2020 年下半年信息安全工程师《综合知识》真题答案及解析

本资料由信管网(www.cnitpm.com)整理发布，供信管网学员使用！

信管网是专业软考中高级与 PMP 考试培训服务网站。提供了考试资讯、考试报名、成绩查询、资料下载、在线答题、考试培训、项目管理人才交流、企业内训等服务。

信管网资料库提供了备考软考的精品学习资料；信管网案例分析频道和论文频道拥有丰富的案例范例和论文范例，信管网考试中心拥有软考中高级历年真题和超过 5000 多道试题免费在线测试；信管网每年指导考生超 100000+人。

信管网——专业、专注、专心，成就你的项目管理师梦想！

信管网：www.cnitpm.com

信管网考试中心：www.cnitpm.com/exam/

信管网培训中心：www.cnitpm.com/wx/

信管网微信公众号

信管网客服微信号

1、2019 年 10 月 26 日，十三届全国人大常委会第十四次会议表决通过了《中华人民共和国密码法》，该法律自（）起施行。

A.2020 年 10 月 1 日

B.2020 年 12 月 1 日

C.2020 年 1 月 1 日

D.2020 年 7 月 1 日

信管网参考答案：C

查看解析：www.cnitpm.com/st/5017117038.html

2、根据自主可控的安全需求，近些年国密算法和标准体系受到越来越多的关注，基于国密算法的应用也得到了快速发展。我国国密标准中的杂凑算法是()

A.SM2

B.SM3

C.SM4

D.SM9

信管网参考答案：B

查看解析：www.cnitpm.com/st/501729236.html

3、信息安全产品通用评测标准 ISO/IEC 15408 一 1999《信息技术、安全技术、信息技术安全性评估准则》(简称 CC)，该标准分为三个部分：第 1 部分“简介和一般模型”、第 2 部分“安全功能要求”和第 3 部分“安全保证要求”，其中（）属于第 2 部分的内容。

A.评估保证级别

B.基本原理

C.保护轮廓

D.技术要求

信管网参考答案：D

查看解析：www.cnitpm.com/st/5017318583.html

4、从网络安全的角度看，网络安全防护系统的设计与实现必须遵守一些基本原则，其中要求网

络安全防护系统是一个多层安全系统，避免成为网络中的“单失效点”，要部署有多重防御系统，该原则是（）

A.纵深防御原则

B.木桶原则

C.最小特权原则

D.最小泄露原则

信管网参考答案：A

查看解析：www.cnitpm.com/st/5017419230.html

5、为确保关键信息基础设施供应链安全，维护国家安全，依据（），2020 年 4 月 27 日，国家互联网信息办公室等 12 个部门联合发布了《网络安全审查办法》，该办法自 2020 年 6 月 1 日实施，将重点评估采购网络产品和服务可能带来的国家安全风险。

A.《中华人民共和国国家安全法》和《中华人民共和国网络安全法》

B.《中华人民共和国国家保密法》和《中华人民共和国网络安全法》

C.《中华人民共和国国家安全法》和《网络安全等级保护条例》

D.《中华人民共和国国家安全法》和《中华人民共和国国家保密法》

信管网参考答案：A

查看解析：www.cnitpm.com/st/5017515860.html

6、密码学根据研究内容可以分为密码编制学和密码分析学。研究密码编制的科学称为密码编制学，研究密码破译的科学称为密码分析学。密码分析学中，根据密码分析者可利用的数据资源，可将攻击密码的类型分为四类，其中适于攻击计算机文件系统和数据库系统的是（）。

A.仅知密文攻击

B.已知明文攻击

C.选择明文攻击

D.选择密文攻击

信管网参考答案：C

查看解析：www.cnitpm.com/st/501762646.html

7、以下关于认证和加密的表述中，错误的是（）

A.加密用以确保数据的保密性

B.认证用以确保报文发送者和接收者的真实性

C.认证和加密都可以阻止对手进行被动攻击

D.身份认证的目的在于识别用户的合法性，阻止非法用户访问系统

信管网参考答案：C

查看解析：www.cnitpm.com/st/5017719556.html

8、为了保护用户的隐私，需要了解用户所关注的隐私数据。当前，个人隐私信息分为一般属性、标识属性和敏感属性，以下属于敏感属性的是（）。

A.姓名

B.年龄

C.肖像

D.财物收入

信管网参考答案：D

查看解析：www.cnitpm.com/st/501782602.html

9、访问控制是对信息系统资源进行保护的重要措施，适当的访问控制能够阻止未经授权的用户有意或者无意地获取资源。计算机系统中，访问控制的任务不包括（） 。

A.审计

B.授权

C.确定存取权限

D.实施存取权限

信管网参考答案：A

查看解析：www.cnitpm.com/st/501797488.html

10、一台连接在以太网内的计算机为了能和其他主机进行通信，需要有网卡支持。网卡接收数据帧的状态有：unicast、broadcast、multicast、promiscuous 等，其中能接收所有类型数据帧的状态是（）

A.unicast

B.broadcast

C.multicast

D.promiscuous

信管网参考答案：D

查看解析：www.cnitpm.com/st/5018010617.html

11、数字签名是对以数字形式存储的消息进行某种处理，产生一种类似于传统手书签名功效的信息处理过程，一个数字签名体制包括：施加签名和验证签名。其中 SM2 数字签名算法的设计是基于（）。

A.背包问题

B.椭圆曲线问题

C.大整数因子分解问题

D.离散对数问题

信管网参考答案：B

查看解析：www.cnitpm.com/st/5018123810.html

12、由于 Internet 规模太大，常把它划分成许多小的自治系统，通常把自治系统内部的路由协议称为内部网关协议，自治系统之间的协议称为外部网关协议。以下属于外部网关协议的是（）。

A.RIP

B.OSPF

C.BGP

D.UDP

信管网参考答案：C

查看解析：www.cnitpm.com/st/5018223980.html

13、Sniffer 可以捕获到达主机端口的网络报文。Sniffer 分为软件和硬件两种，以下工具属于硬件的是（）

A.NetXray

B.Packetboy

C.Netmonitor

D.协议分析仪

信管网参考答案：D

查看解析：www.cnitpm.com/st/5018311798.html

14、所有资源只能由授权方或以授权的方式进行修改，即信息未经授权不能进行改变的特性是指信息的（）。

A.完整性

B.可用性

C.保密性

D.不可抵赖性

信管网参考答案：A

查看解析：www.cnitpm.com/st/5018424799.html

15、在 Widows 操作系统下，要获取某个网络开放端口所对应的应用程序信息，可以使用命令（）。

A.ipconfig

B.traceroute

C.netstat

D.nslookup

信管网参考答案：C

查看解析：www.cnitpm.com/st/5018523495.html

16、报文内容认证使接收方能够确认报文内容的真实性，产生认证码的方式不包括（）.

A.报文加密

B.数字水印

C.MAC

D.HMAC

信管网参考答案：B

查看解析：www.cnitpm.com/st/5018617837.html

17、VPN 即虚拟专用网，是一种依靠 ISP 和其他 NSP 在公用网络中建立专用的、安全的数据通信通道的技术。以下关于虚拟专用网 VPN 的描述中，错误的是（） 。

A.VPN 采用隧道技术实现安全通信

B.第 2 层隧道协议 L2TP 主要由 LAC 和 LNS 构成

C.IPSec 可以实现数据的加密传输

D.点对点隧道协议 PPTP 中的身份验证机制包括 RAP、CHAP、MPPE

信管网参考答案：D

查看解析：www.cnitpm.com/st/501879678.html

18、雪崩效应指明文或密钥的少量变化会引起密文的很大变化。下列密码算法中不具有雪崩效应的是（）

A.AES

B.MD5

C.RC4

D.RSA

信管网参考答案：D

查看解析：www.cnitpm.com/st/5018824746.html

19、移动终端设备常见的数据存储方式包括：①Shared Preferences； ②文件存储； ③SQLite 数据库； ④Content Provider； ⑤网络存储。Android 系统支持的数据存储方式包括（）。

A.①②③④⑤

B.①③⑤

C.①②④⑤

D.②③⑤

信管网参考答案：A

查看解析：www.cnitpm.com/st/501897527.html

20、数字水印技术通过在数字化的多媒体数据中嵌入隐蔽的水印标记，可以有效实现对数字多媒体数据的版权保护等功能。数字水印的解释攻击是以阻止版权所有者对所有权的断言为攻击目的。以下不能有效解决解释攻击的方案是（）

A.引入时间戳机制

B.引入验证码机制

C.作者在注册水印序列的同时对原作品加以注册

D.利用单向水印方案消除水印嵌入过程中的可逆性

信管网参考答案：B

查看解析：www.cnitpm.com/st/5019022722.html

21、僵尸网络是指采用一种或多种传播手段， 将大量主机感染 bot 程序， 从而在控制者和被感染主机之间形成的一个可以一对多控制的网络。以下不属于低尸网络传播过程常见方式的是（）

A.主动攻击漏洞

B.恶意网站脚本

C.字典攻击

D.邮件病毒

信管网参考答案：C

查看解析：www.cnitpm.com/st/501914322.html

22、计算机取证分析工作中常用到包括密码破译、文件特征分析技术、数据恢复与残留数据分析、日志记录文件分析、相关性分析等技术，其中文件特征包括文件系统特征、文件操作特征、文件格式特征、代码或数据特征等。某单位网站被黑客非法入侵并上传了 Webshell，作为安全运维人员应首先从（）入手。

A.Web 服务日志

B.系统日志

C.防火墙日志

D.交换机日志

信管网参考答案：A

查看解析：www.cnitpm.com/st/501929066.html

23、操作系统的安全机制是指在操作系统中利用某种技术、某些软件来实施一个或多个安全服务的过程。操作系统的安全机制不包括（）。

A.标识与鉴别机制

B.访问控制机制

C.密钥管理机制

D.安全审计机制

信管网参考答案：C

查看解析：www.cnitpm.com/st/5019321927.html

24、恶意代码是指为达到恶意目的而专门设计的程序或代码，恶意代码的一般命名格式为：<恶意代码前缀>.<恶意代码名称>.<恶意代码后缀>，常见的恶意代码包括：系统病毒、网络蠕虫、特洛伊木马、宏病毒、后门程序、脚本病毒、捆绑机病毒等。以下属于脚本病毒前缀的是（）。

A.Worm

B.Trojan

C.Binder

D.Script

信管网参考答案：D

查看解析：www.cnitpm.com/st/5019425280.html

25、蜜罐技术是一种主动防御技术，是入侵检测技术的一个重要发展方向。蜜罐有四种不同置方式：诱骗服务、弱化系统、强化系统和用户模式服务器，其中在特定 IP 服务端口进行侦听并对其他应用程序的各种网络请求进行应答，这种应用程序属于（）

A.诱骗服务

B.弱化系统

C.强化系统

D.用户模式服务器

信管网参考答案：A

查看解析：www.cnitpm.com/st/5019521434.html

26、 已知 DES 算法 S 盒如下， 如果该 S 盒的输入为 001011， 则其二进制输出为（）

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

A.1011

B.1100

C.0011

D.1101

信管网参考答案：B

查看解析：www.cnitpm.com/st/5019628722.html

27、域名系统 DNS 的功能是把 Internet 中的主机域名解析为对应的 IP 地址，目前顶级域名(TLD)有国家顶级域名、国际顶级域名、通用顶级域名三大类。最早的顶级域名中，表示非营利组织域名的是（）

A.net

B.org

C.biz

D.mil

信管网参考答案：B

查看解析：www.cnitpm.com/st/5019716264.html

28、SMTP 是一种提供可靠有效的电子邮件传输的协议，采用客户服务器的工作方式，在传输层使用 TCP 协议进行传输。SMTP 发送协议中，传送报文文本的指令是（） 。

A.HELO

B.HELP

C.SEND

D.DATA

信管网参考答案：D

查看解析：www.cnitpm.com/st/5019813386.html

29、有线等效保密协议 WEP 是 IEEE 802.11 标准的一部分，其为了实现机密性采用的加密算法是（）

A.DES

B.AES

C.RC4

D.RSA

信管网参考答案：C

查看解析：www.cnitpm.com/st/5019913597.html

30、片内操作系统 COS 是智能卡芯片内的一个监控软件，一般由通信管理模块、安全管理模块、应用管理模块和文件管理模块四个部分组成。其中对接收命令进行可执行判断是属于（）。

A.通信管理模块

B.安全管理模块

C.应用管理模块

D.文件管理模块

信管网参考答案：C

查看解析：www.cnitpm.com/st/5020013148.html

31、PKI 是一种标准的公钥密码的密钥管理平台，数字证书是 PKI 的基本组成部分。在 PKI 中，X.509 数字证书的内容不包括（）。

A.加密算法标识

B.签名算法标识

C.版本号

D.主体的公开密钥信息

信管网参考答案：A

查看解析：www.cnitpm.com/st/5020117809.html

32、SM4 算法是国家密码管理局于 2012 年 3 月 21 日发布的一种分组密码算法，在我国商用密码体系中，SM4 主要用于数据加密。SM4 算法的分组长度和密钥长度分别为（）.

A.128 位和 64 位

B.128 位和 128 位

C.256 位和 128 位

D.256 位和 256 位

信管网参考答案：B

查看解析：www.cnitpm.com/st/5020222146.html

33、在 PKI 体系中，注册机构 RA 的功能不包括（） 。

A.签发证书

B.认证注册信息的合法性

C.批准证书的申请

D.批准撤销证书的申请

信管网参考答案：A

查看解析：www.cnitpm.com/st/5020313240.html

34、下列关于数字签名说法中，正确的是（）

A.验证和解密过程相同

B.数字签名不可改变

C.验证过程需要用户私钥

D.数字签名不可信

信管网参考答案：B

查看解析：www.cnitpm.com/st/502048564.html

35、2001 年 11 月 26 日，美国政府正式颁布 AES 为美国国家标准。AES 算法的分组长度为 128 位，其可选的密钥长度不包括（）

A.256 位

B.192 位

C.128 位

D.64 位

信管网参考答案：D

查看解析：www.cnitpm.com/st/5020522357.html

36、以下关于 BLP 安全模型的表述中， 错误的是（）

A.BLP 模型既有自主访问控制，又有强制访问控制

B.BLP 模型是一个严格形式化的模型，并给出了形式化的证明

C.BLP 模型控制信息只能由高向低流动

D.BLP 是一种多级安全策略模型

信管网参考答案：C

查看解析：www.cnitpm.com/st/502065741.html

37、无线传感器网络(WSN)是由部署在监测区域内大量的廉价微型传感器节点组成， 通过无线通信方式形成的一个多跳的自组织网络系统。以下 WSN 标准中， 不属于工业标准的是（）。

A.ISA100.11a

B.WIA-PA

C.Zigbee

D.WirelessHART

信管网参考答案：C

查看解析：www.cnitpm.com/st/50207115.html

38、按照行为和功能特性，特洛伊木马可以分为远程控制型木马、信息窃取型木马和破坏型木马等。以下不属于远程控制型木马的是（）。

A、冰河

B.彩虹桥

C.PC Share

D.Trojan-Ransom

信管网参考答案：D

查看解析：www.cnitpm.com/st/5020812505.html

39、数据库恢复是在故障引起数据库瘫痪以及状态不一致以后，将数据库恢复到某个正确状态或一致状态。数据库恢复技术一般有四种策略：基于数据转储的恢复、基于日志的恢复、基于检测点的恢复、基于镜像数据库的恢复，其中数据库管理员定期地将整个数据库复制到磁带或另一个磁盘上保存起来，当数据库失效时，取最近一次的数据库备份来恢复数据的技术称为（）。

A.基于数据转储的恢复

B.基于日志的恢复

C.基于检测点的恢复

D.基于镜像数据库的恢复

信管网参考答案：A

查看解析：www.cnitpm.com/st/502094100.html

40、FTP 是一个交互会话的系统，在进行文件传输时，FTP 的客户和服务器之间需要建立两个 TCP 连接，分别是（）

A.认证连接和数据连接

B.控制连接和数据连接

C.认证连接和控制连接

D.控制连接和登录连接

信管网参考答案：B

查看解析：www.cnitpm.com/st/5021027649.html

41、蠕虫是一种可以独立运行、并且能将自身的一个包含了所有功能的版本传播到其他计算机上的程序。网络蠕虫可以分为：漏洞利用类蠕虫、口令破解类螨虫、电子邮件类蠕虫、P2P 类蠕虫等。以下不属于漏洞利用类蠕虫的是（）

A.CodeRed

B.Slammer

C.MSBlaster

D.IRC-worm

信管网参考答案：D

查看解析：www.cnitpm.com/st/5021119931.html

42、防火墙的体系结构中，屏蔽子网体系结构主要由四个部分构成：周边网络、外部路由器、内部路由器和堡垒主机。其中被称为屏蔽子网体系结构第一道屏障的是（）。

A.周边网络

B.外部路由器

C.内部路由器

D.堡垒主机

信管网参考答案：B

查看解析：www.cnitpm.com/st/5021229409.html

43、等级保护 2.0 对于应用和数据安全，特别增加了个人信息保护的要求。以下关于个人信息保护的描述中，错误的是（）。

A.应仅采集和保存业务必需的用户个人信息

B.应禁止未授权访问和使用用户个人信息

C.应允许对用户个人信息的访问和使用

D.应制定有关用户个人信息保护的管理制度和流程

信管网参考答案：C

查看解析：www.cnitpm.com/st/5021329427.html

44、Snort 是一款开源的网络入侵检测系统，能够执行实时流量分析和 IP 协议网络的数据包记录。以下不属于 Snort 主要配置模式的是（）

A.嗅探

B.审计

C.包记录

D.网络入侵检测

信管网参考答案：B

查看解析：www.cnitpm.com/st/5021415083.html

45、身份认证是证实客户的真实身份与其所声称的身份是否相符的验证过程。目前，计算机及网络系统中常用的身份认证技术主要有：用户名/密码方式、智能卡认证、动态口令、生物特征认证等。其中不属于生物特征的是（）。

A.指纹

B.手指静脉

C.虹膜

D.击键特征

信管网参考答案：D

查看解析：www.cnitpm.com/st/5021510978.html

46、信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害，按照计算机信息系统安全等级保护相关要求，应定义为（）。

A.第一级

B.第二级

C.第三级

D.第四级

信管网参考答案：D

查看解析：www.cnitpm.com/st/502166773.html

47、Web 服务器也称为网站服务器， 可以向浏览器等 Web 客户端提供文档，也可以放置网站文件和数据文件。目前最主流的三个 Web 服务器是 Apache、Nginx、IIS。Web 服务器都会受到 HTTP 协议本身安全问题的困扰，这种类型的信息系统安全漏洞属于（） 。

A.设计型漏洞

B.开发型漏洞

C.运行型漏洞

D.代码型漏洞

信管网参考答案：A

查看解析：www.cnitpm.com/st/5021725788.html

48、《计算机信息系统安全保护等级划分准则》中规定了计算机系统安全保护能力的五个等级，其中要求计算机信息系统可信计算基满足访问监控器需求的是（）

A.系统审计保护级

B.安全标记保护级

C.结构化保护级

D.访问验证保护级

信管网参考答案：D

查看解析：www.cnitpm.com/st/502184471.html

49、在需要保护的信息资产中，（）是最重要的。

A.环境

B.硬件

C.数据

D.软件

信管网参考答案：C

查看解析：www.cnitpm.com/st/5021914897.html

50、重放攻击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。下列技术中，不能抵御重放攻击的是（）.

A.序号

B.明文填充

C.时间戳

D.Nonce

信管网参考答案：B

查看解析：www.cnitpm.com/st/5022029729.html

51、为了应对日益严重的垃圾邮件问题，服务提供商设计和应用了各种垃圾邮件过滤机制，以下

耗费计算资源最多的垃圾邮件过滤机制是（） 。

A.SMTP 身份认证

B.反向名字解析

C.内容过滤

D.黑名单过滤信管网参考答案：C

查看解析：www.cnitpm.com/st/5022110855.html

52、在信息系统安全设计中，保证“信息及时且可靠地被访问和使用”是为了达到保障信息系统（）的目标。

A.可用性

B.保密性

C.可控性

D.完整性

信管网参考答案：A

查看解析：www.cnitpm.com/st/502224443.html

53、数字水印技术是指在数字化的数据内容中嵌入不明显的记号，被嵌入的记号通常是不可见的或者不可察觉的，但是通过计算操作能够实现对该记号的提取和检测。数字水印不能实现（）

A.证据篡改鉴定

B.数字信息版权保护

C.图像识别

D.电子票据防伪

信管网参考答案：C

查看解析：www.cnitpm.com/st/502238165.html

54、安全套接字层超文本传输协议 HTTPS 在 HTTP 的基础上加入了 SSL 协议， 网站的安全协议是 HTTPS 时，该网站浏览时会进行（）处理。

A.增加访问标记

B.身份隐藏

C.口令验证

D.加密

信管网参考答案：D

查看解析：www.cnitpm.com/st/50224740.html

55、无线 Wi-Fi 网络加密方式中，安全性最好的是 WPA-PSK/WPA2-PSK，其加密过程采用了 TKIP 和（）

A.AES

B.DES

C.IDEA

D.RSA

信管网参考答案：A

查看解析：www.cnitpm.com/st/5022512173.html

56、涉及国家安全、国计民生、社会公共利益的商用密码产品与使用网络关键设备和网络安全专用产品的商用密码服务实行（）检测认证制度。

A.备案式

B.自愿式

C.鼓励式

D.强制性

信管网参考答案：D

查看解析：www.cnitpm.com/st/5022616847.html

57、从对信息的破坏性上看，网络攻击可以分为被动攻击和主动攻击，以下属于被动攻击的是（）

A.伪造

B.流量分析

C.拒绝服务

D.中间人攻击

信管网参考答案：B

查看解析：www.cnitpm.com/st/5022711801.html

58、密码工作是党和国家的一项特殊重要工作，直接关系国家政治安全、经济安全、国防安全和信息安全。密码法的通过对全面提升密码工作法治化水平起到了关键性作用。密码法规定国家对密码实行分类管理，密码分类中不包含（）

A.核心密码

B.普通密码

C.商用密码

D.国产密码

信管网参考答案：D

查看解析：www.cnitpm.com/st/502285.html

59、工业控制系统是由各种自动化控制组件和实时数据采集、监测的过程控制组件共同构成，工业控制系统安全面临的主要威胁不包括（）

A.系统漏洞

B.网络攻击

C.设备故障

D.病毒破坏

信管网参考答案：C

查看解析：www.cnitpm.com/st/5022913357.html

60、资产管理是信息安全管理的重要内容，而清楚地识别信息系统相关的财产，并编制资产清单是资产管理的重要步骤。以下关于资产清单的说法中，错误的是（）。

A.资产清单的编制是风险管理的一个重要的先决条件

B.信息安全管理中所涉及的信息资产，即业务数据、合同协议、培训材料等

C.在制定资产清单的时候应根据资产的重要性、业务价值和安全分类，确定与资产重要性相对应的保护级别

D.资产清单中应当包括将资产从灾难中恢复而需要的信息，如资产类型、格式、位置、备份信息、

许可信息等

信管网参考答案：B

查看解析：www.cnitpm.com/st/5023018111.html

61、身份认证是证实客户的真实身份与其所声称的身份是否相符的验证过程。下列各种协议中，不属于身份认证协议的是（）

A.IPSec 协议

B.S/KEY 口令协议

C.X.509 协议

D.Kerberos 协议

信管网参考答案：A

查看解析：www.cnitpm.com/st/5023111359.html

62、恶意代码是指为达到恶意目的而专门设计的程序或者代码。常见的恶意代码类型有：特洛伊木马、蠕虫、病毒、后门、Rootkit、僵尸程序、广告软件。以下恶意代码中，属于宏病毒的是（）

A.Trojan.Bank

B.Macro.Melissa

C.Worm.Blaster.g

D.Trojan.huigezi.a

信管网参考答案：B

查看解析：www.cnitpm.com/st/502321498.html

63、网络安全控制技术指致力于解决诸多如何有效进行介入控制，以及如何保证数据传输的安全性的技术手段。以下不属于网络安全控制技术的是（）。

A.VPN 技术

B.容灾与备份技术

C.入侵检测技术

D.信息认证技术

信管网参考答案：B

查看解析：www.cnitpm.com/st/5023318863.html

64、在安全评估过程中，采取（）手段，可以模拟黑客入侵过程，检测系统安全脆弱性。

A.问卷调查

B.人员访谈

C.渗透测试

D.手工检查

信管网参考答案：C

查看解析：www.cnitpm.com/st/5023413493.html

65、一个密码系统至少由明文、密文、加密算法、解密算法和密钥五个部分组成，而其安全性是由（）决定的。

A、加密算法

B.解密算法

C.加解密算法

D.密钥

信管网参考答案：D

查看解析：www.cnitpm.com/st/502354109.html

66、密码学的基本安全目标主要包括：保密性、完整性、可用性和不可抵赖性。其中确保信息仅被合法用户访问，而不被泄露给非授权的用户、实体或过程，或供其利用的特性是指（）。

A.保密性

B.完整性

C.可用性

D.不可抵赖性

信管网参考答案：A

查看解析：www.cnitpm.com/st/502369421.html

67、等级保护 2.0 强化了对外部人员的管理要求，包括外部人员的访问权限、保密协议的管理要求，以下表述中，错误的是（）。

A.应确保在外部人员接入网络访问系统前先提出书面申请，批准后由专人开设账号、分配权限，并登记备案

B.外部人员离场后应及时清除其所有的访问权限

C.获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息

D.获得系统访问授权的外部人员，离场后可保留远程访问权限

信管网参考答案：D

查看解析：www.cnitpm.com/st/5023718231.html

68、根据加密和解密过程所采用密钥的特点可以将加密算法分为对称加密算法和非对称加密算法两类，以下属于对称加密算法的是（）.

A.RSA

B.MD5

C.IDEA

D.SHA-128

信管网参考答案：C

查看解析：www.cnitpm.com/st/5023825249.html

69、移位密码的加密对象为英文字母，移位密码采用对明文消息的每一个英文字母向前推移固定 key 位的方式实现加密。设 key=6，则明文“SEC”对应的密文为（）

A.YKI

B.ZLI

C.XJG

D.MYW

信管网参考答案：A

查看解析：www.cnitpm.com/st/502396132.html

70、国家密码管理局发布的《无线局域网产品须使用的系列密码算法》，其中规定密钥协商算法应使用的是（）

A.PKI

B.DSA

C.CPK

D.ECDH

信管网参考答案：D

查看解析：www.cnitpm.com/st/5024025987.html

71~75、Symmetric-key cryptosystems use the（） key for encryption and decryption of a message,though a message or group of messages may have a different key than others. A significant disadvantage of symmetric ciphers is the key management necessary to use them securely.Each distinct pair of communicating parties must, ideally, share a different key, and perhaps each ciphertext exchanged as well. The number of keys required increases as the square of the number of network members,which very quickly requires complex key management schemes to keep them all straight and secret. The difficulty of securely establishing a secret（）between two communicating parties, when a secure channel doesn't already exist between them, also presents a chicken-and-egg problem which is a considerable practical obstacle for cryptography users in the real world.

Whitfield Difñie and Martin Hellman, authors of the first paper on public-key cryptography.

In a groundbreaking 1976 paper, Whitfield Diffie and Martin Hellman proposed the notion of public-key (also, more generally, called asymmetric key) cryptography in which two different but mathematically related keys are used-a public key and a private key. A public key system is so constructed that calculation of one key (the private key) is computationally infeasible（）the other (the public key), even though they are necessarily related. Instead, both keys are generated secretly, as an interrelated pair. The historian David Kahn described public-key cryptography as “the most revolutionary new concept in the field since poly-alphabetic substitution emerged in the Renaissance”.

In public-key cryptosystems, the ( ) key may be freely distributed, while its paired private key must remain secret. The public key is typically used for encryption, while the private or secret key is used for decryption. Diffie and Hellman showed that public-key cryptography was possible by presenting the Diffie-Hellman key exchange protocol.

In 1978, Ronald Rivest, Adi Shamir, and Len Adleman invented( ),another public-key system.

In 1997, it finally became publicly known that asymmetric key cryptography had been invented by James H. Ellis at GCHQ,a British intelligence organization, and that, in the early 1970s,both the Diffie-Hellman and RSA algorithms had been previously developed(by Malcolm J. Williamson and Clifford Cocks, respectively).

(1) A. different

B. same

C.public

D. private

(2)A. plaintext

B. stream

C.ciphertext

D.key

(3)A.from

B. in

C.to

D.of

(4)A.public

B.private

C.symmetric

D.asymmetric

(5) A.DES

B.AES

C.RSA

D.IDEA

信管网参考答案：B、D、A、A、C

查看解析：www.cnitpm.com/st/5024120248.html