请标注好题号，把答案写在考试答题纸

1.是非判断题（20 分，每题 1 分，“v”表示正确，“x”表示错误）

(1) 网络安全和信息化是相辅相成的，安全是发展的前提，发展是安全的保障，安全和发展要同步推进。

(2) 密码算法公开不仅有利于密码技术的推广应用和标准化，而且有利于增加用户使用的信心。

(3) 目前而言，DES 算法是不安全的，其主要原因是密码分析者已找到破译 DES 算法的有效方法了。

(4) 在 RSA 算法中，n 是公开的，且已知 n=p*q(其中 p 和 q 是素数)，所以，p 或 q 是很容易推算出来的。

(5) Diffie 和 Hellman 提出的 DH 密钥交换方案虽然能够解决密钥分发问题，但这个方案并不完美，主要原因在于不方便，不实用。

(6) 数字证书是公开的、可复制的，那么数字证书的内容是容易被人修改和伪造的。

(7) 哈希函数的安全性是指根据已知的哈希值不能推出对应的消息原文。

(8) 计算机病毒技术与黑客技术将日益融合，且物质利益或特殊目的将成为推动计算机病毒发展的最大动力。

(9) 由于计算机病毒是可执行程序，所以，打开 Web 网页是不可能传染计算机病毒的。

(10) 虚拟专用网 VPN 是指通过一个公共网络建立一个临时的、安全的连接，是一条穿过混乱公用网络的安全和稳定隧道，能提供与专用网络一样的安全和功能保障。

(11) 防火墙是网络安全的重要一环，通过合理地配置防火墙，不仅能够防范来自外网的攻击，而且也能够防范来自内部网络的攻击。

(12) 目前，网络攻击基本来自于个人行为，其目的获取经济利益。

(13) 拒绝服务攻击 Dos 的目的就是导致服务器不能正常提供服务，这种攻击就是毁坏服务器，或者断网断电等破坏物理设备的方法来实现的。

(14) 身份认证往往是许多应用系统中安全保护的第一道设防，它的失败可能导致整个应用系统安全的失败。

(15) 零知识证明是指证明者 P 试图使验证者 V 相信某个论断是正确的，但却不向 V 提供任何有用的信息，或者说在 P 论证的过程中 V 得不到任何有用的信息。

(16) 磁盘阵列可以在部分磁盘损坏的情况下，仍能保证系统不中断地连续运行，并支持热插拔技术，所以，有了磁盘阵列就不需要数据备份了。

(17)由于数据备份会影响系统正常运行，而且数据备份的内容也常常用不上，所以，数据备份**不是**系统不可缺少的部分。

(18)安全技术和安全管理的关系中，技术(产品)更重要，即技术(产品)高超但管理混乱的系统远比技术(产品)不高但管理良好的系统安全。

(19)社会工程学攻击正在成为黑客攻击的必备手段，甚至，在所有重大黑客事件中，社工攻击几乎都是先锋队主力军。

(20)网络安全态势感知系统能够有利于增强网络安全防御能力和威慑能力。

2．选择题（20 分，每题 1 分，每题只有一个选项最符合题目要求）

(1)现代密码史的关键事件中，下面哪个事件是现代密码史上第二次质的飞跃。

A. Shannon 发表题为《保密系统的通信理论》　　B.DES 的公布

C. Diffe 和 Hellman 发表了《密码学的新方向》　　D.RSA 的公布

(2)与公钥密码体制相比，下面哪项是对称密码体制的优点。

A.加解密速度快　　B.密钥分发简单　　C.有数据扩展　　D.易实现数字签名

(3)信息安全保障模型，简称 PD2R，其中 D 指（　　）。

A.保护　　B.检测　　C.反应　　D.恢复

(4)Enigma 密码设备中哪个部件是增加了其密码算法的复杂度。

A.键盘　　B.接线板　　C.轮子　　D.反射器

(5)2003 年出现的“冲击波”病毒给全球互联网带来的直接损失大约有几十亿美元，这种病毒传染方式是利用(　　)。

A.U 盘　　B.文件下载　　C.电子邮件　　D.漏洞

(6)计算机病毒最基本特征是（　　）。

A.传染性　　B.非授权性　　C.衍生性　　D.破坏性

(7)在现有的计算能力条件下，公钥密码算法 RSA 被认为是安全的最小密钥长度是（　　）。

A.128 位　　B.256 位　　C.1024 位　　D.2048 位

(8)数字签名技术**不能**解决下面的哪项网络空间安全存在的问题。

A.保密性　　B.完整性　　C.认证性　　D.不可否认性

(9)攻击通常是有明确的目标的，阻断攻击是一种针对系统（　　）的攻击。

A.机密性　　B.完整性　　C.认证性　　D.可用性

(10)伪造攻击是非授权者在系统中冒充合法的实体，下面哪个攻击是属于伪造攻击的。

A.替换攻击　　B.DNS 攻击　　C.木马攻击　　D.Dos 攻击

(11)防火墙哪项技术能够实现不公开内部服务器真实 IP 地址及隐藏内部网络结

构。

A.包过滤技术　B.MAP(地址/端口映射)　C.IP与MAC的绑定　D.带宽管理

(12)下面这段描述是指哪款网络安全产品,即能够对网络和主机的安全性进行风险分析和评估的软件,是一种能自动检测远程或本地主机系统在安全性方面存在弱点和隐患的程序包。

A.防火墙　B.入侵检测系统　C.漏洞扫描器　D.安全审计系统

(13)RAID5是一种存储性能、数据安全和存储成本兼顾的存储解决方案,当这方案实施时出现(　　)磁盘数据损坏后,这个技术是能够恢复被损坏的数据。

A.一个　B.二个　C.三个　D.四个

(14)针对数据应用(重要)程度不同,提供不同级别数据安全的解决方案,下面那个方案凸显其数据是最重要的。(　　)

A.数据拷贝　B.网络备份　C.远程热备　D.容灾备份

(15)根据用户的生物特征辨别用户身份是目前常用的一种身份认证技术,当前最多地应用于身份认证的生物特征是(　　)。

A.指纹　B.笔迹　C.声音　D.虹膜

(16)下面哪项安全技术指对信息系统中与安全有关的活动及其相关信息进行识别、记录、存储和分析。

A.身份认证技术　B.访问控制技术　C.安全审计技术　D.数据备份技术

(17)“一般通过电子邮件等电子通信方式进行,主要是针对特定人群目标的钓鱼攻击,比如企业高层,特定的政府部门以及其他敏感的企业”,上面这段描述是指下面的哪个攻击。

A.网络钓鱼攻击　B.网络鱼叉攻击　C.网络钓鲸攻击　D.网络水坑攻击

(18)PDCA模型是信息安全管理体系(ISMS)的一个典型模型,其中C是指(　　)。

A.计划　B.实施　C.检查　D.改进

(19)容灾可以理解为是以(　　)作为基本支撑、以网络作为基本传输手段、以容错软硬件技术为直接技术手段、以管理技术为重要辅助手段的综合系统。

A.硬件设备　B.存储系统　C.系统软件　D.应用系统

(20)社会工程学攻击是目前常用的一种攻击手段,有时会取得意想不到的效果,下面哪个选项与社会工程学攻击关联最密切。

A.穷举服务器系统的密码　B.收集服务器的地址、端口等

C.DDOS攻击服务器　D.了解服务器管理员的生活习惯、性格等

3.填空题(20分,每空1分)

(1)Enigma密码机出现是近代密码发展史中里程碑的事件,从这个事件得到启示,

实用密码设备应必备四要素，即_____、_____、成本、易用。

(2) 一个密码系统(体制)是由明文、密文、加密算法、_____、_____五部分组成的

(3) 恶意代码的通用特征是指_____、恶意目的、_____、难以卸载、破坏性。

(4) 消息认证的目的是指_____、_____。

(5) 木马攻击核心技术在于**植入**，而植入常用方式有主动和被动，通常**主动**是指_____，**被动**是指_____。

(6) 防火墙的主要性能参数包括_____、_____、丢包率、并发连接数、平均无故障时间、最大允许加载规则数。

(7) 数据备份的根本目的，是重新利用，即数据恢复，而数据恢复是应用恢复的基础，应用恢复的两个主要指标是_____和_____。

(8) 指纹身份认证的主要方式：_____和_____。

(9) 安全态势感知是在大规模网络环境中，对能够引起网络态势发生变化的所有安全要素进行_____、_____、评估以及预测未来的发展趋势，从而进行决策和行动。

(10) 信息安全管理主要遵循的原则：策略明确原则、系统工程原则、综合保障原则、_____、首长负责原则、预防为主原则、_____、动态持续原则、成本效益原则、均衡防护原则。

4. 简答题（共 30 分，每题 5 分）

(1) 网络空间安全面临威胁很多，譬如窃取、篡改、假冒、抵赖、破坏等，这门课所介绍的哪些安全技术能分别抵御上述提及的威胁。

(2) 请描述公钥密码体制实现加解密的过程。

(3) 请简要描述防火墙发展的趋势。

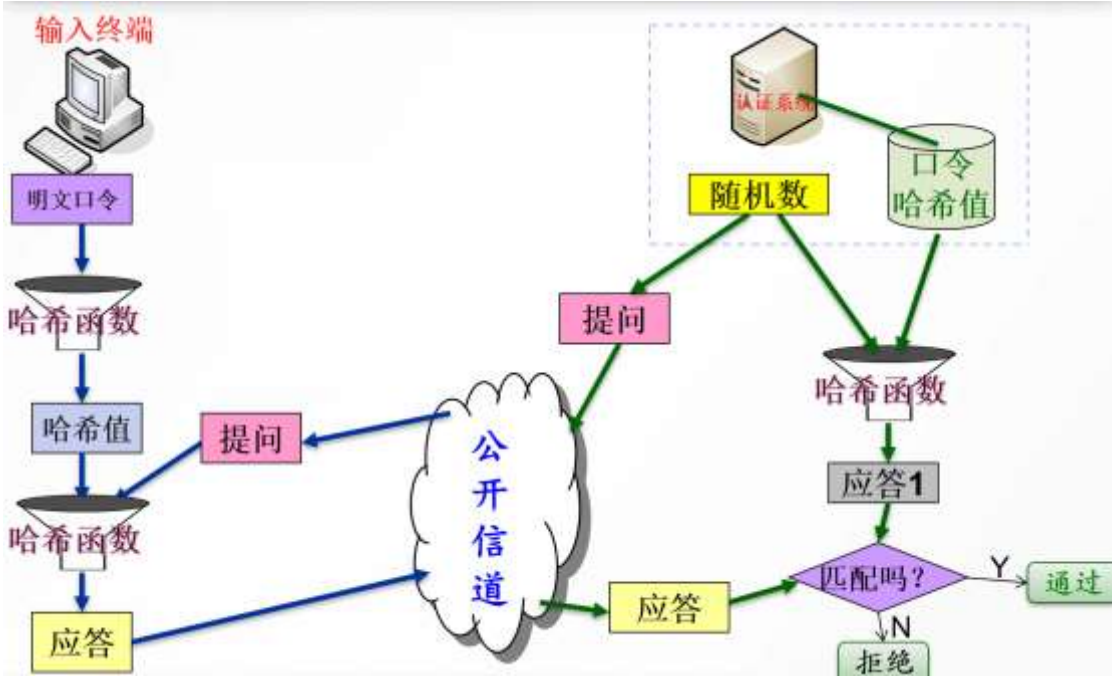
(4) 以 TCP 三次握手为例描述 DoS 攻击基本思想。

(5) 相比早期附属存储形式，集中存储的好处有哪些。

(6) 社会工程学攻击目前常见的攻击方式，常常取得意想不到的成果，作为你自己本人，如何预防和抵御社会工程学攻击，请至少指出 5 点。

5. 分析题（共 10 分）

下图举例描述基于口令的验证过程：



请回答以下问题：

(1) 口令信息能实现安全传输吗？(1 分) 为什么？(3 分)

(2) 管理员知道用户的口令吗？(1 分) 为什么？(2 分)

(3) 提问(随机数)的作用是什么？(1 分) 为什么？(2 分)