一题目

三重DES 加密使用（ ）个密钥对明文进行 3 次加密，其密钥长度为（ ）位。

问题1选项
A.1
B.2
C.3
D.4

问题2选项
A.56
B.112
C.128
D.168

答案

第1题:B

第2题:B

解析

https://www.educity.cn/tiku/91629.html

3DES算法：密码学中，3DES是三重数据加密算法通称。它相当于是对每个数据块用二个密钥应用三次DES加密算法。由于计算机运算能力的增强，原版DES密码的密钥长度变得容易被暴力破解；3DES即是设计用来提供一种相对简单的方法，即通过增加DES的密钥长度来避免类似的攻击，而不是设计一种全新的块密码算法。密钥长度是112位。

二题目

DES是一种（ ）加密算法，其密钥长度为56位，3DES是基于DES的加密方式，对明文进行3次DES操作，以提高加密强度，其密钥长度是（ ）位。

问题1选项
A.共享密钥
B.公开密钥
C.报文摘要
D.访问控制

问题2选项
A.56
B.112
C.128
D.168

答案

第1题:A

第2题:B

解析

DES算法：加密前，对明文进行分组，每组64位数据，对每一个64位的数据进行加密，产生一组64位的密文，最后把各组的密文串接起来，得出整个密文，其中密钥为64位（实际56位，有8位用于校验）
DES算法：密码学中，3DES是三重数据加密算法通称。它相当于是对每个数据块应用三次DES加密算法（第一次和第三次密钥一样，所以认为密钥长度是112位。）

三题目

3DES的密钥长度为（ ）。

问题1选项
A.56
B.112
C.128
D.168

答案

B

解析

三重DES是DES的改进算法，它使用两把密钥对报文做三次DES加密，效果相当于将DES密钥的长度加倍，客服可DES长度较短的缺点。

本来应该使用3个不同的密钥进行三次加密，这样就可以把密钥的长度加长到3 * 56 =158位。但许多密码设计者认为168位的密钥已经超过实际需要，所以便在第一层和第三层使用了相同的密钥。之所以没有直接使用两重DES，是因为第二层DES不是十分安全，它对一种称为“中间可遇”的密码分析攻击极为脆弱，所以最终使用了两个密钥的三重DES加密操作。

四题目

某Web网站向CA申请了数字证书。用户登录该网站时，通过验证 （） ，可确认该数字证书的有效性，从而 （）。

问题1选项
A.CA的签名
B.网站的签名
C.会话密钥
D.DES密码

问题2选项
A.向网站确认自己的身份
B.获取访问网站的权限
C.和网站进行双向认证
D.验证该网站的真伪

答案

第1题:A

第2题:D

解析

数字证书能够验证一个实体身份，而这是在保证数字证书本身有效性这一前提下才能够实现的。验证数字证书的有效性是通过验证颁发证书的CA的签名实现的。

五题目

数字签名首先需要生成消息摘要，然后发送方用自己的私钥对报文摘要进行加密， 接收方用发送方的公钥验证真伪。生成消息摘要的目的是（ ），对摘要进行加密的目的是（ ）。

问题1选项
A.防止窃听
B.防止抵赖
C.防止篡改
D.防止重放

问题2选项
A.防止窃听
B.防止抵赖
C.防止篡改
D.防止重放

答案

第1题:C

第2题:B

解析

https://www.educity.cn/tiku/455089.html

消息摘要是对原文信息提取特征值，做这个操作，当原始信息被篡改时，我们能及时感知到，所以能防止篡改。

而对消息摘要“加密”，虽然做的是加密操作，但并无加密的作用。因为私钥加密时，公钥解密。公钥谁都能获取到，所以谁都能解，故无法防止窃听，但可以防止抵赖。 所以对摘要进行加密的目的是防止抵赖。

六题目

以下关于第三方认证服务的叙述中，正确的是（ ）。

问题1选项
A.Kerberos认证服务中保存数字证书的服务器叫CA
B.第三方认证服务的两种体制分别是Kerberos和PKI
C.PKI体制中保存数字证书的服务器叫KDC
D.Kerberos的中文全称是“公钥基础设施”

答案

B

解析

https://www.educity.cn/tiku/74380.html

目前最常用的第三方认证服务包括：PKI/CA 和Kerberos。PKI/CA是基于非对称密钥体系的，Kerberos是基于对称密钥体系的。
PKI （ Public Key Infrastructure ）指的是公钥基础设施。 CA （ Certificate Authority ）指的是认证中心。 PKI 从技术上解决了网络通信安全的种种障碍。 CA从运营、管理、规范、法律、人员等多个角度来解决网络信任问题。由此，人们统称为“PKI/CA ”。从总体构架来看， PKI/CA 主要由最终用户、认证中心和注册机构来组成。
Kerberos 是一种网络认证协议，其设计目标是通过密钥系统为客户机 / 服务器应用程序提供强大的认证服务。该认证过程的实现不依赖于主机操作系统的认证，无需基于主机地址的信任，不要求网络上所有主机的物理安全，并假定网络上传送的数据包可以被任意地读取、修改和插入数据。在以上情况下， Kerberos 作为一种可信任的第三方认证服务，是通过传统的密码技术（如：共享密钥）执行认证服务的。
认证过程具体如下：客户机向认证服务器（AS）发送请求，要求得到某服务器的证书，然后 AS 的响应包含这些用客户端密钥加密的证书。证书的构成为： 1） 服务器 “ticket” ； 2） 一个临时加密密钥（又称为会话密钥 “session key”） 。客户机将 ticket （包括用服务器密钥加密的客户机身份和一份会话密钥的拷贝）传送到服务器上。会话密钥可以（现已经由客户机和服务器共享）用来认证客户机或认证服务器，也可用来为通信双方以后的通讯提供加密服务，或通过交换独立子会话密钥为通信双方提供进一步的通信加密服务。
KDC（密码学中的密钥分发中心）是密钥体系的一部分，旨在减少密钥体制所固有的交换密钥时所面临的风险。
KDC在kerberos中通常提供两种服务：Authentication Service （AS）认证服务和Ticket-Granting Service （TGS）：授予票据服务。

七题目

完整的信息安全系统至少包含三类措施，即技术方面的安全措施、管理方面的安全措施和相应的（ ）。其中，信息安全的技术措施主要有：信息加密、数字签名、身份鉴别、访问控制、网络控制技术、反病毒技术、（ ）。

问题1选项
A.用户需求
B.政策法律
C.市场需求
D.领域需求

问题2选项
A.数据备份和数据测试
B.数据迁移和数据备份
C.数据备份和灾难恢复

D.数据迁移和数据测试

答案

第1题:B

第2题:C

解析

https://www.educity.cn/tiku/60098222.html

一个完整的信息安全系统至少包含三类措施：技术方面的安全措施，管理方面的安全措施和相应的政策法律。

信息安全技术涉及到信息传输的安全、信息存储的安全以及对网络传输信息内容的审计三方面，当然也包括对用户的鉴别和授权。

信息安全的技术措施主要有：信息加密、数字签名、身份鉴别、访问控制、网络控制技术、反病毒技术、数据备份和灾难恢复。

实现安全管理，应有专门的安全管理机构；有专门的安全管理人员；有逐步完善的管理制度；有逐步提供的安全技术设施。 信息安全管理主要涉及以下几个方面：人事管理：设备管理；场地管理；存储媒体管理；软件管理；网络管理；密码和密钥管理。 国内的相关法规：中华人民共和国计算机安全保护条例、中华人民共和国商用密码条例 中华人民共和国计算机信息网络国际联网管理暂行办法、关于对与国际联网的计算机信息系统进行备案工作的通知、计算机信息网络国际联网安全保护管理办法等。

八题目

在进行软件系统安全性分析时，（）保证信息不泄露给未授权的用户、实体或过程；完整性保证信息的完整和准确，防止信息被非法修改；（）保证对信息的传播及内容具有控制的能力，防止为非法者所用。

问题1选项
A.完整性
B.不可否认性
C.可控性
D.机密性

问题2选项
A.完整性
B.安全审计
C.加密性
D.可控性

答案

第1题:D

第2题:D

解析

https://www.educity.cn/tiku/60098386.html

安全性(security）是指系统在向合法用户提供服务的同时能够阻止非授权用户使用的企图或拒绝服务的能力。

安全性又可划分为机密性（信息不泄露给未授权的用户、实体或过程）、完整性（保证信息的完整和准确，防止信息被篡改）、不可否认性（不可抵赖，即由于某种机制的存在，发送者不能否认自己发送信息的行为和信息的内容。）及可控性（对信息的传播及内容具有控制的能力，防止为非法者所用）等特性。

九题目

信息系统面临多种类型的网络安全威胁。其中，信息泄露是指信息被泄露或透露给某个非授权的实体；（）是指数据被非授权地进行增删、修改或破坏而受到损失；（）是指对信息或其他资源的合法访问被无条件地阻止；（）是指通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究，从而发现有价值的信息和规律。

问题1选项
A.非法使用
B.破坏信息的完整性
C.授权侵犯
D.计算机病毒

问题2选项
A.拒绝服务
B.陷阱门
C.旁路控制
D.业务欺骗

问题3选项
A.特洛伊木马
B.业务欺骗
C.物理侵入
D.业务流分析

答案

第1题:B

第2题:A

第3题:D

解析

https://www.educity.cn/tiku/60171741.html

网络安全威胁根据威胁根据其性质，可以归结为下面一些类型：
信息泄露：信息泄露是指信息被泄露给某个非授权的实体。
破坏信息的完整性：只有得到允许的人才能够修改数据，保证数据的一致性，防止数据被非法用户进行篡改。
拒绝服务：这种类型的网络安全威胁是指黑客使用分布式拒绝服务攻击，使目标服务器过度负荷，导致网络服务停止运行。
业务流分析：通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究，从中发现有价值的信息和规律。
假冒：通过欺骗通信系统或用户，达到将非法用户冒充成为合法用户或者特权小的用户冒充成为特权大的用户的目

的。黑客大多采用假冒攻击。

十题目

安全性是根据系统可能受到的安全威胁的类型来分类的。其中，（ ）保证信息不泄露给未授权的用户、实体或过程；（ ）保证信息的完整和准确，防止信息被篡改。

问题1选项
A.可控性
B.机密性
C.安全审计
D.健壮性

问题2选项
A.可控性
B.完整性
C.不可否认性
D.安全审计

答案

第1题:B

第2题:B

十一题目

以下关于区块链应用系统中“挖矿”行为的描述中，错误的是（）。

问题1选项
A.矿工“挖矿”取得区块链的记账权，同时获得代币奖励
B.“挖矿”本质上是在尝试计算一个Hash碰撞
C.“挖矿”是一种工作量证明机制
D.可以防止比特币的双花攻击

答案

D

解析

比特币网络通过“挖矿”来生成新的比特币。所谓“挖矿”实质上是用计算机解决一项复杂的数学问题，来保证比特币网络分布式记账系统的一致性。比特币网络会自动调整数学问题的难度，让整个网络约每10分钟得到一个合格答案。随后比特币网络会新生成一定量的比特币作为区块奖励，奖励获得答案的人。A选项正确。
本质上，挖矿的过程就是计算哈希函数，并以此来确认交易的过程。哈希函数值具有不可篡改、不可逆性。但哈希函数输入的原始数据长度是不定长的，可以随意长度，而得出的摘要值是固定长度的。因此，存在一个可能，同样一个哈希值对应的不止一个数据串。这个现象就是哈希碰撞。B选项正确。
工作量证明机制（PoW）是我们最熟知的一种共识机制。工作量证明机制PoW就是工作越多，收益越大。这里的工作就是计算出一个满足规则的随机数，谁能最快地计算出唯一的数字，谁就能做信息公示人。C选项正确。

“双花”问题是指一笔数字现金在交易中被反复使用的现象。传统的加密数字货币和其他数字资产，都具有无限可复制性，人们在交易过程中，难以确认这笔数字现金是否已经产生过一次交易。在区块链技术中，中本聪通过对产生的每一个区块盖上时间戳（时间戳相当于区块链公证人）的方式保证了交易记录的真实性，保证每笔货币被支付后，不能再用于其他支付。在这个过程中，当且仅当包含在区块中的所有交易都是有效的且之前从未存在过的，其他节点才认同该区块的有效性。所以双花攻击解决的方法就是通过时间戳。用户发起的每一笔交易都有时间记录，“挖矿”行为不能防止双花攻击，D选项错误。

十二题目

在网络操作系统环境中，当用户A的文件或文件夹被共享时，（ ），这是因为访问用户A的计算机或网络的人（ ）。

问题1选项
A.其安全性与未共享时相比将会有所提高
B.其安全性与未共享时相比将会有所下降
C.其可靠性与未共享时相比将会有所提高
D.其方便性与未共享时相比将会有所下降

问题2选项
A.只能够读取，而不能修改共享文件夹中的文件
B.可能能够读取，但不能复制或更改共享文件夹中的文件
C.可能能够读取、复制或更改共享文件夹中的文件

答案

第1题:B

第2题:C

解析

https://www.educity.cn/tiku/86857.html

在操作系统中，用户A可以共享存储在计算机、网络和Web上的文件和文件夹，但当用户A共享文件或文件夹时，其安全性与未共享时相比将会有所下降，这是因为访问用户A的计算机或网络的人可能能够读取、复制或更改共享文件夹中的文件。

十三题目

安全攸关系统在软件需求分析阶段，应提出安全性需求。软件安全性需求是指通过约束软件的行为，使其不会出现（ ）。软件安全需求的获取是根据已知的（ ），如软件危害条件等以及其他一些类似的系统数据和通用惯例，完成通用软件安全性需求的裁剪和特定软件安全性需求的获取工作。

问题1选项
A.不可接受的系统安全的行为
B.有可能影响系统可靠性的行为
C.不可接受的违反系统安全的行为
D.系统不安全的事故

问题2选项
A.系统信息
B.系统属性
C.软件属性
D.代码信息

答案

第1题:C

第2题:A

解析

https://www.educity.cn/tiku/20994405.html

安全攸关系统：是指系统失效会对生命或者健康构成威胁的系统，存在于航空、航天、汽车、轨道交通等领域，对安全性要求很高。
通常在需求分析阶段就必须考虑安全性需求了。
安全性需求：是指通过约束软件的行为，使其不会出现不可接受的违反系统安全的行为需求。所以第一空选择C选项。选项A中，不会出现系统安全的行为，这种说法本身就是错误的；B选项是对可靠性的说明；D选项事故是系统不安全的后果。
需求本身就是根据已知的系统信息来进行获取的，所以第二空选择A选项，系统信息。

十四题目

SYN Flooding攻击的原理是（）。

问题1选项
A.利用TCP三次握手，恶意造成大量TCP半连接，耗尽服务器资源，导致系统拒绝服务
B.操作系统在实现TCP/IP协议栈时，不能很好地处理TCP报文的序列号紊乱问题，导致系统崩溃
C.操作系统在实现TCP/IP协议栈时，不能很好地处理IP分片包的重叠情况，导致系统崩溃
D.操作系统协议栈在处理IP分片时，对于重组后超大的IP数据包不能很好地处理，导致缓存溢出而系统崩溃

答案

A

解析

SYN Flood攻击利用TCP三次握手的一个漏洞向目标计算机发动攻击。攻击者向目标计算机发送TCP连接请求（SYN报文），然后对于目标返回的SYN-ACK报文不作回应。目标计算机如果没有收到攻击者的ACK回应，就会一直等待，形成半连接，直到连接超时才释放。攻击者利用这种方式发送大量TCP SYN报文，让目标计算机上生成大量的半连接，迫使其大量资源浪费在这些半连接上。目标计算机一旦资源耗尽，就会出现速度极慢、正常的用户不能接入等情况。攻击者还可以伪造SYN报文，其源地址是伪造的或者不存在的地址，向目标计算机发起攻击。SYN Flooding攻击与TCP报文的处理过程没有很大的关系。

十五题目

流量分析属于（ ）方式。

问题1选项
A.被动攻击
B.主动攻击
C.物理攻击
D.分发攻击

答案

A

解析

https://www.educity.cn/tiku/89797.html

计算机网络上的通信面临以下四种威胁：
（1）截获：攻击者从网络上窃听他人的通信内容。
（2）中断：攻击者有意中断他人在网络上的通信。
（3）篡改：攻击者故意篡改网络中传送的报文。
（4）伪造：攻击者伪造信息在网络上的传送。
以上的四种威胁可以划分为两大类，即被动攻击和主动攻击。在上述情况中，截获信息的攻击属于被动攻击，而中断、篡改和伪造信息的攻击称为主动攻击。

十六题目

采用Kerberos系统进行认证时，可以在报文中加入（ ）来防止重放攻击。

问题1选项
A.会话密钥
B.时间戳
C.用户ID
D.私有密钥

答案

B

解析

重放攻击（Replay Attacks）又称重播攻击、回放攻击或新鲜性攻击（Freshness Attacks），是指攻击者发送一个目的主机已接收过的包，来达到欺骗系统的目的，主要用于身份认证过程，破坏认证的正确性。
Kerberos系统采用的是时间戳方案来防止重放攻击，这种方案中，发送的数据包是带时间戳的，服务器可以根据时间戳来判断是否为重放包，以此防止重放攻击。

十七题目

（ ）针对TCP连接进行攻击。

问题1选项
A.拒绝服务
B.暴力攻击
C.网络侦察
D.特洛伊木马

答案

A

解析

Syn flooding是利用TCP连接进行的拒绝服务攻击。