1．是非判断题

(1) 密码协议的执行者必须了解协议，并同意且遵循它来完成所有步骤。(V)

(2) 密码协议的公平性通常采用“分割和选择”技术来实现的。(V)

(3) 零知识证明是指证明者能够在不向验证者提供任何有用信息的情况下，使验证者相信某个论断是正确的。(V)

(4) 零知识证明是一种理想的密码协议，实际应用中很难实现。(X)

(5) 在比特承诺协议中，一旦 Alice 向 Bob 承诺，Bob 就知道这个承诺的内容，只是这个承诺是不能更改。(X) 注：公开后 Bob 才知道

(6) 基于对称加密体制的比特承诺协议中，两个随机数可以都由 Alice 选取，Alice 在承诺阶段传给 Bob 一个，揭示承诺时提供另一个。(X) 注：双方各选一个随机数

(7) 一个公平掷币协议要保证对弈双方 Alice 和 Bob 各有 50%的机会获胜，而对弈方的欺骗行为需要可信第三方介入才能被揭示。(X) 注：不需要可信第三方

(8) 公平掷币协议是一个不经意传送协议的应用举例。(V)

(9) 安全多方计算起源于图灵奖获得者姚启智(Andrew C. Yao)先生于 1982 年提出的百万富翁问题。(V)

(10) 安全多方计算是指在一个互不信任的多用户网络中，参与的多用户需要可信第三方参与才能完成既可靠又能保护用户隐私的计算任务。(X) 注：不需要可信第三方

(11) 电子现金系统的不可跟踪性是指银行和商店合谋都不能跟踪用户的消费情况。(V)

(12) 由于有效的电子货币是可以复制的，所以，电子现金方案是无法阻止多重花费的行为。(X)

(13) 电子投票的匿名性是指除了统计者外任何人都不能将选票和投票人对应起来以确定某个投票人所投选票的具体内容。(X)

(14) 电子投票的可验证性是指任何投票人都可以检查自己的投票是否被正确统计，以及其他任何关心投票结果的人都可以验证统计结果的正确性。(V)

(15) 可信赖的第三方在一个拍卖系统中是一个不可或缺的组成部分，但在拍卖过程中，它一般不参与，只有出现纠纷时才介入。(V)

(16) 拍卖系统的匿名性是指在整个过程中都不能泄露投标者的身份，即使投标者中标也不能。(X) 注：揭示中标者身份并能被验证

(17) 拍卖系统的同一拍卖投标中，投标者的多次标价不能关联到同一投标者。(V)

(18) (X)

2．选择题

(1) 密码协议使用“分割和选择”技术来实现 (C) 性。

A. 验证　B. 完整　C. 公平　D. 匿名

(2) 用户在使用应用系统之前首先要执行身份识别协议，而这个协议一般应满足(B)。

A. 不经意传输　B. 零知识证明　C. 安全多方计算　D. 比特承诺

(3) 图灵奖获得者姚启智(Andrew C. Yao)先生于 1982 年提出了百万富翁问题而引出 (C) 理论。

A. 不经意传输　B. 零知识证明　C. 安全多方计算　D. 比特承诺

(4) 在计算机网络中，彼此互不信任的通信双方若要求签署一项合同时，最有可能用到下面哪个协议。（ D ）

A. 不经意传输　B. 零知识证明　C. 安全多方计算　D. 比特承诺

(5) 在计算机网络中，一场比赛或游戏需要对弈双方中一方首先开始，这就涉及到谁有这个优先权的问题，而解决的方式常通过（ A ）来实现。

A. 不经意传输　B. 零知识证明　C. 安全多方计算　D. 比特承诺

(6) 在计算机网络中，假设某公司的n个职员想了解他们每月的平均薪水有多少？但是每个职员又不想让任何其它人知道自己的薪水，那么最有可能用到下面哪个协议。（ C ）

A. 不经意传输　B. 零知识证明　C. 安全多方计算　D. 比特承诺

(7) 在电子投票中，为了实现投票者所投票内容的匿名性，最有可能使用的签名方案是（ D ）。

A. 代理签名　B. 群签名　C. 多重签名　D. 盲签名

(8) 在电子投票中，下列哪种舞弊协议将不会被发现。（ D ）

A. 记票者假装没有收到选票而将有效选票丢弃。

B. 记票者和管理者联合进行舞弊。

C. 投票者和管理者联合进行舞弊。

D. 管理者在有投票人弃权的情况下舞弊。

(9) 在电子拍卖中，只有注册的竞拍者能够出价，未中标时实现竞拍者身份的匿名性，为实现这个目标，最有可能使用的签名方案是（ D ）。

A. 代理签名　B. 群签名　C. 多重签名　D. 盲签名

(10) 在电子拍卖中，（ C ）的参与才能揭示中标者的身份。

A. 拍卖管理员　B. 注册管理员　C. 注册管理员和拍卖管理员　D. 不需要任何人

(11) 一般而言，电子现金是（ B ）的电子支付。

A. 在线、即付型　B. 离线、可转换支付

C. 离线、无匿名支付　D. 后付型、匿名支付

(12) 电子现金系统的匿名性包括不可跟踪性和不可联系性，为实现这个目标，最有可能使用的签名方案是（ B ）。

A. 普通数字签名　B. 强盲签名　C. 弱盲签名　D. 部分盲签名

3．填空题

(1) 密码协议必须是清楚的，“清楚”的含义是_协议中每一步必须明确，不存在歧义_；密码协议必须是完整的，“完整”的含义是_协议中每种可能情况必须规定具体动作_。

(2) 零知识证明分为_完全_零知识证明、_计算_零知识证明和_统计_零知识证明三类。

(3) Schnorr 身份认证协议效率高的主要原因是 _无需多次重复执行证明与验证协议_。

(4) 比特承诺协议必须具有以下两个安全性质：__隐蔽性__和__绑定性__。

(5) Blum 不经意传送协议中选取的大素数 p 和 q 必须满足 $p,q \equiv 3 \pmod 4$，其原因是：_求 x^2=a mod p 和 x^2=a mod q 的根相对容易_。

(6) 一个公平掷币协议至少要满足以下 3 个条件：_对弈双方各有 50%机会获胜_和_对弈

双方有任一方出现欺骗则规定欺骗方失败_、_协议结束后对弈双方都知道结果是否公平_。

(7) 一个安全多方计算协议要满足以下 3 个条件：_参与者诚实输入他的秘密值_和_保证参与者输入值的安全性_、_非参与者或参与者合谋都不能破坏协议的安全性_。

(8) 电子现金系统由_取款协议_、_支付协议_和_存款协议_三个协议组成。

(9) 电子现金系统的安全性主要指电子现金的_不可伪造性_和_不可重用性_，它的匿名性包括_不可跟踪性_和_不可关联性_。

(10) 一般而言，电子投票包含三个步骤：_注册_、_投票_和_计票_。

(11) 电子投票有多种安全要求，其中，“所有的选票都是保密的，任何人都不能将选票和投票人对应起来以确定某个投票人所投选票的具体内容” 是指_匿名性_；“任何投票人都可以检查自己的投票是否被正确统计，以及其他任何关心投票结果的人都可以验证统计结果的正确性”是_公开可验证_性。

(12) 一个电子拍卖系统通常主要由参与人员、_布告栏_和_保密数据库_等部分组成，其参与人员主要包括_注册管理员_、_拍卖管理员_和_投标者_三类。

(13) 电子拍卖的安全特性很多，其中，标价不能泄露投标者身份的特性称为_匿名性_，能追踪最后获胜投标者的特性称为_可追踪性_。

4．术语解释

(1) 密码协议

(2) 分割和选择协议

(3) 零知识证明

(4) 比特承诺协议

(5) 不经意传送协议

(6) 公平掷币协议

(7) 安全多方计算协议