全国计算机技术与软件专业技术资格（水平）考试指定用书

信息安全工程师
2016 至 2018 年试题分析与解答

全国计算机专业技术资格考试办公室　主编

清 华 大 学 出 版 社
北　京

内 容 简 介

信息安全工程师考试是全国计算机技术与软件专业技术资格（水平）考试的中级职称考试，是历年各级考试报名中的热点之一。本书汇集了从 2016 年到 2018 年的所有试题和权威的解析，参加考试的考生，认真读懂本书的内容后，将更加了解考题的思路，对提升自己考试通过率的信心会有极大的帮助。

图书在版编目（CIP）数据

信息安全工程师 2016 至 2018 年试题分析与解答/全国计算机专业技术资格考试办公室主编.
—北京：清华大学出版社，2019.10
全国计算机技术与软件专业技术资格（水平）考试指定用书
ISBN 978-7-302-53906-3

Ⅰ. ①信…　Ⅱ. ①全…　Ⅲ. ①信息处理－资格考试－题解　Ⅳ. ①G202-44

中国版本图书馆 CIP 数据核字（2019）第 209537 号

责任编辑：杨如林
封面设计：何凤霞
责任校对：徐俊伟
责任印制：

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn, http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：
经　　销：全国新华书店
开　　本：185mm×230mm　　**印　张：**7.5　　**防伪页：**1　　**字　数：**163 千字
版　　次：2019 年 12 月第 1 版　　**印　次：**2019 年 12 月第 1 次印刷
定　　价：29.00 元

产品编号：084054-01

前　言

根据国家有关的政策性文件，全国计算机技术与软件专业技术资格（水平）考试（以下简称“计算机软件考试”）已经成为计算机软件、计算机网络、计算机应用、信息系统、信息服务领域高级工程师、工程师、助理工程师（技术员）国家职称资格考试。而且，根据信息技术人才年轻化的特点和要求，报考这种资格考试不限学历与资历条件，以不拘一格选拔人才。现在，软件设计师、程序员、网络工程师、数据库系统工程师、系统分析师、系统架构设计师和信息系统项目管理师等资格的考试标准已经实现了中国与日本互认，程序员和软件设计师等资格的考试标准已经实现了中国和韩国互认。

计算机软件考试规模发展很快，年报考规模已经超过 50 万人，二十多年来，累计报考人数超过 500 万人。

计算机软件考试已经成为我国著名的 IT 考试品牌，其证书的含金量之高已得到社会的公认。计算机软件考试的有关信息见网站www.ruankao.org.cn中的资格考试栏目。

对考生来说，学习历年试题分析与解答是理解考试大纲的最有效、最具体的途径。

为帮助考生复习备考，全国计算机专业技术资格考试办公室组织编写了信息安全工程师 2016 至 2018 年的试题分析与解答，以便于考生测试自己的水平，发现自己的弱点，更有针对性、更系统地学习。

计算机软件考试的试题质量高，包括了职业岗位所需的各个方面的知识和技术，不但包括技术知识，还包括法律法规、标准、专业英语、管理等方面的知识；不但注重广度，而且还有一定的深度；不但要求考生具有扎实的基础知识，还要具有丰富的实践经验。

这些试题中，包含了一些富有创意的试题，一些与实践结合得很好的试题，一些富有启发性的试题，具有较高的社会引用率，对学校教师、培训指导者、研究工作者都是很有帮助的。

由于作者水平有限，时间仓促，书中难免有错误和疏漏之处，诚恳地期望各位专家和读者批评指正，对此，我们将深表感激。

编者

2019 年 9 月

目　录

第 3 章　2017 上半年信息安全工程师上午试题分析与解答

试题（1）

根据密码分析者可利用的数据资源来分类，可将密码攻击的类型分为四类，其中密码分析者能够选择密文并获得相应明文的攻击密码的类型属于（1）。

（1）A．仅知密文攻击　　B．选择密文攻击

C．已知明文攻击　　D．选择明文攻击

试题（1）分析

本题考查密码学方面的基础知识。

根据密码分析者可利用的数据资源来分类，可将密码攻击的类型分为四类：

① 唯密文攻击（Ciphertext only attack）：攻击者有一些消息的密文，这些密文都是用相同的加密算法进行加密得到的。

② 已知明文攻击（Know plaintext attack）：攻击者不仅可以得到一些消息的密文，而且也知道对应的明文。

③ 选择明文攻击（Chosen plaintext attack）：攻击者不仅可以得到一些消息的密文和相应的明文，而且还可以选择被加密的明文。

④ 选择密文攻击（Chosen ciphertext attack）：攻击者能够选择一些不同的被加密的密文并得到与其对应的明文信息，攻击者的任务是推算出加密密钥。

参考答案

（1）B

试题（2）

《计算机信息系统安全保护等级划分准则》（GB 17859—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（2）。

（2）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

试题（2）分析

本题考查计算机系统安全等级保护方面的基础知识。

《计算机信息系统安全保护等级划分准则》是我国计算机信息系统安全保护等级系列标准的基础，是进行计算机信息系统安全等级保护制度建设的基础性标准，也是信息安全评估和管理的重要基础。该标准虽然不具备技术上的可操作性，但其基本准则却是我国多类信息系统划分保护等级和确定等级保护措施的指导原则和策略依据。此标准将

计算机信息系统安全保护从低到高划分为 5 个等级，即用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级。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结构化保护级。

参考答案

（2）D

试题（3）

1949 年，（3）发表了题为《保密系统的通信理论》的文章，为密码技术的研究奠定了理论基础，由此密码学成了一门科学。

（3）A．Shannon　　B．Diffie　　C．Hellman　　D．Shamir

试题（3）分析

本题考查密码学史方面的基础知识。

1949 年，Shannon 发表了题为《保密系统的通信理论》的文章，为密码技术的研究奠定了理论基础，由此密码学成了一门科学。

参考答案

（3）A

试题（4）

（4）属于对称加密算法。

（4）A．ElGamal　　B．DES　　C．MD5　　D．RSA

试题（4）分析

本题考查密码学方面的基础知识。

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两类：对称加密算法和非对称密码算法。

对称加密算法也称为传统加密算法，是指解密密钥与加密密钥相同或者能够从加密密钥中直接推算出解密密钥的加密算法。通常在大多数对称加密算法中解密密钥与加密密钥是相同的，所以这类加密算法要求 Alice 和 Bob 在进行保密通信前，通过安全的方式商定一个密钥。对称加密算法的安全性依赖于密钥的管理。

公开密钥加密算法也称为公钥加密算法，是指用来解密的密钥不同于进行加密的密钥，也不能够通过加密密钥直接推算出解密密钥。一般情况下，加密密钥是可以公开的，任何人都可以应用加密密钥来对信息进行加密，但只有拥有解密密钥的人才可以解密出被加密的信息。在以上过程中，加密密钥称为公钥，解密密钥称为私钥。

属于对称加密算法的是 DES。

参考答案

（4）B

试题（5）

凯撒密码体制是一种代表性的古典密码算法。在凯撒密码体制中，设密钥参数 k=3，

依次对明文“zhongguo”进行加密，则相应的密文为__（5）__。

（5）A．ckrqjjxr　　B．cdrqjjxr　　C．akrqjjxr　　D．ckrqiixr

试题（5）分析

本题考查密码学方面的基础知识，凯撒密码是移位密码的一个特例。

移位密码体制：

令 $M=C=K=Z_{26}$。对任意的 $key\in Z_{26}$，$x\in M$，$y\in C$，定义：

$$e_{key}(x)=(x+key)\bmod 26$$

$$d_{key}(y)=(y-key)\bmod 26$$

在使用移位密码体制对英文字母进行加密之前，首先需要在 26 个英文字母与 Z_{26} 中的元素之间建立一一对应关系，然后应用以上密码体制进行相应的加密计算和解密计算。

移位密码中，当取密钥 $key=3$ 时，得到的移位密码称为凯撒密码。根据加密原则，没加密的密文为“ckrqjjxr”。

参考答案

（5）A

试题（6）

在信息系统安全防护体系设计中，保证“信息系统中数据不被非法修改、破坏、丢失等”是为了达到防护体系的__（6）__的目标。

（6）A．可用性　　B．保密性　　C．可控性　　D．完整性

试题（6）分析

本题考查信息系统安全防护体系方面的基础知识。

信息系统的安全防护是一项非常复杂的工程，围绕它目前已经形成了众多安全技术，包括身份认证、访问控制、内容安全、审计和跟踪、响应和恢复等。在信息系统安全防护体系设计中，保证“信息系统中数据不被非法修改、破坏、丢失等”是为了达到防护体系完整性的目标。

参考答案

（6）D

试题（7）

下列技术中，不能预防重放攻击的是__（7）__。

（7）A．时间戳　　B．nonce　　C．明文填充　　D．序号

试题（7）分析

本题考查防重放攻击方面的基础知识。

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，主要用于身份认证过程，破坏认证的正确性。重放攻击可以由发起者也可以由拦截并重发该数据的敌方进行。攻击者利用网络监听或者其他方式盗取认证凭据，之后再把它重新

发给认证服务器。重放攻击在任何网络通信过程中都可能发生，是黑客常用的攻击方式之一。预防重放攻击的方式包括时间戳、nonce、序号等。

参考答案

（7）C

试题（8）

计算机取证主要是对电子证据的获取、分析、归档和描述的过程，而电子证据需要在法庭上作为证据展示，进行计算机取证时应当充分考虑电子证据的真实性和电子证据的证明力。除了相关准备之外，计算机取证步骤通常不包括__（8）__。

（8）A．保护目标计算机系统　　B．确定电子证据

C．收集电子证据、保全电子证据　　D．清除恶意代码

试题（8）分析

本题考查计算机取证方面的基础知识。

计算机取证主要是对电子证据的获取、分析、归档和描述的过程，而电子证据需要在法庭上作为证据展示，进行计算机取证时应当充分考虑电子证据的真实性和电子证据的证明力。计算机取证工作一般按照下面步骤进行：

① 在取证检查中，保护目标计算机系统，避免发生任何的改变、伤害、数据破坏或病毒感染；

② 搜索目标系统中的所有文件。包括现存的正常文件，已经被删除但仍存在于磁盘上（即还没有被新文件覆盖）的文件，隐藏文件，受到密码保护的文件和加密文件；

③ 全部（或尽可能）恢复发现的已删除文件；

④ 最大程度地显示操作系统或应用程序使用的隐藏文件、临时文件和交换文件的内容；

⑤ 如果可能且法律允许，访问被保护或加密文件的内容；

⑥ 分析在磁盘的特殊区域中发现的所有相关数据；

⑦ 打印对目标计算机系统的全面分析结果，然后给出分析结论，包括系统的整体情况，发现的文件结构、数据和作者的信息，对信息的任何隐藏、删除、保护、加密企图，以及在调查中发现的其他的相关信息；

⑧ 给出必需的专家证明。

参考答案

（8）D

试题（9）

数字水印是通过数字信号处理的方法，在数字化的多媒体数据中，嵌入隐蔽的水印标记，其应用领域不包括__（9）__。

（9）A．版权保护　　B．票据防伪

C．证据篡改鉴定　　D．图像增强

试题（9）分析

本题考查数字水印方面的基础知识。

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。水印信息与原始数据紧密结合并隐藏其中，成为一个整体。

数字水印的主要应用领域包括：原始数据的真伪鉴别、证据篡改鉴定、数据侦测和跟踪、数字产品版权保护等。

参考答案

（9）D

试题（10）

信息系统安全测评方法中的模糊测试是一种黑盒测试技术，它将大量的畸形数据输入到目标程序中，通过监测程序的异常来发现被测程序中可能存在的安全漏洞。关于模糊测试，以下说法错误的是__（10）__。

（10）A．与白盒测试相比，具有更好的适用性

B．模糊测试是一种自动化的动态漏洞挖掘技术，不存在误报，也不需要人工进行大量的逆向分析工作

C．模糊测试不需要程序的源代码就可以发现问题

D．模糊测试受限于被测系统的内部实现细节和复杂度

试题（10）分析

本题考查信息系统安全测评方法。

信息系统安全测评方法中的模糊测试是一种黑盒测试技术，它将大量的畸形数据输入到目标程序中，通过监测程序的异常来发现被测程序中可能存在的安全漏洞。模糊测试不需要程序的源代码就可以发现问题，是一种自动化的动态漏洞挖掘技术，不存在误报，也不需要人工进行大量的逆向分析工作，与白盒测试相比，具有更好的适用性。

参考答案

（10）D

试题（11）

下列攻击中，不能导致网络瘫痪的是__（11）__。

（11）A．溢出攻击　　B．钓鱼攻击

C．邮件炸弹攻击　　D．拒绝服务攻击

试题（11）分析

本题考查网络攻击方面的基础知识。

网络攻击是指利用网络存在的漏洞和安全缺陷对网络系统的硬件、软件及系统中的数据进行的攻击。从对信息的破坏性上看，攻击类型可以分为被动攻击和主动攻击，其中常见的主动攻击有篡改消息、伪造、拒绝服务等，常见的被动攻击有流量分析、窃听

等。其中钓鱼攻击不能导致网络瘫痪。

参考答案

（11）B

试题（12）

（12）是一种通过对信息进行均衡、全面的防护，提高整个系统最低安全性能的原则。

（12）A．木桶原则　　B．保密原则

C．等级化原则　　D．最小特权原则

试题（12）分析

本题考查信息安全基本原则的内容。

木桶原则是一种通过对信息进行均衡、全面的防护，提高整个系统最低安全性能的原则。

参考答案

（12）A

试题（13）

网站的安全协议是 https 时，该网站浏览时会进行（13）处理。

（13）A．增加访问标记　　B．加密

C．身份隐藏　　D．口令验证

试题（13）分析

本题考查安全协议 https 的基础知识。

超文本传输协议 http 协议被用于在 Web 浏览器和网站服务器之间传递信息。http 协议以明文方式发送内容，不提供任何方式的数据加密，如果攻击者截取了 Web 浏览器和网站服务器之间的传输报文，就可以直接读懂其中的信息，因此 http 协议不适合传输一些敏感信息。为了数据传输的安全，研究者提出了安全套接字层超文本传输协议 https，https 在 http 的基础上加入了 SSL 协议，SSL 依靠证书来验证服务器的身份，并为浏览器和服务器之间的通信加密。

参考答案

（13）B

试题（14）

被动攻击通常包含（14）。

（14）A．拒绝服务攻击　　B．欺骗攻击

C．窃听攻击　　D．数据驱动攻击

试题（14）分析

本题考查被动攻击方面的基础知识。

网络攻击是指利用网络存在的漏洞和安全缺陷对网络系统的硬件、软件及系统中的

数据进行的攻击。从对信息的破坏性上看，攻击类型可以分为被动攻击和主动攻击，其中主动攻击会导致某些数据流的篡改和虚假数据流的产生，常见的主动攻击有篡改消息、伪造、拒绝服务等；被动攻击中攻击者不对数据信息做任何修改。截取/窃听是指在未经用户同意和认可的情况下攻击者获得了信息或相关数据，常见的被动攻击有窃听、流量分析、破解弱加密的数据流等攻击方式等。

参考答案

（14）C

试题（15）

以下网络攻击方式中，（15）实施的攻击不是网络钓鱼的常用手段。

（15）A．利用社会工程学

B．利用虚假的电子商务网站

C．利用假冒网上银行、网上证券网站

D．利用蜜罐

试题（15）分析

本题考查网络钓鱼方面的基础知识。

网络钓鱼是通过大量发送声称来自于银行或其他知名机构的欺骗性垃圾邮件，意图引诱收信人给出敏感信息的一种攻击方式。网络钓鱼的常用手段包括：利用社会工程学、利用虚假的电子商务网站、利用假冒网上银行、网上证券网站等。

参考答案

（15）D

试题（16）

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。一个数字签名体制通常包括两个部分：（16）。

（16）A．施加签名和验证签名　　B．数字证书和身份认证

C．身份消息加密和解密　　D．数字证书和消息摘要

试题（16）分析

本题考查数字签名方面的知识。

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。它通常将某个算法作用于需要签名的消息，生成一种带有操作者身份信息的编码。一个数字签名体制一般包含两个组成部分，即签名算法（Signature Algorithm）和验证算法（Verification Algorithm）。签名算法用于对消息产生数字签名，它通常受一个签名密钥的控制，签名算法或者签名密钥是保密的，由签名者掌握；验证算法用于对消息的数字签名进行验证，根据签名是否有效，验证算法能够给出该签名为“真”或者“假”的结论。验证算法通常也受一个验证密钥的控制，但验证算法和验证密钥应当是公开的，以便需要验证签名的人能够方便地验证。

参考答案

（16）A

试题（17）

身份识别在信息安全领域有着广泛的应用，通过识别用户的生理特征来认证用户的身份是安全性很高的身份认证方法。如果把人体特征用于身份识别，则它应该具有不可复制的特点，必须具有（17）。

（17）A．唯一性和保密性　　B．唯一性和稳定性

C．保密性和可识别性　　D．稳定性和可识别性

试题（17）分析

本题考查身份识别方面的基础知识。

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以下几种：用户名/密码方式、智能卡认证、动态口令、USB Key 认证、生物特征认证等。原则上用于身份认证的生物特征必须具有普遍性、唯一性、稳定性、可采集性。

参考答案

（17）B

试题（18）

ISO 制定的安全体系结构描述了 5 种安全服务，以下不属于这 5 种安全服务的是（18）。

（18）A．鉴别服务　　B．数据报过滤

C．访问控制　　D．数据完整性

试题（18）分析

本题考查 ISO 制定的安全体系结构方面的基础知识。

ISO 制定的安全体系结构的安全目标是实现信息安全保密性、完整性与可用性的具体化，其包含的安全服务包括：鉴别服务、访问控制、数据完整性、抗抵赖性、数据保密。

参考答案

（18）B

试题（19）

在使用复杂度不高的口令时，容易产生弱口令的安全脆弱性，被攻击者利用，从而破解用户账户。下列设置的口令中，（19）具有最好的口令复杂度。

（19）A．morrison　　B．Wm.$*F2m5@

C．27776394　　D．wangjingl977

试题（19）分析

本题考查弱口令方面的基础知识。

弱口令是指容易被别人猜测到或被破解工具破解的口令均为弱口令，这类弱口令往往仅包含简单数字和字母，很容易被别人破解，从而使用户的计算机面临风险。安全的口令应该满足：口令长度不小于 8 个字符、口令不应该为连续的某个字符、口令应该为大写字母（A～Z）、小写字母（a～z）、数字（0～9）和特殊字符的组合等。

参考答案

（19）B

试题（20）

工控系统广泛应用于电力、石化、医药、航天等领域，已经成为国家关键基础设施的重要组成部分。作为信息基础设施的基础，电力工控系统安全面临的主要威胁不包括（20）。

（20）A．内部人为风险　　B．黑客攻击

C．设备损耗　　D．病毒破坏

试题（20）分析

本题考查工控系统安全方面的基础知识。

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。工控系统安全面临的主要威胁包括：内部人为风险、黑客攻击、病毒破坏、系统漏洞等。工业控制系统信息安全技术涉及方案部署、风险评估、生命周期、管理体系、项目工程、产品认证、工业控制系统入侵检测与入侵防护、工业控制系统补丁管理等。

参考答案

（20）C

试题（21）

对日志数据进行审计检查，属于（21）类控制措施。

（21）A．预防　　B．检测　　C．威慑　　D．修正

试题（21）分析

本题考查日志数据审计方面的基础知识。

日志审计是负责收集企业范围内的安全和系统的信息，有效的分析来自异构系统的安全事件数据，通过归类、合并、优化、直观的呈现等方法，使企业员工轻松地识别网络环境中潜在的恶意威胁活动。对日志数据进行审计检查，属于检测类控制措施。

参考答案

（21）B

试题（22）

攻击者通过对目标主机进行端口扫描，可以直接获得（22）。

（22）A．目标主机的口令

B．给目标主机种植木马

C．目标主机使用了什么操作系统

D．目标主机开放了哪些端口服务

试题（22）分析

本题考查端口扫描方面的基础知识。

端口扫描是指逐个对一段端口或指定的端口进行扫描，通过扫描结果可以知道一台计算机上都提供了哪些服务，然后就可以通过所提供的这些服务的已知漏洞进行攻击。攻击者通过对目标主机进行端口扫描，可以搜集到很多关于目标主机的各种很有参考价值的信息，如攻击者可以直接获得目标主机开放了哪些端口服务的信息。

参考答案

（22）D

试题（23）

以下关于 NAT 的说法中，错误的是__（23）__。

（23）A．NAT 允许一个机构专用 Intranet 中的主机透明地连接到公共域中的主机，无需每台内部主机都拥有注册的（已经越来越缺乏的）全局互联网地址

B．静态 NAT 是设置起来最简单和最容易实现的一种地址转换方式，内部网络中的每个主机都被永久映射成外部网络中的某个合法地址

C．动态 NAT 主要应用于拨号和频繁的远程连接，当远程用户连接上之后，动态 NAT 就会分配给用户一个 IP 地址，当用户断开时，这个 IP 地址就会被释放而留待以后使用

D．动态 NAT 又叫网络地址端口转换 NAPT

试题（23）分析

本题考查 NAT 基础知识。

NAT（Network Address Translation，网络地址转换）能有效解决 IP 地址不足的问题，而且还能够有效避免来自网络外部的攻击，隐藏并保护网络内部的计算机。NAT 允许一个机构专用 Intranet 中的主机透明地连接到公共域中的主机，无需每台内部主机都拥有注册的（已经越来越缺乏的）全局互联网地址。静态 NAT 是设置起来最简单和最容易实现的一种地址转换方式，内部网络中的每个主机都被永久映射成外部网络中的某个合法地址。动态 NAT 主要应用于拨号和频繁的远程连接，当远程用户连接上之后，动态 NAT 就会分配给用户一个 IP 地址，当用户断开时，这个 IP 地址就会被释放而留待以后使用。

参考答案

（23）D

试题（24）

应用代理防火墙的主要优点是__（24）__。

（24）A．加密强度更高　　B．安全控制更细化、更灵活

C．安全服务的透明性更好　　D．服务对象更广泛

试题（24）分析

本题考查防火墙基础知识。

应用代理防火墙也被称为代理服务器，它针对特定的网络应用服务协议使用指定的数据过滤逻辑，并在过滤的同时，对数据包进行必要的分析、登记和统计，形成报告。应用代理防火墙的优点是安全性较高，可以针对应用层进行侦测和扫描，安全控制更细化、更灵活。

参考答案

（24）B

试题（25）

从安全属性对各种网络攻击进行分类，阻断攻击是针对（25）的攻击。

（25）A．机密性　　B．可用性　　C．完整性　　D．真实性

试题（25）分析

本题考查安全属性和攻击方面的基础知识。

信息安全的基本属性包括完整性、保密性、不可否认性、可用性和可控性。拒绝服务攻击是指利用网络上已被攻陷的电脑向某一特定的目标电脑发动密集式的拒绝服务要求，借以把目标电脑的网络资源及系统资源耗尽，使之无法向真正正常请求的用户提供服务，阻断攻击是针对可用性的攻击。

参考答案

（25）B

试题（26）

下列各种协议中，不属于身份认证协议的是（26）。

（26）A．S/Key 口令协议　　B．Kerberos 协议

C．X.509 协议　　D．IPSec 协议

试题（26）分析

本题考查身份认证协议方面的基础知识。

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。常见的身份认证协议包括 S/Key 口令协议、Kerberos 协议、X.509 协议等。

参考答案

（26）D

试题（27）

我国制定的关于无线局域网安全的强制性标准是（27）。

（27）A．IEEE 802.11　　B．WPA

C．WAPI　　D．WEP

试题（27）分析

本题考查无线局域网安全标准方面的基础知识。

当前全球无线局域网领域仅有的两个标准，分别是美国行业标准组织提出的 IEEE 802.11 系列标准以及中国提出的 WAPI 标准。WAPI 是我国首个在计算机宽带无线网络通信领域自主创新并拥有知识产权的安全接入技术标准，WAPI 全称是无线局域网鉴别和保密基础结构，是一种安全协议，同时也是中国无线局域网安全强制性标准。

参考答案

（27）C

试题（28）

以下恶意代码中，属于宏病毒的是（28）。

（28）A．Macro.Melissa　　B．Trojan.huigezi.a

C．Worm.Blaster.g　　D．Backdoor.Agobot.frt

试题（28）分析

本题考查宏病毒方面的知识。

宏病毒是一种寄存在文档或模板的宏中的计算机病毒。一旦打开这样的文档，其中的宏就会被执行，于是宏病毒就会被激活，转移到计算机上，并驻留在 Normal 模板上。常见的宏病毒包括 Macro.Melissa、Nuclear 宏病毒等。

参考答案

（28）A

试题（29）

容灾的目的和实质是（29）。

（29）A．实现对系统数据的备份　　B．提升用户的安全预期

C．保持信息系统的业务持续性　　D．信息系统的必要补充

试题（29）分析

本题考查系统灾备方面的基础知识。

容灾系统是指在相隔较远的异地，建立两套或多套功能相同的 IT 系统，可以进行健康状态监视和功能切换，当一处系统因意外（如火灾、地震等）停止工作时，整个应用系统可以切换到另一处，使得该系统功能可以继续正常工作。容灾的目的和实质是保持信息系统的业务持续性。

参考答案

（29）C

试题（30）

安卓的系统架构从上层到下层包括：应用程序层、应用程序框架层、系统库和安卓运行时、Linux 内核。其中，文件访问控制的安全服务位于（30）。

（30）A．应用程序层　　B．应用程序框架层

C．系统库和安卓运行时　　D．Linux 内核

试题（30）分析

本题考查安卓系统架构知识。

安卓系统架构是指安卓系统的体系结构，是一个分层的架构，共分为四层，从上层到下层依次为：应用程序层、应用程序框架层、系统库和安卓运行时、Linux 内核。安卓的核心系统服务依赖于 Linux 内核，如安全性、内存管理、进程管理、网络协议栈和驱动模型等，其中文件访问控制的安全服务位于 Linux 内核。

参考答案

（30）D

试题（31）

下面不属于 PKI 组成部分的是__（31）__。

（31）A．证书主体　　B．使用证书的应用和系统

C．证书权威机构　　D．AS

试题（31）分析

本题考查 PKI 的基础知识。

PKI（Public Key Infrastructure）即公钥基础设施，是一种支持公开密钥管理并能支持认证、加密、完整性和可追究性服务的基础设施。一个完整的 PKI 系统必须具有权威认证中心 CA（Certificate Authority）、注册中心 RA（Registration Authority）、数字证书库、密钥备份与恢复系统、证书撤销处理系统、PKI 应用接口系统 API 等基本构成部分。

参考答案

（31）D

试题（32）

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__（32）__。

（32）A．保密性　　B．可用性　　C．完整性　　D．可认证性

试题（32）分析

本题考查 SSL 协议方面的知识。

SSL 协议即 SSL（Secure Sockets Layer）安全套接层协议，它位于TCP/IP 协议与各种应用层协议之间，为数据通信提供安全支持。SSL 协议可分为两层：

① SSL 记录协议（SSL Record Protocol）：它建立在可靠的传输协议（如 TCP）之上，为高层协议提供数据封装、压缩、加密等基本功能的支持。

② SSL握手协议（SSL Handshake Protocol）：它建立在 SSL 记录协议之上，用于在实际的数据传输开始前，通信双方进行身份认证、协商加密算法、交换加密密钥等。

SSL 协议提供的安全服务包括：认证用户和服务器，确保数据发送到正确的客户机和服务器；加密数据以防止数据中途被窃取；维护数据的完整性，确保数据在传输过程中不被改变。

参考答案

（32）B

试题（33）

通过具有 IPSec 功能的路由器构建 VPN 的过程中，采用的应用模式是__（33）__。

（33）A．隧道模式　　B．保密模式　　C．传输模式　　D．压缩模式

试题（33）分析

本题考查 VPN 方面的知识。

VPN 即虚拟专用网络，其主要功能是在公用网络上建立专用网络，进行加密通信，VPN 网关通过对数据包的加密和数据包目标地址的转换实现远程访问。IPSec 是一种由 IETF 设计的端到端的确保基于 IP 通信的数据安全性的机制。IPSec VPN 是基于 IPSec 协议的 VPN 技术，由 IPSec 协议提供隧道安全保障。

参考答案

（33）A

试题（34）

安全策略表达模型是一种对安全需求与安全策略的抽象概念模型，一般分为：自主访问控制模型和强制访问控制模型。以下属于自主访问控制模型的是__（34）__。

（34）A．BLP 模型　　B．HRU 模型

C．BN 模型　　D．基于角色的访问控制模型

试题（34）分析

本题考查访问控制模型方面的知识。

访问控制是指主体依据某些控制策略或权限对客体本身或是其资源进行的不同授权访问，是网络安全防范和保护的主要策略，它的主要任务是保证网络资源不被非法使用和非常规访问，一般分为自主访问控制模型和强制访问控制模型。自主访问控制（Discretionary Access Control，DAC）是最常用的一种存取访问控制机制，文件的拥有者可以按照自己的意愿精确指定系统中的其他用户对此文件的访问权。强制访问控制（Mandatory Access Control，MAC），是一种不允许主体干涉的访问控制类型。它是基于安全标识和信息分级等信息敏感性的访问控制，通过比较资源的敏感性与主体的级别来确定是否允许访问。

参考答案

（34）B

试题（35）

SHA1 算法的消息摘要长度是__（35）__位。

（35）A．128　　B．160　　C．256　　D．512

试题（35）分析

本题考查 Hash 函数方面的基础知识。

SHA1 算法也称安全哈希算法，SHA1 会产生一个 160 位的消息摘要。

参考答案

（35）B

试题（36）

A 方有一对密钥（KA_{pub}，KA_{pri}），B 方有一对密钥（KB_{pub}，KB_{pri}），A 方给 B 方发送信息 M，对信息 M 加密为：M’=KB_{pub}（KA_{pri}（M））。B 方收到密文，正确的解密方案是（36）。

（36）A．KB_{pub}（KA_{pri}（M’））　　B．KA_{pub}（KA_{pub}（M’））

C．KA_{pub}（KB_{pri}（M’））　　D．KB_{pri}（KA_{pri}（M’））

试题（36）分析

本题考查密码学方面的基础知识。

公钥密码采用两个具有一一对应关系的密钥对 $k=(pk,sk)$ 使加密和解密的过程相分离。当两个用户希望借助公钥体制进行保密通信时，发信方 Alice 用收信方 Bob 的公开密钥 pk 加密消息并发送给接收方；而接收方 Alice 使用与公钥相对应的私钥 sk 进行解密。因此，正确的解密方案是 KA_{pub}（KB_{pri}（M’））。

参考答案

（36）C

试题（37）

有线等效保密协议 WEP 采用 RC4 流密码技术实现保密性，标准的 64 位 WEP 使用的密钥和初始向量长度分别是（37）。

（37）A．32 位和 32 位　　B．48 位和 16 位

C．56 位和 8 位　　D．40 位和 24 位

试题（37）分析

本题考查有线等效保密协议 WEP 方面的基础知识。

有线等效保密协议 WEP 是由 802.11 标准定义的，是最基本的无线安全加密措施，用于在无线局域网中保护链路层数据。WEP 加密采用静态的保密密钥，各 WLAN 终端使用相同的密钥访问无线网络。标准的 64 位 WEP 使用的密钥和初始向量长度分别是 40 位和 24 位。

参考答案

（37）D

试题（38）

文件型病毒不能感染的文件类型是（38）。

（38）A．COM 类型　　B．HTML 类型

C．SYS 类型　　D．EXE 类型

试题（38）分析

本题考查计算机病毒方面的基础知识。

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。它可以隐藏在看起来无害的程序中，也可以生成自身的拷贝并插入到其他程序中。文件型病毒系计算机病毒的一种，主要通过感染计算机中的可执行文件（.exe）和命令文件（.com）。文件型病毒是对计算机的源文件进行修改，使其成为新的带毒文件。一旦计算机运行该文件就会被感染，从而达到传播的目的。

参考答案

（38）B

试题（39）

在非安全的通信环境中，为了保证消息来源的可靠性，通常采用的安全防护技术是（39）。

（39）A．信息隐藏技术　　B．数据加密技术

C．消息认证技术　　D．数字水印技术

试题（39）分析

本题考查信息认证方面的基础知识。

信息的可认证性是信息安全的一个重要方面。认证的目的有两个：一是验证信息的完整性，即验证信息在传送或存储过程中未被窜改、重放或延迟等。二是验证信息发送者是真的，而不是冒充的。认证是防止敌手对系统进行主动攻击（如伪造、篡改信息等）的一种重要技术。

参考答案

（39）C

试题（40）

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。现有的审计系统包括（40）三大功能模块。

（40）A．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

B．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

C．系统日志采集与挖掘、安全事件记录及查询、安全响应报警

D．审计事件特征提取、审计事件特征匹配、安全响应报警

试题（40）分析

本题考查安全审计方面的基础知识。

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。现有的审计系统包括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三大功能模块。

参考答案

（40）A

试题（41）

计算机病毒的生命周期一般包括__（41）__四个阶段。

（41）A．开发阶段、传播阶段、发现阶段、清除阶段

B．开发阶段、潜伏阶段、传播阶段、清除阶段

C．潜伏阶段、传播阶段、发现阶段、清除阶段

D．潜伏阶段、传播阶段、触发阶段、发作阶段

试题（41）分析

本题考查计算机病毒方面的基础知识。

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。它可以隐藏在看起来无害的程序中，也可以生成自身的拷贝并插入到其他程序中。计算机病毒的生命周期一般包括潜伏阶段、传播阶段、触发阶段、发作阶段四个阶段。

参考答案

（41）D

试题（42）

下面关于跨站攻击描述不正确的是__（42）__。

（42）A．跨站脚本攻击指的是恶意攻击者向 Web 页面里插入恶意的 html 代码

B．跨站脚本攻击简称 XSS

C．跨站脚本攻击也可称作 CSS

D．跨站脚本攻击是主动攻击

试题（42）分析

本题考查跨站攻击方面的知识。

跨站攻击是指攻击者利用网站程序对用户的输入过滤不足造成的，输入可以显示在页面上对其他用户造成影响的 HTML 代码，从而盗取用户资料、利用用户身份进行某种动作或者对访问者进行病毒侵害的一种攻击方式。跨站脚本攻击简称为 XSS，也可称作 CSS，指的是恶意攻击者向 Web 页面里插入恶意的 HTML 代码。

参考答案

（42）D

试题（43）

以下不属于信息安全风险评估中需要识别的对象是__（43）__。

（43）A．资产识别　　B．威胁识别

C．风险识别　　D．脆弱性识别

试题（43）分析

本题考查信息安全风险评估方面的知识。

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。信息安全风险评估中需要识别的对象包括：资产识别、威胁识别、脆弱性识别。

参考答案

（43）C

试题（44）

安全漏洞扫描技术是一类重要的网络安全技术。当前，网络安全漏洞扫描技术的两大核心技术是（44）。

（44）A．PING 扫描技术和端口扫描技术

B．端口扫描技术和漏洞扫描技术

C．操作系统探测和漏洞扫描技术

D．PING 扫描技术和操作系统探测

试题（44）分析

本题考查安全漏洞扫描技术方面的基础知识。

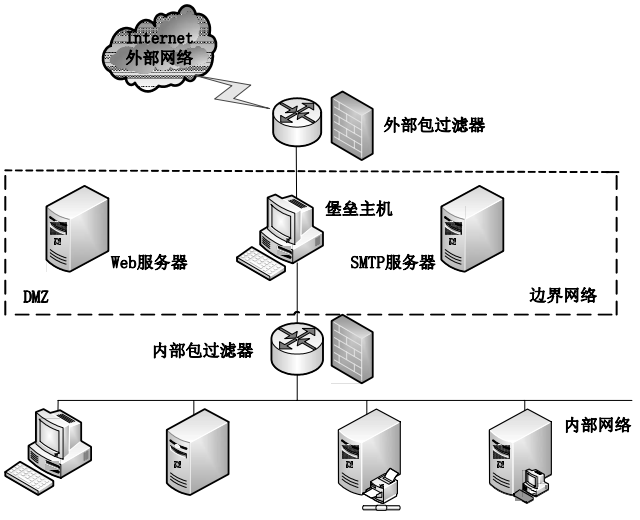
漏洞扫描是指基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用漏洞的一种安全检测（渗透攻击）行为。当前，网络安全漏洞扫描技术的两大核心技术是端口扫描技术和漏洞扫描技术。

参考答案

（44）B

试题（45）

防火墙的经典体系结构主要有三种，下图给出的是（45）体系结构。



（45）A．双重宿主主机　　B．（被）屏蔽主机

C．（被）屏蔽子网　　D．混合模式

试题（45）分析

本题考查防火墙体系结构方面的基础知识。

防火墙是一种隔离控制技术，在机构内的网络和不安全的网络之间设置屏障，阻止对信息资源的非法访问，也可以使用防火墙阻止重要信息从企业的网络上被非法输出。防火墙的经典体系结构主要有双重宿主主机体系结构、屏蔽主机体系结构和屏蔽子网体系结构。

参考答案

（45）C

试题（46）

计算机系统的安全级别分为四级： D、C（C1、C2）、B（B1、B2、B3）和 A。其中被称为选择性保护级的是（46）。

（46）A．C1　　B．C2　　C．B1　　D．B2

试题（46）分析

本题考查计算机系统安全级别方面的基础知识。

计算机系统安全的主要目标是监督保障系统运行的安全性，保障系统自身的安全性，标识系统中的用户，进行身份认证，依据系统安全策略对用户的操作行为进行监控。计算机系统的安全级别就是计算机系统的安全等级，分为四组七个等级：D、C（C1、C2）、B（B1、B2、B3）和 A。

D 级别是最低的安全级别，对系统提供最小的安全防护。

C 级别有 C1 级和 C2 级两个子系统。C1 级称为选择性保护级，可以实现自主安全防护，对用户和数据的分离，保护或限制用户权限的传播。C2 级具有访问控制环境的权利，比 C1 的访问控制划分的更为详细，能够实现受控安全保护、个人账户管理、审计和资源隔离。这个级别的系统包括 UNIX、Linux 和 Windows NT 系统。

C 级别属于自由选择性安全保护，在设计上有自我保护和审计功能，可对主体行为进行审计与约束。

B 级别包括 B1、B2 和 B3 三个级别，B 级别能够提供强制性安全保护和多级安全。强制防护是指定义及保持标记的完整性，信息资源的拥有者不具有更改自身的权限，系统数据完全处于访问控制管理的监督下。

B1 级称为标识安全保护。B2 级称为结构保护级别，要求访问控制的所有对象都有安全标签以实现低级别的用户不能访问敏感信息，对于设备、端口等也应标注安全级别。B3 级别称为安全域保护级别，这个级别使用安装硬件的方式来加强域的安全，比如用内存管理硬件来防止无授权访问。

A 级别称为验证设计级（Verity Design），是目前最高的安全级别。在 A 级别中，安

全的设计必须给出形式化设计说明和验证，需要有严格的数学推导过程，同时应该包含秘密信道和可信分布的分析。

参考答案

（46）A

试题（47）

IP 地址欺骗的发生过程，下列顺序正确的是（47）。①确定要攻击的主机 A；②发现和它有信任关系的主机 B；③猜测序列号；④成功连接，留下后门；⑤将 B 利用某种方法攻击瘫痪。

（47）A．①②⑤③④　　B．①②③④⑤

C．①②④③⑤　　D．②①⑤③④

试题（47）分析

本题考查 IP 地址欺骗的基本流程。

IP 地址欺骗是冒充身份通过认证来骗取信任的攻击方式，是使一台主机信任另外一台主机的复杂技术。IP 地址欺骗是指行动产生的 IP 数据包为伪造的源 IP 地址，以便冒充其他系统或发件人的身份。IP 地址欺骗的基本流程是：确定要攻击的主机 A；发现和它有信任关系的主机 B；将 B 利用某种方法攻击瘫痪；猜测序列号；成功连接，留下后门。

参考答案

（47）A

试题（48）

以下不属于网络安全控制技术的是（48）。

（48）A．防火墙技术　　B．数据备份与容灾技术

C．入侵检测技术　　D．访问控制技术

试题（48）分析

本题考查网络安全控制技术方面的基础知识。

网络安全控制技术指致力于解决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，主要包括物理安全分析技术，网络结构安全分析技术，系统安全分析技术，管理安全分析技术，及其他的安全服务和安全机制策略等。网络安全控制技术包括防火墙技术、入侵检测技术、访问控制技术等。

参考答案

（48）B

试题（49）

以下关于认证技术的叙述中，错误的是（49）。

（49）A．基于生物特征认证一般分为验证和识别两个过程

B．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

C．数字签名的结果是十六进制的字符串

D．消息认证能够确定接收方收到的消息是否被篡改过

试题（49）分析

本题考查信息认证方面的基础知识。

信息的可认证性是信息安全的一个重要方面。认证的目的有两个：一是验证信息的完整性，即验证信息在传送或存储过程中未被窜改、重放或延迟等；二是验证信息发送者是真的，而不是冒充的。认证是防止敌手对系统进行主动攻击（如伪造、篡改信息等）的一种重要技术。实现信息认证涉及的主要技术包括：信息的完整性检验、数字签名技术和身份识别技术等技术。

参考答案

（49）C

试题（50）

为了防御网络监听，最常用的方法是（50）。

（50）A．采用物理传输（非网络）　　B．信息加密

C．无线网　　D．使用专线传输

试题（50）分析

本题考查网络监听方面的基础知识。

网络监听是一种监视网络状态、数据流程以及网络上信息传输的管理工具，它可以将网络界面设定成监听模式，并且可以截获网络上所传输的信息。为了防御网络监听，最常用的方法是信息加密。

参考答案

（50）B

试题（51）

能有效控制内部网络和外部网络之间的访问及数据传输，从而达到保护内部网络的信息不受外部非授权用户的访问和对不良信息的过滤的安全技术是（51）。

（51）A．入侵检测　　B．反病毒软件

C．防火墙　　D．计算机取证

试题（51）分析

本题考查防火墙的基础知识。

防火墙是一种能有效控制内部网络和外部网络之间的访问及数据传输，从而达到保护内部网络的信息不受外部非授权用户的访问和对不良信息进行过滤的安全技术。

参考答案

（51）C

试题（52）

包过滤技术防火墙在过滤数据包时，一般不关心（52）。

（52）A．数据包的源地址　　B．数据包的目的地址
　　C．数据包的协议类型　　D．数据包的内容

试题（52）分析

本题考查包过滤技术防火墙的基础知识。

防火墙是一种能有效控制内部网络和外部网络之间的访问及数据传输，从而达到保护内部网络的信息不受外部非授权用户的访问和对不良信息进行过滤的安全技术。包过滤防火墙技术是在 IP 层实现的，它可以只用路由器就能够实现。它设置在网络层，首先应建立一定数量的信息过滤表，信息过滤表是以收到的数据包头信息为基础而建成的。信息包头含有数据包源 IP 地址、目的 IP 地址、传输协议类型（TCP、UDP、ICMP 等）、协议源端口号、协议目的端口号、连接请求方向等。当一个数据包满足过滤表中的规则时，则允许数据包通过，否则禁止通过。

参考答案

（52）D

试题（53）

密码分析的目的是__（53）__。

（53）A．发现加密算法　　B．发现密钥或者密文对应的明文
　　C．发现解密算法　　D．发现攻击者

试题（53）分析

本题考查密码学方面的基础知识。

密码分析是指通过研究密码变化的客观规律，并将其应用于破译密码，实现获取通信信息的技术。密码分析的目的是发现密钥或者密文对应的明文。

参考答案

（53）B

试题（54）

下列关于数字签名说法正确的是__（54）__。

（54）A．数字签名是不可信的　　B．数字签名容易被伪造
　　C．数字签名容易抵赖　　D．数字签名不可改变

试题（54）分析

本题考查数字签名方面的基础知识。

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。它通常将某个算法作用于需要签名的消息，生成一种带有操作者身份信息的编码。数字签名主要用来解决信息的不可信、被伪造、抵赖等问题，数字签名具有不可改变性。

参考答案

（54）D

试题（55）

以下关于公钥基础设施（PKI）的说法中，正确的是（55）。

（55）A．PKI 可以解决公钥可信性问题　B．PKI 不能解决公钥可信性问题

C．PKI 只能由政府来建立　D．PKI 不提供数字证书查询服务

试题（55）分析

本题考查 PKI 方面的基础知识。

公钥基础设施（PKI）是一种遵循既定标准的密钥管理平台，它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系。PKI 可以解决公钥可信性问题。

参考答案

（55）A

试题（56）

下列关于公钥体制说法不正确的是（56）。

（56）A．在一个公钥体制中，一般存在公钥和私钥两类密钥

B．公钥体制中仅根据加密密钥来确定解密密钥在计算上是可行的

C．公钥体制中的公钥可以以明文方式发送

D．公钥密码中的私钥可以用来进行数字签名

试题（56）分析

本题考查公钥密码体制方面的基础知识。

公开密钥加密算法也称为公钥加密算法，是指用来解密的密钥不同于进行加密的密钥，也不能够通过加密密钥直接推算出解密密钥。一般情况下，加密密钥是可以公开的，任何人都可以应用加密密钥来对信息进行加密，但只有拥有解密密钥的人才可以解密出被加密的信息。

参考答案

（56）B

试题（57）

无线传感器网络容易受到各种恶意攻击，以下关于其防御手段说法错误的是（57）。

（57）A．采用干扰区内节点切换通信频率的方式抵御干扰

B．通过向独立多路径发送验证数据来发现异常节点

C．利用中心节点监视网络中其他所有节点来发现恶意节点

D．利用安全并具有弹性的时间同步协议对抗外部攻击和被俘获节点的影响

试题（57）分析

本题考查无线传感器网络防御方面的基础知识。

无线传感器网络（Wireless Sensor Network，WSN）是由大量的静止或移动的传感器

以自组织和多跳的方式构成的无线网络，以协作地感知、采集、处理和传输网络覆盖地理区域内被感知对象的信息，并最终把这些信息发送给网络的所有者。无线传感器网络容易受到各种恶意攻击，采用干扰区内节点切换通信频率的方式抵御干扰，通过向独立多路径发送验证数据来发现异常节点，利用安全并具有弹性的时间同步协议对抗外部攻击和被俘获节点的影响。

参考答案

（57）C

试题（58）

属于第二层的 VPN 隧道协议是（58）。

（58）A．IPSec　　B．PPTP　　C．GRE　　D．IPv4

试题（58）分析

本题考查 VPN 方面的基础知识。

VPN 被定义为通过一个公用网络（通常是因特网）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。虚拟专用网是对企业内部网的扩展。VPN 的基本原理是：在公共通信网上为需要进行保密通信的通信双方建立虚拟的专用通信通道，并且所有传输数据均经过加密后再在网络中进行传输，这样做可以有效保证机密数据传输的安全性。在虚拟专用网中，任意两个节点之间的连接并没有传统专用网所需的端到端的物理链路，虚拟的专用网络通过某种公共网络资源动态组成。属于第二层的 VPN 隧道协议是 PPTP。

参考答案

（58）B

试题（59）

信息隐藏主要研究如何将机密信息秘密隐藏于另一公开的信息中。以下关于利用多媒体数据来隐藏机密信息的叙述中，错误的是（59）。

（59）A．多媒体信息本身有很大的冗余性

B．多媒体信息本身编码效率很高

C．人眼或人耳对某些信息有一定的掩蔽效应

D．信息嵌入到多媒体信息中不影响多媒体本身的传送和使用

试题（59）分析

本题考查信息隐藏方面的基础知识。

信息隐藏又称为信息伪装，就是通过减少载体的某种冗余，如空间冗余、数据冗余等，来隐藏敏感信息，达到某种特殊的目的。利用多媒体数据来隐藏机密信息，多媒体信息本身有很大的冗余性，人眼或人耳对某些信息有一定的掩蔽效应，信息嵌入到多媒体信息中不影响多媒体信息本身的传送和使用。

参考答案

（59）B

试题（60）

证书授权中心（CA）的主要职责不包含__（60）__。

（60）A．证书管理　　B．证书签发

C．证书加密　　D．证书撤销

试题（60）分析

本题考查 PKI 证书授权中心的基础知识。

在 PKI 体系中，认证中心 CA 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。CA 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捆绑在一起，在网上验证用户的身份，同时 CA 还负责证书废止列表 CRL 的登记和发布。由于 CA 是一个各方都信任的机构，其签发的数字证书也是大家都信任的，从而保证了证书所代表的通信双方身份的可信性。

参考答案

（60）C

试题（61）

X.509 数字证书的内容不包括__（61）__。

（61）A．版本号　　B．签名算法标识

C．加密算法标识　　D．主体的公开密钥信息

试题（61）分析

本题考查 PKIX.509 数字证书的基础知识。

数字证书如同日常生活中使用的身份证明，它是持有者在网络上证明自己身份的凭证。X.509 定义的数字证书包括 3 部分：证书内容、签名算法和使用签名算法对证书内容所作的签名。X.509 数字证书的具体内容包括：

① 证书版本号：用于识别数字证书版本号，版本号可以是 V1、V2 和 V3，目前常用的是 V3。

② 证书序列号：是由 CA 分配给数字证书的唯一的数字类型的标识符，当数字证书被撤销时，将此证书序列号放入由 CA 签发的证书撤销列表 CRL。

③ 签名算法标识：是用来标识对证书进行签名的算法和算法包含的参数，X.509 规定，这个算法同证书格式中出现的签名算法必须是同一个算法。

④ 证书签发机构：签发数字证书的 CA 的名称。

⑤ 证书有效期：证书启用和废止的日期和时间，表明证书在该时间段内有效。

⑥ 证书对应的主体：证书持有者的名称。

⑦ 证书主体的公钥算法：包括证书主体的签名算法、需要的参数和公钥参数。

⑧ 证书签发机构唯一标识：该项为可选项。

⑨ 证书主体唯一标识：该项为可选项。

⑩ 扩展项：X.509 证书的 V3 版本还规定了证书的扩展项。

参考答案

（61）C

试题（62）

如果在某大型公司本地与异地分公司之间建立一个 VPN 连接，应该建立的 VPN 类型是（62）。

（62）A．内部 VPN　　B．外部 VPN

C．外联网 VPN　　D．远程 VPN

试题（62）分析

本题考查 VPN 连接方面的知识。

VPN 的基本原理是：在公共通信网上为需要进行保密通信的通信双方建立虚拟的专用通信通道，并且所有传输数据均经过加密后再在网络中进行传输，这样做可以有效保证机密数据传输的安全性。在虚拟专用网中，任意两个节点之间的连接并没有传统专用网所需的端到端的物理链路，虚拟的专用网络通过某种公共网络资源动态组成。如果在某大型公司本地与异地分公司之间建立一个 VPN 连接，应该建立的 VPN 类型是远程 VPN。

参考答案

（62）D

试题（63）

网络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，以下有关蜜罐说法不正确的是（63）。

（63）A．蜜罐系统是一个包含漏洞的诱骗系统，它通过模拟一个或者多个易受攻击的主机和服务，给攻击者提供一个容易攻击的目标

B．使用蜜罐技术，可以使目标系统得以保护，便于研究入侵者的攻击行为

C．如果没人攻击，蜜罐系统就变得毫无意义

D．蜜罐系统会直接提高计算机网络安全等级，是其他安全策略不可替代的

试题（63）分析

本题考查网络蜜罐技术知识。

蜜罐技术是一种对攻击方进行欺骗的技术，通过布置一些作为诱饵的主机、网络服务或者信息，诱使攻击方对它们实施攻击，从而可以对攻击行为进行捕获和分析，了解攻击方所使用的工具与方法，推测攻击意图和动机，能够让防御方清晰地了解他们所面对的安全威胁，并通过技术和管理手段来增强实际系统的安全防护能力。网络蜜罐技术是一种主动防御技术，是防范入侵检测技术的一个重要发展方向。

参考答案

（63）D

试题（64）

以下不属于代码静态分析的方法是__（64）__。

（64）A．内存扫描　　B．模式匹配

C．定理证明　　D．模型检测

试题（64）分析

本题考查代码分析方面的知识。

代码静态分析是指在不运行代码的方式下，通过词法分析、语法分析、控制流、数据流分析等技术对程序代码进行扫描，验证代码是否满足规范性、安全性、可靠性、可维护性等指标的一种代码分析技术。常见的代码静态分析方法包括：模式匹配、定理证明、模型检测。

参考答案

（64）A

试题（65）

SM4 是一种分组密码算法，其分组长度和密钥长度分别为__（65）__。

（65）A．64 位和 128 位　　B．128 位和 128 位

C．128 位和 256 位　　D．256 位和 256 位

试题（65）分析

本题考查分组密码算法 SM4。

分组密码算法 SM4 的分组长度和密钥长度分别为 128 位和 128 位。

参考答案

（65）B

试题（66）

设在 RSA 的公钥密码体制中，公钥为(e,n)=(7,55)，则私钥 d=__（66）__。

（66）A．8　　B．13　　C．23　　D．37

试题（66）分析

本题考查公钥密码算法 RSA。

1978 年，MIT 的三名数学家 R. Rivest、A. Shamir 和 L. Adleman 提出了著名的公钥密码体制，即 RSA 公钥算法。该算法是基于指数加密概念的，它以两个大素数的乘积作为算法的公钥来加密消息，而密文的解密必须知道相应的两个大素数。

基于大数分解问题是指为了产生公钥和私钥，首先独立地选取两个大素数 p 和 q（注：为了获得最大程度的安全性，p 和 q 的长度应该差不多，都应为长度在 100 位以上的十进制数字）。然后计算下式

$$n = p \times q \text{ 和 } \varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$$

这里 $\varphi(n)$ 表示 n 的欧拉函数，即 $\varphi(n)$ 为比 n 小且与 n 互素的正整数的个数。

随机选取一个满足 $1<e<\varphi(n)$ 且 $\gcd(e,\varphi(n))=1$ 的整数 e，那么 e 存在模 $\varphi(n)$ 下的乘法逆元 $d=e^{-1} \mod \varphi(n)$，d 可由扩展的欧几里得算法求得。

参考答案

（66）C

试题（67）

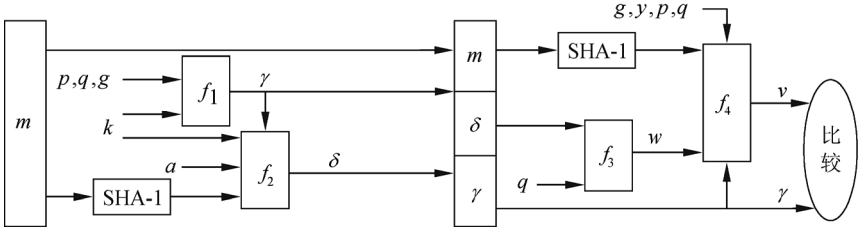
DSS 数字签名标准的核心是数字签名算法 DSA，该签名算法中杂凑函数采用的是（67）。

（67）A．SHA1　　B．MD5　　C．MD4　　D．SHA2

试题（67）分析

本题考查数字签名方面的知识。

DSS 数字签名标准使用的算法称为数字签名算法 DSA（Digital Signature Algorithm），它是在 ElGamal 和 Schnorr 两个方案基础上设计出来的，其基本流程如下：



参考答案

（67）A

试题（68）

2017 年 6 月 1 日，（68）开始施行。

（68）A.《中华人民共和国计算机信息系统安全保护条例》

B.《计算机信息系统国际联网保密管理规定》

C.《中华人民共和国网络安全法》

D.《中华人民共和国电子签名法》

试题（68）分析

本题考查网络安全法方面的知识。

《中华人民共和国网络安全法》于 2017 年 6 月 1 日开始施行。

参考答案

（68）C

试题（69）

面向数据挖掘的隐私保护技术主要解决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。从数据挖掘的角度看，不属于隐

私保护技术的是（69）。

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

试题（69）分析

本题考查隐私保护方面的基础知识。

面向数据挖掘的隐私保护技术主要解决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。从数据挖掘的角度看，隐私保护技术包括基于数据失真的隐私保护技术、基于数据匿名化的隐私保护技术和基于数据加密的隐私保护技术。

参考答案

（69）C

试题（70）

强制访问控制（MAC）是一种不允许主体干涉的访问控制类型。根据 MAC 的安全级别，用户与访问的信息的读写关系有四种类型，其中能保证数据完整性的读写组合方式是（70）。

（70）A．上读-下写　　B．上读-上写
　　C．下读-下写　　D．下读-上写

试题（70）分析

本题考查强制访问控制方面的知识。

强制访问控制（Mandatory Access Control，MAC）是一种不允许主体干涉的访问控制类型。它是基于安全标识和信息分级等信息敏感性的访问控制，通过比较资源的敏感性与主体的级别来确定是否允许访问。系统将所有主体和客体分成不同的安全等级，给予客体的安全等级能反映出客体本身的敏感程度；主体的安全等级标志着用户不会将信息透露给未经授权的用户。根据 MAC 的安全级别，用户与访问的信息的读写关系有四种类型，其中能保证数据完整性的读写组合方式是上读下写。

参考答案

（70）A

试题（71）～（75）

There are different ways to perform IP based DoS Attacks. The most common IP based DoS attack is that an attacker sends an extensive amount of connection establishment （71） (e.g. TCP SYN requests) to establish hanging connections with the controller or a DPS. Such a way, the attacker can consume the network resources which should be available for legitimate users. In other （72）, the attacker inserts a large amount of （73） packets to the data plane by spoofing all or part of the header fields with random values. These incoming packets will trigger table-misses and send lots of packet-in flow request messages to the network

controller to saturate the controller resources. In some cases, an （74） who gains access to DPS can artificially generate lots of random packet-in flow request messages to saturate the control channel and the controller resources. Moreover, the lack of diversity among DPSs fuels the fast propagation of such attacks.

Legacy mobile backhaul devices are inherently protected against the propagation of attacks due to complex and vendor specific equipment. Moreover, legacy backhaul devices do not require frequent communication with core control devices in a manner similar to DPSs communicating with the centralized controller. These features minimize both the impact and propagation of DoS attacks. Moreover, the legacy backhaul devices are controlled as a joint effort of multiple network elements. For instance, a single Long Term Evolution (LTE) eNodeB is connected up to 32 MMEs. Therefore, DoS/DDoS attack on a single core element will not terminate the entire operation of a backhaul device （75） the network.

（71）A．message	B．information	C．requests	D．data
（72）A．methods	B．cases	C．hands	D．sections
（73）A．bad	B．real	C．fake	D．new
（74）A．user	B．administrator	C．editor	D．attacker
（75）A．or	B．of	C．in	D．to

参考译文

执行基于 IP 的 DoS 攻击有不同的方法。攻击者最常用的是发送大量的连接建立请求（例如 TCP SYN 请求）来建立与控制器或 DPS 的挂接。这样一来，攻击者就可以消耗合法用户所需的网络资源。在其他情况下，攻击者通过用随机值欺骗所有或部分头字段，将大量假数据包插入数据域。这些传入的数据包将触发表丢失，并在流请求消息中发送大量包到网络控制器以使得控制器资源达到饱和。在某些情况下，获得 DPS 的攻击者可以人为地在流请求消息中生成大量随机包，使得控制信道和控制器资源饱和。此外，DPS 间缺乏多样性也加速了这种攻击的快速传播。

传统的移动回程设备由于其复杂性以及供应商专属性质，天生是防止攻击传播的。此外，传统的回程装置不需要与核心控制设备频繁交流，而 DPS 与中央控制器的通信则需要。这些特性减少了 DoS 攻击的影响和传播。此外，传统的回程设备是作为多个网络元素的联合工作方式来控制的。例如，一个单一的长期演进（LTE）基站连接多达 32 个 MME（负责信令处理的关键节点）。因此，对单个核心元素的 DoS 攻击不会终止回程设备或网络的整个操作。

参考答案

（71）C （72）B （73）C （74）D （75）A

第 5 章　2018 上半年信息安全工程师上午试题分析与解答

试题（1）

2016 年 11 月 7 日，十二届全国人大常委会第二十四次会议以 154 票赞成、1 票弃权，表决通过了《中华人民共和国网络安全法》。该法律由全国人民代表大会常务委员会于 2016 年 11 月 7 日发布，自（1）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

试题（1）分析

《中华人民共和国网络安全法》已由中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议于 2016 年 11 月 7 日通过，自 2017 年 6 月 1 日起施行。

参考答案

（1）B

试题（2）

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）。

（2）A．SM2　　B．SM3　　C．SM4　　D．SM9

试题（2）分析

本题考查我国商用密码的相关知识。

标识密码将用户的标识（如邮件地址、手机号码、QQ 号码等）作为公钥，省略了交换数字证书和公钥过程，使得安全系统变得易于部署和管理，非常适合端对端离线安全通信、云端数据加密、基于属性加密、基于策略加密的各种场合。2008 年标识密码算法正式获得国家密码管理局颁发的商密算法型号：SM9（商密九号算法），为我国标识密码技术的应用奠定了坚实的基础。

参考答案

（2）D

试题（3）

《计算机信息系统安全保护等级划分准则》（GB 17859—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）。

（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

试题（3）分析

本题考查计算机信息系统安全等级保护相关知识。

GB 17859—1999 标准规定了计算机系统安全保护能力的五个等级：第一级为用户自主保护级；第二级为系统审计保护级；第三级为安全标记保护级；第四级为结构化保护级；第五级为访问验证保护级。

其中第四级结构化保护级的计算机信息系统可信计算建立于一个明确定义的形式化安全策略模型之上，它要求将第三级系统中的自主和强制访问控制扩展到所有主体与客体。

参考答案

（3）D

试题（4）

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）__。

（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

试题（4）分析

本题考查密码分析方法相关知识。

数学分析攻击是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，通过数学求解的方法来破译密码。

参考答案

（4）A

试题（5）

《中华人民共和国网络安全法》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__（5）__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

试题（5）分析

本题考查网络安全法相关法条的基础知识。

《中华人民共和国网络安全法》第八条明确规定了网信部门是负责统筹和监督网络安全工作的机构。管理归属网信部门，企业需积极配合。

参考答案

（5）C

试题（6）

一个密码系统如果用 E 表示加密运算，D 表示解密运算，M 表示明文，C 表示密文，则下面描述必然成立的是__（6）__。

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

试题（6）分析

本题考查对称密码系统加密和解密之间的关系。

对消息 M 加密以后再用相同密钥解密就可以恢复消息明文 M。

参考答案

（6）B

试题（7）

S/Key 口令是一种一次性口令生成方案，它可以对抗__（7）__。

（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

试题（7）分析

本题考查一次性口令生成方案的安全性。

S/Key 每次使用时临时生成一个口令，从而可以有效抵御口令的重放攻击。

参考答案

（7）C

试题（8）

面向数据挖掘的隐私保护技术主要解决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。从数据挖掘的角度，不属于隐私保护技术的是__（8）__。

（8）A．基于数据分析的隐私保护技术　　B．基于数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

试题（8）分析

本题考查隐私保护技术。

利用数据挖掘实现隐私保护技术可以通过数据失真、数据匿名化和数据加密来实现。

参考答案

（8）A

试题（9）

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）__。

（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

试题（9）分析

本题考查网络安全系统设计需要遵循的基本原则。

Kerckhoffs 准则认为，一个安全保护系统的安全性不是建立在它的算法对于对手来

说是保密的，而是应该建立在它所选择的密钥对于对手来说是保密的。这显然不是网络安全在防护设计时所包含的内容。

参考答案

（9）D

试题（10）

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威胁类型。数据显示，目前安卓平台恶意软件主要有（10）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

试题（10）分析

本题考查安卓平台下的恶意软件分类方法。

利用安卓手机移动平台传播恶意软件是目前主流传播途径，涉及的主要类型有远控、吸费、窃取隐私和破坏系统。

参考答案

（10）A

试题（11）

以下关于认证技术的描述中，错误的是（11）。

（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

试题（11）分析

本题考查身份认证技术。

数字签名是只有信息的发送者才能产生而别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者所发送信息真实性的一个有效证明。数字签名的本质是消息进行某种计算得到包含用户特定特征的字符串，十六进制只是其中的一种表示形式而已。

参考答案

（11）C

试题（12）

对信息进行均衡、全面的防护，提高整个系统“安全最低点”的安全性能，这种安全原则被称为（12）。

（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

试题（12）分析

本题考查网络安全系统设计原则。

网络信息安全的木桶原则是指对信息均衡、全面地进行保护。“木桶的最大容积取决于最短的一块木板”。安全机制和安全服务设计的首要目的是防止最常用的攻击手段，根本目的是提高整个系统的“安全最低点”的安全性能。

参考答案

（12）B

试题（13）

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，以下属于主动防御技术的是（13）。

（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

试题（13）分析

本题考查主动和被动安全防御技术。

上述安全防御技术中，只有蜜罐技术利用信息欺骗技术，主动获取攻击者的各种攻击信息，学习攻击使用的行为、方法和手段。

参考答案

（13）A

试题（14）

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）。

（14）A．可用性　　B．完整性

C．机密性　　D．可控性

试题（14）分析

本题考查网络安全的安全目标。

网络信息安全与保密的目标主要表现在系统的机密性、完整性、真实性、可靠性、可用性、不可抵赖性等方面。机密性是网络信息不被泄露给非授权的用户、实体或过程，或供其利用的特性。

参考答案

（14）C

试题（15）

按照密码系统对明文的处理方法，密码系统可以分为（15）。

（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

试题（15）分析

本题考查密码系统组成基础知识。

密码系统通常从 3 个独立的方面进行分类：

一是按将明文转化为密文的操作类型分为替换密码和移位密码；

二是按明文的处理方法可分为分组密码（块密码）和序列密码（流密码）；

三是按密钥的使用个数分为对称密码体制和非对称密码体制。

参考答案

（15）D

试题（16）

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）__。

（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

试题（16）分析

本题考查数字签名相关知识。

数字签名就是只有信息的发送者才能产生的别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。数字签名是非对称密钥加密技术与数字摘要技术的应用。

参考答案

（16）C

试题（17）

以下选项中，不属于生物识别方法的是__（17）__。

（17）A．掌纹识别　　B．个人标记号识别　　C．人脸识别　　D．指纹识别

试题（17）分析

本题考查身份认证技术与生物识别技术。

生物识别技术是通过计算机与光学、声学、生物传感器和生物统计学原理等高科技手段密切结合，利用人体固有的生理特性（如指纹、脸、虹膜等）和行为特征（如笔迹、声音、步态等）来进行个人身份的鉴定。

参考答案

（17）B

试题（18）

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）__。

（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

试题（18）分析

本题考查计算机犯罪和取证相关基础知识。

计算机取证可以在离线或者在线状态下完成。

参考答案

（18）A

试题（19）

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）。

（19）A．使用 MySQL 自带的命令 mysqladmin 设置 root 口令

B．使用 set password 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

试题（19）分析

本题考查口令安全和数据库安全操作。

修改数据库 MySQL 下的访问控制列表是无法完成口令设置的。

参考答案

（19）D

试题（20）

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）。

（20）A．保密性　　B．隐蔽性　　C．可见性　　D．完整性

试题（20）分析

本题考查数字水印技术。

数字版权标识水印是目前研究最多的一类数字水印。数字作品既是商品又是知识作品，这种双重性决定了版权标识水印主要强调隐蔽性、保密性、鲁棒性，而对数据量的要求相对较小。

参考答案

（20）C

试题（21）

（21）是一种通过不断对网络服务系统进行干扰，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

试题（21）分析

本题考查常见的网络攻击方法。

拒绝服务攻击是攻击者想办法让目标机器停止提供服务，是黑客常用的攻击手段之一。对网络带宽进行的消耗性攻击只是拒绝服务攻击的一小部分，只要能够对目标造成麻烦，使某些服务被暂停甚至主机死机，都属于拒绝服务攻击。

参考答案

（21）B

试题（22）

在访问因特网时，为了防止 Web 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）。

（22）A．将要访问的 Web 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

试题（22）分析

本题考查互联网安全使用常识。

要阻止恶意代码对计算机的破坏，必须限制页面中恶意代码的权限或者禁止其执行，选项中只有 A 有此功能。

参考答案

（22）A

试题（23）

下列说法中，错误的是（23）。

（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

试题（23）分析

本题考查常规网络攻击和网络安全的基本概念。

抵赖是事后否认某些网络行为，与黑客没有关系。

参考答案

（23）B

试题（24）

Linux 系统的运行日志存储的目录是__（24）__。

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

试题（24）分析

本题考查主机安全和日志安全。

Linux 系统默认配置下，日志文件通常都保存在“/var/log”目录下。

参考答案

（24）A

试题（25）

电子邮件已经成为传播恶意代码的重要途径之一，为了有效防止电子邮件中的恶意代码，应该用__（25）__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

试题（25）分析

本题考查电子邮件传播恶意代码的载体。

根据恶意代码的形式和执行方法，通过纯文本方式打开邮件可以防止恶意代码被执行，从而避免中毒。

参考答案

（25）B

试题（26）

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）__。

（26）A．0110　　B．1001　　C．0100　　D．0101

试题（26）分析

本题考查 DES 加密算法的 S 盒替换运算。

根据 S 盒运算规则，第一、六位确定行：10=2，第二、三、四、五确定列：0001=1，从而唯一确定元素 6，再转换成二进制。

参考答案

（26）A

试题（27）

以下关于 TCP 协议的描述，错误的是__（27）__。

（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

试题（27）分析

本题考查计算机网络协议的基础知识。

TCP 作为可靠的传输协议，在真正开始数据传输之前需要三次握手建立连接，而不是二次握手。

参考答案

（27）C

试题（28）

Kerberos 是一种常用的身份认证协议，它采用的加密算法是__（28）__。

（28）A．Elgamal　　B．DES　　C．MD5　　D．RSA

试题（28）分析

本题考查身份认证协议。

Kerberos 是一种网络认证协议，主要用于计算机网络的身份鉴别。其特点是用户只需要输入一次身份验证信息就可以凭借此验证获得的票据访问多个服务，它采用 DES 加密算法。

参考答案

（28）B

试题（29）

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）__。

（29）A．流量分析　　B．后门　　C．拒绝服务攻击　　D．特洛伊木马

试题（29）分析

本题考查主动被动攻击技术。

嗅探或者网络流量分析是通过分析网络数据包从中获取敏感信息，属于被动攻击。

参考答案

（29）A

试题（30）

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）__。

（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

试题（30）分析

本题考查数据安全和隐私保护。

从个人隐私保护的角度来说，公众运营商信息是公开的，不属于被保护的信息。

参考答案

（30）D

试题（31）

以下关于数字证书的叙述中，错误的是__（31）__。

（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

试题（31）分析

本题考查公钥密码系统的数字证书基本概念。

数字证书的格式普遍采用的是 X.509V3 国际标准，一个标准的 X.509 数字证书包含以下一些内容：

- 证书的版本信息；
- 证书的序列号，每个证书都有一个唯一的证书序列号；
- 证书所使用的签名算法；
- 证书的发行机构名称，命名规则一般采用 X.500 格式；
- 证书的有效期，通用的证书一般采用 UTC 时间格式，它的计时范围为 1950—2049；
- 证书所有人的名称，命名规则一般采用 X.500 格式；
- 证书所有人的公开密钥（注意不是 CA 的公开密钥）；
- 证书发行者对证书的签名。

参考答案

（31）A

试题（32）

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__（32）__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

试题（32）分析

本题考查国密算法基础知识。

我国 SM2 与 SM9 数字签名算法的 ISO/IEC14888-3/AMD1《带附录的数字签名第 3

部分：基于离散对数的机制补篇 1》获得一致通过，成为 ISO/IEC 国际标准，进入标准发布阶段。

SM2 和 SM9 数字签名算法是我国 SM2 椭圆曲线密码算法标准和 SM9 标识密码算法标准的重要组成部分，用于实现数字签名、保障身份的真实性、数据的完整性和行为的不可否认性等，是网络空间安全的核心技术和基础支撑。

参考答案

（32）D

试题（33）

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损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）__。

（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

试题（33）分析

本题考查数字水印安全。

置乱攻击将严重损害图像使用价值。

参考答案

（33）C

试题（34）

数字信封技术能够__（34）__。

（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

试题（34）分析

本题考查数字信封技术。

数字信封技术是用密码技术的手段保证只有规定的信息接受者才能获取信息的安全技术。

参考答案

（34）B

试题（35）

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）__。

（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

试题（35）分析

本题考查 DES 加密算法。

DES 加密算法的密钥长度为 56 位，子密钥为 48 位，分组长度为 64 位。

参考答案

（35）B

试题（36）

甲不但怀疑乙发给他的信遭人篡改，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）。

（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

试题（36）分析

本题考查证书机构和数字证书。

CA 中心又称 CA 机构，即证书授权中心（Certificate Authority），或称证书授权机构，作为电子商务交易中受信任的第三方，承担公钥体系中公钥的合法性检验的责任。

参考答案

（36）C

试题（37）

WiFi 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）。

（37）A．WPA 和 WPA2　　B．WEP

C．WPA-PSK　　D．WPA2-PSK

试题（37）分析

本题考查无线安全中的加密算法。

WEP 加密算法存在严重安全漏洞，在 WPA 加密的认证方式中已经废弃。

参考答案

（37）B

试题（38）

特洛伊木马攻击的威胁类型属于（38）。

（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

试题（38）分析

本题考查恶意代码安全威胁。

恶意代码需要找到一种植入的方法以传播自己和感染其他系统。

参考答案

（38）C

试题（39）

信息通过网络进行传输的过程中，存在着被篡改的风险，为了解决这一安全隐患，

通常采用的安全防护技术是__（39）__。

（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

试题（39）分析

本题考查安全目标相关的网络安全技术。

消息认证通过采用哈希算法实现数据的完整性。

参考答案

（39）C

试题（40）

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）__。

（40）A．可用性　　B．完整性　　C．保密性　　D．可认证性

试题（40）分析

本题考查安全套接层协议基础知识。

SSL 协议在传统的传输层协议基础上增加安全功能，但可用性不是其设计目标。

参考答案

（40）A

试题（41）

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）__。

（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

试题（41）分析

本题考查病毒的查杀基本概念。

杀毒软件对于部分新型未知的病毒是无法查杀的。

参考答案

（41）D

试题（42）

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）__。

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

试题（42）分析

本题考查 IP 地址，各类私有地址如下。

A 类：10.0.0.0～10.255.255.255；

B 类：172.16.0.0～172.31.255.255；

C 类：192.168.0.0～192.168.255.255。

参考答案

（42）B

试题（43）

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（43）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

试题（43）分析

本题考查风险评估基本概念。

风险评估是组织确定信息安全需求的过程，包括风险评估准备、风险因素识别、风险程度分析和风险等级评价。

参考答案

（43）C

试题（44）

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）。

（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

试题（44）分析

本题考查深度流检测技术。

深度流检测技术深入分析不同类型的网络分组中的字段信息和关联分组实现异常行为检测，但对检测到的恶意行为不提供响应能力。

参考答案

（44）D

试题（45）

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（45）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

试题（45）分析

本题考查操作系统安全审计功能。

操作系统为了完成审计功能需要收集、记录审计事件，并提供查询过滤分析等相关功能模块。

参考答案

（45）C

试题（46）

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）__。

（46）A．计算机犯罪具有高智能性，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

试题（46）分析

本题考查网络犯罪和取证分析。

计算机犯罪的犯罪现场就是计算机所在的系统。

参考答案

（46）C

试题（47）

攻击者通过对目标主机进行端口扫描，可以直接获得__（47）__。

（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

试题（47）分析

本题考查信息获取和扫描技术。

题目考查的端口扫描，那么直接能获得信息只能是端口开放服务信息，其他信息都需要进一步分析协议栈实现或者破解才能获得。

参考答案

（47）B

试题（48）

WPKI（无线公开密钥体系）是基于无线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）__。

（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

试题（48）分析

本题考查无线网络安全。

WPKI 并不是一个全新的 PKI 标准，它是传统的 PKI 技术应用于无线环境的优化扩展。它采用了优化的 ECC 椭圆曲线加密和压缩的 X.509 数字证书。

参考答案

（48）D

试题（49）

文件型病毒不能感染的文件类型是（49）。

（49）A．SYS 型　　B．EXE 类型　　C．COM 型　　D．HTML 型

试题（49）分析

本题考查恶意代码基本概念。

文件型病毒通常感染可执行文件或者 pdf 以及 doc 等文档文件，由于 html 文件无法嵌入二进制执行代码，且是文本格式，不易隐藏代码，所以无法感染。

参考答案

（49）D

试题（50）

网络系统中针对海量数据的加密，通常不采用（50）方式。

（50）A．会话加密　　B．公钥加密　　C．链路加密　　D．端对端加密

试题（50）分析

本题考查加密机制基础知识。

由于公钥加密需要较大的计算量，通常不采用公钥加密方式。

参考答案

（50）B

试题（51）

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）。

（51）A．窃听　　B．重放　　C．克隆　　D．欺诈

试题（51）分析

本题考查无线网络安全。

克隆网络中的 AP 使得用户每天所连接的那个看似安全的无线 AP，就是被克隆伪装的恶意 AP。

参考答案

（51）C

试题（52）

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

WAPI 的描述，正确的是（52）。

（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 WAI 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

试题（52）分析

本题考查无线局域网安全标准。

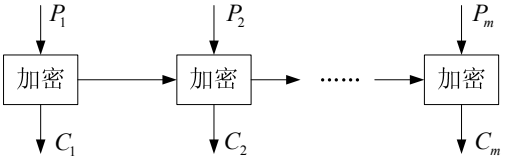
WAPI 鉴别及密钥管理的方式有两种，即基于证书和基于预共享密钥 PSK。若采用基于证书的方式，整个过程包括证书鉴别、单播密钥协商与组播密钥通告；若采用预共享密钥的方式，整个过程则为单播密钥协商与组播密钥通告。WAPI 采用双向鉴别机制。

参考答案

（52）D

试题（53）

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（53）模式（图中 P_i 表示明文分组，C_i 表示密文分组）。



（53）A．ECB　　B．CFB　　C．CBC　　D．OFB

试题（53）分析

本题考查分组密码的操作模式。

根据图示，每个明文分组的加密都是互相独立的，因此其加密模式属于 ECB 模式。

参考答案

（53）A

试题（54）

关于祖冲之算法的安全性分析不正确的是（54）。

（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钥分析

试题（54）分析

本题考查祖冲之加密算法。

祖冲之算法集是由我国学者自主设计的加密和完整性算法，是一种流密码。算法由 3 个基本部分组成，依次为比特重组、非线性函数 F、线性反馈移位寄存器（LFSR）。

参考答案

（54）B

试题（55）

以下关于 IPSec 协议的叙述中，正确的是__（55）__。

（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

试题（55）分析

本题考查 VPN 基础知识。

VPN 作为 IP 协议安全问题的解决方案，提供了机密性、认证和完整性功能。

参考答案

（55）A

试题（56）

不属于物理安全威胁的是__（56）__。

（56）A．电源故障　　B．物理攻击　　C．自然灾害　　D．字典攻击

试题（56）分析

本题考查网络安全威胁。

字典攻击属于网络服务的暴力破解，不属于物理安全威胁。

参考答案

（56）D

试题（57）

以下关于网络钓鱼的说法中，不正确的是__（57）__。

（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

试题（57）分析

本题考查网络钓鱼安全风险。

通过邮件和 Web 恶意链接是两种常见的钓鱼方式，因此和 Web 服务有直接关系。

参考答案

（57）B

试题（58）

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）__。

（58）A．不可上读　　B．不可上写　　C．不可下读　　D．不可下写

试题（58）分析

本题考查网络安全模型。

BLP 保密模型基于两种规则来保障数据的保密性与敏感度：（简单安全特性）上读（NRU），主体不可读安全级别高于它的数据；（星属性安全特性）下写（NWD），主体不可写安全级别低于它的数据。

参考答案

（58）A

试题（59）

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）__。

（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

试题（59）分析

本题考查安全电子交易协议基本概念。

安全电子交易协议 SET 是一种应用于因特网（Internet）环境下，以信用卡为基础的安全电子交付协议，它给出了一套电子交易的过程规范。通过 SET 协议可以实现电子商务交易中的加密、认证、密钥管理机制等，保证了在因特网上使用信用卡进行在线购物的安全。

参考答案

（59）C

试题（60）

在 PKI 中，关于 RA 的功能，描述正确的是__（60）__。

（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捆绑在一起，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

试题（60）分析

本题考查 CA 机构和组成。

数字证书注册中心也称为 RA（Registration Authority），是数字证书认证中心的证书发放、管理的延伸。主要负责证书申请者的信息录入、审核以及证书发放等工作，同时，对发放的证书完成相应的管理功能。

参考答案

（60）D

试题（61）

以下关于 VPN 的叙述中，正确的是__（61）__。

（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 不能同时实现对消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，不具备数据加密功能

试题（61）分析

本题考查 VPN 基本概念。

VPN 是虚拟专用网，所谓虚拟指的是公用公网网络线路，并提供了加密、认证和完整性等安全能力，可以有效降低在公共网络上传输数据的风险，即使信息被截获也不会泄密。

参考答案

（61）A

试题（62）

对于定义在 $GF(p)$ 上的椭圆曲线，取素数 $p=11$，椭圆曲线 $y^2=x^3+x+6 \bmod 11$，则以下是椭圆曲线模 11 平方剩余的是__（62）__。

（62）A．$x=1$　　B．$x=3$　　C．$x=6$　　D．$x=9$

试题（62）分析

本题考查椭圆曲线密码。

参考答案

（62）B

试题（63）

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 IP 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）__。

（63）A．IP 源地址　　B．源端口　　C．IP 目的地址　　D．协议

试题（63）分析

本题考查防火墙。

基于网络层的分组信息无法包括传输层的源端口信息。

参考答案

（63）B

试题（64）

以下关于网络流量监控的叙述中，不正确的是__（64）__。

（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

试题（64）分析

本题考查网络流量监控。

网络流量监控工作在网络层、传输层，通常无法对数据进行过滤。

参考答案

（64）C

试题（65）

设在 RSA 的公钥密码体制中，公钥为 $(e,n)=(7,55)$，则私钥 $d=$__（65）__。

（65）A．11　　B．15　　C．17　　D．23

试题（65）分析

本题考查 RSA 公钥算法。

计算 ed 模 40=1。

参考答案

（65）D

试题（66）

下列关于公钥密码体制说法不正确的是__（66）__。

（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钥来确定解密密钥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

试题（66）分析

本题考查公钥密码算法。

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不可行的。

参考答案

（66）B

试题（67）

SM3 密码杂凑算法的消息分组长度为__（67）__比特。

（67）A．64　　B．128　　C．512　　D．1024

试题（67）分析

本题 SM3 算法。

SM3 密码杂凑算法的描述 SM3 密码杂凑算法采用 Merkle-Damgard 结构，消息分组长度为 512b，摘要长度 256b。

参考答案

（67）C

试题（68）

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）__的。

（68）A．实际安全　　B．可证明安全　　C．无条件安全　　D．绝对安全

试题（68）分析

本题考查密码安全。

如果破解密码算法所需的代价或者时间超过一定限度，表示密码实际是安全的。

参考答案

（68）A

试题（69）

a=17，*b*=2，则满足 *a* 与 *b* 取模同余的是__（69）__。

（69）A．4　　B．5　　C．6　　D．7

试题（69）分析

本题考查数学基础知识。

需要是 5 的倍数。

参考答案

（69）B

试题（70）

利用公开密钥算法进行数据加密时，采用的方式是__（70）__。

（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密

试题（70）分析

本题考查公钥加密算法应用。

公钥和私钥是一对，可以互为加解密密钥。

参考答案

（70）C

试题（71）～（75）

Trust is typically interpreted as a subjective belief in the reliability, honesty and security of an entity on which we depend （71） our welfare. In online environments we depend on a wide spectrum 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 trusted component of a system must work correctly in order for the security of that system to hold, meaning that when a trusted （72） fails, then the systems and applications that depend on it can （73） 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 trusted 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 security 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 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 of identities in online environments. Trust management becomes a component of （74） 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 authorisation policies in personalised services.

Establishing trust always has a cost, so that having complex trust requirements 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 simple 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 __（75）__ 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

参考译文

信任通常被解释为是对我们赖以生存的实体的可靠性、诚实性和安全性的一种主观信念。在在线环境中，我们依赖于各种各样的东西，从计算机硬件、软件和数据到人员和组织。安全解决方案总是根据特定的策略假定某些实体的功能。信任就是做出这种假设，因此，受信任的实体与根据策略假定起作用的实体是相同的。这样做的结果，就是系统的受信任组件必须正确工作，以保持该系统的安全性，这意味着当受信任组件发生故障时，依赖它的系统和应用程序将不再被视为安全的。该原则的一个经常被引用的表述是："可信系统或组件是可以破坏您的安全策略的系统或组件"（当可信系统失败时会发生这种情况）。这同样适用于受信任方，如服务提供商（简称 SP）。也就是说，为了确保预期的安全性和服务质量，它必须按照商定或假定的政策进行操作。从该分析中得出的一个矛盾结论是，当增加服务基础设施所依赖的受信任组件和参与方的数量时，安全保证可能会减少。这是因为由许多受信任组件组成的基础结构的安全性通常遵循最弱链接的原则，也就是说，在许多情况下，整体安全性只能与所有受信任组件中最不可靠或最不安全的部分一样强。我们不能避免使用可信的安全组件，但越少越好。在设计身份管理架构时，这一点很重要，也就是说，在身份管理模型中，受信任方越少，所能实现的安全性就越强。

将身份和信任的社会结构转化为数字和计算概念有助于设计和实施大规模在线市场和社区，并在融合移动和互联网环境中发挥重要作用。身份管理（以下简称 IDM）是关于识别和验证在线环境中身份的正确性。当不同的当事方在身份提供和认证方面相互依赖时，信任管理就成为 IDM 的一个组成部分。因此，IDM 和信任管理以复杂的方式

相互依赖，因为要信任相应实体的质量和可靠性，必须信任标识本身的正确性。在定义个性化服务中的授权策略时，IDM 也是一个基本概念。

建立信任总是有成本的，因此拥有复杂的信任需求通常会导致建立所需信任的高开销。为了降低成本，将鼓励利益相关者在信任要求方面“抄近路”，这可能导致安全性不足。挑战在于设计具有相对简单信任要求的 IDM 系统。加密机制通常是 IDM 解决方案的核心组件，例如，用于实体和数据身份验证。使用密码学，通常可以将信任从最初存在的地方传播到需要信任的地方。初始信任的建立通常发生在物理世界中，随后的信任传播通常以自动化的方式在线进行。

参考答案

（71）D （72）C （73）A （74）B （75）A