# 信息安全试题答案
# (07172)

一、单项选择题（每小题 1 分，共 30 分）

在每小题的四个备选答案中选出一个正确答案，并将其代码写在题干后面的括号内。不选、错选或多选者，该题无分。

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1. B | 2. D | 3. C | 4. D | 5. B | 6. C | 7. C | 8. D | 9. B | 10. C |
| 11. B | 12. A | 13. B | 14. C | 15. B | 16. C | 17. D | 18. C | 19. D | 20. D |
| 21. A | 22. D | 23. B | 24. B | 25. A | 26. C | 27. A | 28. B | 29. D | 30. C |

二、多项选择题（每小题 2 分，共 20 分）

在每小题的五个备选答案中选出二至五个正确答案，并将其代码写在题干后面的括号内。多选、少选、不选或错选者，该题无分。

| | | | | |
|---|---|---|---|---|
| 1. ABCE | 2. ABC | 3. ACD | 4. ACE | 5. AE |
| 6. ADE | 7. ABE | 8. BCD | 9. ACDE | 10. CE |

三、名词解释（每小题 3 分，共 12 分）

1. 站点认证

为了确保通信安全，在正式传送报文之前，应首先认证通信是否在双方确定的站点之间进行，这一过程称为站点认证。这种站点认证是通过验证加密的数据能否成功地在两个站点间进行传送来实现的。

2. 密钥托管

密钥托管是指用户在向 CA 申请数据加密证书之前，必须把自己的密钥分成 t 份交给可信赖的 t 个托管人。任何一位托管人都无法通过自己存储的部分用户密钥恢复完整的用户密码。只有这 t 个人存储的密钥合在一起才能得到用户的完整密钥。

3. 虚拟专用网

虚拟专用网（VPN）是指将物理上分布在不同地点的网络通过公用网络连接成逻辑上的虚拟子网，采用认证、访问控制、密码技术等在公用网络上构建专用网络的技术。

4. 信息安全

我们把信息安全定义为："一个国家的社会信息化状态不受外来威胁与侵害；一个国家的信息技术体系不受外来的威胁与侵害。"

四、简答题（每小题 5 分，共 20 分）

1. 个人信息安全隐患有哪几类？

个人信息安全存在的隐患可分为如下几类：

（1）信息的截获和窃取

（2）信息的篡改

（3）信息假冒

（4）交易抵赖

（5）信息损毁



2. 防火墙作用是什么？优越性有哪些？

防火墙是由一组相关软件和硬件组成的，采用由系统管理员定义的规则，对一个安全网络之间的数据流进行保护。

它的优越性有：(1)它可以控制不安全的服务，只有授权的协议和服务才能通过防火墙；(2)它能对站点进行访问控制，防止非法访问；(3)它可把安全软件集中地放在防火墙系统中，集中实施安全保护；(4)它强化私有权，防止攻击者截取别人的信息；(5)它能对所有的访问做出日志记录。

3. 计算机取证有哪些技术？为什么要研究计算机反取证技术？

计算机取证包括物理证据获取和信息发现两个阶段，涉及到电子证据获取技术、电子证据数据保全技术、电子证据数据分析技术和电子证据数据鉴定技术。

研究反取证技术意义非常重大，一方面可以了解入侵者有哪些常用手段用来掩盖甚至擦除入侵痕迹；另一方面可以在了解这些手段的基础上，开发出更加有效、实用的计算机取证工具，从而加大对计算机犯罪的打击力度，保证信息系统的安全性。

4. 信息系统的安全需求分析包括哪些内容？

信息系统的安全需求分析包括：

（1）与环境相关的安全需求；

（2）与安全功能相关的安全需求；

（3）与安全性能相关的安全需求；

（4）与服务相关的安全需求；

（5）与管理有关的安全需求。

五、论述题（共 18 分）

1. DES 的工作模式有哪几种？DES 的评价怎样？(10 分)

DES 的工作模式有四种：电子密码本（ECB）、密码分组链接（CBC）、输出反馈（OFB）和密文反馈（CFB）。ANSI 银行标准中规定加密用 ECB 和 CBC 方式，鉴别用 CBC 和 n-位的 CFB 方式。

从对密码学领域的贡献来看，DES 推动了密码学在理论和实践技术上的发展，具体表现在以下几个方面：

它公开展示了能完全适应某一历史阶段中信息安全要求的一种密码体制的构造方法；

它是世界上第一个数据加密标准，它确立了这样一个原则，即算法的细节可以公开而密码的使用法仍是保密的；

它表明用分组密码作为对密码算法标准化这种方法是方便可行的；

由 DES 的出现而引起的讨论及附带的标准化工作已经确立了安全使用分组密码的若干准则；

由于 DES 的出现，推动了密码分析理论和技术的快速发展，出现了差分分析、线性分析等多种新的有效的密码分析方法。

2. 公钥基础设施的基本组件包括哪些？其作用是什么？(8 分)