

全国计算机技术与软件专业技术资格（水平）考试

2016 年下半年 信息安全工程师 上午试卷与解析

（考试时间 9:00~11:30 共 150 分钟）

请按下述要求正确填写答题卡

1. 在答题卡的指定位置上正确写入你的姓名和准考证号，并用正规 2B 铅笔在你写入的准考证号下填涂准考证号。
2. 本试卷的试题中共有 75 个空格，需要全部解答，每个空格 1 分，满分 75 分。
3. 每个空格对应一个序号，有 A、B、C、D 四个选项，请选择一个最恰当的选项作为解答，在答题卡相应序号下填涂该选项。
4. 解答前务必阅读例题和答题卡上的例题填涂样式及填涂注意事项。解答时用正规 2B 铅笔正确填涂选项，如需修改，请用橡皮擦干净，否则会导致不能正确评分。

本资料由信管网(www.cnitpm.com)整理发布，欢迎到信管网资料库免费下载学习资料

信管网是专业信息安全工程师网站。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、证书挂靠、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信息安全工程师的精品学习资料；信管网案例分析频道拥有丰富的案例范例，信管网考试中心拥有历年所有真题和超过 4000 多道试题免费在线测试；信管网培训中心每年指导考生超 4000 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/peixun/

注: 以下答案和解析仅供参考, 最终答案以信管网和软题库考试系统答案为准

<http://www.ruantiku.com>

<http://www.cnitpm.com/exam/>

2016 下半年信息安全工程师真题与查分专题 (综合、案例): <http://www.cnitpm.com/zt/2016xaqcf/>

1、以下有关信息安全管理职责的叙述, 不正确的是 ()

- A、信息安全管理应该对网络的总体安全布局进行规划
- B、信息安全管理应该对信息系统安全事件进行处理
- C、信息安全管理应该负责为用户编写安全应用程序
- D、信息安全管理应该对安全设备进行优化配置

信管网解析:

信息安全管理员的职责包括对网络的总体安全布局进行规划, 对信息系统安全事件进行处理, 对安全设备进行优化配置等职责。为用户编写安全应用程序不属于信息安全管理员的职责范围。

信管网参考答案: C

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

2、国家密码管理局于 2006 年发布了“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、DH
- B、ECDSA
- C、ECDH
- D、CPK

信管网解析:

国家密码管理局公告 (2016 年第 7 号):

一、无线局域网产品须采用下列经批准的密码算法: 1、对称密码算法: SMS4; 2、签名算法: ECDSA; 3、密钥协商算法: ECDH; 4、杂凑算法: SHA-256; 5、随机数生成算法: 自行选择。其中, ECDSA 和 ECDH 密码算法须采用我局指定的椭圆曲线和参数。二、无线局域网产品使用的 SMS4 密码算法编制文本以及 ECDSA、ECDH 密码算法的椭圆曲线和参数, 授权由国家商用密码管理办公室网站 (www.oscca.gov.cn) 发布。三、无线局域网产品的密码检测指定商用密码检测中心承担。

信息安全工程师教程: 密码管理: <http://www.cnitpm.com/pm1/41537.html>

信管网参考答案: C

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

3、以下网络攻击中, () 属于被动攻击

- A、拒绝服务攻击
- B、重放
- C、假冒
- D、流量分析

信管网解析:

主动攻击被动攻击的区别: 干扰还是不干扰? 被动一般都是窃听

信息安全攻击类型: 主动攻击和被动攻击: <http://www.cnitpm.com/pm/32965.html>

信管网参考答案: D

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

4、() 不属于对称加密算法

- A、IDEA
- B、DES
- C、RCS
- D、RSA

信管网解析:

idea、des、rc5 都属于对称加密算法, rsa 属于非对称加密算法。

密码技术: 对称加密算法与非对称加密算法: <http://www.cnitpm.com/pm/29747.html>

信管网参考答案: D

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

5、面向身份信息的认证应用中, 最常用的认证方法是 ()

- A、基于数据库的认证
- B、基于摘要算法认证
- C、基于 PKI 认证
- D、基于账户名/口令认证

信管网解析:

在面向身份信息认证应用中最常用的方式是基于账户名和口令认证, 比如日常常用的操作系统登录, 邮件系统登录等都需要输入对应的用户名和密码才能进入系统。

信息安全技术知识: 用户名/密码方式: <http://www.cnitpm.com/pm1/39015.html>

信管网参考答案: D

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

6、如果发送方使用的加密密钥和接收方使用的解密密钥不相同, 从其中一个密钥难以推出另一个密钥, 这样的系统称为 ()

- A、公钥加密系统
- B、单密钥加密系统
- C、对称加密系统
- D、常规加密系统

信管网解析:

公钥加密系统又称之为非对称加密系统, 其使用的加密密钥和解密密钥不同, 从其中的一个密钥难以推出另一个密钥。

信息安全技术知识: 公钥密码体制: <http://www.cnitpm.com/pm1/37650.html>

信管网参考答案: A

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

7、S/Key 口令是一种一次性口令生产方案, 它可以对抗 ()

- A、恶意代码木马攻击
- B、拒绝服务攻击
- C、协议分析攻击
- D、重放攻击

信管网解析:

服务端发送过来一个随机数, 客户端使用共享密码多次 hash, 服务端同样的操作。

信息安全技术知识: 一次性口令(One-Time Password): <http://www.cnitpm.com/pm1/39172.html>

信管网参考答案: D

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

8、防火墙作为一种被广泛使用的网络安全防御技术, 其自身有一些限制, 它不能阻止 ()

- A、内部威胁和病毒威胁
- B、外部攻击
- C、外部攻击、外部威胁和病毒威胁
- D、外部攻击和外部威胁

信管网解析:

防火墙是一种位于内部网络与外部网络之间的网络安全系统, 内外网络通信时, 依照特定的规则, 允许或是限制传输的数据通过。它不能防范内部威胁及病毒威胁。

信息安全技术知识: 防火墙的作用及局限性: <http://www.cnitpm.com/pm1/40879.html>

信管网参考答案: A

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

9、以下行为中, 不属于威胁计算机网络安全因素的是 ()

- A、操作员安全配置不当而造成的安全漏洞
- B、在不影响网络正常工作的情况下, 进行截获、窃取、破译以获得重要机密信息
- C、安装非正版软件
- D、安装蜜罐系统

信管网解析:

蜜罐好比是情报收集系统。好比是故意让人攻击的目标, 引诱黑客前来攻击。所以攻击者入侵后, 你就可以知道他是如何得逞的, 随时了解针对服务器发动的最新的攻击和漏洞。它是一种防御手段。

信息安全工程师教程: 蜜罐概述: <http://www.cnitpm.com/pm1/41449.html>

信管网参考答案: D

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

10、电子商务系统除了面临一般的信息系统所涉及的安全威胁之外, 更容易成为黑客分子的攻击目标, 其安全性需求普遍高于一般的信息系统, 电子商务系统中的信息安全需求不包括 ()

- A、交易的真实性
- B、交易的保密性和完整性
- C、交易的可撤销性
- D、交易的不可抵赖性

信管网解析:

电子商务交易安全需求包括交易的保密性、完整性、真实性、不可抵赖性。交易的可撤销性不属于电子商务交易安全需求。

信息安全工程师教程: 电子商务安全概念及其特点: <http://www.cnitpm.com/pm/35346.html>

信管网参考答案: C

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

11、以下关于认证技术的叙述中, 错误的是 (): 做例子分析, 答题技巧: 很多题目都有技巧

- A、指纹识别技术的利用可以分为验证和识别
- B、数字签名是十六进制的字符串
- C、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
- D、消息认证能够确定接收方收到的消息是否被篡改过

信管网解析:

A 选项: (没毛病, 或者说有点小瑕疵)

B 选项: (字符串两个字有瑕疵, 也没有这么说的)

C 选项: (是一种验证方法没错, 对信息系统中试题这瑕疵就老大了, 但是再仔细一想, 这里可能是个错别字: 实体, 这样就通顺了对吧)

D 选项: (没毛病)

信息安全技术知识: 数字签名: <http://www.cnitpm.com/pm1/38741.html>

信管网参考答案: B

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

12、有一种原则是对信息进行均衡、全面的防护, 提高整个系统的安全性能, 该原则称为 ()

- A、动态化原则
- B、木桶原则
- C、等级性原则
- D、整体原则

信管网解析:

整体原则是对信息进行均衡、全面的防护, 提高整个系统的“安全最低点”的安全性能。

信管网参考答案: D

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

13、在以下网络威胁中, () 不属于信息泄露

- A、数据窃听
- B、流量分析
- C、偷窃用户账户
- D、暴力破解

信管网解析:

暴力破解的基本思想是根据题目的部分条件确定答案的大致范围, 并在此范围内对所有可能的情况逐一验证, 直到全部情况验证完毕。它不属于信息泄露。

信息安全工程师教程: 身份认证技术口令猜测技术-brute force (暴力攻击):

<http://www.cnitpm.com/pm1/38777.html>

信管网参考答案: D

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

14、未授权的实体得到了数据的访问权, 这属于对安全的 ()

- A、机密性
- B、完整性
- C、合法性
- D、可用性

信管网解析:

保密性是指网络信息不被泄露给非授权的用户、实体或过程, 即信息只为授权用户使用。

信息安全技术知识: 安全需求: <http://www.cnitpm.com/pm1/35697.html>

信管网参考答案: A

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

15、按照密码系统对明文的处理方法, 密码系统可以分为 ()

- A、置换密码系统和易位密码
- B、密码学系统和密码分析学系统
- C、对称密码系统和非对称密码系统
- D、分组密码系统和序列密码系统

信管网解析:

按照密码系统对明文的处理方法, 密码系统可以分为分组密码系统和序列密码系统。

信息安全技术知识: 置换密码: <http://www.cnitpm.com/pm1/36385.html>

信管网参考答案: A

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

16、数字签名最常见的实现方法是建立在 () 的组合基础之上

- A、公钥密码体制和对称密码体制
- B、对称密码体制和 MD5 摘要算法
- C、公钥密码体制和单向安全散列函数算法 (排除法)
- D、公证系统和 MD4 摘要算法

信管网解析:

数字签名可以利用公钥密码体制、对称密码体制或者公证系统来实现。最常见的的实现方法是建立在公钥密码体制和单向安全散列函数算法的组合基础之上。

信息安全技术知识: 数字签名: <http://www.cnitpm.com/pm1/38741.html>

信管网参考答案: C

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

17、以下选项中, 不属于生物识别方法的是 ()

- A、指纹识别
- B、声音识别
- C、虹膜识别
- D、个人标记号识别

信管网解析:

指纹识别、声音识别、虹膜识别都属于生物识别方法, 个人标记号不属于生物识别方法。

信息安全工程师教程: 身份认证-生物特征识别: <http://www.cnitpm.com/pm1/41453.html>

信管网参考答案: D

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

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、有法律效应的确定和提取。以下关于计算机取证的描述中, 错误的是 ()

- A、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提取和归档
- B、计算机取证围绕电子证据进行, 电子证据具有高科技性等特点
- C、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, 必须在开计算机的状态下进行
- D、计算机取证是一门在犯罪进行过程中或之后收集证据

信管网解析:

计算机取证包括保护目标计算机系统、确定电子证据、收集电子证据和保存电子证据。对现场计算机的部分通用处理原则有: 已经开机的计算机不要关机, 关机的计算机不要开机。

信息安全工程师教程: 计算机取证的基本概念: <http://www.cnitpm.com/pm1/41456.html>

信管网参考答案: C

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

19、注入语句: `http: //xxx.xxx.xxx/abc.asp?p=YY and user>0` 不仅可以判断服务器的后台数据库是否为 SQL-SERVER, 还可以得到 ()

- A、当前连接数据库的用户数据
- B、当前连接数据库的用户名
- C、当前连接数据库的用户口令
- D、当前连接的数据库名

信管网解析:

(这题没有一个对的, 只有一种可能, 就是报错) 注入语句: `http: //xxx. xxx.xxx/abc.asp?p=yy A N D user>0`, 服务器运行“`S E L E C T * from 表名 where 字段=yy A N D user > 0`”显然, 该语句不能正常执行会出错, 从其错误信息中不仅可以获知该服务器的后台数据库是否为 sql-server, 还可以得到当前连接的数据库的用户名。

信管网参考答案: B

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.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, 可以有效地对数字多媒体数据的版权保护等功能。以下各项中, 不属于数字水印在数字版权保护必须满足的基本应用需求的是 ()

- A、安全性
- B、隐蔽性
- C、鲁棒性
- D、可见性

信管网解析:

(作为例子, 排除法解题) 数字水印必须满足的基本应用需求是安全性、隐蔽性、鲁棒性。

信息安全工程师教程: 数字水印技术-数字水印概论: <http://www.cnitpm.com/pm1/36009.html>

信管网参考答案: D

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

21、有一种攻击是不断对网络服务系统进行干扰, 改变其正常的作业流程, 执行无关程序使系统响应减慢甚至瘫痪。这种攻击叫做 ()

- A、重放攻击
- B、拒绝服务攻击
- C、反射攻击
- D、服务攻击

信管网解析:

拒绝服务攻击是不断对网络服务系统进行干扰, 改变其正常的作业流程, 执行无关程序使系统响应减慢甚至瘫痪。

拒绝服务攻击 (DoS): <http://www.cnitpm.com/pm/35094.html>

信管网参考答案: B

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

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 ()

- 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、在浏览器中安装数字证书
- C、利用 IP 安全协议访问 Web 站点
- D、利用 SSL 访问 Web 站点

信管网解析:

本题考查点是因特网中防止 web 页面的恶意代码对自己计算机的损害而采取的防范措施。为了防止 web 页面中恶意代码对自己计算机的损害,可以将要访问的 web 站点按其可信度分配到浏览器的不同安全区域。划分不同安全区域是浏览器为保护用户计算机免受恶意代码的危害而采取的一种技术。通常浏览器将 web 站点按其可信度分配到不同的区域,针对不同的区域指定不同的文件下载方式。

信息安全工程师教程: Web 安全威胁防护技术-跨站脚本(XSS): <http://www.cnitpm.com/pm1/41066.html>

信管网参考答案: A

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

23、下列说法中,错误的是 ()

- A、服务攻击是针对某种特定攻击的网络应用的攻击
- B、主要的渗入威胁有特洛伊木马和陷阱
- C、非服务攻击是针对网络层协议而进行的
- D、对于在线业务系统的安全风险评估,应采用最小影响原则

信管网解析:

渗入威胁: 假冒、旁路、非授权访问、侵犯等

植入威胁: 木马、后门、陷阱

信息安全工程师教程: 特洛伊木马: <http://www.cnitpm.com/pm1/41490.html>

信管网参考答案: B

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

24、依据国家信息安全等级保护相关标准,军用不对外公开的信息系统至少应该属于 ()

- A、二级及二级以上
- B、三级及三级以上
- C、四级及四级以上
- D、五级

信管网解析:

(图片) 国家安全,一般损害就是 3 级

信息安全技术知识: 信息安全政策-等级保护: <http://www.cnitpm.com/pm1/41459.html>

信管网参考答案: B

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

25、电子邮件是传播恶意代码的重要途径,为了防止电子邮件中的恶意代码的攻击,用 () 方式阅读电子邮件

- A、网页
- B、纯文本
- C、程序

D、会话

信管网解析:

文本文件通常不会受电子邮件中的恶意代码的感染或携带恶意代码。

信息安全工程师教程: Web 安全威胁分类-跨站脚本(XSS): <http://www.cnitpm.com/pm1/40688.html>

信管网参考答案: B

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

26、已知 DES 算法的 S 盒如下:

如果该 S 盒的输入 110011, 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	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

A、0110

B、1001

C、0100

D、0101

信管网解析:

输入 A1A2A3A4A5A6 列: A2-A5 (1001:9) 行: A1A6 (11:3)

DES 算法主要有哪几个步骤: <http://www.cnitpm.com/pm1/33858.html>

信管网参考答案: C

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

27、在 IPv4 的数据报格式中, 字段 () 最适合于携带隐藏信息

A、生存时间

B、源 IP 地址

C、版本

D、标识

信管网解析:

A 选项: (肯定不行, 每跳都修改)

B 选项: (肯定不行, 路由查询)

C 选项: (4Bit)

D 选项: (16Bit) (发生数据包软件的一个计数器, 每产生一个数据报, 用这个数标识, 如果底层分片, 就复制)

系统集成项目管理工程师教程第 2 版: 标识技术: <http://www.cnitpm.com/pm1/35468.html>

信管网参考答案: D

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

28、Kerberos 是一种常用的身份认证协议，它采用的加密算法是（）

- A、Elgamal
- B、DES
- C、MD5
- D、RSA

信管网解析：

kerberos 是一种常用的身份认证协议，它采用数据加密标准（des）加密算法进行加密。

信息安全技术知识：Kerberos 概述：<http://www.cnitpm.com/pm1/40048.html>

信管网参考答案：B

最终答案以信管网题库为准：<http://www.cnitpm.com/pm1/37841.html>

29、以下关于加密技术的叙述中，错误的是（）

- A、对称密码体制的加密密钥和解密密钥是相同的
- B、密码分析的目的就是千方百计地寻找密钥或明文
- C、对称密码体制中加密算法和解密算法是保密的
- D、所有的密钥都有生存周期

信管网解析：

对于一个好的密码体制，其安全强度应该不依赖密码体制本身的保密，而只依赖于密钥。

信息系统集成专业技术知识：信息安全-加密技术：<http://www.cnitpm.com/pm1/37263.html>

信管网参考答案：C

最终答案以信管网题库为准：<http://www.cnitpm.com/pm1/37841.html>

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构成威胁。以下各项中，不需要被保护的属性是（）

- A、用户身份（ID）
- B、用户位置信息
- C、终端设备信息
- D、公众运营商信息

信管网解析：

公众运营商是公开信息，比如移动公司，不需要被保护。

系统集成项目管理工程师第 2 版：网络安全：<http://www.cnitpm.com/pm1/35743.html>

信管网参考答案：D

最终答案以信管网题库为准：<http://www.cnitpm.com/pm1/37841.html>

31、以下关于数字证书的叙述中，错误的是（）

- A、证书通常由 CA 安全认证中心发放（CA 是签发机构）
- B、证书携带持有者的公开密钥（看看）
- C、证书的有效性可以通过验证持有者的签名（自己签发给自己的证书，可以这样验证）
- D、证书通常携带 CA 的公开密钥（有颁发机构信息，通过信息可以查询到颁发机构的签名证书，利用签名证书验证证书）

信管网解析：

证书的验证过程：这张证书是由颁发机构的证书签名的，我要用颁发机构的证书验证真伪，但是颁发机构的证书同样需要验证下真伪，颁发机构的证书又是用另一个高级的证书签发的，所以这样一级级递归，到头就是验证根证书。根证书是一个比较特别的证书，他是 CA 自己签发给自己的，用户对根证书的信任代表

对证书链的信任。

信息安全工程师教程: 电子商务数字证书技术: <http://www.cnitpm.com/pm1/35401.html>

信管网参考答案: D

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

32、密码分析学是研究密码破译的科学, 在密码分析过程中, 破译密文的关键是 ()

- A、截获密文
- B、截获密文并获得密钥
- C、截获密文, 了解加密算法和解密算法
- D、截获密文, 获得密钥并了解解密算法

信管网解析:

破译密文的关键是截获密文, 获得密钥并了解其解密算法。

信息安全技术知识: 密码分析方法: <http://www.cnitpm.com/pm1/35946.html>

信管网参考答案: D

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

33、利用公开密钥算法进行数据加密时, 采用的方法是 ()

- 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

信管网解析:

在进行加密时, 发送方用对方的公钥加密, 接收方用自己的私钥解密。

关于公钥加密私钥解密与私钥加密公钥解密说明: <http://www.cnitpm.com/pm1/40633.html>

信管网参考答案: C

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

34、数字信封技术能够 ()

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

信管网解析:

数字信封使用私有密钥加密算法并利用接收人的公钥对要传输的数据进行加密, 以保证数据信息在传输过程中的安全性。

信息系统集成专业技术知识: 信息安全-加密技术数字签名与数字信封:

<http://www.cnitpm.com/pm1/37283.html>

信管网参考答案: B

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

35、在 DES 加密算法中, 密钥长度和被加密的分组长度分别是 ()

- A、56 位和 64 位
- B、56 位和 56 位
- C、64 位和 64 位

D、64 位和 56 位

信管网解析:

des 算法的密钥分组长度为 64 位, 除去 8 位校验位, 实际密钥长度为 56 位, 被加密的分组长度为 64 位。

信息安全技术知识: DES 加密过程: <http://www.cnitpm.com/pm1/36445.html>

信管网参考答案: A

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

36、甲不但怀疑乙发给他的被人篡改, 而且怀疑乙的公钥也是被人冒充的, 为了消除甲的疑虑, 甲和乙决定找一个双方都信任的第三方来签发数字证书, 这个第三方为 ()

A、国际电信联盟电信标准分部 (ITU-T)

B、国家安全局 (NSA)

C、认证中心 (CA)

D、国家标准化组织 (ISO)

信管网解析:

通信双方进行保密通信时, 通常会通过双方信任的第三方认证中心 ca 来签发数字证书。

什么是 CA 认证: <http://www.cnitpm.com/pm/33710.html>

信管网参考答案: C

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

37、WI-FI 网络安全接入是一种保护无线网络安全的系统, WPA 加密模式不包括 ()

A、WPA 和 WPA2

B、WPA-PSK

C、WEP

D、WPA2-PSK

信管网解析:

wpa 有 wpa 和 wpa2 两个标准, 是一种保护无线电脑网络(wi-fi)安全的系统, 有四种认证方式: wpa、wpa-psk、wpa2 和 wpa2-psk。

信息安全工程师教程: wi-fi 网络安全接入 (wpa/wpa2): <http://www.cnitpm.com/pm1/41482.html>

信管网参考答案: C

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

38、特洛伊木马攻击的威胁类型属于 ()

A、授权侵犯威胁

B、渗入威胁

C、植入威胁

D、旁路控制威胁

信管网解析:

主要的渗入威胁有假冒、旁路、授权侵犯, 主要的植入威胁有特洛伊木马和陷阱。

信息安全工程师教程: 特洛伊木马: <http://www.cnitpm.com/pm1/41490.html>

信管网参考答案: C

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

39、信息通过网络进行传输的过程中, 存在着被篡改的风险, 为了解决这一安全问题, 通常采用的安全防护技术是 ()

- A、加密技术
- B、匿名技术
- C、消息认证技术
- D、数据备份技术

信管网解析:

消息认证就是验证消息的完整性,当接收方收到发送方的报文时,接收方能够验证收到的报文是真实的和未被篡改的。

信息安全技术知识:消息认证与数字签名-认证的目的: <http://www.cnitpm.com/pm1/38351.html>

信管网参考答案: C

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

40、甲收到一份来自乙的电子订单后,将订单中的货物送达到乙时,乙否认自己曾经发送过这份订单,为了解除这种纷争,采用的安全技术是 ()

- A、数字签名技术
- B、数字证书
- C、消息认证码
- D、身份认证技术

信管网解析:

数字签名技术能使签名者事后不能抵赖自己的签名,任何其他人不能伪造签名以及能在公正的仲裁者面前通过验证签名来确认其真伪。

信息安全工程师考点梳理 (5): 数字签名与认证: <http://www.cnitpm.com/pm1/37109.html>

信管网参考答案: A

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

41、目前使用的防杀病毒软件的作用是 ()

- 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

信管网解析:

防杀毒软件的作用是检查计算机是否感染已知病毒并清除它们,而对于那未知的或者是更高级的病毒无能为力。

重要的网络安全技术之杀毒软件: <http://www.cnitpm.com/pm/33234.html>

信管网参考答案: D

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

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 ()

- A、172.168.1.2
- B、10.1.2.3
- C、168.1.2.3
- D、192.172.1.2

信管网解析:

专用 ip 地址范围:

A 类 1 个: 10.0.0.0/8

B 类 16 个: 172.16.0.0/16, 16 - 31

C 类 1 个: 192.168.0.0/24

信息安全工程师教程: ipv4 协议-vlsm 和 cidr: <http://www.cnitpm.com/pm1/41505.html>

信管网参考答案: B

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

43、下列报告中, 不属于信息安全风险评估识别阶段的是 ()

- A、资产价值分析报告
- B、风险评估报告
- C、威胁分析报告
- D、已有安全威胁分析报告

信管网解析:

风险评估报告属于信息安全风险分析阶段的输出报告。

信息系统项目管理师知识: 风险识别及历年真题: <http://www.cnitpm.com/pm1/40085.html>

信管网参考答案: B

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

44、计算机犯罪是指利用信息科学技术且以计算机跟踪对象的犯罪行为, 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 ()

- A、计算机犯罪具有隐蔽性
- B、计算机犯罪具有高智能性, 罪犯可能掌握一些其他高科技手段
- C、计算机犯罪具有很强的破坏性
- D、计算机犯罪没有犯罪现场 (电子取证、现场勘探)

信管网解析:

计算机犯罪现场是指计算机犯罪嫌疑人实施犯罪行为的地点和遗留有与计算机犯罪有关的痕迹、物品 (包括电子数据、电子设备等) 或其他物证的场所。

计算机犯罪的特点和防范: <http://www.cnitpm.com/pm/33717.html>

信管网参考答案: D

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

45、以下对 OSI (开放系统互联) 参考模型中数据链路层的功能叙述中, 描述最贴切是 ()

- A、保证数据正确的顺序、无差错和完整
- B、控制报文通过网络的路由选择 (网络层)
- C、提供用户与网络的接口
- D、处理信号通过介质的传输 (物理层)

信管网解析:

数据链路层最基本的服务是将源计算机网络层来的数据可靠的传输到相邻节点的目标计算机的网络层。为达到这一目的, 数据链路层必须具备一系列相应的功能, 主要有: 1、如何将数据组合成数据块 (在数据链路层中将这种数据块称为帧, 帧是数据链路层的传送单位); 2、如何控制帧在物理信道上的传输, 包括如何处理传输差错, 如何调节发送速率以使之与接收方相匹配; 3、在两个网路实体之间提供数据链路通路的建立、维持和释放管理。

信息系统网络知识里的各层网络协议: <http://www.cnitpm.com/pm/33091.html>

信管网参考答案: A

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

46、深度流检测技术就是以流为基本研究对象,判断网络流是否异常的一种网络安全技术,其主要组成部分通常不包括()

- A、流特征选择
- B、流特征提供
- C、分类器
- D、响应

信管网解析:

深度流检测技术主要分为三部分:流特征选择、流特征提取、分类器。

信息安全工程师教程:协议分析-深度流检测技术(DFI): <http://www.cnitpm.com/pm1/37280.html>

信管网参考答案: D

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

47、一个全局的安全框架必须包含的安全结构因素是()

- A、审计、完整性、保密性、可用性
- B、审计、完整性、身份认证、保密性、可用性
- C、审计、完整性、身份认证、可用性
- D、审计、完整性、身份认证、保密性

信管网解析:

一个全局的安全框架必须包含的安全结构因素有审计、完整性、身份认证、保密性,可用性、真实性。

信息安全技术知识:安全机制: <http://www.cnitpm.com/pm1/35672.html>

信管网参考答案: B

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

48、以下不属于网络安全控制技术的是()

- A、防火墙技术
- B、访问控制
- C、入侵检测技术
- D、差错控制

信管网解析:

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;差错控制技术是在数字通信过程中利用编码的方法对错误进行控制,以提高数字传输的准确性,不属于网络安全控制技术。

系统集成项目管理工程师第2版:网络安全: <http://www.cnitpm.com/pm1/35743.html>

信管网参考答案: D

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

49、病毒的引导过程不包含()

- A、保证计算机或网络系统的原有功能
- B、窃取系统部分内存
- C、使自身有关代码取代或扩充原有系统功能
- D、删除引导扇区

信管网解析:

病毒的引导过程包括:

(1)驻留内存病毒若要发挥其破坏作用,一般要驻留内存。为此就必须开辟所用内存空间或覆盖系统占用

的部分内存空间, 有的病毒不驻留内存。

(2) 窃取系统控制权在病毒程序驻留内存后, 必须使有关部分取代或扩充系统的原有功能, 并窃取系统的控制权。此后病毒程序依据其设计思想, 隐蔽自己, 等待时机, 在条件成熟时, 再进行传染和破坏。

(3) 恢复系统功能病毒为隐蔽自己, 驻留内存后还要恢复系统, 使系统不会死机, 只有这样才能等待时机成熟后, 进行感染和破坏的目的。

简述病毒程序的结构和机制: <http://www.cnitpm.com/pm/33579.html>

信管网参考答案: D

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

50、网络系统中针对海量数据的加密, 通常不采用 ()

- A、链路加密
- B、会话加密
- C、公钥加密
- D、端对端加密

信管网解析:

公钥加密加密算法复杂且加解密效率低, 一般只适用于少量数据的加密。

信息安全技术知识: 利用公钥密码分配对称密钥: <http://www.cnitpm.com/pm1/38062.html>

信管网参考答案: C

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

51、安全备份的策略不包括 ()

- A、所有网络基础设施设备的配置和软件
- B、所有提供网络服务的服务器配置
- C、网络服务 (备份策略是为了保证服务持续性)
- D、定期验证备份文件的正确性和完整性

信管网解析:

网络服务是指一些在网络上运行的、面向服务的、基于分布式程序的软件模块, 通常采用 http 和 xml 等互联网通用标准, 使人们可以在不同的地方通过不同的终端设备访问 web 上的数据, 如网上订票, 查看订座情况。

信息安全工程师教程: 网络容灾备份系统的应用: <http://www.cnitpm.com/pm1/38675.html>

信管网参考答案: C

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

52、以下关于安全套接层协议 (SSL) 的叙述中, 错误的是 ()

- A、是一种应用层安全协议 (介于传输层与应用层之间)
- B、为 TCP/IP 连接提供数据加密
- C、为 TCP/IP 连接提供服务器认证
- D、提供数据安全机制

信管网解析:

ssl 位于应用层和传输层之间, 它可以为任何基于 tcp 等可靠连接的应用层协议提供安全性保证。

信息安全技术知识: SSL 协议: <http://www.cnitpm.com/pm1/40107.html>

信管网参考答案: A

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

53、入侵检测系统放置在防火墙内部所带来的好处是 ()

- A、减少对防火墙的攻击
- B、降低入侵检测
- C、增加对低层次攻击的检测
- D、增加检测能力和检测范围

信管网解析:

ids 实时检测可以及时发现一些防火墙没有发现的入侵行为, 发行入侵行为的规律, 这样防火墙就可以将这些规律加入规则之中, 提高防火墙的防护力度, 降低入侵检测系统的误报率。

入侵检测系统和防火墙的区别和联系: <http://www.cnitpm.com/pm/7059.html>

信管网参考答案: B

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

54、智能卡是指粘贴或嵌有集成电路芯片的一种便携式卡片塑胶, 智能卡的片内操作系统 (COS) 是智能卡芯片内的一个监控软件, 以下不属于 COS 组成部分的是 ()

- A、通讯管理模块 (Transmission Manager)
- B、数据管理模块
- C、安全管理模块
- D、文件管理模块 (File Manager)

信管网解析:

四大模块: 通信管理、命令解析、文件管理、安全管理

信息安全工程师教程: 智能卡的 cos: <http://www.cnitpm.com/pm1/41520.html>

信管网参考答案: B

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

55、以下关于 IPSec 协议的叙述中, 正确的是 ()

- A、IPSec 协议是解决 IP 协议安全问题的一种方案
- B、IPSec 协议不能提供完整性 (HASH 函数)
- C、IPSec 协议不能提供机密性保护
- D、IPSec 协议不能提供认证功能 (AH, ESP 都提供认证)

信管网解析:

ipsec 协议是一种开放标准的框架结构, 通过使用加密的安全服务以确保在 internet 协议网络上进行保密而安全的通讯, 是解决 ip 协议安全问题的一种方案, 它能提供完整性、保密性、反重播性、不可否认性、认证等功能。

信息安全工程师教程: ip 安全协议 (ipsec): <http://www.cnitpm.com/pm1/41533.html>

信管网参考答案: A

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

56、不属于物理安全威胁的是 ()

- A、自然灾害
- B、物理攻击
- C、硬件故障
- D、系统安全管理人员培训不够

信管网解析:

物理安全是指在物理媒介层次上对存储和传输的信息加以保护, 它是保护计算机网络设备、设施免遭地震、

水灾、火灾等环境事故以及人为操作错误或各种计算机犯罪行为而导致破坏的过程。

信息系统安全技术体系: <http://www.cnitpm.com/pm/27624.html>

信管网参考答案: D

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

57、以下关于网络钓鱼的说法中, 不正确的是 ()

- A、网络钓鱼融合了伪装、欺骗等多种攻击方式
- B、网络钓鱼与 Web 服务没有关系
- C、典型的网络钓鱼攻击都将被攻击者引诱到一个通过精心设计的钓鱼网站上
- D、网络钓鱼是“社会工程攻击”是一种形式

信管网解析:

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(如用户名、口令、帐号 id、atm pin 码或信用卡详细信息)的一种攻击方式, 最典型的网络钓鱼攻击将收信人引诱到一个通过精心设计与目标组织非常相似的钓鱼网站上, 并获取收信人在此网站上输入的个人敏感信息, 通常这个过程不会让受害者警觉, 它是“社会工程攻击”的一种形式。

信息安全工程师教程: 网络钓鱼: <http://www.cnitpm.com/pm1/41536.html>

信管网参考答案: B

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

58、以下关于隧道技术说法不正确的是 ()

- A、隧道技术可以用来解决 TCP/IP 协议的某种安全威胁问题
- B、隧道技术的本质是用一种协议来传输另外一种协议
- C、IPSec 协议中不会使用隧道技术 (IPsec 有隧道和传输两种模式)
- D、虚拟专用网中可以采用隧道技术

信管网解析:

隧道技术是一种通过使用互联网络的基础设施在网络之间传递数据的方式, 使用隧道传递的数据(或负载)可以是不同协议的数据帧或包, 隧道协议将其它协议的数据帧或包重新封装然后通过隧道发送。协议包括: pptp 协议、l2tp 协议、ipsec 协议、vpn 协议等。

信息安全工程师教程: 基于隧道协议的 VPN: <http://www.cnitpm.com/pm1/38445.html>

信管网参考答案: C

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

59、安全电子交易协议 SET 是有 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 ()

- A、SET 是一种基于流密码的协议 (公钥算法 RSA, 对称密码算法是 DES)
- B、SET 不需要可信的第三方认证中心的参与 (第三方: 支付网关)
- 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 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 (数字签名、身份认证的过程)

信管网解析:

set 协议是应用层的协议, 是一种基于消息流的协议, 一个基于可信的第三方认证中心的方案。set 改变了支付系统中各个参与者之间交互的方式, 电子支付始于持卡人。

信息安全工程师教程: 电子商务安全协议-SET 协议简介: <http://www.cnitpm.com/pm1/35422.html>

信管网参考答案: C

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

60、在 PKI 中, 不属于 CA 的任务是 ()

- A、证书的颁发
- B、证书的审改
- C、证书的备份
- D、证书的加密

信管网解析:

ca 是 pki 的信任基础, ca 负责签发证书、管理和撤销证书, 包括证书的审批及备份等。

什么是 CA 认证: <http://www.cnitpm.com/pm/33710.html>

信管网参考答案: D

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

61、以下关于 VPN 的叙述中, 正确的是 ()

- A、VPN 指的是用户通过公用网络建立的临时的、安全的连接
- B、VPN 指的是用户自己租用线路, 和公共网络物理上完全隔离的、安全的线路
- C、VPN 不能做到信息认证和身份认证
- D、VPN 只能提供身份认证, 不能提供数据加密的功能

信管网解析:

vpn 即虚拟专用网, 是企业网在因特网等公共网络上的延伸, 通过一个私有的通道在公共网络上创建一个临时的、安全的私有连接。

信息安全工程师教程: VPN 技术及应用: <http://www.cnitpm.com/pm1/38430.html>

信管网参考答案: A

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

62、扫描技术 ()

- A、只能作为攻击工具
- B、只能作为防御工具
- C、只能作为检查系统漏洞的工具
- D、既可以作为攻击工具, 也可以作为防御工具

信管网解析:

通常的扫描技术采用两种策略: 被动式和主动式。被动式策略是基于主机的, 主动式策略是基于网络的, 它通过网络对远程的目标主机建立连接, 并发送请求, 分析其返回信息, 从而分析远程主机漏洞。既可以作为攻击工具, 也可以作为防御工具。

信息安全工程师教程: 网络安全漏洞扫描技术及应用-网络安全漏洞扫描的工作原理:

<http://www.cnitpm.com/pm1/38355.html>

信管网参考答案: D

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

63、包过滤技术防火墙在过滤数据包时, 一般不关心 ()

- A、数据包的源地址
- B、数据包的协议类型
- C、数据包的目的地地址
- D、数据包的内容

信管网解析:

数据包过滤是通过对数据包的 ip 头和 tcp 头或 udp 头的检查来实现的, 不检查数据包的内容。

数据包过滤的安全策略基于哪几种方式: <http://www.cnitpm.com/pm/33807.html>

信管网参考答案: D

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

64、以下关于网络流量监控的叙述中, 不正确的是 ()

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

信管网解析:

流量监控指的是对数据流进行的监控, 通常包括出数据、入数据的速度、总流量。不能过滤敏感数据。

信息安全工程师教程: 网络安全产品的配置与使用-网络流量监控技术:

<http://www.cnitpm.com/pm1/37173.html>

信管网参考答案: C

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

65、两个密钥三重 DES 加密: $C=C_{K1}[D_{K2}[E_{K1}[P]]]$, $K1 \neq K2$, 其中有效的密钥为 () 应该是 EDE

- A、56
- B、128
- C、168
- D、112

信管网解析:

3des 的密钥长度为 168 位。

信息安全技术知识: 三重 DES: <http://www.cnitpm.com/pm1/36762.html>

信管网参考答案: D

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

66、设在 RSA 的公钥密码体制中, 公钥为 $(c, n) = (13, 35)$, 则私钥为 ()

- A、11
- B、13
- C、15
- D、17

信管网解析:

$$N = p * q = 35 = 5 * 7$$

$$F = (5-1) * (7-1) = 24$$

$$e1 = 13$$

$$e2 * e1 \bmod 24 = 1 \rightarrow e2 = 13$$

- (1) 选择一对不同的、足够大的素数 p, q。
- (2) 计算 $n=pq$ 。
- (3) 计算 $f(n)=(p-1)(q-1)$, 同时对 p, q 严加保密, 不让任何人知道。
- (4) 找一个与 $f(n)$ 互质的数 e, 且 $1 < e < f(n)$ 。
- (5) 计算 d, 使得 $de \equiv 1 \bmod f(n)$ 。这个公式也可以表达为 $d \equiv e^{-1} \bmod f(n)$

信息安全技术知识: 公钥密码体制: <http://www.cnitpm.com/pm1/37650.html>

信管网参考答案: B

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

67、杂凑函数 SHA1 的输入分组长度为 () 比特

- A、128
- B、256
- C、512
- D、1024

信管网解析:

sha-1 算法对输入按 512 位进行分组, 并以分组为单位进行处理。

信息安全技术知识: Hash 函数与安全的 Hash 函数的要求: <http://www.cnitpm.com/pm1/38462.html>

信管网参考答案: C

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

68、AES 结构由以下 4 个不同的模块组成, 其中 () 是非线性模块

- A、字节代换
- B、行移位
- C、列混淆
- D、轮密钥加

信管网解析:

每一轮又包括: SubBytes、ShiftRows、MixColumns、AddRoundKey

1. AddRoundKey — 矩阵中的每一个字节都与该次轮密钥 (round key) 做 XOR 运算; 每个子密钥由密钥生成方案产生。
2. SubBytes — 通过个非线性的替换函数, 用查找表的方式把每个字节替换成对应的字节。
3. ShiftRows — 将矩阵中的每个横列进行循环式移位。
4. MixColumns — 为了充分混合矩阵中各个直行的操作。这个步骤使用线性转换来混合每列的四个字节。

信息安全技术知识: AES 加密: <http://www.cnitpm.com/pm1/36841.html>

信管网参考答案: A

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

69、 $67 \bmod 119$ 的逆元是 () 乘法逆元

- A、52
- B、67
- C、16
- D、19

信管网解析:

设 S 为一有二元运算 $*$ 的集合。若 e 为 $(S, *)$ 的单位元且 $a*b=e$, 则 a 称为 b 的左逆元素且 b 称为 a 的右逆元素。

信息安全技术知识: 乘法密码、乘法密码举例: <http://www.cnitpm.com/pm1/36080.html>

信管网参考答案: C

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

70、在 DES 算法中, 需要进行 16 轮加密, 每一轮的子密钥长度为 ()

- A、16
- B、32
- C、48
- D、64

信管网解析:

des 算法中, 64 位密钥经过置换选择 1、循环左移、置换选择 2 等变换, 产生 16 个 48 位长的子密钥。

信息安全技术知识: DES 子密钥产生: <http://www.cnitpm.com/pm1/36551.html>

信管网参考答案: C

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>

71-75 (1) is the science of hiding information. Whereas the goal of cryptography is to make data unreadable by a third party. the goal of steganography ([, stegə'nɒ grəfi]隐写术) is to hide the data from a third party. In this article, I will discuss what steganography is, what purposes it serves, and will provide an example using available software.

There are a large number of steganographic (2) that most of us are familiar with (especially if you watch a lot of spy movies), ranging from invisible ink and microdots to secreting a hidden message in the second letter of each word of a large body of text and spread spectrum radio communication. With computers and networks, there are many other ways of hiding informations, such as:

Covert channels (c,g, Loki and some distributed denial-of-service tools use the Internet Control (3) Protocol, or ICMP, as the communication channel between the “bad guy” and a compromised system)

Hidden text within Web pages

Hiding files in “plain sight” (c,g. what better place to “hide” a file than with an important sounding name in the c:\winnt\system32 directory)

Null ciphers(c,g, using the first letter of each word to form a hidden message in an otherwise innocuous text)

steganography today, however, is significantly more (4) than the example about suggest, allowing a user to hide large amounts of information within image and audio. These forms of steganography often are used in conjunction with cryptography so the information is double protected; first it is encrypted and then hidden so that an advertisement first. find the information (an often difficult task in and of itself) and the decrypted it.

The simplest approach to hiding data within an image file is called (5) signature insertion. In this method, we can take the binary representation of the hidden data and the bit of each byte within the covert image. If we are using 24-bit color the amount and will be minimum and indiscernible to the human eye.

(1) A、Cryptography

B、Geography

C、Stenography

D、Steganography

(2) A、methods

B、software

C、tools

D、services

(3) A、Member

B、Management

C、Message

D、Mail

- (4) A、powerful
B、sophistication ([sə, fɪ stɪ ' keɪ ʃ n]可理解为先进)
C、advanced
D、easy

- (5) A、least (LSB: *least significant bit*)
B、most
C、much
D、less

信管网解析:

LSB 隐写

- LSB 全称 **least significant bit**，最低有效位
- PNG 文件中的图像像素一般是由 **RGB** 三原色（红绿蓝）组成，每一种颜色占用 8 位，取值范围为 0x00~0xFF，即有 256 种颜色，一共包含了 256 的 3 次方的颜色，即 16777216 种颜色
- 人类的眼睛可以区分约 1000 万种不同的颜色
- 这意味着人类的眼睛无法区分余下的颜色大约有 6777216 种
- **LSB 隐写**就是修改 RGB 颜色分量的最低二进制位（LSB），而人类的眼睛不会注意到这前后的变化
- 每个像素可以携带 3 比特的信息

信管网参考答案: A、A、C、B、A

最终答案以信管网题库为准: <http://www.cnitpm.com/pm1/37841.html>