2018 年上半年信息安全工程师考试上午真题答案与解析:
http://www.educity.cn/tiku/tp41600.html

2018 年上半年信息安全工程师考试上午真题

● 2016 年 11 月 7 日,十二届全国人大常会第二十四次会议以 154 票赞成,1 票弃权,表决通过了《网络安全法》。该法律由全国人民代表大会常务员会于 2016 年 11 月 7 日发布,自(　　)起施行。

（1）A. 2017 年 1 月 1 日
B. 2017 年 6 月 1 日
C. 2017 年 7 月 1 日
D. 2017 年 10 月 1 日

● 近些年,基于标识的密码技术受到越来越多的关注,标识密码算法的应用也得到了快速发展,我国国密标准中的标识密码算法是（　　）。

（2）A. SM2
B. SM3
C. SM4
D. SM9

● 《计算机信息系统安全保护等级划分准则》(GB17859-1999)中规定了计算机系统安全保护能力的五个等级，其中要求对所有主体和客体进行自主和强制访问控制的是（　　）。

（3）A. 用户自主保护级
B. 系统审计保护级
C. 安全标记保护级
D. 结构化保护级

● 密码分析者针对加解密算法的数学基础和某些密码学特性,根据数学方法破译密码的攻击方式称为（　　）。

（4）A. 数学分析攻击
B. 差分分析攻击
C. 基于物理的攻击
D. 穷举攻击

● 《网络安全法》明确了国家落实网络安全工作的职能部门和职责，其中明确规定由（　　）负责统筹协调网络安全工作和相关监督管理工作。

（5）A. 中央网络安全与信息化小组
B. 国务院
C. 国家网信部门
D. 国家公安部门

● 一个密码系统如果用 E 表示加密运算，D 表小解密运算，M 表示明文,C 表示密文,则下面描述必然成立的是（　　）。

（6）A.　E(E(M))=C
B. D(E(M))=M
C. D(E(M))=C
D. D(D(M))=M

● S/key 口令是一种一次性口令生成方案，它可以对抗（　　）。

（7）A. 恶意代码攻击
B. 暴力分析攻击
C. 重放攻击
D. 协议分析攻击

● 面向数据挖掘的隐私保护技术主要解高层应用中的隐私保护问题，致力于研究如何根据不同数据挖掘操作的特征来实现对隐私的保护，从数据挖的角度,不属于隐私保护技术的是（　　）。

（8）A. 基于数据分析的隐私保护技术
B. 基于微据失真的隐私保护技术
C. 基于数据匿名化的隐私保护技术
D. 基于数据加密的隐私保护技术

● 从网络安全的角度看，以下原则中不属于网络安全防护体系在设计和实现时需要遵循的基本原则的是（　　）。

（9）A. 最小权限原则
B. 纵深防御原则
C. 安全性与代价平衡原则
D. Kerckhoffs 原则

● 恶意软件是目前移动智能终端上被不法分子利用最多、对用户造成危害和损失最大的安全成胁类型。数据显示，目前安卓平台恶意软件主要有（　　）四种类型。

（10）A. 远程控制木马、话费吸取类、隐私窃取类和系统破坏类
B. 远程控制木马、话费吸取类、系统破坏类和硬件资源消耗类
C. 远程控制木马、话费吸取类、隐私窃取类和恶意推广
D. 远程控制木马、话费吸取类、系统破坏类和恶意推广

● 以下关于认证技术的描述中，错误的是（　　）。

（11）A. 身份认证是用来对信息系统中实体的合法性进行验证的方法
B. 消息认证能够验证消息的完整性
C. 数字签名是十六进制的字符串
D. 指纹识别技术包括验证和识别两个部分

● 对信息进行均衡、全面的防护，提高整个系统“安全最低点”的全性能，这种安全原则被称为（　　）。

（12）A. 最小特权原则
B. 木桶原则
C. 等级化原则
D. 最小泄露原则

● 网络安全技术可以分为主动防御技术和被动防御技术两大类，以下属于主动防技术的是（　　）。

（13）A. 蜜罐技术
B. 入侵检测技术
C. 防火墙技术
D. 恶意代码扫描技术

● 如果未经授权的实体得到了数据的访问权，这属于破坏了信息的（　　）。

（14）A. 可用性
B. 完整性
C. 机密性
D. 可控性

● 按照密码系统对明文的处理方法,密码系统可以分为（　　）。

（15）A. 对称密码系统和公钥密码系统
B. 对称密码系统和非对称密码系统
C. 数据加密系统和数字签名系统
D. 分组密码系统和序列密码系统

● 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,实现数字签名最常见的方法是（　　）。

（16）A. 数字证书和 PKI 系统相结合
B. 对称密码体制和 MD5 算法相结合
C. 公钥密码体制和单向安全 Hash 函数算法相结合
D. 公钥密码体制和对称密码体制相结合

● 以下选项中,不属于生物识别方法的是（　　）。

（17）A. 掌纹识别
B. 个人标记号识别
C. 人脸识别
D. 指纹识别

● 计算机取证是将计算机调查和分析技术应用于对潜在的,有法律效力的证据的确定与提取.以下关于计算机取证的描述中,错误的是（　　）。

（18）A. 计算机取证包括保护目标计算机系统、确定收集和保存电子证据,必须在开机的状态下进行
B. 计算机取证围绕电子证据进行,电子证据具有高科技性、无形性和易破坏性等特点
C. 计算机取证包括对以磁介质编码信息方式存储的计算机证据的保护、确认、提取和归档
D. 计算机取证是一门在犯罪进行过程中或之后收集证据的技术

● 在缺省安装数据库管理系统 MySQL 后，root 用户拥有所有权限且是空口令，为了安全起见，必须为 root 用户设置口令，以下口令设置方法中，不正确的是（　　）。

（19）A. 使用 MySQL 自带的命令 mysqladmin 设置 root 口令
B. 使用 setpassword 设置口令
C. 登录数据库,修改数据库 mysql 下 user 表的字段内容设置口令
D. 登录数据库,修改数据库 mysql 下的访问控制列表内容设置口令

● 数字水印技术通过在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。以下不属于数字水印在数字版权保护中必须满足的基本应用需求的是（　　）。

（20）A. 保密性
B. 隐蔽性
C. 可见性
D. 完整性

● （　　）是一种通过不断对网络服务系统进行扰,影响其正常的作业流程,使系统响应减慢甚至瘫痪的攻击方式。

（21）A. 暴力攻击

B.拒绝服务攻击
C.重放攻击
D.欺骗攻击

● 在访问因特网时,为了防止 Wb 页面中恶意代码对自己计算机的损害,可以采取的防范措施是（　　）。

（22）A. 将要访问的 Wb 站点按其可信度分配到浏览器的不同安全区域
B.利用 SSL 访问 Web 站点
C.在浏览器中安装数字证书
D.利用 IP 安全协议访问 Web 站点

● 下列说法中,错误的是（　　）。

（23）A. 数据被非授权地增删、修改或破坏都属于破坏数据的完整性
B.抵赖是一种来自黑客的攻击
C. 非授权访问是指某一资源被某个非授权的人,或以非授权的方式使用
D.重放攻击是指出于非法目的,将所截获的某次合法的通信数据进行拷贝而重新发送

● Linux 系统的运行日志存储的目录是（　　）。

（24）A. /var/log
B./usr/log
C./etc/log
D./tmp/log

● 电子邮件已经成为传播恶意代码的重途径之一,为了有效防止电子邮件中的恶意代码,应该用（　　）的方式阅读电子邮件。

（25）A. 应用软件
B.纯文本
C.网页
D.在线

● 已知 DES 算法 S 盒如下:

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

如果该 S 盒的输入为 100010,则其二进制输出为（　　）。

（26）A. 0110

B.1001
C.0100
D.0101

● 以下关于 TCP 协议的描述,错误的是（　　）。

（27）A. TCP 是 Internet 传输层的协议,可以为应用层的不同协议提供服务
B.TCP 是面向连接的协议,提供可靠、全双工的、面向字节流的端到端的服务
C.TCP 使用二次握手来建立连接,具有很好的可靠性
D.TCP 每发送一个报文段,就对这个报文段设置一次计时器

● Kerberos 是一种常用的身份认证协议,它采用的加密算法是（　　）。

（28）A. Elgamal
B.DES
C.MD5
D.RSA

● 人为的安全威胁包括主动攻击和被动攻击,以下属于被动攻击的是（　　）。

（29）A. 流量分析
B.后门
C.拒绝服务攻击
D.特洛伊木马

● 移动用户有些属性信息需要受到保护,这些信息一旦泄露,会对公众用户的生命财产安全造成威胁.以下各项中,不需要被保护的属性是（　　）。

（30）A. 终端设备信息
B.用户通话信息
C.用户位置信息
D.公众运营商信息

● 以下关于数字证书的叙述中,错误的是（　　）。

（31）A. 证书通常携带 CA 的公开密钥
B.证书携带持有者的签名算法标识
C.证书的有效性可以通过验证持有者的签名验证
D.证书通常由 CA 安全认证中心发放

● 2017 年 11 月,在德国柏林召开的第 55 次 ISO/IEC 信息安全分技术委员会(SC27)会议上,我国专家组提出的（　　）算法一致通过成为国际标准。

（32）A. SM2 与 SM3

B.SM3 与 SM4
C.SM4 与 SM9
D.SM9 与 SM2

● 典型的水印攻击方式包括:鲁棒性攻击、表达攻击、解释攻击和法律攻击.其中鲁棒性攻击是指在不害图像使用价值的前提下减弱、移去或破坏水印的一类攻击方式.以下不属于鲁棒性攻击的是（　　）。

（33）A. 像素值失真攻击
B.敏感性分析攻击
C.置乱攻击
D.梯度下降攻击

● 数字信封技术能够（　　）。

（34）A. 隐藏发送者的真实身份
B.保证数据在传输过程中的安全性
C. 对发送者和接收者的身份进行认证
D.防止交易中的抵赖发生

● 在 DES 加密算法中,子密钥的长度和加密分组的长度分别是（　　）。

（35）A. 56 位和 64 位
B.48 位和 64 位
C.48 位和 56 位
D.64 位和 64 位

● 甲不但怀疑乙发给他的信遭人幕改,而且怀疑乙的公钥也是被人冒充的,为了消除甲的疑虑,甲和乙需要找一个双方都信任的第三方来签发数字证书,这个第三方是（　　）。

（36）A. 注册中心 RA
B.国家信息安全测评认证中心
C.认证中心 CA
D.国际电信联盟 ITU

● WI-FI 网络安全接入是一种保护无线网络安全的系统,WPA 加密的认证方式不包括（　　）。

（37）A. WPA 和 WPA2
B.WEP
C.WPA-PSK
D.WPA2-PSK

● 特洛伊木马攻击的威胁类型属于（　　）。

（38）A. 旁路控制威胁
B. 网络欺骗
C. 植入威胁
D. 授权侵犯威胁

● 信息通过网络进行传输的过程中,存在着被慕改的风险,为了解决这一安全隐患通常采用的安全防护技术是（　　）。

（39）A. 信息隐藏技术
B. 数据加密技术
C. 消息认证技术
D. 数据备份技术

● SSL 协议是对称密码技术和公钥密码技术相结合的协议,该协议不能提供的安全服务是（　　）。

（40）A. 可用性
B. 完整性
C. 保密性
D. 可认证性

● 计算机病毒是指一种能够通过自身复制传染,起破坏作用的计算机程序,目前使用的防杀病毒软件的主要作用是（　　）。

（41）A. 检查计算机是否感染病毒,清除已感染的任何病毒
B. 杜绝病毒对计算机的侵害
C. 查出已感染的任何病毒,清除部分已感染病毒
D. 检查计算机是否感染病毒,清除部分已感染病毒

● IP 地址分为全球地址和专用地址,以下属于专用地址的是（　　）。

（42）A. 192.172.1.2
B. 10.1.2.3
C. 168.1.2.3
D. 172.168.1.2

● 信息安全风险评估是依照科学的风险管理程序和方法,充分地对组成系统的各部分所面临的危险因素进行分析评价,针对系统存在的安全问题,根据系统对其自身的安全需求,提出有效的安全措施,达到最大限度减少风险,降低危害和确保系统安全运行的目的,风险评估的过程包括（　　）四个阶段。

（43）A. 风险评估准备、漏洞检测、风险计算和风险等级评价
B. 资产识别、漏洞检测,风险计算和风险等级评价
C. 风险评估准备、风险因素识别、风险程度分析和风险等级评价

D.资产识别、风险因素识别、风险程度分析和风险等级评价

● 深度流检测技术是一种主要通过判断网络流是否异常来进行安全防护的网络安全技术,深度流检测系统通常不包括（　　）。

（44）A. 流特征提取单元
B.流特征选择单元
C.分类器
D.响应单元

● 操作系统的安全审计是指对系统中有关安全的活动进行记录、检查和审核的过程，为了完成审计功能，审计系统需要包括（　　）三大功能模块。

（45）A. 审计数据挖掘,审计事件记录及查询、审计事件分析及响应报警
B.审计事件特征提取、审计事件特征匹配、安全响应报警
C.审计事件收集及过滤、审计事件记录及查询,审计事件分析及响应报警系统
D.日志采集与挖掘、安全事件记录及查询、安全响应报警

● 计算机犯罪是指利用信息科学技术且以计算机为犯罪对象的犯罪行为,与其他类型的犯罪相比,具有明显的特征,下列说法中错误的是（　　）。

（46）A. 计算机犯罪有高智能性,罪犯可能掌握一些高科技手段
B.计算机犯罪具有破坏性
C.计算机犯罪没有犯罪现场
D.计算机犯罪具有隐蔽性

● 攻击者通过对目标主机进行端口扫可以直接获得（　　）。

（47）A. 目标主机的操作系统信息
B.目标主机开放端口服务信息
C.目标主机的登录口令
D.目标主机的硬件设备信息

● WPKI（无线公开密钥体系）是基于无网络环境的一套遵循既定标准的密钥及证书管理平台,该平台采用的加密算法是（　　）。

（48）A. SM4
B.优化的 RSA 加密算法
C.SM9
D.优化的椭圆曲线加密算法

● 文件型病毒不能感染的文件类型是（　　）。

（49）A. SYS 型

B.EXE 类型
C.COM 型
D.HTML 型

● 网络系统中针对海量数据的加密,通常不采用（　　）方式。

（50）A. 会话加密
B.公钥加密
C.链路加密
D.端对端加密

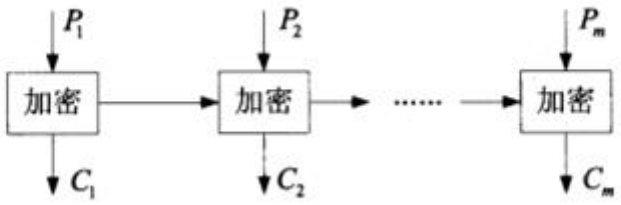
● 对无线网络的攻击可以分为:对无线接口的攻击、对无线设备的攻击和对无线网络的攻击。以下属于对无线设备攻击的是（　　）。

（51）A. 窃听
B.重放
C.克隆
D.欺诈

● 无线局域网鉴别和保密体系 WAPI 是我国无线局域网安全强制性标准,以下关于 WAP 的描述,正确的是（　　）。

（52）A. WAPI 从应用模式上分为单点式、分布式和集中式
B.WAPI 与 WIFI 认证方式类似,均采用单向加密的认证技术
C.WAPI 包括两部分:WAI 和 WPI,其中 WAl 采用对称密码算法实现加、解密操作
D.WAPI 的密钥管理方式包括基于证书和基于预共享秘密两种方式

● 分组密码常用的工作模式包括:电码本模式（ECB 模式）、密码反馈模式（CFB 模式）,密码分组链接模式（CBC 模式）,输出反馈模式（OFB 模式）。下图描述的是（　　）模式（图中 P_i 表示明文分组,C_i 表示密文分组）



（53）A. ECB 模式
B.CFB 模式
C.CBC 模式
D.OFB 模式

● 关于祖冲之算法的安全性分析不正确的是（　　）。

（54）A. 祖冲之算法输出序列的随机性好,周期足够大
B.祖冲之算法的输出具有良好的线性、混淆特性和扩散特性
C.祖冲之算法可以抵抗已知的序列密码分析方法
D.祖冲之算法可以抵抗弱密分析

● 以下关于 IPSec 协议的叙述中,正确的是（　　）。

（55）A. IPSec 协议是 IP 协议安全问题的一种解决方案
B.IPSec 协议不提供机密性保护机制
C.IPSec 协议不提供认证功能
D.IPSec 协议不提供完整性验证机制

● 不属于物理安全威胁的是（　　）。

（56）A. 电源故障
B.物理攻击
C.自然灾害
D.字典攻击

● 以下关于网络钓鱼的说法中,不正确的是（　　）。

（57）A. 网络钓鱼属于社会工程攻击
B.网络钓鱼与 Web 服务没有关系
C.典型的网络钓鱼攻击是将被攻击者引诱到一个钓鱼网站
D.网络钓鱼融合了伪装、欺骗等多种攻击方式

● Bell-LaPadual 模型(简称 BLP 模型)是最早的一种安全模型,也是最著名的多级安全策略模型,BLP 模型的简单安全特性是指（　　）。

（58）A. 不可上读
B.不可上写
C.不可下读
D.不可下写

● 安全电子交易协议 SET 是由 VISA 和 Mastercard 两大信用卡组织联合开发的电子商务安全协议,以下关于 SET 的叙述中,正确的是（　　）。

（59）A. SET 通过向电子商务各参与方发放验证码来确认各方的身份,保证网上支付的安全性
B.SET 不需要可信第三方认证中心的参与
C.SET 要实现的主要目标包括保障付款安全、确定应用的互通性和达到全球市场的可接受性
D.SET 协议主要使用的技术包括:流密码、公钥密码和数字签名等

● 在 PKI 中,关于 RA 的功能,描述正确的是（　　）。

（60）A. RA 是整个 PKI 体系中各方都承认的一个值得信赖的、公正的第三方机构
B. RA 负责产生,分配并管理 PKI 结构下的所有用户的数字证书,把用户的公钥和用户的其他信息绑在一起,在网上验证用户的身份
C. RA 负责证书废止列表 CRL 的登记和发布
D. RA 负责证书申请者的信息录入,审核以及证书的发放等任务,同时,对发放的证书完成相应的管理功能

● 以下关于 VPN 的叙述中,正确的是（　　）。

（61）A. VPN 通过加密数据保证通过公网传输的信息即使被他人截获也不会泄露
B. VPN 指用户自己租用线路,和公共网络物理上完全隔离的、安全的线路
C. VPN 不能同时实溶息的认证和对身份的认证
D. VPN 通过身份认证实现安全目标,不具数据加密功能

● 对于定义在 GF(p)上的椭圆曲线,取素数 P=11,椭圆曲线 $y^2=x^3+x+6 \bmod 11$,则以下是椭圆曲线 11 平方剩余的是（　　）。

（62）A. x=1
B. x=3
C. x=6
D. x=9

● 当防火墙在网络层实现信息过滤与控制时,主要针对 TCP/IP 协议中的数据包头制定规则匹配条件并实施过滤,该规则的匹配条件不包括（　　）。

（63）A. IP 源地址
B. 源端口
C. IP 目的地址
D. 协议

● 以下关于网络流量监控的叙述中,不正确的是（　　）。

（64）A. 网络流量监控分析的基础是协议行为解析技术
B. 数据采集探针是专门用于获取网络链路流量数据的硬件设备
C. 流量监控能够有效实现对敏感数据的过滤
D. 流量监测中所监测的流量通常采集自主机节点、服务器、路由器接口、链路和路径等

● 设在 RSA 的公钥密码体制中,公钥为(e,n)=(7，55),则私钥 d=（　　）。

（65）A. 11

B.15
C.17
D.23

● 下列关于公钥密码体制说法不正确的是（　　）。

（66）A. 在一个公钥密码体制中,一般存在公钥和私钥两个密钥
B.公钥密码体制中仅根据密码算法和加密密钥来确定解密密钥在计算上是可行的
C.公钥密码体制中仅根据密码算法和加密密来确定解密密在计算上是不可行的
D.公钥密码体制中的私钥可以用来进行数字签名

● SM3 密码杂凑算法的消息分组长度为（　　）比特。

（67）A. 64
B.128
C.512
D.1024

● 如果破译加密算法所需要的计算能力和计算时间是现实条件所不具备的,那么就认为相应的密码体制是（　　）。

（68）A. 实际安全
B.可证明安全
C.无条件安全
D.绝对安全

● a=17,b=2,则满足 a 与 b 取模同余的是（　　）。

（69）A. 4
B.5
C.6
D.7

● 利用公开密钥算法进行数据加密时,采用的方式是（　　）。

（70）A. 发送方用公开密钥加密,接收方用公开密钥解密
B.发送方用私有密钥加密,接收方用私有密钥解密
C.发送方用公开密钥加密,接收方用私有密钥解密
D.发送方用私有密钥加密,接收方用公开密钥解

● Trust is typically interpreted as a subjective belief in the reliability, honesty and security of an entity on which we depend (　　) our welfare .In online environments we depend on a wide spectrun

of things , ranging from computer hardware,software and data to people and organizations. A security solution always assumes certain entities function according to specific policies.To trust is precisely to make this sort of assumptions , hence , a trusted entity is the same as an entity that is assumed to function according to policy . A consequence of this is that a trust component of a system must work correctly in order for the security of that system to hold, meaning that when a trusted ( ) fails , then the sytems and applications that depend on it can ( ) be considered secure . An often cited articulation of this principle is:" a trusted system or component is one that can break your security policy" (which happens when the trust system fails). The same applies to a trusted party such as a service provider (SP for short)that is , it must operate according to the agreed or assumed policy in order to ensure the expected level of securty and quality of services . A paradoxical conclusion to be drawn from this analysis is that security assurance may decrease when increasing the number of trusted components and parties that a service infrastructure depends on . This is because the security of an infrastructure consisting of many Trusted components typically follows the principle of the weakest link , that is ,in many situations the the overall security can only be as strong as the least reliable or least secure of all the trusted components. We cannot avoid using trusted security components,but the fewer the better. This is important to understand when designing the identity management architectures,that is, fewer the trusted parties in an identity management model , stronger the security that can be achieved by it .

The transfer of the social constructs of identity and trust into digital and computational concepts helps in designing and implementing large scale online markets and communities,and also plays an important role in the converging mobile and Internet environments . Identity management (denoted Idm hereafter) is about recognizing and verifying the correctness o

f identitied in online environment . Trust management becomes a component of （ ） whenever different parties rely on each other for identity provision and authentication . IdM and Trust management therefore depend on each other in complex ways because the correctness of the identity itself must be trusted for the quality and reliability of the corresponding entity to be trusted. IdM is also an essential concept when defining authorisat ion policies in personalised services.

Establishing trust always has a cost , so that having complex tru st requirement typically leads to high overhead in establishing the required trust . To reduce costs there will be incentives for stakeholders to “ cut corners ” regarding trust requirements , which could lead to inadequate security . The challenge is to design IdM systems with relatively si mple trust requirements. Cryptographic mechanisms are often a core component of IdM solutions, for example, for entity and data authentication. With cryptography, it is often possible to propagate trust from where it initially exists to where it is needed . The establishment of initial （ ） usually takes place in the physical world, and the subsequent propagation of trust happens online, often in an automated manner.

（71）A. with
B. on
C. of
D. for
（72）A. entity
B. person
C. component
D. thing
（73）A. No longer
B. never
C. always
D. often
（74）A. SP
B. IdM
C. Internet
D. entity
（75）A. trust
B. cost
C. IdM
D. solution