成都信息工程大学考试试卷

2018——2019 学年第一学期

课程名称：信息安全理论与技术　使用班级：物联网 2016 级　试卷形式：闭卷☑

试题	一	二	三	四	五	总分
得分						

一、填空题（每空 1 分，共 10 分）

1. ISO 安全体系包含了哪三部分_____、_____、和_____。
2. 写出对称密码体制的三个缺点_____、_____、和_____。
3. 信息收集可以利用_____技术和_____技术，也可以利用网络现有资源及社会工程学来实现。
4. 为了配置管理方便，内网中需要向外网提供服务的服务器往往放在一个独立的网段，这个网段便是_____。
5. _____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。

二、选择题（每题 1 分，共 20 分，请将选择结果填入下面的表格中。）

1	2	3	4	5	6	7	8	9	10

1. 如果 m 表示明文,c 表示密文,E 代表加密变换,D 代表解密变换,则下列表达式中描述加密过程的是（　　）

A. c=E(m)　　B. c=D(m)　　C. m=E(c)　　D. m=D(c)

2. RSA 属于（　　）

A. 传统密码体制　　B. 非对称密码体制
C. 现代密码体制　　D. 对称密码体制

3. 防止发送方否认的方法是（　　）

A. 消息认证　　B. 保密
C. 日志　　D. 数字签名

4. 以下（　　）不是包过滤防火墙主要过滤的信息。

A. 源 IP 地址　　B. 目的 IP 地址
C. 时间　　D. 端口号

5. PKI 解决了信息系统中的（　　）问题

A. 身份信任　　B. 权限管理
C. 安全审计　　D. 加密

6. VPN 的加密手段　　）

A. 具有加密功能的防火墙
B. 具有加密功能的路由器
C. VPN 内的各台主机对各自的信息进行相应的加密
D. 单独的加密手段

7. 不是计算机病毒所具有的特点（　　）

A. 传染性　　B. 破坏性
C. 潜伏性　　D. 可预见性

8. IPSec 协议工作在（　　）层次。

A. 数据链路层　　B. 网络层
C. 应用层　　D. 传输层

9. PKI 的主要理论基础是（　　）

A. 对称密码算法　　B. 公钥密码算法
C. 量子密码　　D. 摘要算法

10. 入侵检测技术可以分为误用检测和（　）两大类。

A. 病毒检测　　B. 详细检测
C. 异常检测　　D. 漏洞检测

系名_____ 班级_____ 姓名_____ 学号_____ 密封线内不答题

三、判断题（每题 1 分，共 10 分，请将判断的结果填入下面表格中。）

1	2	3	4	5	6	7	8	9	10

1. 网络边界保护中主要采用防火墙系统，为了保证其有效发挥作用，应当避免在内网 和外网之间存在不经过防火墙控制的其他通信连接。 （ ）
2. 在我国，不是很严重的网络犯罪行为只要没被抓住，就不需要接受刑法的相关处罚 （ ）
3. 一个完整的信息安全保障体系，应当包括安全策略、保护(Protection)、检测(Detection)、响应(Reaction)四个主要环节。 （ ）
4. 脆弱性分析技术，也被通俗地称为漏洞扫描技术。其中，有端口扫描、IP 扫描和嗅探。 （ ）
5. 信息安全等同于网络安全。 （ ）
6. 分析密码算法主要有三种方法：穷举法、统计分析法和密码技术分析法。 （ ）
7. 恶意代码可通过依附或者隐藏与系统的方法，感染引导区，在杀毒软件未启动前获得系统某些高级权限。 （ ）
8. 口令认证机制的安全性弱，可以使得攻击者破解合法用户帐户信息，进而非法获得系统和资源访问权限。 （ ）
9. 误用入侵检测大部分依赖与攻击者的技术。 （ ）
10. 屏蔽路由器是防火墙最基本的构件,它有日志功能,可以记录攻击者的信息。 （ ）

四、简答题（每题 5 分，共 30 分）

1. 什么是网络安全？网络安全有哪些特征？

2. 简述公钥密码体制的优点？

3. Kerberos 是一种身份鉴别服务。简述 Kerberos 的设计目标以及 Kerberos 的四个基本实体。

4. 一个证书的生命周期包括哪几个阶段，并做简要阐述。

系名_____ 班级_____ 姓名_____ 学号_____

密 封 线 内 不 答 题

5. 请叙述端口扫描的过程。

6. 简写五个防火墙的缺点。

五、综合应用题（每题 15 分，共 30 分）

1. 假设你的服务器长期受到拒绝服务攻击，请提出一个解决方案。

2. 甲要给异地公司开视频会议，想要全过程保密，现要通过互联网进行通信，且假设不存在可信的第三方，请详述实现过程。

8

物联网 161 第二套试卷答案

一．填空题

1. 安全服务、安全机制、安全管理
2. 密钥分发困难、密钥管理困难、无法源认证
3. 扫描、嗅探
4. 非军事化区
5. 隧道

二．选择题

A、B、D、C、A、C、D、B、B、C

三.判断题

对错错错错对对对错错

四．简答题

第一题：.

1.网络安全：本质上就是网络上信息的安全，指网络系统的硬件，软件及其系统中的数据安全。

2.四大特征：保密性，完整性，可用性，可控性。

第二题：

1.便于管理。网络中的每一个用户只需要保护自己的私钥，则 N 个用户仅需产生 N 对密钥。

2.密钥分配简单。不需要秘密的通道和复杂的协议来传送密钥。公钥可基于公开的渠道分发给其他用户，而私钥则由用户自己保管。

3.可以实现数字签名。

第三题：

设计目标：1. 安全性。 2. 可靠性。 3. 对用户透明性。 4. 可伸缩。

四个基本实体：1. Kerberos 客户机。 2. 认证服务器。 3. 票据许可服务器。 4. 应用服务器。

第四题：

1.初始化：注册、密钥对产生、提交申请、审核检查、证书签发、密钥备份

2.颁发：证书检索、证书验证、证书存储、密钥恢复、密钥更新

3.撤销：证书过期、证书撤销、密钥历史、密钥档案

第五题：

1.攻击者向要测试的端口发送一个 SYN 探测包

2.若收到目标端口的 SYN/ACK 数据包表示端口开放；

若收到目标端口的 RST/ACK 数据包表示端口关闭

3.攻击者向目标端口发送 RST 数据包，重置 TCP 链接，防止对方记录

第六题：

1.防火墙不能防范不经防火墙的攻击

2.防火墙不能防范来自内部网络的攻击

3.防火墙不能防范感染了病毒的软件和文件传输

4.防火墙不能防范利用目标网络协议中的缺陷进行攻击

5.防火墙不能防范利用服务器系统漏洞进行攻击

6.防火请不能防范新的网络安全问题

7.防火墙限制了有用的网络服务

以上任写 5 点即可

五.综合题

第一题:

1.确保所有服务器采用最新的系统,并打上安全补丁

2.删除多余的网络服务,从而减少网络协议的漏洞

3.设置防火墙,过滤掉所有可能伪造的数据包

4.确保从服务器相应的目录或文件数据库中删除未使用的服务

5.禁止内部网络通过 Modern 连接至 PSTN 系统

6.禁止使用网络访问程序

7.限制在防火墙外与网络文件共享

8.在防火墙上运行端口映射程序或端口扫描程序

9.检查所有网络设备、主机和服务器系统的日志

10.确保管理人员对所有主机进行检查

第二题：

甲与异地公司搭建 Host 对 Host 的 VPN。要求通信双方的所有主机均支持 IPsec 协议，两个异地 VPN 的网关必须支持 IPsec 协议。对视频数据经过 IPsec 协议处理，这样所有的通信链路都是安全的。

成都信息工程大学考试试卷

2018——2019 学年第一学期

课程名称：信息安全理论与技术　使用班级：物联网 2016 级　试卷形式：闭卷☒

试题	一	二	三	四	五	总分
得分						

一、填空题（每空 1 分，共 10 分）

1. 信息安全五个特征为_____、完整性、_____、和_____、_____。
2. 密码学包含两方面内容：_____和_____。
3. 防火墙具有较强的_____能力。
4. 数字证书的生命周期包括_____、_____和_____三个阶段。

二、选择题（每题 1 分，共 20 分，请将选择结果填入下面的表格中。）

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20

1. 密码学的目的是（　）

A.研究数据加密　　B.研究数据解密

C.研究数据保密　　D.研究信息安全

2. 下面哪种方式属于黑客主动攻击（　）

A.缓冲区溢出　　B.运行恶意软件

C.浏览恶意代码网页　　D.打开病毒附件

3. 描述数字信息的接收方能够准确的验证发送方身份的技术术语是（　）

A.加密　　B.解密

C.对称加密　　D.数字签名

4. 公钥密码基础设施 PKI 解决了信息系统中的（　）问题。

A.身份信任　　B.权限管理

C.安全审计　　D.加密

5. IPSec 协议工作在（　）。

A.数据链路层　　B.网络层

C.应用层　　D.传输层

6. PKI 的主要组成不包括下（　）

A.证书授权 CA　　B. SSL

C.注册授权 RA　　D. 证书存储库 CR

7. 一般而言，Internet 防火墙建立在一个网络的（　）

A.内部子网之间传送信息的中　　B. 每个子网的内部

C.内部网络与外部网络的交叉点　　D.部分内部网络与外部网络的结合处

8. 1999 年，我国发布的第一个信息安全等级保护的国家标准 GB17895-1999，提出将信息系统的安全等级划分为（　）个等级，并提出每个级别的安全功能要求。

A.7　　B.8

C.5　　D.6

9. PKI 技术的广泛应用能满足人们对网络交易安全保障的需要，（　）不属于 PKI 技术应用模式。

A.网上证券　　B.安全电子邮件

C.电子商务　　D.文件存储

10. 下列关于会话密钥说法中正确的是（　）

A.会话密钥大多是临时的、动态的

B.会话密钥一般由非对称密码算法产生

C.会话密钥位于整个密钥层次的最高层

D.若通信双方公用一个密钥则称为私有密钥

系名_____班级_____密封线内不答题_____姓名_____学号_____

系名_____班级_____姓名_____学号_____ 密封线内不答题

11. PKI 技术不提供以下哪种服务。（　　）

A.认证　　B.可控性

C.机密性　　D.不可否认性

12. 下列哪项方法不是在交换网络中实现的嗅探方法。（　　）

A.UDP 端口扫描　　B.MAC 洪泛

C.MAC 欺骗　　D.ARP 欺骗

13. 下列关于数字签名的说法中错误的是（　　）

A.签名是可信的　　B.签名是不可抵赖的

C.签名是不可复制的　　D.签名是可伪造的

14. 以下说法正确的是（　　）

A.防火墙不能防范来自内部网络的攻击

B.防火墙不能限制有用的网络服务

C.防火墙不能防范不经由防火墙的攻击

D.防火墙不能防范感染感染了病毒的软件或文件传输

15. 下列那种现象不是由于 DoS 攻击造成的（　　）。

A.被攻击的主机上有大量等待的 TCP 连接

B.网络中充斥着大量无用的数据包，源地址为假

C.访问某网页面时速度变得很慢，有时甚至无法访问

D.访问某页面时出现页面错误提示

16. 入侵检测系统（IDS）的分类不包括（　　）。

A.基于主机的入侵检测系统　　B.基于网络的入侵检测系统

C.基于应用的入侵检测系统　　D.分布式入侵检测系统

17. 按照溢出缓冲区所在的区域类型来划分，可分为（　　）。

A.栈溢出和堆溢出　　B.主贮存器溢出和辅存储器溢出

C.随机存储器溢出和只读存储器溢出　　D.堆栈溢出和队列溢出

18. IP 欺骗的危害主要直接表现在（　　）。

A.以可信任的身份与用户主机建立连接和更改源 IP 地址，隐藏攻击者身份，消除攻击痕迹。

B.以可信任的身份与服务器建立连接和伪造源 IP 地址，隐藏攻击者身份，消除攻击痕迹。

C.以可信任的身份与客户端建立连接和伪造源 IP 地址，隐藏攻击者身份，消除攻击痕迹。

D.以可信任的身份与服务器建立连接和更改源和目标 IP 地址，隐藏攻击者身份，消除攻击痕迹。

19. 对口令进行安全性管理和使用，最终是为了（　　）。

A.口令不被攻击者非法获得　　B.规范用户操作行为

C.保证用户帐户的安全性　　D.防止攻击者非法获得访问和操作权限

20. 防火墙最主要被部署在（　　）位置。

A.网络边界　　B.骨干线路

C.重要服务器　　D.桌面终端

三、判断题（每题 1 分，共 10 分，请将判断的结果填入下面表格中。）

1	2	3	4	5	6	7	8	9	10

1. ISO 安全体系结构包括了安全服务、安全机制和安全管理三部分。（　　）
2. 现代加密技术主要分为对称加密和非对称加密两种。（　　）
3. 理论上数据恢复密钥只能由一个所信赖的委托人持有（委托人可以是政府机构、法院或由合同的私人组织）（　　）
4. 数字证书主要包括证书所有者的信息、证书所有者的公开密钥和证书颁发机构的签名。（　　）
5. 典型的 PKI 系统包括证书认证中心 CA、注册机构 RA、证书发布系统和 PKI 应用。（　　）
6. 嗅探技术比扫描技术更加隐蔽。（　　）
7. 缓冲区溢出按照溢出缓冲区所在的区域类型来划分，可以分为栈溢出和整型溢出。（　　）
8. 恶意代码会占用磁盘存储空间，但不会破坏数据。（　　）
9. 访问控制对机密性、完整性起直接的作用。（　　）
10. 防火墙常见的有数据包过滤路由器、代理网关和状态检测等类型（　　）

2

系名_____ 班级_____ 姓名_____ 学号_____ 密封线内不答题

四、简答题（每题 5 分，共 30 分）

1. 比较对称密码和非对称密码算法的优缺点。

2. 简述 Kerberos V4 的认证过程。

3. 生活中，我们常用 PGP 对消息进行签名和加密，请描述发送端和接收端 PGP 实体执行的操作步骤。

4. 什么是数字证书？数字证书的认证过程包含哪些内容？

5. 请例举恶意代码的预防技术。

6. 简述防火墙的定义和功能。

3

系名_____班级_____姓名_____学号_____

密封线内不答题

五、综合应用题（每题 15 分，共 30 分）

1. 自 2017 年 5 月，一种新型的电脑病毒——勒索病毒，袭击全球 150 多个国家，这种病毒 87.7%的攻击是通过漏洞发起的，感染电脑后，利用本地的互联网访问权限连接至黑客的 C&C 服务器，进而上传本机信息并下载加密私钥与公钥，利用私钥和公钥对文件进行加密，除了黑客本人，其他人基本不可能破解。达到勒索的目的。

   （1） 黑客是通过非正规途径生成私钥和公钥，那么可以从哪些合理途径获取公钥？

   （2） 为了防止电脑被攻击，我们引入了入侵检测技术，入侵检测主要执行哪些任务来实现实时保护？

2. 某企业有分支机构设在外地，每天日常的信息资源流动（如电子邮件、公文流转等）都通过长途电话拨号进入总部，每月的长途话费开销数万元，而且由于拨号网络的速度限制，用户都普遍反应网络效率甚低。请设计一个方案应用 VPN 技术解决该企业现在存在的问题。

4

信息安全理论与技术参考答案

一、 填空题

1. 保密性、可用性、可控性、可审查性 p2

2. 密码编译学、密码分析学 P39

3. 抗攻击 P159

4. 证书初始化注册阶段、颁发使用阶段、撤销阶段 P111

二、 选择题

1-5: CADAB 6-10: BCCDA

11-15: BADBC 16-20: CABDA

三、 判断题

1-5: ✓ × × ✓ × 6-10: ✓ × × ✓ ✓

四、 简答题

1. P52、P62

2. P101

3. 信安实验一实验原理

4. P109、P110

5. P155

6. P159、P160

五、 综合应用题

1. (1) P81

(2) P182

2. P193

信息安全理论与技术试题（162）

一、填空题（每空 1 分，共 10 分）

1. 信息安全五个性质为保密性、完整性、_____、_____、和可审查性。
2. 公钥分配的四种途径包括公开发布、公用目录、_____、_____。
3. 请写出三种对称密码算法_____、_____、_____。
4. 典型的木马采用_____模式进行工作。
5. 根据检测技术，IDS 可以分为：_____和_____。

二、判断题（每题 1 分，共 10 分）

1. 只要投资充足，技术措施完备，就能够保证百分之百的信息安全。（　　）
2. 如果加密算法被破解，数字签名是可以被伪造的。（　　）
3. 传统密码与现代密码的分界线就是加密算法是否公开。（　　）
4. DES 以 64 位为分组对数据加密，且加密和解密使同一算法。（　　）
5. 防火墙工作在物理层，而病毒在应用层，所以防火墙不能防范感染了病毒的软件或文件的传输。（　　）
6. IP 地址欺骗可以实现对防火墙的攻击。（　　）
7. 误用检测虽然比异常检测的准确率高，但是不能检测未知的攻击类型。（　　）
8. PMI 是 PKI 的一种，都是基础设施。（　　）
9. Host to VPN 网关模式要求两个网络内部的主机支持 IPSec 协议。（　　）
10. 目前常用的操作系统中的文件系统，使用的是自主访问控制方式。（　　）

三、选择题（每题 1 分，共 20 分）

1. 数据在存储过程中发生了非法访问行为，这破坏了信息安全的____属性。（　　）

A 保密性　　B 完整性　　C 不可否认性　　D 可用性

2. 下列说法中属于古典密码学基本处理技巧的是（　　）

A. 无条件安全也称为理论安全　　B. 无条件安全也称为实际安全

C. 计算上安全也称为理论安全　　D. 以上都不正确

3. 下列不属于古典密码体制的是（　　）

A. 单表密码　B. 多表密码　C. 序列密码　D. 非对称密码

4. 下列关于数字签名的说法错误的是（　　）

A. 签名是可信的　B. 签名的消息是不可改变的

C. 签名是可以复制的　　D. 签名是不可抵赖的

5. 下列不属于认证技术的是（　　）

A. 静态密码　B. 数字签名　C. 生物识别认证　D. DES 算法

6. 采用扫描技术进行攻击的基本过程是（　　）

A. IP 扫描—端口扫描—漏洞扫描　　B. IP 扫描—漏洞扫描—端口扫描

C. 端口扫描—漏洞扫描—IP 扫描　　D. 漏洞扫描—IP 扫描—端口扫描

7. 下列关于消息摘要的说法正确的是（　　）

A. 消息摘要的长度不固定　　B. 消息摘要不是随机的

C. 输入的消息不同则摘要也不同　　D. 产生消息摘要的函数是双向函数

8. NIDS 是（　　）。

A. 分布式防火墙系统　　B. 网络安全扫描系统

C. 网络入侵检测系统　　D. 网络防火墙系统

9. PKI 技术的广泛应用能满足人们对网络交易安全保障的需要，下列不属于 PKI 技术应用模式。（　　）

A. 网上证券　B. 安全电子邮件　C. 电子商务　D. 文件存储

10. 在下列四项中，不属于计算机病毒特征的是（　　）。

A.　潜伏性　　B. 传播性　　C. 免疫性　　D. 激发性

11. 计算机病毒通常是（　　）。

A.　一条命令　　B. 一段程序代码　　C. 一个标记　　D. 一个文件

12. 描述数字信息的接受方能够准确的验证发送方身份的技术术语是（　　）。

A. 加密　　B. 解密

C. 对称加密　　D. 数字签名

13. 1999 年，我国发布的第一个信息安全等级保护的国家标准 GB 17859—1999，提出将信息系统的安全等级划分为____个等级，并提出每个级别的安全功能要求。（　　）

A 7　　B 8　　C 6　　D 5

14. 下列关于网络欺骗的说法错误的是（　　）

A. IP 欺骗是以其他主机 IP 作为源 IP 向目标主机发送数据包。

B. 电子邮件欺骗是伪造电子邮件头。

C. 钓鱼网站属于 Web 欺骗。

D. ARP 欺骗在 Internet 上没有作用。

15. 以下不是包过滤防火墙主要过滤的信息是（　　）

A. 时间　B. 源 IP 地址　C. 骨干路线　D. 重要服务器

16. 下列哪种攻击不属于拒绝服务攻击（　　）

A. SYN Flood　B. Land 攻击　C. 死 ping　D. ARP 欺骗

17. 防火墙最主要被部署在___位置。（　　）

A. 网络边界　B. 骨干路线　C. 重要服务器　D. 桌面终端

18. 现代密码体系公开（　　）

A. 私钥　B. 加密算法　C. 公钥　D: 主密钥

19 数字证书采用___密码体制（　　）

A. 公钥　B. 私钥　C. 主密钥　D. 次主密钥

20 认证协议主要有哪两种（　　）

A. 对称认证和非对称认证　　B. 单向认证和双向认证

C. 静态认证和动态认证　　D. 加密认证和不加密认证

四、简答题（每题 5 分，共 30 分）

1. 请分析对称密码算法和非对称密码算法各自的优缺点。

2. 简述集中式密钥分配方案的过程。

3. 什么是 PKI?

4. 简述防火墙的功能。

5. 简述缓冲区两种类型及其特点。

6. 什么是拒绝服务攻击，请列举三个拒绝服务攻击。

五、综合题（每题 15 分，共 30 分）

1. 基于对称密码的认证过程如下所示：

①A→KDC:IDA || IDB || Ra

②KDC→A:EKa[Ra || IDB || Ks || EKb[Ks || IDA]]

③A→B:EKb[Ks || IDA]

④B→A:EKs[Rb]

⑤A→B:EKs[Rb-1]

根据上述认证过程，

(1) 用简单文字描述以上认证过程。

(2) 分析这种人证方式可能会受到的潜在攻击。

(3) 针对(2)中的潜在攻击，该如何改进。

2. 试分析网络欺骗四种类型的基本原理，并描述 IP 欺骗的具体步骤。

2

一、 选择题

1、 描述数字信息的接收方能够准确的验证发送方身份的技术术语是（）

A、加密　　B、解密　　C、对称加密　　D、数字证书

2、用户从CA安全认证中心申请自己的证书，并将该证书装入浏览器的只要目的是（）

A、避免他人假冒自己　　B、验证Web服务器的真实性

C、验证Web浏览器的真实性　　D、防止第三方偷看传输的信息

3、下列不属于特殊安全机制的是（）

A、加密　　B、数字签名　C、审核跟踪　　D、身份验证

4、DES算法用来加密的密钥有多少位（）

A、24　　B、56　　C、64　　D、128

5、数据存储过程中发生了非法访问行为，这破坏了信息安全的_____属性（）。

A、保密性　　B、完整性　　C、不可否认性　　D、可用性

6、计算机病毒的实时监控属于_____类的技术措施（）。

A、保护　　B、检测　　C、响应　　D、恢复

7、PKI的主要组成不包括（ ）

A、证书授权CA　　B、SSL　　C、注册授权RA　　D、证书存储库CR

8、防火墙能够（ ）

A、防范恶意的知情者　　B、防范通过它的恶意连接

C、防备新的网络安全问题　　D、完全防止传送已被病毒感染的软件或文件

9、使网络服务器中充斥着大量要求回复的信息，消耗带宽，导致网络或系统停止正常服务，这属于（ ）漏洞

A、拒绝服务　　B、文件共享　　C、BIND漏洞　　D、远程过程调用

10、不属于黑客被动攻击的是（ ）

A、缓冲区溢出　　B、运行恶意软件　C、浏览恶意代码网页　　D、打开病毒附件

11、网络信息未经授权不能进行改变的特性是____（ ）。

A 完整性 B 可用性 C 可靠性 D 保密性

12、VPN是____的简称（ ）。

A Visual Private Network B Virtual Private NetWork

13、____是最常用的公钥密码算法（ ）。

A RSA　B DSA　C 椭圆曲线　D 量子密码

14、PKI支持的服务不包括_____。

A. 非对称密钥技术及证书管理　　B. 目录服务

C. 对称密钥的产生和分发　　D. 访问控制服务

15、假设使用一种加密算法，它的加密方法很简单：将每一个字母加5，即a加密成f。这种算法的密钥就是5，那么它属于_____（ ）。

A. 对称加密技术 B. 分组密码技术

C. 公钥加密技术 D. 单向函数密码技术

16、A方有一对密钥（KA公开，KA秘密），B方有一对密钥（KB公开，KB秘密），A方向B方发送数字签名M，对信息M加密为：M'=KB公开（KA秘密（M））。B方收到密文的解密方案是_____（ ）。

A. KB公开（KA秘密（M'）） B. KA公开（KA公开（M'））

C. KA公开（KB秘密（M'）） D. KB秘密（KA秘密（M'））

17、数字签名要预先使用单向Hash函数进行处理的原因是_____（ ）。

A. 多一道加密工序使密文更难破译

B. 提高密文的计算速度

C. 缩小签名密文的长度，加快数字签名和验证签名的运算速度

D. 保证密文能正确还原成明文

18、PKI的主要理论基础是____（ ）。

A 对称密码算法 B 公钥密码算法 C 量子密码 D 摘要算法

19、基于通信双方共同拥有的但是不为别人知道的秘密，利用计算机强大的计算能力，以该秘密作为加密和解密的密钥的认证是（ ）。

A. 公钥认证　　B. 零知识认证

C. 共享密钥认证 D. 口令认证

20、入侵检测系统提供的基本服务功能包括（ ）。

A、异常检测和入侵检测　　B、入侵检测和攻击警告

C、异常检测和攻击警告　　D、异常检测、入侵检测和攻击警告

二、 填空题（每空一分）

1、信息安全的五大特征：_____、完整性、可用性、可控性、可审查性。

2、_____是PKI最基本的元素。

3、一个证书的生命周期主要包括三个阶段，证书初始化阶段、颁发使用阶段和_____。

4、虚拟专用网被定义为通过一个公用网路（通常是因特网）建立一个_____、_____的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。

5、密钥加密密钥（key encryption key）用于对会话密钥或下层密钥进行保护，也称为次主密钥、_____。

6、古典密码包括 代替密码和置换密码两种，_____和非对称密码体制都属于现代密码体制。

7、根据使用密码体制的不同可将数字签名分为_____的数字签名 和 基于公钥密码体制的数字签名 ，根据其实现目的的不同，一般又可将其分为 直接数字签名 和 可仲裁数字签名 。

8、DES算法密钥是64位，其中密钥有效位是_____位。RSA算法的安全是基于分解两个大素数的积的困难。

9、密码系统包括以下4个方面：明文空间、_____、密钥空间和密码算法

三、 判断题

1、公钥密码体制算法用一个密钥进行加密，而用另一个不同但是有关的密钥进行解密（ ）。

2、在来自可信站点的电子邮件中输入个人或财务信息是安全的（ ）。

3、防火墙可以有效的防止内网的攻击（ ）。

4、现代密码体制中，数据的安全是基于算法的保密（ ）。

5、RSA算法属于公开密钥密码算法，应用范围广泛，在数字签名、加/解密和身份认证方面都有应用（ ）。

6、PMI是一个综合系统，用来实现权限和证书的产生、管理、存储、分发和撤销等功能（ ）。

7、在防火墙的设计策略中，安全的策略是除非明确允许，否则禁止所有的服务器的设计策略（ ）。

8、数字签名要预先使用单向Hash函数进行处理的原因是缩小签名密文的长度，加快数字签名和验证签名的运算速度（ ）。

9、 RSA 属于对称密码体制（ ）。

10、基于通信双方共同拥有的但是不为别人知道的秘密，利用计算机强大的计算能力，以该秘密作为加密和解密的密钥的认证是公钥认证（ ）。

四、 解答题

1、简述 Hash 函数计算过程以及 Hash 函数解决的问题。

2、对比对称密码算法和公钥密码体制的不同之处，分析出各自的优缺点，

3、简述 Host-VPN 网关模式的是如何建立安全信道的。

4、对称密码算法存在哪些问题？

5、什么是数字证书？现有的数字证书由谁颁发，遵循什么标准，有什么特点？

6、OSI 安全体系结构的第三个主要部分就是安全管理，简述安全管理包含哪三部分。

五、 综合题

1、某企业有分支机构设在外地，每天日常的信息资源流动（如电子邮件、公文流转等）都通过长途电话拨号进入总部，每月的长途话费开销数万元，而且由于拨号网络的速度限制，用户都普遍反应网络效率甚低。请设计一个方案应用 VPN 技术解决该企业现在存在的问题。

3、S 拥有所有用户的公开密钥，用户 A 使用协议

A → S: A || B || Ra

S → A: S || Ss(S || A || Ra || Kb)

其中 Ss( )表示 S 利用私有密钥签名

向 S 申请 B 的公开密钥 Kb。上述协议存在问题吗？若存在，请说明此问题；若不存在，请给出理由。