技术建立一个新的密钥用于保护他们的通信，这个密钥称为共享密钥。
7.为了认证任何信息是在签名中包含文本域的一个重要原因。
8.简化了密钥管理是公钥技术较对称密码的一大优势，在商业应用中非常有用。
9.密钥完整性保证了攻击者不能修改会话密钥。
10.在密钥传输协议中，会话密钥是所有协议用户输入参数的函数。
11.基本的 DH 协议的基础限制是缺乏对发送消息的认证。
12.所有的基于 DH 的密钥协商协议都要使用暂时密钥。
13.应用 DH 密钥交换的加密密钥交换协议的大致思想是传输用口令加密的短暂公钥作为共享密钥。
14.在用户匿名的认证协议中，通常用户与服务器建立会话，一旦会话建立，服务器不知道跟谁通信。
15.可否认认证协议的目标是接受者能够确认给定消息的来源且能够向第三方证明消息发送者的身份。

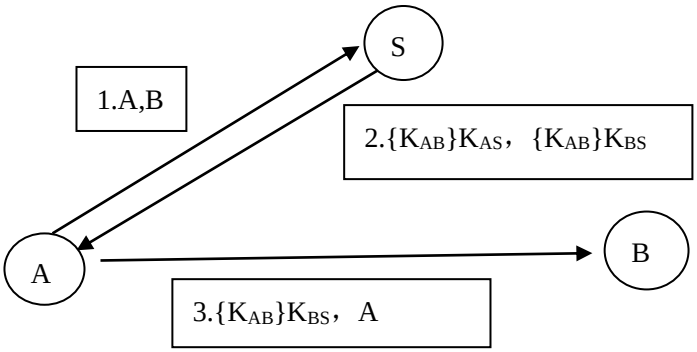
四、简答

1.在无线局域网环境下，主要的可实现的威胁有哪些？（至少五个）
2.密钥建立协议的结构是什么？
3.公钥协议的 Anderson-Needham 鲁棒性原则有哪些？（至少五个）

4.基于口令的密钥建立协议的特殊性质和需求是什么？

5.密钥建立协议的基本目标是什么？

6.在创建密钥建立协议时，两个用户表示为 A 和 B，可信的服务器表示为 S。协议的目的就是使 A 和 B 建立一个新的密钥 K_{AB} 并用它来保护通信。S 的任务是生成 K_{AB} 并把它发送给 A 和 B。假设服务器 S 初始时和系统的每个用户都共享一个秘密密钥。密钥 K_{AS} 由 A 和 S 共享，K_{BS} 由 B 和 S 共享，这些共享的密钥称为长期密钥，我们将利用长期密钥建立会话密钥。如下图所示：



该协议在开放的环境中也是不安全的，该协议的问题不在于它泄露了秘密密钥，而在于没有保护信息—“还有谁拥有密钥”。对该协议的一种攻击是：攻击者 C 拦截 A 传给 B 的消息，并用 D 的身份标识替换 A 的身份标识（D 可以是任何标识，包括 C 自己的标识）。结果 B 相信他和 D 共享密钥，而事实上他和 A 共享密钥。另外该协议还容易受到内部攻击。为避免这两种由于缺少认证的攻击，请给出改进的协议。（画图说明即可）

7.实体认证协议的第四个协议如下图所示，它提供了双向认证。如果从 A 中发出的加密消息中不包含 B 的标识，则该协议容易遭受到反射攻击 。请给出该协议遭受到的反射攻击。（画图说明）

1.B→A：N_B

2.A→B：$\{N_A，N_B，B\}K_{AB}$

3.B→A：$\{N_B，N_A\}K_{AB}$

8.下图显示了 ISO/IEC 11770-3 标准中最简单的密钥传输协议机制 1。A 选择会话密钥并用 B 的公钥加密后发送给 B，加密的消息中还包括 A 的标识和时间戳 T_A（或用计数器代替）。在这个协议中以及在标准的所有协议中，使用的公钥加密方法能提供不可延展性和语义安全性。试分析该机制的优缺点。

1.A→B：$E_B(A，K_{AB}，T_A)$

9.在基本的 Diffie-Hellman 协议中，两个成员 A 和 B 公开地同意元素 g 生成一个乘法群 G。他们在分别在 1~G 的阶的范围中选择随机数 r_A 和 r_B。A 计算 $t_A = g^{r_A}$，B 计算 $t_B = g^{r_B}$ 并进行交换，如下图所示。共享秘密 $Z_{AB} = g^{r_A r_B}$，A 和 B 都能由幂的同态性计算这个值。①改正下图中的错误（另行画图）②最初是在非零整数模的一个大素数 p 的乘法域 Z_p^* 中描述 DH 密钥协商协议，现在常把协议产生的群 G 定义为 Z_p^* 素数阶为 q 的子群这样做的好处有

哪些？

共享信息：群 G 的生成员 g

A B

---

10. 具有隐私保护的认证密钥交换协议有哪些？

11. 一般来说，一个完全的群组通信，至少要满足哪 5 个方面的安全性需求？同时还要满足哪 5 个服务质量的需求？

答案：

一、名词解释

1.RFID：无线射频识别是一种非接触式自动识别技术。

2.RFID 标签也被称为电子标签或职能标签，它是带有天线的芯片，芯片中存储有能够识别目标的信息。

3.RFID 主动干扰是指标签用户通过一个设备主动广播无线电信号用于阻止或破坏附近的 RFID 读写器操作。

4.RFID 读写器实际上是一个带有天线的无线发射与接收设备，处理能力、存储空间都比较大。

5.时间戳：消息发送者在消息中加入消息发送的当前时间。

6.密钥传输协议：密钥传输协议是密钥建立协议。在协议中一个成员选择会话密钥并安全的传输给其他的一个或多个成员。

7.会话密钥的不可控性：任何协议参与者都不能使得会话密钥是他预先选取的值的能力，则称该协议具有会话密钥的不可控性。

8.密钥协商协议：密钥协商协议是密钥建立协议。在协议中，会话密钥是所有协议用户输入参数的函数。

9 密钥的完整性：攻击者不能修改会话密钥。对于传输协议而言，密钥完整性是指只有密钥发起者所选择的密钥才被接受。对于密钥协商协议，密钥完整性是指只有协议参与者输入的已知函数所产生的密钥才能被接受。

10.密钥确认：协议参与的一方要确认另一方（可能未鉴别）已经拥有了密钥。

11.未知密钥共享安全：在协议参与者不知道的情况下，A 是不能被迫与协议参与者 B 分享一个会话密钥，具有该性质的协议称协议提供了未知密钥共享安全。

12.前向安全：如果一或多个协议参与者的长期私钥泄露了，不会导致旧的会话密钥泄露，则称该协议提供了部分前向安全；如果所有协议者的长期私钥泄露了，不会导致旧的会话密钥泄露，则称该协议有完善前向安全。

二、填空

1.开放系统认证　共享密钥认证

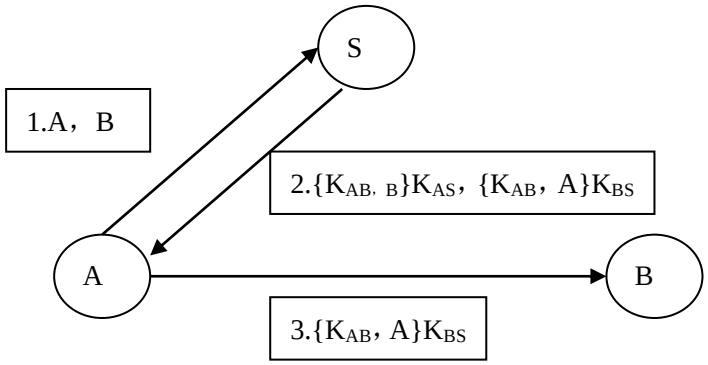
2.被动式标签　半被动式标签　主动式标签

3.数据安全　隐私　复制

4.时间戳　一次性随机数　计数器

5.认证性　　可否认性
6.认证服务器 AS　　票据服务器 TGS
7.基本的未知密钥共享
8.会话密钥
9.数字签名
10.挑战—响应
11.技术
三、判断
1.对　2.错　3.错　4.对　5.对　6.错　7.对　8.错　9.对　10.错　11.对　12.错　13.对 14.对　15.错
四、简答
1. 无授权访问、窃听、伪装、篡改信息、重放、错误路由、删除信息、网络泛洪
2. (1) 哪些密钥是已经建立的（例如长期密钥）。
(2) 会话密钥如何产生。
(3) 参与密钥建立的用户的数目。
3. (1) 在加密前。如果在加密数据上签名，则不能保证签名人知道被加密的数据。
(2) 注意区分实体。尽可能避免将同一密钥用于两个不同的目的（如签名和加密），并能区分同一协议的不同运行。
（3）在签名和解密数据时，小心别当敌手的信使。
（4）可虑到所有的比特，那些提供模糊性、冗余和计算机复杂性等。
（5）不要假设其他人的“秘密”是秘密，CA 除外。
（6）不要加是收到的消息有特定的形式，除非你能验证。
（7）要明确安全参数。
4.(1) 用户仅拥有小信息熵的秘密。
（2）离线字典攻击不可行。
（3）在线字典攻击不可行。
5.(1) 隐式密钥认证：协议参与的一方要确信只有身份确定的协议参与另一方才能知道共享密钥。
（2）密钥确认：协议参与的一方要确认另一方已经拥有了共享的密钥。
（3）显式密钥认证：同时提供隐式密钥认证和密钥确认。

6.



7.

1.B→C(A)：N_B

1´.C(A) →B：N_B

2´.B→C(A)：{N_B´，N_B}K_{AB}

2.C(A) →B：{N_B´，N_B}K_{AB}

3.B→C(A)：{N_B，N_B´}K_{AB}

8.优点：从 A 的角度来看，机制 1 提供了一个好的密钥，由于 A 可以选择新鲜的密钥并且加密方法保证仅 A 和 B 知道密钥。

缺点：A 不能得到 B 的确认也不能保证 B 是有效的。另外，由于没有对密钥起源的认证，B 不能确保是和谁共享这个密钥。

9.改错

$t_A = g^{r_A}$ t_A $t_B = g^{r_B}$

$Z_{AB} = t_B^{r_A}$ t_B $Z_{AB} = t_A^{r_B}$

好处：（1）可以避免多次攻击（2）可以节省计算量

10.（1）可否认的认证密钥交换协议。

（2）通信匿名的认证密钥交换协议。

（3）用户匿名的认证密钥交换协议。

11.（1）群组安全。非群组成员无法得到群组通信密钥。

（2）前向安全。一个成员离开群组后，它无法再得到新的密钥，从而保证其无法解密离开后的通信数据。

（3）后向安全。新加入的成员无法得到先前的群密钥，从而保证其无法解密加入前的通信数据。

（4）抵抗合谋攻击。避免多个群组成员联合起来破解系统。

（5）密钥独立。一个通信密钥的泄露，不会导致其他密钥泄露。

服务质量需求：

（1）低带宽占用 （2）低通信延迟 （3）1 影响 N （4）服务鲁棒性 （5）服务可靠性

第五章 零知识证明

一 、填空

1. 零知识证明起源于_____。

2. 零知识证明具有正确性、_____、_____。

3. 零知识证明的简单模型有_____、分割选择协议、一般的协议。

4. 交互式零知识证明包括_____的零知识证明和_____的零知识证明。

5. 在零知识证明协议（P,V）中，要求证明者 P 和验证者 V 之间依次执行若干轮，通常称为_____；要求 P 和 V_____的一次把这些轮全部完成，称为并行协议。

6. 非交互式零知识证明包括两种模型，一种是_____的非交互式零知识证明，另一种是知识的非交互式零知识证明。

7、对一个语言 L 的非交互式证明系统有两个阶段构成，第一个阶段是_____阶段，主要建立证明者和验证者拥有的某些共同信息以及他们各自拥有的某些秘密信息；第二个阶段是_____，证明者选择并向验证者证明定理。

二、判断

1.知识签名从本质上看是一种交互式的零知识证明。 （ ）

2.与交互式零知识证明相比，非交互零知识证明是连接的。 （ ）

3.对一个语言 L 的非交互式证明系统有两个阶段构成，第一个阶段允许证明者和验证者之间进行交互，而在第二个阶段，证明者选择并向验证者证明定理时是非交互的。 （ ）

4.分割选择协议中，若 P 将东西切成两半，则 P 先选择其中之一，剩下的再由另一方拿走。 （ ）

5.非交互式零知识证明是一种特殊的非交互证明系统，它要求在证明中不允许泄露任何有用的信息。 （ ）

6.零知识证明起源于最小泄露证明 。 （ ）

7.非交互式零知识证明验证中，定理的证明能被系统中的任何用户验证则我们称证明是公开可验证的。（ ）

三、名词解释

1.（2 分）P 类问题：

2.（2 分）NP 类问题：

3.（3 分）交互式零知识证明：

4.（3 分）知识签名：

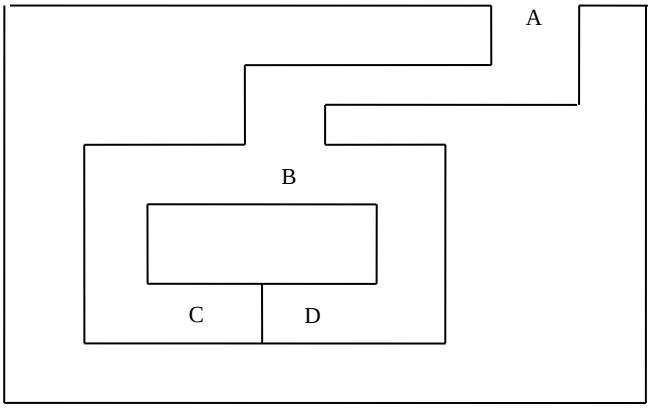
四、简答题

1.（4 分）请说一下零知识证明的定义。

2.（6 分）零知识证明满足三个性质，请简述一下这三个性质。

3. （6 分）请列举几个 NP 完全问题（至少三个）。

4.（8 分）根据下图简述一下洞穴协议的内容。



第五章零知识证明答案

一、填空

1. 最小泄露证明。

2.完备性、零知识性

3.洞穴协议

4.成员、知识

5.串行协议、并行

6.成员或定理

7.预处理阶段、定理证明阶段

二、判断

1．× 2.×3.√ 4.× 5.√ 6.√7.√

三、名词解释

1.P 类问题：在计算机学科中，存在多项式时间的算法的一类问题，称之为 P 类问题。

2.NP 类问题：像旅行商问题、命题表达式可满足问题，至今没有找到多项式时间算法解得一类问题，称之为 NP 类问题。

3.交互式零知识证明：是指执行协议的双方证明者 P 和验证者 V 进行有连接的通信，一方 P 执行完一步协议后，对方产生应答，P 再相应做出反应，以交互式应答的方式执行完整的协议。

4.知识签名实际上是一种数学构造，签名者通过这种数学方法，可以在不泄露秘密的情况下向其他人证明他知道这个秘密。知识签名从本质上来看是一种非交互式的零知识证明或最小泄露证明。

四、简答题

1.零知识证明：

指的是证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。证明者向验证者证明并使其相信自己知道或拥有某一消息，但证明过程不能向验证者泄漏任何关于被证明消息的信息。

2.零知识证明满足三个性质：

（1）正确性。证明者 P 无法欺骗验证者 V。换言之，若证明者 P 不知道一个定理的证明方法，则 P 使验证者 V 相信他会证明定理的概率很低。

（2）完备性。验证者 V 无法欺骗证明者 P。若 P 知道一个定理的证明方法，则 P 使 V 以绝对优势的概率相信他能证明。

（3）零知识性。验证者无法获取任何额外的知识。

3. 旅行商问题、三方匹配问题、三方满足问题、顶点覆盖问题、哈密顿回路问题等。

4.（1）V 站在 A 点。

（2）P 进入任何一点 C 或 D。

（3）当 P 进洞后，V 走向 B 点。

（4）V 叫 P:（a）从左边走出来或(b)从右边出来。

（5）P 按照要求实现（有咒语）。

（6）P 和 V 重复执行（1）~（5）共 N 次。

若 P 不知道咒语，则在 B 点，只有 50%的机会猜中 V 的要求，协议执行 n 次，则只有 2^{-n} 次机会完全猜中。此洞穴问题可以转化为数学问题，P 知道解决某个难题的秘密信息，而 V 通过与 P 交互作用验证其真伪。

第六章

一、名词解释

1、选择性泄露

2、单一数字证书内容泄露

3、多个数字证书内容泄露

4、Merkle 树

二、判断

1、选择性泄露的完整性是指：当证书持有者决定泄露证书私有属性信息的时候，泄露出来的值可以是未经认证的过的。（）

2、选择性泄露的访问控制指：从证书泄露出来的私有属性的值必须是证书持有者自己愿意泄露的。（）

3、在使用 Hash 函数的选择性泄露协议中产生随机值 rv 的目的是为了抵抗“字典攻击”。（）

4、Merkle 树的优点是：使用很少的存储空间；缺点是：效率随着字段的增加而增加。（）

5、Huffman 树需要较多的存储空间，但是效率较高。（）

三、填空题

1.选择性泄露就是在不影响双方的前提下，让证书持有者可以有选择的泄露证书和当前会话的有关信息，而隐藏无关信息，来保护双方的隐私。

2.实现数字证书的选择性泄露必须包含以下几个特性：保密性、完整性。

3 从证书包含的信息数量来看，数字证书的选择性泄露分为两种：单一数字证书内容泄露和。

4.单一数字证书的优点是，这样对证书持有者来说，管理证书比较方便，缺点是，需要考虑每个属性的安全性，而且实际验证的时候，有些信息可能会缺乏一定的。

5 多个数字证书的有点是，重点比较突出，缺点就是因为证书较多，管理起来比较麻烦，而且有时候，单个证书中也可能包含有敏感信息。当只用 Hash 函数的选择性泄露协议时，甲方认为乙方可以访问相关的信息时就把

6 和发送给乙方，乙方调用 Hash 函数，并将 Hash 后的值和证书上的信息比较。

7 Hash 函数的优点，缺点。

四、简答

1.比较 Merkle 树方案和 Huffman 树方案的优缺点。

2.比较单一数字证书内容泄露和多个数字证书内容泄露的优缺点。

五、计算

1.假定在 20 次会话中，E-mail 需要出示 20 次，姓名需要出示 12 次，性别需要出示 5 次，而生日需要出示 1 次。根据 Huffman 编码算法，画出 Huffman 树。

答案：

一、

1.在不影响通信双方会话的前提下，让证书持有者可以有选择的泄露证书和当前会话的相关信息，而隐藏无关信息，来保护双方的隐私。

2.一个整数中包含有多个属性，这些属性首先处于隐藏状态。

3.通信双方之间互相展示的证书比较多，均多于一个，而每个证书上包含的属性比较少。

4.是一个 Hash 树，每一个叶子存放经过 Hash 后的散列码 H（M），而根和内部节点的值是他们孩子相连接后的 Hash 值。

二、

1.错。必须是经过 CA 认证的。

2.对。

3.对。

4.错。随着字段的增加而下降。

5.错。需要的存储空间较少。

三、

1.通信

2.访问控制、性能、实用性

3.多个数字证书内容泄露

4.一张证书上会有很多信息、含有信息较多、权威性

5.属性单一

6.访问相关信息、相关随机数

7.算法简单实现容易、需要比较大的存储空间

四、

1. 解：Merkle 树方案的优点：无论有多少个属性，证书上只需要存放最终的 root 就可以，极大地节约了证书的存储空间；缺点：随着证书属性的增加，无关信息也就随着增加，增加了计算量，效率也就下降了。Huffman 树方案的优点：Huffman 树考虑到了每个节点出示的概率，这就使得出示概率高的节点在树中的深度要比出示概率低的节点要低，从而减少了树的搜索路径长度，提高了效率；缺点：Huffman 树构建时，每个节点的权值时根据长期统计得来的，因而在一些统计和实际并不相符合的情况下，效率不一定比 Merkle 树高。

2. 解：单一数字证书内容泄露的优点：一张证书上面含有很多信息，这样对证书持有者来说，管理证书比较方便；缺点：含有的信息比较多，需要考虑每个属性的安全性，而且实际验证的时候，有些信息可能会缺

乏一定的权威性。多个数字证书内容泄露的优点：每个证书的属性比较单一，重点比较突出；缺点：因为证书比较多，管理起来比较麻烦，而且有时候，单个证书中也可能含有敏感信息，这就还需要用到单一数字证书内容泄露来保护相关的属性。

五、

解：书 131 页图 6.7。

安全协议 第七章练习题

第七章

一、填空（每空 1 分）1.一个不可否认的签名方案有三部分组成、以及。

2.公平盲签名比盲签名增加了一个特性，即建立一个，通过可信中心的授权，签名者可追踪签名。

3.部分盲签名较好的克服了的一些固有的缺点。

4.若至多可以用来对一个消息进行签名，否则签名就可能被伪造，我们称这种签名为。

5.一次性数字签名的优点是和较快，特别适用于要求计算复杂性低的芯片卡中。

6.环签名是一种没有的类群签名方案，环中任何一个成员可以代表整个环进行签名。

7.环签名建立在的基础之上。

8.环签名具有和签名者的完美匿名性的特点。

9.不可否认签名的主要特点是没有的参与，就不能验证签名的真伪。

10.门限签名是最普通、最常用的。

11.盲签名是签名者对所签文件内容是。

二、判断（每题 1 分）1.不可否认签名和普通数字签名最本质的不同在于对于不可否认签名，在得不到签名者配合情况下其他人不能正确进行签名验证，从而可以防止非法复制和扩散签名者所签署的文件。

（）2.盲签名是指签名人不仅完成对文件的签名工作，并了解所签文件的内容。

（）3.部分盲签名这里的部分就意味着代签名的消息是由签名申请方和签名方共同生成的。

（）4.在 Rabin 的一次签名方案中签名的验证只需要签名者。

（）5.在群签名中，一旦消息被签名，除了指定的群管理者，没有人你能够确定该签名是哪个特定的群成员签署的。

（）6.环签名中有主管，需要预先建立群组以及撤销环成员等级。

（）7.环签名的签名者拥有完美匿名性。

（）8.任何人都不能区别代理人产生的代理签名和正常签名。

（）9.批签名是指能够用一次签名动作，完成对若干个不同消息的签名。

并且以后可以对每一条消息对立的进行验证。

（）10.认证加密方案不同于数字签名在于发送者完成一个认证加密签名后，除了指定的接收者之外的其他任何第三方都不能确定这个认证加密签名是发送者所签。

() 11.使用防失败-数字签名，签名者可以对自己的签名进行抵赖，

同时即使攻击者分析出密钥，也可以伪造签名者的签名。

（）12.第一个有效的失败-终止签名方案包括①构造参数②签名过程③验证过程。

（）13.在指定验证者签名中只有验证者可以验证签名的有效性，其他人都不能确信这个签名是否有效。

（）14.前向安全签名确保了泄漏秘密的时段以前的所有签名的有效性。

（）15.门限签名是最普通、最常用的群体签名。

（）

三、名词解释（每题 3 分）1.盲签名 2.群签名 3.环签名 4.代理签名 5.批验证 6.批签名 7.认证加密 8.失败—终止签名

四、简答 1.不可否认签名和普通数字签名最本质的区别在于（4 分）？ 2．盲签名与普通签名相比两个显著的特点是什么（4 分）？ 3.一个好的群签名方案需要具备哪些特点（列举 5 个以上，共 5 分）？ 4.代理签名具有哪些安全需求（5 分）？ 5.批验证签名协议基本思想是什么（5 分）?6.一个记名签名应该满足什么要求（5 分）？ 7.代理签名的

基本类型有哪些（3 分）?答案

一、填空

1、签名算法、验证协议、否认协议；

2、可信中心；

3、盲签名；

4、一次性数字签名；

5、产生、证实；

6、管理者；

7、公钥密码体制；

8、无须设置；

9、签名者；

10、群体签名；

11、不知道的；

二、判断 1—5√×√×√6—10×√×√√11—15×√√√√

三、名词解释 1.盲签名指签名人只是完成对文件的签名工作，并不了解所签文件的内容。

2.群签名在群签名方案中，群的成员可以代表群进行签名，签名可用单一的群公开密钥验证。

一旦消息被签名，除了指定的群管理者，没有人能够确定该签名是哪个特定的群成员签署的。

3.环签名环签名方案是一种没有管理者的类群签名方案，环中任何一个成员都可以代表整个环进行签名，而验证者只知道签名这个环，但不知道谁才是真正的签名者。

4.代理签名指当某个签名者（原是签名者）由于某种原因不能签名时，将签名权委派给他人（代理签名者）代替自己行使签名权。

5.批验证将多个签名由同一个签名者签发的放在一起，形成一个“批”，对该批进行验证，如果该批通过验证，则接受该批中的所有签名，否则，拒绝批中所有签名。

6.批签名指能够用一次签名动作，完成对若干个不同的消息的签名，并且以后可以对每条消息独立的进行认证。

7.认证加密只有指定接受者能够恢复出消息，然后对消息进行验证，从而可以保护消息免泄漏。

8.失败—终止签名是一种经过强化安全性的数字签名，用以防范强大计算资源的攻击者。

四、简答 1．对于不可否认签名，在得不到签名者配合的情况下其他人不能正确进行签名验证，从而可以防止非法复制和扩散签名者所属的文件。

2．

（1）签名者不知道自己所签署的数据内容；

（2）在签名被签名申请者泄漏后，签名者不能追踪签名。

3．正确性、匿名性、不可伪造性、不可关联性、可跟踪性、抗合谋攻击性、防陷害攻击。

4．安全需求不可伪造性、可验证性、可鉴别性、不可否认性、可区别性。

5．批验证签名协议基本思想是将多个签名由同一个签名者签发的放在一起，形成一个“批”，对该批进行验证，如果该批通过验证，则接受该批中的所有签名，否则，拒绝批中所有签名。

6．只有被记名者才能验证记名者生成的签名（即使记名者也无法验证签名)；只有被记名者才能向第三方证明签名是由记名者生成的签名，并且签名是有效的（即使记名者也无法证明签名是有效的)。

7.基本类型完全委托型、部分委托型、带委任状的委托型。

内容仅供参考