数据安全与保密

第9章　安全性、可靠性与系统性能评测

根据考试大纲，本章要求考生掌握以下知识点：

安全性基本概念；

防治计算机病毒、防范计算机犯罪；

加密与解密机制；

存取控制、防闯入、安全管理措施；

诊断与容错；

系统可靠性分析评价；

计算机系统性能评测方式；

风险分析、风险类型、抗风险措施和内部控制。

有关风险分析的内容，请读者参考本书有关软件工程的章节。

9.1　数据安全与保密

国际标准化委员会对计算机安全的定义提出如下建议："为数据处理系统建立和采取的技术的、管理的安全保护措施，用来保护计算机硬件、软件、数据不因偶然的、恶意的原因而遭破坏、更改和泄露".计算机系统的安全主要包括网络安全、操作系统安全和数据库安全三个方面。

各级网络安全技术如图9-1所示，包括各种安全技术和安全协议，分别对应于OSI七层网络协议的某一层或某几层，其中数据加密是计算机安全中最重要的技术措施之一。

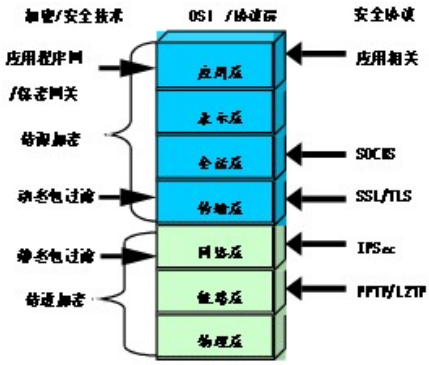

图9-1　网络安全技术层次结构图

上一节　　本书简介　　下一节

数据加密算法

9.1.1　数据加密算法

数据加密是对明文（未经加密的数据）按照某种加密算法（数据的变换算法）进行处理，形成密文（经加密后的数据）。这样一来，密文即使被截获，截获方也无法或难以解码，从而防止泄露信息。

数据加密和数据解密是一对可逆的过程，数据加密是用加密算法E和加密密钥K1将明文P变换成密文C,表示为：

$$C = E_{K1}(P)$$

数据解密是数据加密的逆过程，用解密算法D和解密密钥K2,将密文C转换成明文P,表示为：

$$P = D_{K2}(C)$$

按照加密密钥K1和解密密钥K2的异同，有两种密钥体制。

秘密密钥加密体制K1=K2:加密和解密采用相同的密钥，因而又称为对称密码体制。因为加密速度快，通常用来加密大批量的数据。典型的方法有日本NTT公司的快速数据加密标准（FEA）、瑞士的国际数据加密算法（IDEA）和美国的数据加密标准（DES）。

公开密钥加密体制K1≠K2:又称不对称密码体制，其加密和解密使用不同的密钥；其中一个密钥是公开的，另一个密钥则是保密的。由于加密速度较慢，所以往往用在数据量较小的通信业务中。典型的公开密钥加密方法有RSA和NTT的ESIGN.

加密算法主要达到以下四点目的：提供高质量的数据保护，防止数据未经授权的泄露和未被察觉的修改；应具有相当高的复杂性，使得破译的开销超过可能获得的利益，同时又要便于理解和掌握；密码体制的安全性应该不依赖于算法的保密，其安全性仅以加密密钥的保密为基础；实现经济，运行有效，并且适用于多种完全不同的应用。

1.DES数据加密算法

DES（数据加密标准）是国际标准化组织（ISO）核准的一种加密算法，自1976年公布以来得到广泛的应用，但近年来对它的安全性提出了疑问。1986年美国政府宣布不再支持DES作为美国数据加密标准，但同时又不准公布用来代替DES的加密算法。

一般DES算法的密钥长度为56位，为了加速DES算法和RSA算法的执行过程，可以用硬件电路来实现加密和解密。针对DES密钥短的问题，科学家又研制了80位的密钥，以及在DES的基础上采用三重DES和双密钥加密的方法。即用两个56位的密钥K1、K2,发送方用K1加密，K2解密，再使用K1加密。接收方则使用K1解密，K2加密，再使用K1解密，其效果相当于将密钥长度加倍。

DES算法的入口参数有三个：Key、Data、Mode.其中Key为8个字节共64位，是DES算法的工作密钥；Data也为8个字节64位，是要被加密或被解密的数据；Mode为DES的工作方式，有两种：加密或解密。

DES算法是这样工作的：如Mode为加密，则用Key 去把数据Data进行加密， 生成Data的密码形式（64位）作为DES的输出结果；如Mode为解密，则用Key去把密码形式的数据Data解密，还原为Data的明码形式（64位）作为DES的输出结果。在通信网络的两端，双方约定一致的Key,在通信的源点用Key对核心数据进行DES加密，然后以密码形式在公共通信网络（如电话网）中传输到通信网络的终点，数据到达目的地后，用同样的Key对密码数据进行解密，便再现了明码形式的核心数据。这样，便保证了核心数据（如PIN、MAC等）在公共通信网中传输的安全性和可靠性。通过定期在通信网络的源端和目的端同时改用新的Key,可以进一步提高数据的保密性。

2.其他数据加密算法

RSA算法的密钥长度为512位。RSA算法的保密性取决于数学上将一个大数分解为两个素数的问

题的难度，根据已有的数学方法，其计算量极大，破解很难。但是加密/解密时要进行大指数模运算，因此加密/解密速度很慢，影响推广使用。

国际数据加密算法（IDEA）在1990年正式公布。这种算法是在DES算法的基础上发展起来的，类似于三重DES.发展IDEA也是因为感到DES具有密钥太短等缺点，IDEA的密钥为128位，这么长的密钥在今后若干年内应该是安全的。

1993年4月16日，美国政府推出了cipper密码芯片，该芯片采用美国国家安全局设计的Skipjack加密算法。采用Cipper的加密体制能为信息传输提供高等级的安全和保密，该体制是以防篡改硬件器件（Cipper芯片）和密钥Escrow（第三方托管）系统为基础的。

1994年2月14日，美国政府宣布了Escrow加密标准，其加密算法使用Skipjack.该算法采用80位密钥和合法强制访问字段（aw Enforcement Access Fied,EAF），以便在防篡改芯片和硬件上实现。由于使用了80位的密钥，Skipjack算法具有较高的强度。

身份认证技术

9.1.2 身份认证技术

主要以数字签名技术为例说明。在某些商业或金融领域内，由于其行业要求，需要防止通信的一方否认或伪造通信内容，这时通常采用数字签名的方法。

数字签名用来保证信息传输过程中信息的完整和提供信息发送者的身份认证和不可抵赖性，该技术利用公开密钥算法对于电子信息进行数学变换，通过这一过程，数字签名存在于文档之中，不能被复制。该技术在具体工作时，首先发送方对信息施以数学变换，所得的变换信息与原信息唯一对应；在接收方进行逆变换，就能够得到原始信息。只要数学变换方法优良，变换后的信息在传输中就具有更强的安全性，很难被破译、篡改。这一过程称为加密，对应的反变换过程称为解密。

数字签名的算法很多，应用最为广泛的3种是：Hash签名、DSS签名、RSA签名。这3种算法可单独使用，也可综合在一起使用。

1.Hash签名

Hash签名不属于强计算密集型算法，应用较广泛。很多少量现金付款系统，如DEC的Miicent和CyberCash的CyberCoin等都使用Hash签名。使用较快的算法，可以降低服务器资源的消耗，减轻中央服务器的负荷。Hash的主要局限是接收方必须持有用户密钥的副本以检验签名，因为双方都知道生成签名的密钥，较容易攻破，存在伪造签名的可能。如果中央或用户计算机中有一个被攻破，那么其安全性就受到了威胁。

Hash签名是最主要的数字签名方法，也称之为数字摘要法、数字指纹法。它与RSA数字签名不同，该数字签名方法将数字签名与要发送的信息紧密联系在一起，它更适合于电子商务活动。将一个商务合同的个体内容与签名结合在一起，比合同和签名分开传递，更增加了可信度和安全性。

2.RSA和DSS签名

RSA和DSS都采用了公钥算法，不存在Hash的局限性。

RSA是最流行的一种加密标准，许多产品的内核中都有RSA的软件和类库，早在Internet飞速发展之前，RSA数据安全公司就负责数字签名软件与Macintosh操作系统的集成，在Appe的协作软件PowerTak上还增加了拖放签名功能，用户只要把需要加密的数据拖到相应的图标上，就完成了电子形式的数字签名。RSA与Microsoft、IBM、Sun和Digita都签订了许可协议，使在其生产线上加入了类似的签名特性。RSA既可以用来加密数据，也可以用于身份认证。

用RSA或其他公开密钥密码算法进行数字签名的最大方便是没有密钥分配问题（网络越复杂、网络用户越多，其优点越明显）。因为公开密钥加密使用两个不同的密钥，其中有一个是公开的，另一个是保密的。公开密钥可以保存在系统目录内、未加密的电子邮件信息中、电话黄页（商业电话）上或公告牌里，网上的任何用户都可获得公开密钥。而保密密钥是用户专用的，由用户本身持有，它可以对由公开密钥加密信息进行解密。

RSA算法中数字签名技术实际上是通过一个Hash函数来实现的。数字签名的特点是它代表了文件的特征，文件如果发生改变，数字签名的值也将发生变化。不同的文件将得到不同的数字签名。

DSS是由美国国家标准化研究院和国家安全局共同开发的。由于该算法由美国政府颁布实施，主要用于与美国政府有商业往来的企业或组织，其他团体则较少使用。

DSS的一个重要特点是两个素数公开，这样，当使用别人的p和q时，即使不知道私钥，我们也能确认它们是随机产生的，还是做了手脚。RSA算法做不到这一点。

对数字签名和公开密钥加密技术来说，都会面临公开密钥的分发问题，即如何把一个用户的公钥以一种安全可靠的方式发送给需要的另一方。这就要求管理这些公钥的系统必须是值得信赖的。在这样的系统中，如果小王想要给老张发送一些加密数据，就需要知道老张的公开密钥；如果老张想要检验小王发来文档的数字签名，就需要知道小王的公开密钥。

所以，必须有一项技术来解决公钥与合法拥有者身份的绑定问题。假设有一个人自称某一个公钥是自己的，必须有一定的措施和技术来对其进行验证。

数字证书是解决这一问题的有效方法。它通常是一个签名文档，标记特定对象的公开密钥。数字证书由一个认证中心（CA）签发，认证中心类似于现实生活中公证人的角色，它具有权威性，是一个普遍可信的第三方。当通信双方都信任同一个CA时，两者就可以得到对方的公开密钥，从而能进行秘密通信、签名和检验。

CA是Certificate Authority的缩写，是证书授权的意思。在电子商务系统中，所有实体的证书都是由证书授权中心即CA中心分发并签名的。一个完整、安全的电子商务系统必须建立起一个完整、合理的CA体系。CA体系由证书审批部门和证书操作部门组成。

电子商务的安全是通过使用加密手段来达到的，公开密钥加密技术是电子商务系统中主要的加密技术，主要用于对称加密密钥的分发（数字信封）和数字签名，以实现身份认证和信息的完整性检验，以预防交易的抵赖等。CA体系为用户的公钥签发证书，以实现公钥的分发并证明其有效性。该证书证明了用户拥有证书中列出的公开密钥。证书是一个经证书授权中心签名的包含公开密钥拥有者信息以及公开密钥的文件。CA机构的数字签名使得攻击者不能伪造和篡改证书。证书的格式遵循X.509标准。

CA机构应包括两大部门：一是审核授权部门（RA:Registry Authority），它负责对证书申请者

进行资格审查，决定是否同意给该申请者发放证书，并承担因审核错误引起的、为不满足资格证书申请者发放证书所引起的一切后果，因此它应由能够承担这些责任的机构担任；另一个是证书操作部门（CP:Certificate Processor），负责为已授权的申请者制作、发放和管理证书，并承担因操作运营所产生的一切后果，包括失密和为没有获得授权者发放证书等，它可以由审核授权部门自己担任，也可委托给第三方担任。

CA体系具有一定的层次结构，它由根CA、品牌CA、地方CA,以及持卡人CA、商家CA、支付网关CA等不同层次构成，上一级CA负责下一级CA数字证书的申请、签发及管理工作。通过一个完整的CA认证体系，可以有效地实现对数字证书的验证。每一份数字证书都与上一级的签名证书相关联，最终通过安全认证链追溯到一个已知的可信赖的机构。由此便可以对各级数字证书的有效性进行验证。根CA的密钥由一个自签证书分配，根证书的公开密钥对所有各方公开，它是CA体系中的最高层。

信息网络安全协议

9.1.3 信息网络安全协议

目前，已经提出了大量的实用安全协议，有代表性的有：电子商务协议，IPSec协议，TS协议，简单网络管理协议（SNMP），PGP协议，PEM协议，S-HTTP协议，S/MIME协议等。对实用安全协议的安全性分析，特别是对电子商务协议、IPSec协议、TS协议的分析是当前协议研究中的热点。典型的电子商务协议有SET协议、iKP协议等。另外，值得注意的是Kaiar逻辑，它是目前分析电子商务协议的最有效的一种形式化方法。

为了实现安全IP,Internet工程任务组IETF于1994年开始了一项IP安全工程，专门成立了IP安全协议工作组IPSEC,来制定和推动一套称为IPSec的IP安全协议标准。其目标就是把安全集成到IP层，以便对Internet的安全业务提供低层的支持。IETF于1995年8月公布了一系列关于IPSec的建议标准。IPSec适用于IPv4和下一代IP协议IPv6,并且是IPv6自身必备的安全机制。但由于IPSec还比较新，正处于研究发展和完善阶段。

在国际上，电子商务的安全机制正在走向成熟，并逐渐形成了一些国际规范，比较有代表性的有SS协议和SET协议。

1.SS协议

SS（Security Socket ayer）协议是Netscape Communication 开发的传输层安全协议，用于在Internet上传送机密文件。该协议向基于TCP/IP的客户/服务器应用程序提供了客户端和服务器的鉴别、数据完整性及信息机密性等安全措施。该协议在应用程序进行数据交换前通过交换SS初始握手信息来实现有关安全特性的审查。

SS首先要建立一条安全的连接，然后使用公钥加密方法传输数据。常用的浏览器（Netscape

Navigator,Internet Exporer）都支持SS,许多Web站点利用SS获取用户的机密信息，例如信用卡号等。使用SS连接的UR,以<https://开头>.另外一种在互联网上传送机密数据的协议是安全的超文本协议S-HTTP（Security Hypertext Transfer Protoco）。SSK是在客户机和服务器之间建立一条安全的连接，而S-HTTP是安全地传送单个报文，属于应用层协议，因而这两个协议并非竞争的技术，而是互相补充的。SOCKS是IETF的一个正式的标准，用于代理基于TCP/IP的网络应用。SOCKS系统包含两个元素--SOCKS服务器和SOCKS客户机。SOCKS服务器实现于应用层，而SOCKS客户机实现于应用层和传输层之间。这个协议的主要作用是在两个没有直接IP联系的主机之间实现通信。

当客户机需要访问应用服务器时，客户机首先连接到SOCKS代理服务器上，代理服务器再连接到应用服务器上。代理服务器在客户机和应用服务器之间传送数据，如图9-2所示。对于应用服务器，代理服务器是客户机。

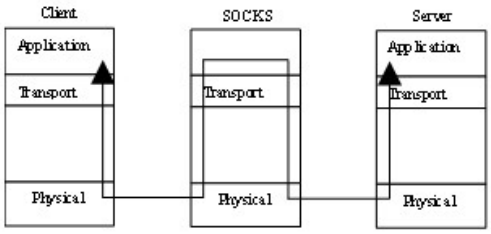

图9-2 代理服务器传送数据图

2.SET协议

SET（Secure Eectronic Transaction）协议向基于信用卡进行电子化交易的应用提供了实现安全措施的规则。1995年，信用卡国际组织、资讯业者及网络安全专业团体等开始组成策略联盟，共同研究开发电子商务的安全交易系统。1996年6月，由IBM,Master Card Internationa,Visa Internationa,Microsoft, Netscape,GTE,ViriSign,SAIC,Terisa共同制定的标准SET（Secure Eectronic Transaction）正式公告，涵盖了信用卡在电子商务交易中的交易协定、信息保密、资料完整即数字认证、数字签名等。这一标准被公认为全球网络的标准，其交易形态将成为未来"电子商务"的典范。

SET协议规定了交易各方进行安全交易的具体流程。在SET协议中，使用DES对称密钥算法、RSA非对称密钥算法等提供数据加密、数字签名、数字信封等功能，给信息在网络中的传输提供了安全性保证。SET协议通过DES算法和RSA算法的结合使用，保证了数据的一致性和完整性，并可实现交易以预防抵赖；通过数字信封、双重签章，确保用户信息的隐私性和关联性。

SET协议执行步骤与常规的信用卡交易过程基本相同，只是它是通过因特网来实现的。在SET协议系统中，参与交易的主要有4种实体：持卡人、电子商家、收单银行、发卡银行。持卡人主要指持有信用卡的消费者；电子商家主要职能是支持网络购物的电子商店等提供电子交易服务的企业组织；收单银行主要使用支付系统的专用网关提供各商家的因特网在线借款服务；发卡银行负责处理信用卡的发放、账目管理、付款清算等。

此外，在协议系统中，还有认证中心，它是一些发卡机构共同委派的公证代理组织，其主要功能是产生、分配和管理发卡人、商家和参与电子交易等。

SET协议规定的工作流程如下：用户向商家发送购货单和一份经过签名、加密的信托书。书中的信用卡号是经过加密的，商家无从得知；商家把信托书传送到收单银行，收单银行可以解密信用卡号，并通过认证验证签名；收单银行向发卡银行查问，确认用户信用卡是否属实；发卡银行认可并签证该笔交易；收单银行认可商家并签证此交易；商家向用户传送货物和收据；交易成功，商家向

收单银行索款；收单银行按合同将货款划给商家；发卡银行向用户定期寄去信用卡消费账单。

SET协议规定了参加电子交易各方在交易中的行为规范和信息交换的过程和规则，有助于实现安全、可靠的电子商务，得到了IBM、VeriFone、HP、Microsoft、Netscape等一些著名网络和计算机公司的支持。但是，SET协议实施起来很复杂，因而在短期内推广SET协议还存在一定的困难。

防火墙技术

9.1.4 防火墙技术

防火墙是位于两个（或多个）网络间，实施网络间访问控制的一组组件的集合，它是一套建立在内外网络边界上的过滤封锁机制。它满足以下条件：内部和外部之间的所有网络数据流必须经过防火墙，只有符合安全政策的数据流才能通过防火墙，防火墙自身应对渗透免疫。归纳起来，防火墙的功能有：过滤掉不安全服务和非法用户；控制对特殊站点的访问；提供了监视Internet安全和预警的方便端点。

设置防火墙的目的是为了保护内部不受来自Internet的攻击，为了创建安全域，为了增强一个机构内部网络的安全策略。防火墙需要满足两大需求：保障内部网络安全和保证内部网络同外部网的连通；通常内部网络被认为是安全和可信赖的，而外部网络（通常是Internet）被认为是不安全和不可信赖的。

防火墙如果从实现方式上来分，分为硬件防火墙和软件防火墙两类，我们通常意义上讲的硬防火墙为硬件防火墙，它是通过硬件和软件的结合来达到隔离内、外部网络的目的，价格较贵，但效果较好，一般小型企业和个人很难实现；软件防火墙是通过纯软件的方式来达到的，这类防火墙只能通过一定的规则来达到限制一些非法用户访问内部网的目的。

实现防火墙的产品主要两大类：一类是网络级防火墙，另一类是应用级防火墙。目前一种趋势是把这两种技术结合起来。

网络级防火墙

也称为过滤型防火墙。事实上是一种具有特殊功能的路由器，采用报文动态过滤技术，能够动态地检查流过的TCP/IP报文或分组头，根据企业所定义的规则，决定禁止某些报文通过或者允许某些报文通过，允许通过的报文将按照路由表设定的路径进行信息转发。相应的防火墙软件工作在传输层与网络层。

状态检测防火墙又称动态包过滤，是在传统包过滤上的功能扩展。状态检测防火墙在网络层由一个检查引擎截获数据包并抽取出与应用层状态有关的信息，并以此作为依据决定对该连接是接受还是拒绝。这种技术提供了高度安全的解决方案，同时也具有较好的性能、适应性和可扩展性。状态检测防火墙一般也包括一些代理级的服务，它们提供附加的对特定应用程序数据内容的支持。状态检测技术最适合提供对UDP协议的有限支持。它将所有通过防火墙的UDP分组均视为一个虚拟连

接，当反向应答分组送达时，就认为一个虚拟连接已经建立。状态检测防火墙克服了包过滤防火墙和应用代理服务器的局限性，不仅仅检测"to"或"from"的地址，而且也不要求每个访问的应用都有代理。

应用级防火墙

也称为应用网关型防火墙，目前已大多采用代理服务机制，即采用一个网关来管理应用服务，在其上安装对应于每种服务的特殊代码（代理服务程序），在此网关上控制与监督各类应用层服务的网络连接。比如对外部用户（或内部用户）的FTP,TENET,SMTP等服务请求，检查用户的真实身份、请求合法性和源IP地址、目的地IP地址等，从而由网关决定接受或拒绝该服务请求，对于可接受的服务请求由代理服务机制连接内部网与外部网。代理服务程序的配置由企业网络管理员所控制。

目前常用的应用级防火墙大致有4种类型，分别适合于不同规模的企业内部网：双穴机网关、屏蔽主机网关、屏蔽子网网关和应用代理服务器。一个共同点是需要有一台主机（堡垒主机）来负责通信登记、信息转发和控制服务提供等任务。

双穴主机（dua-homed）网关：由堡垒主机作为应用网关，其中装有两块网卡分别连接外因特网和受保护的内部网，该主机运行防火墙软件，具有两个IP地址，并且能隔离内部主机与外部主机之间的所有可能连接。

屏蔽主机（screened host）网关：也称甄别主机网关。在外部因特网与被保护的企业内部网之间插入了堡垒主机和路由器，通常是由IP分组过滤路由器去过滤或甄别出可能的不安全连接，再把所有授权的应用服务连接转向应用网关的代理服务机制。

屏蔽子网（screened subnet）网关：也称甄别子网网关，适合于较大规模的网络使用。

即在外部因特网与被保护的企业内部网之间插入了一个独立的子网，比如在子网中有两个路由器和一台堡垒主机（其上运行防火墙软件作为应用网关），内部网与外部网的一方各有一个分组过滤路由器，可根据不同甄别规则接受或拒绝网络通信，子网中的堡垒主机（或其他可供共享的服务器资源）是外部网与内部网都可能访问的唯一系统。

应用代理服务器（Appication Gateway Proxy）：在网络应用层提供授权检查及代理服务。当外部某台主机试图访问受保护网络时，必须先在防火墙上经过身份认证。通过身份认证后，防火墙运行一个专门为该网络设计的程序，把外部主机与内部主机连接。在这个过程中，防火墙可以限制用户访问的主机、访问时间及访问的方式。同样，受保护网络内部用户访问外部网时也需先登录到防火墙上，通过验证后，才可访问。

应用网关代理的优点是既可以隐藏内部IP地址，又可以给单个用户授权，即使攻击者盗用了一个合法的IP地址，也通不过严格的身份认证。因此应用网关比报文过滤具有更高的安全性。但是这种认证使得应用网关不透明，用户每次连接都要受到认证，这给用户带来许多不便。这种代理技术需要为每个应用写专门的程序。

9.2 诊断与容错

诊断与容错技术是提高系统可靠度及可用度的有效手段。

上一节 本书简介 下一节

第 9 章：安全性、可靠性与系统性能评测 作者：希赛教育软考学院 来源：希赛网 2014年03月13日

诊断技术

9.2.1 诊断技术

故障诊断包括故障检测和故障定位两个方面。故障检测是指测试并确认计算机系统有无故障的过程，故障定位是指判定在系统的哪个子系统、功能块或器件发生了故障。前者确定故障的存在，后者确定故障的位置。

故障诊断可以联机进行，也可以脱机进行。联机故障诊断是在系统中投入一定的冗余资源，使系统能够输出一些额外的信息，用以指示系统是否发生故障或者系统中哪个部件发生了故障。脱机故障诊断是指在系统非运行期间，借助外部干预来确认系统是否发生故障或者系统中哪个部件发生了故障。

通常用诊断覆盖率和诊断分辨率来衡量诊断技术的有效性。诊断覆盖率是指系统中任意一个故障能够被检测到的概率。诊断分辨率是指诊断所能指出的故障部件的大小。分辨率最低的诊断只能指出故障在系统中，此时，诊断只起到检测的作用。

1.联机诊断技术

联机诊断是指在系统运行期间对故障进行揭露和定位，其原理是在系统中投入一定的冗余资源，使系统不仅能够输出其功能所要求的信息，而且输出一些额外的信息，用以指示系统是否发生了故障或者系统的哪个部件发生了故障。其方法是通过对输出进行编码和校验来实现的。

可以把一个组合电路的输出向量Z看做是输入向量为X和内部故障a的函数，即：

$$Z = F(X, a)$$

电路无故障的输出可用表示$Z = F(X, \lambda)$，此电路的正常输出集为：

$$S = \{Z = F(X, \lambda) | X \in N\}$$

式中N是电路的正常输入向量集。

如果电路的正常输出集S是检错码，则称该电路为自校验电路。无故障时输出码向量，预定故障发生时，输出非码向量。输出端连接校验器，当非码向量出现时，给出差错指示。

如果电路的正常输出集是诊错码，则称该电路为自诊断电路，无故障时输出码向量，预定故障发生时，输出非码向量。输出端连接校正器，当非码向量出现时，校正器确定差错的位置，并纠正差错。

也就是说，一个具有校验或者诊断功能的系统，其所有可能的输出值的集合U由S和U–S两部分组成，当系统没有故障时，系统输出S中的元素，一旦系统发生故障，则输出U–S中的元素。

2.脱机诊断技术

联机诊断技术一般应用于系统的运行期间，而在系统的检测、调试或者维护期间，一般采用脱机诊断技术。脱机诊断技术的实现是借助测试仪器等外部干预来确认系统是否发生故障，或者系统中的哪个部件发生了故障。

脱机诊断的模型如图9-3所示。

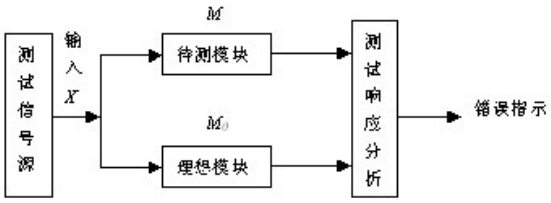

图9-3 脱机测试与诊断的模型

理想模块可以是与待测模块相同的已知无故障模块，也可以是存储在计算机中的模块的真值表。总之，理想模块满足以下条件，对于任意输入，理想模块的输出M0（X）恒为正常。

对于待测模块来说，可以把其输出M看成是输入X和内部故障f的函数，即：

$$M = M(X, f)$$

在一个模块M中，如果一个故障集Fd中的每一个故障f,都存在一个输入X使得：

$$M(X, f) \neq M_0(X)$$

则称模块对于Fd是可检测的。F_d称为该模块的可测故障集。

在一个对于故障集F_d可测的模块M中，如果对于一个故障集 $F_e \subseteq F_d$ 中的任意两个故障f_1和f_2,存在一个输入X使：

$$M(X, f_1) \neq M(X, f_2)$$

则称模块对于F_e是可诊断的。F_e称为模块的可诊断故障集。

3.故障诊断的主要方法

通常，故障诊断的主要方法有下述3种。

对电路直接进行测试的故障测试法：将被测试的系统划分成若干个测试域，并向这些域发出一系列测试码，然后收集并分析被测试区的返回码，以确定故障位置或找出产生故障的元器件。这种按线路内部的电路结构逐个进行测试的方法，将随着电路规模的增大急剧地增加复杂性。因此，对计算机系统往往是先采用下面提到的按功能测试的方法诊断到某一出故障的功能部件，然后再对这一部件的电路进行测试，或者干脆把这一产生故障的功能部件整个替换掉。

检查诊断程序法：用机器语言写的"检查诊断程序"来进行诊断的方法是一种功能测试法。它利用机器指令功能来对系统某些部件进行测试。但由于一条指令的正确执行，往往涉及许多部件，因此故障定位所需的诊断时间较长；而且要求系统必须有能力保证诊断程序的正确执行，否则计算机连程序都不能运行，更谈不上诊断了。

微诊断法：在微程序控制的计算机中用微指令对系统进行诊断叫做微诊断法。由微指令组成的微诊断程序存放在控制存储器中或者先存在外存储器中，诊断法也是一种功能测试法。不论采用指令或微指令进行诊断都是采用滚雪球的方法。先对系统的某一部分进行测试，如果没有发现错误，就在这部分的基础上对其他未测试部分进行测试。如同滚雪球般，越滚越大，直到全部测试完成。

容错技术

9.2.2 容错技术

容错是指计算机系统在运行过程中发生一定的硬件故障或软件错误时仍能保持正常工作而不影响正确结果的一种性能或措施。具有容错能力的计算机称为容错计算机，容错采用冗余方法来消除故障影响。

提高计算机可靠性的技术可以分为避错技术和容错技术。后者主要运用冗余技术来抵消由于故障所引起的影响。冗余技术是计算机容错技术的基础，一般可分为下列几种类型。

硬件冗余：以检测或屏蔽故障为目的而增加一定硬件设备的方法。

软件冗余：为了检测或屏蔽软件中的差错而增加一些在正常运行时所不需要的软件方法。

信息冗余：除实现正常功能所需要的信息外，再添加一些信息，以保证运行结果正确，纠错码就是信息冗余的例子。

时间冗余：使用附加一定时间的方法来完成系统功能。这些附加的时间主要用在故障检测、复执或故障屏蔽上。

简单的双机备份：在20世纪60年代主要利用双处理机或双机的方法来达到容错的目的。例如把关键的元件（处理机、存储器等）或整个计算机设置两套：一是系统运行时使用，另一份作为备份。根据系统的工作情况又可分为热备份和冷备份两种。

热备份（双重系统）：两套系统同时同步运行，当联机子系统检测到错误时，退出服务进行检修，而由热备份子系统接替工作。

冷备份（双工系统）：处于冷备份的子系统平时停机或者运行与联机系统无关的运算，当联机子系统产生故障时，人工或自动进行切换，使冷备份系统成为联机系统。在冷备份时，不能保证从程序端点处精确地连续工作，因为备份机不能取得原来的机器上当前运行的全部数据。

操作系统支持的双机容错：20世纪在70年代中期出现了软件和硬件结构的容错方法。该方法在操作系统的层次上支持联机维修，即故障部分退出后运行、进行维修并重新投入运行都不影响正在运行的应用程序。该结构特点是系统内包括双处理器、双存储器、双输入/输出控制器、不间断工作的电源，以及与之适应的操作系统等。因此，上述硬件的责任一部分发生故障都不会影响系统的继续工作。系统容错是在操作系统控制下进行的，在每个处理机上都保持了反映所有系统资源状态的表格，以及本机和其他机器的工作进程。

系统可靠性评价和系统性能评价方法

9.3 系统可靠性评价和系统性能评价方法

本节将介绍系统可靠性评价和系统性能评价方法。

第 9 章：安全性、可靠性与系统性能评测　作者：希赛教育软考学院　来源：希赛网　2014年03月13日

系统可靠性评价的组合模型

9.3.1 系统可靠性评价的组合模型

组合模型是计算容错系统可靠性最常用的方法。一个系统只要满足以下条件，就可以用组合模型来计算其可靠性。

系统只有两种状态：运行状态和失效状态；

系统可以划分成若干个不重叠的部件，每个部件也只有两种状态：运行状态和失效状态；

部件的失效是独立的；

系统失效当且仅当系统中的剩余资源不满足系统运行的最低资源要求（系统的状态只依赖于部件的状态）时；

已知每个部件的可靠性，可靠性指可用度或可靠度等概率参数。

组合模型的目标就是根据各部件的可靠性R_i来计算系统的可靠度R_{sys}，组合模型的基本思想如下。

1）枚举所有系统状态

假设系统被划分为n个部件，则系统状态是一个n维向量，$q=(s_1,s_2,\cdots,s_n)$其中：

S_i={0,如果部件i处于运行状态；1,如果部件i处于失效状态（$i=1,2,\cdots,n$）},一个具有n个部件的系统共有2^n个状态。

2）计算每个系统状态的概率

系统状态的概率是指系统处于该状态的概率。设系统状态$q=(s_1,s_2,\cdots,s_n)$，q的所有0分量对应的部件用来A_0表示（A_0是所有处于运行状态的部件的集合），q的所有1分量对应的部件用A_1来表示（是所有处于失效状态的部件的集合）。于是，系统状态取得概率为：

$$P_q=(\prod_{i\in A_0}R_i)(\prod_{j\in A_1}(1-R_j))$$

3）可靠性计算

（1）串联系统

假设一个系统由n个子系统组成，当且仅当所有的子系统都能正常工作时，系统才能正常工作，这种系统称为串联系统，如图9-4所示。

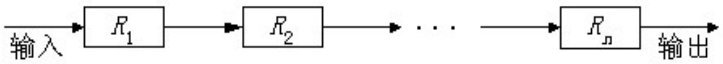

图9-4 串联系统

设系统各个子系统的可靠性分别用表示$R_1,R_2,\cdots,R_n$，则系统的可靠性

$R = R_1 \times R_2 \times \cdots \times R_n$。

如果系统的各个子系统的失效率分别用 $\lambda_1, \lambda_2, \cdots, \lambda_n$ 来表示，则系统的失效率 $\lambda = \lambda_1 + \lambda_2 + \cdots + \lambda_n$。

（2）并联系统

假如一个系统由n个子系统组成，只要有一个子系统能够正常工作，系统就能正常工作，如图9-5所示。

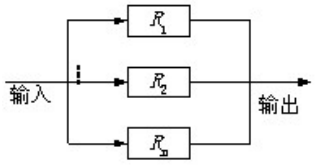

图9-5 并联系统

设系统各个子系统的可靠性分别用 $R_1, R_2, \cdots, R_n$ 表示，则系统的可靠性 $R = 1-(1-R_1)\times(1-R_2)\times\cdots\times(1-R_n)$。

假如所有子系统的失效率均为λ，则系统的失效率为μ：

$$\mu = \frac{1}{\frac{1}{\lambda}\sum_{j=1}^{n}\frac{1}{j}}$$

在并联系统中只有一个子系统是真正需要的，其余n–1个子系统称为冗余子系统，随着冗余子系统数量的增加，系统的平均无故障时间也增加了。

（3）模冗余系统

m模冗余系统由m个（m=2n+1为奇数）相同的子系统和一个表决器组成，经过表决器表决后，m个子系统中占多数相同结果的输出作为系统的输出，如图9-6所示。

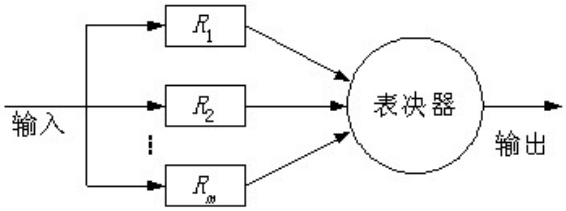

图9-6 模冗余系统

在m个子系统中，只有n+1个或n+1个以上子系统能正常工作，系统就能正常工作，输出正确结果。假设表决器是完全可靠的，每个子系统的可靠性为R0,则m模冗余系统的可靠性为：

$$\sum_{i=n+1}^{m} C_m^i R_0^i (1-R_0)^{m-i}$$

上一节　本书简介　下一节

系统可靠性评价的马尔柯夫模型

9.3.2 系统可靠性评价的马尔柯夫模型

马尔柯夫模型是系统可靠性评价中用到的最重要的模型，它的两个核心概念是状态和状态转

移。系统的状态表示了在任何瞬间用于描述该系统所必须知道的一切。对于可靠性分析，马尔柯夫模型的每个状态表示了有效和失效模块的不同组合。如果每个模块都是处于有效和失效两种情况之一，则一个n模块的系统的完整模型有2n个状态。

状态转移是指随着时间的流逝，因模块的失效和修复，系统发生的状态变化。

作为马尔柯夫模型基础的基本假设是：给定状态的转移概率仅取决于当前的状态。系统从一个状态i转移到另一个状态j的转移率定义为单位时间内从状态i转移到状态j的概率。对于一个模块来说，从运行状态到失效状态的转移率就是模块的失效率，从失效状态到运行状态的转移率就是模块的修复率。一个失效率为λ，修复率为μ的模块的状态图如图9-7所示。

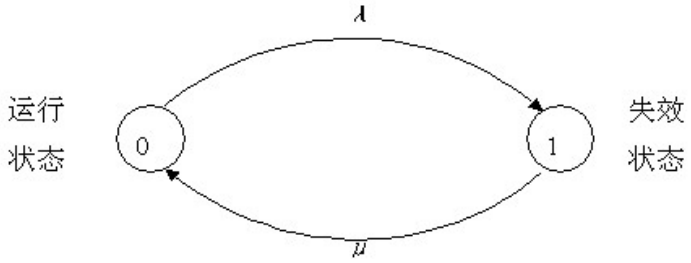

图9-7 （λ，μ）模块的状态图

对于由n个模块构成的系统，共有 2^n 个状态。从理论上说，任意两个状态之间都存在转移的可能性。但因失效是独立的，在很短的时间内发生多个失效的可能性远小于发生一个失效的可能性。因此，我们只考虑任一时刻只有一个模块失效的转移；同样，也只考虑任意时刻只有一个模块修复的转移。系统的状态图也可以表示为层次图。第一层只有一个状态，对应于所有模块都运行的情况；第二层有n个状态，对应于一个模块失效的各种情况；第 $i+1$ 层有 C_n^i 个状态，对应于n个模块中有i个失效的各种情况；第 $n+1$ 层也只有一个状态，对应于全部模块都失效的情况。

根据系统的状态图，可以计算出系统处于任意状态的概率。

设系统在t时刻处于状态0和1的概率分别为P0（t）和P1（t），于是，在 $t+\Delta t$ 时刻系统处于0状态的概率为：

$$P_0(t+\Delta t) = P_0(t) - P_0(t)\cdot\lambda\cdot\Delta t + P_1(t)\cdot\mu\cdot\Delta t$$

同样，在 $t+\Delta t$ 时刻系统处于1状态的概率为：

$$P_1(t+\Delta t) = P_1(t) + P_0(t)\cdot\lambda\cdot\Delta t - P_1(t)\cdot\mu\cdot\Delta t$$

令 $\Delta t \to 0$ 取极限得微分方程组：

$$\begin{bmatrix}\dot{P}_0(t)\\ \dot{P}_1(t)\end{bmatrix} = \begin{bmatrix}-\lambda & \mu\\ \lambda & -\mu\end{bmatrix}\begin{bmatrix}P_0(t)\\ P_1(t)\end{bmatrix}$$

其中，$\dot{P}_i(t)$ 是对t的一阶导数（$i=0,1$）。

只要解此微分方程组就可以得出P0（t）和P1（t）。

上一节　本书简介　下一节

系统性能评价

9.3.3 系统性能评价

计算机的性能主要反映了一个系统的使用价值，即性能价格比。性能的含义很广泛，主要包括系统处理能力（或吞吐率）、响应速度、可靠性、可使用性、可维护性等。这些性能既有定量的指标，又有定性的指标。

1.性能评价的常用指标及方法

1）时钟频率

计算机的时钟频率在一定程度上反映了机器速度，一般来说，主频越高，速度越快。但是相同频率、不同体系结构的机器，其速度可能会相差很多倍，因此，还需要用其他方法来测定机器性能。与时钟频率相关的另一个概念是性能因子，即CPI指每条指令的平均时钟周期。

$$\mathrm{CPU}_{\mathrm{time}} = 指令数 \times \mathrm{CPI} \times 时钟周期 = 指令数 \times \mathrm{CPI} / 时钟频率$$

2）指令执行速度

在计算机发展的初期，曾用加法指令的运算速度来衡量计算机的速度，速度是计算机的主要性能指标之一。因为加法指令的运算速度大体上可反映出乘法、除法等其他算术运算的速度，而且逻辑运算、转移指令等简单指令的执行时间往往设计成与加法指令相同，因此加法指令的运算速度有一定代表性。表征机器运算速度的单位通常有MIPS（Million Instruction Per Second,每秒百万条指令）、MFLOPS（Million Floating-point Instruction Per Second,每秒浮点指令数）。

MIPS=指令数/（执行时间×1 000 000）

MIPS大小和指令集有关，不同指令集的计算机间的MIPS不能比较；在同一台计算机上MIPS是变化的，因程序不同而变化；有时MIPS会出现矛盾，比如带有硬件浮点处理器的计算机；MIPS中，除了包含运算指令外，还包含取数、存数、转移等指令在内；MIPS只适宜于评估标量机；相对MIPS指相对参照机而言的MIPS,通常用VAX-11/780机处理能力为1MIPS.

MFLOPS=浮点指令数/（执行时间×1 000 000）

与机器和程序有关，测量浮点运算时，比MIPS准确；MFLOPS比较适宜于评估向量计算机；MFLOPS与MIPS之间的换算关系为：$1\mathrm{MFLOPS} \approx 3\mathrm{MIPS}$；MFLOPS只能用来衡量机器浮点操作的性能，而不能体现机器的整体性能。例如编译程序，不管机器的性能有多好，它的MFLOPS不会太高；MFLOPS是基于操作而非指令的，所以它可以用来比较两种不同的机器；单个程序的MFLOPS值并不能反映机器的性能；MFLOPS依赖于操作类型，例如100%的浮点加要远快于100%的浮点除。

3）等效指令速度法

随着计算机指令系统的发展，指令的种类大大增加，用单位指令的MIPS值来表征机器的运算速度的局限性日益暴露，因此很快出现了改进的办法，称之为吉普森（Gibson）混合法或等效指令速度法。

等效指令速度法统计各类指令在程序中所占的比例，并进行折算。设某类指令i在程序中所占比例为wi,执行时间为t_i,则等效指令的执行时间为：

$$T = \sum (W_i * t_i)$$

式中n为指令的种类数。

4）数据处理速率法

因为在不同程度上，各类指令的使用频率是不同的，所以固定比例方法存在着很大的局限性；而且数据长度与指令功能的强弱对解题的速度影响极大。同时这种方法也不能反映现代计算机中高

速缓冲存储器、流水线、交叉存储等结构的影响。具有这种结构的计算机的性能不仅与指令的执行频率有关，而且也与指令的执行顺序与地址分布有关。

数据处理速率PDR法采用计算"数据处理速率"值的方法来衡量机器性能，PDR值越大，机器性能越好。PDR与每条指令和每个操作数的平均位数及每条指令的平均运算速度有关，其计算方法如下：

$$\mathrm{PDR} = L / R$$

其中：$L = 0.85G + 0.15H + 0.4J + 0.15K$

$R = 0.85M + 0.09N + 0.06P$

式中，G是每条定点指令的位数；M是平均定点加发时间；H是每条浮点指令位数；N是平均浮点加发时间；J是定点操作数的位数；P是平均浮点乘法时间；K是浮点操作数的位数。

此外，还做了如下规定：G>20位、H>30位；从主存取一条指令的时间等于取一个字的时间；指令与操作数存放在主存，无变址或间址操作；允许有并行或先行取址指令功能，此时选择平均取指令时间。PDR值主要对CPU和主存储器的速度进行度量，但不适合衡量机器的整体速度，因为它没有涉及Cache、多功能部件等技术性能的影响。

5）核心程序法

上述性能评价方法主要针对CPU（有时包括主存），它没有考虑诸如I/O结构、操作系统、编译程序的效率等对系统性能的影响。因此，难以准确评价计算机的实际工作能力。

核心程序法是研究较多的一种方法，它把应用程序中用得最频繁的那部分核心程序作为评价计算机性能的标准程序，在不同的机器上运行，测得其执行时间，作为各类机器性能评价的依据。机器软硬件结构的特点能在核心程序中得到反映，但是核心程序各个部分之间的联系较小。由于程序短，所以访问存储器的局部性特征很明显，以致Cache的命中率比一般程序高。

基准程序法是目前一致承认的测试性能的较好方法，有多种多样的基准程序，如主要测试整数性能的基准程序，测试浮点性能的基准程序等。

2.计算机性能评价技术

1）分析技术

方法：在一定假设条件下，计算机系统参数与性能指标参数之间存在着某种函数关系，按其工作负载的驱动条件列出方程，用数学方法求解。

特点：具有理论的严密性，节约人力和物力，可用于设计中的系统。

数学工具：通常用排队论模型进行分析。

发展：从脱离实际的假设发展到近似求解。

近似求解算法：聚合法、均值分析法、扩散法等。

2）模拟技术

包含的内容及步骤：

按被评价系统的运行特性建立工作负载模型；

按系统可能有的工作负载特性建立工作负载模型；

语言编写模拟程序；

模仿被评价系统的运行；

设计模拟实验，依照评价目标，选择与目标有关因素，得出实验值，再进行统计、分析。

特点：可应用于设计中或实际应用中的系统；可与分析技术相结合，构成一个混合系统。分析

和模拟技术最后均需要通过测量技术验证。

3）测量技术

测量技术只能对已投入使用的系统进行测量，通常采用不同层次的基准测试程序评估。

评估层次有实际应用程序、核心程序、合成测试程序三个层次，但必须均为国际性组织认可的程序。

对评估结果进行分析和统计来保证评估结果的准确性。

3.基准测试程序

1）整数测试程序

Dhrystone是一个综合性的基准测试程序，它是为了测试编译器和CPU处理整数指令和控制功能的有效性，人为地选择一些"典型指令"综合起来形成的测试程序。

用C语言编写的Dhrystone基准程序用了100条语句，由下列操作组成：各种赋值语句；各种数据类型的数据区；各种控制语句；过程调用和参数传送；整数运算和逻辑操作。

Dhrystone程序测试的结果为每秒1757Dhrystones,为便于比较，人们假设1 VAX MIPS=1757Dhrystones每秒，将被测机器的结果除以1757,就得到被测机器相对VAX 11/780的MIPS值。有些厂家在宣布机器性能时就用Dhrystone MIPS值作为各自机器的MIPS值。

不过不同厂家在测试MIPS值时，使用的基准程序一般不一样，因此不同厂家机器的MIPS值有时虽然相同的，但是性能却可能相差很大，那是因为各厂家在设计计算机时针对不同的应用领域：如科学和工程应用、商业管理应用、图形处理应用等，而采用了不同的体系结构和实现方法。同一个厂家的机器，采用相同的体系结构，用相同的基准程序测试，得到的MIPS值越大，一般说明机器速度越快。

2）浮点测试程序

在计算机科学工程应用领域内，浮点计算工作量占很大比例，因此机器的浮点性能对系统的应用有很大的影响。有些机器只标出单个浮点操作性能，如浮点加法、浮点乘法时间。而大部分工作站则用Linpack和Whetstone基准程序测得浮点性能。Linpack主要测试向量性能和高速缓存性能。Whetstone是一个综合性测试程序，除测试浮点操作外，还测试整数计算和功能调用等性能。

Linpack基准测试程序：是一个用Fortran语言写成的子程序软件包，称为基本线性代数子程序包，此程序完成的主要操作是浮点加法和浮点乘法操作。测量计算机系统的Linpack性能时，让机器运行Linpack程序，测量运行时间，将结果用MFLOPS表示。

当解n阶线性代数方程组时，n越大，向量化程度越高。其关系如表9-1所示。

表9-1　n与向量化的关系

矩阵规模	100×100	300×300	1000×1000
向量化百分比	80%	95%	98%

向量化百分比指的是向量成分的计算量占整个程序计算量的百分比。在同一台机器中，向量化程度越高，机器的运算速度越快，因为不管n的大小，求解方程时花的非向量操作的时间差不多是相等的。

Whetstone基准测试程序：Whetstone是用Fortran语言编写的综合性测试程序，主要由执行浮点运算、整数算术运算、功能调用、数组变址、条件转移和超越函数的程序组成。Whetstone的测试结果用Kwips表示，1Kwips表示机器每秒钟能执行1000条Whetstone指令。

3）SPEC基准程序

SPEC是System PerformanceEvaluation Cooperative的缩写，是几十家世界知名计算机大厂商所支持的非盈利的合作组织，旨在开发共同认可的标准基准程序。

SPEC基准程序是由SPEC开发的一组用于计算机性能综合评价的程序。以对VAX11/780机的测试结果作为基数，其他计算机的测试结果以相对于这个基数的比率来表示。SPEC基准程序能较全面地反映机器性能，具有一定的参考价值。

4）TPC基准程序

TPC是Transaction Processing Council（事务处理委员会）的缩写，TPC基准程序是由TPC开发的评价计算机事务处理性能的测试程序，用以评价计算机在事务处理、数据库处理、企业管理与决策支持系统等方面的性能。TPC成立于1988年，目前已有40多个成员，几乎包括了所有主要的商用计算机系统和数据库系统。该基准程序的评测结果用每秒完成的事务处理数TPC来表示。TPC基准测试程序在商业界范围内建立了用于衡量机器性能及性能价格比的标准。

例题分析

9.4 例题分析

例题1（2011年5月试题6）

某计算机系统由图7-8所示的部件构成，假定每个部件的千小时可靠度都为R,则该系统的千小时可靠度为（6）。

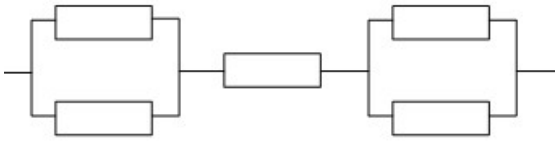

图7-8 部件构成图

（6）A.R+2R/4　B.R+R2/4　C.R（1-（1-R）^{2}）　D.R（1-（1-R）^{2}）^{2}

例题分析：

本题考查系统可靠性。

计算机系统是一个复杂的系统，而且影响其可靠性的因素也非常繁复，很难直接对其进行可靠性分析。若采用串联方式，则系统可靠性为每个部件的乘积R=R1×R2×R3×…×Rn;若采用并联方式，则系统的可靠性为R=1-（1-R1）×（1-R2）×（1-R3）×…×（1-Rn）。

在本题中，既有并联又有串联，计算时首先我们要分别计算图中两个并联后的可靠度，它们分别为1-（1-R）2,然后是三者串联，根据串联的计算公式，可得系统的可靠度为R×1-（1-R）^{2}×1-（1-R）^{2}= R（1-（1-R）^{2}）^{2}.因此本题答案选D.

例题答案：（6）D

例题2（2011年5月试题7）

用户A从CA获得用户B的数字证书，并利用 （7） 验证数字证书的真实性。

（7）A.B的公钥　　B.B的私钥　　C.CA的公钥　　D.CA的私钥

例题分析：

本题主要考查数字证书的相关知识。

数字证书就是互联网通讯中标志通讯各方身份信息的一系列数据，就好比日常生活中个人身份证一样。数字证书是由一个权威机构证书授权中心（CA）发行的。最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。其中证书授权中心的数字签名是用它自己的私钥完成的，而它的公钥也是公开的，大家可以通过它的公钥来验证该证书是否是某证书授权中心发行的，以达到验证数字证书的真实性。因此本题答案选C.

例题答案：（7）C

例题3（2011年5月试题8）

宏病毒一般感染以 （8） 为扩展名的文件。

（8）A.EXE　　B.COM　　C.DOC　　D.DLL

例题分析：

宏病毒是一种脚本病毒，它的最主要特征是它是一种寄存在文档或模板的宏中的计算机病毒。宏病毒主要感染文件有 Word、Excel 的文档。并且会驻留在Normal面板上。宏病毒的前缀是：Macro,第二前缀是：Word、Excel其中之一。如：Macro.Word.WhiteScreen、美丽莎（Macro.Melissa）等。

在本题中，题目给出的4个选项中，扩展名为DOC的一般为Word文档，因此容易感染宏病毒。

例题答案：（8）C

例题4（2011年5月试题9）

在IE浏览器中，安全级别最高的区域设置是 （9） .

（9）A.Internet　　B.本地Intranet　　C.可信任站点　　D.受限站点

例题分析：

在IE浏览器中，安全级别最高的区域设置是受限站点。

其中Internet区域设置适用于Internet网站，但不适用于列在受信任和受限制区域的网站；本地Intranet区域设置适用于在Intranet中找到的所有网站；可信任站点区域设置适用于你信任的网站；而受限站点区域设置适用于可能会损坏你计算机或文件的网站，它的安全级别最高。

例题答案：（9）D

网络的功能、分类与组成

从古代的驿站、八百里快马，到近代的电报、电话，人类对于通信的追求从未间断过，信息的处理与通信技术的革新一直伴随社会的发展。

而作为20世纪人类最伟大、最卓越的发明，个人计算机的出现与发展使得人们获得了以前无法想法的信息处理能力，为了将这些强大的信息处理设备连接起来，避免出现"信息孤岛"现象，就催生了"计算机网络",这一新时代的通信技术。网络技术使得计算机的功能得到了大大的加强，使用范围得到了很大的扩展。

10.1 网络的功能、分类与组成

什么是计算机网络呢？计算机网络是指由通信线路互相连接的许多独立自主工作的计算机构成的资源共享集合体，它是计算机技术和通信技术相结合的产物。其中，通信线路并不专指铜导线，还可以是光纤，甚至可以是一些无界的媒体：如激光、微波、红外线等。在这个定义中，我们可以知道如下内容。

计算机网络的作用：资源共享；

计算机网络的组成：许多独立自主工作的计算机；

计算机网络的实现方式：使用通信线路互相连接。

另外，早期的计算机网络是以一台或几台大型的计算机为中心的，但是由于计算机技术的十倍速发展，小型机甚至是微型机都拥有了惊人的处理能力，而且在整体性能上均已超过了早期的大型计算机。所以网络的重心开始有了偏向，开始体现共享这一原则，也就是所有的计算机都具备了独立自主工作的能力。计算机网络从共享大型计算机的计算能力发展为共享存储在计算机内的信息，这也是时代发展所致。

上一节　本书简介　下一节

第 10 章：计算机网络基础知识　作者：希赛教育软考学院　来源：希赛网　2014年01月27日

计算机网络的分类

10.1.1 计算机网络的分类

我们经常根据计算机网络的传输距离来进行分类，这是因为计算机间的距离、所要求的传输速度就决定了网络技术之间的差异。

不同传输距离的网络可以分为局域网、城域网、广域网三种。局域网的相关技术是基于处理近距离传输而设计和发展而来的，而广域网的相关技术是基于处理远距离传输而设计和发展而来的，城域网则是为一个城市网络设计的相关技术。

1.局域网

局域网（Local Area Network,LAN），是基于传输距离较短的前提下所发展的相关技术的集合，用于将小区域内的各种计算机设备和通信设备互联在一起组成资源共享的通信网络。在局域网中常见的传输媒介有：双绞线、细/粗同轴电缆、微波、射频信号、红外等。其主要特点如下。

距离短：0.1km~25km,可以是一个建筑物内、一个校园内或办公室内。

速度快：4Mb/s~1Gb/s,从早期的4Mb/s、10Mb/s、100Mb/s发展到现在的1000Mb/s（1Gb/s），而且现在还在不断向前发展。

高可靠性：由于距离很近，传输相当可靠，有极低的误码率。

成本较低：由于覆盖的地域较小，因此传输媒介、网络设备的价格都相对较便宜，管理也比较简单。

根据不同的技术采用具体的实现方法，局域网有以太网（Ethernet）、令牌环网络（Token Ring）、Apple Talk网络、ArcNet网络几种类型。这些"名满天下"的网络都曾经是一个时代的"风云人物",但随着时代的发展，都逐渐退出了历史的舞台：ArcNet似乎已经过时，而IBM的Token Ring及苹果电脑公司的Apple Talk逐渐成为公司的私有物品，因为与开放网络的精神有违，所以限制了其自身的发展。

所以，现今几乎所有的局域网都是基于以太网（Ethernet）实现的。它最早起源于美国夏威夷大学，后来不断发展完善，其相关技术已进行了标准化。以太网标准推出后，3COM、AT&T等大公司都纷纷推出自己的以太网产品，使得其得到了迅猛的发展。如今，以太网产品已遍布世界各地，它对计算机网络技术的发展起到了举足轻重的作用。以太网组建较为容易，各设备之间的兼容性较好，目前主流的服务器操作系统如Windows NT Server 4.0、Windows 2000 Server、Windows XP Server、NetWare、Linux和UNIX,以及单机操作系统Windows 9x/Me/2000/XP都能够良好地支持以太网。以太网以其"易于组建、维护、管理"的特点，深深吸引了用户。现在采用以太网构建的局域网已近90%,而且比例还在上升中。

当然随着应用需求的不断提高，也对局域网技术提出了新的挑战。为了迎合新的需求，科学家们也进行了不懈的研究，出现了一批像FDDI一样的新技术，使得局域网技术得到了长足发展。

2.广域网

广域网（Wide Area Network,WAN）是基于传输距离较长的前提下所发展的相关技术的集合，用于将大区域范围内的各种计算机设备和通信设备互联在一起组成一个资源共享的通信网络。其主要特点如下。

长距离：是跨越城市、甚至是联通全球远距离连接。

低速率： 一般情况下，广域网的传输速率是以Kb/s为单位的。当然随着应用的需要，引起技术的不断创新，现在也出现了许多像ISDN、ADSL这样的高速广域网，其传输速率也能达到Mb/s,当然费用也大大地提高了。

高成本：相对于城域网、局域网来说，广域网的架设成本是很昂贵的，当然它所带来的经济效益也是极大的。就像现在的Internet,就给世界带来了前所未有的大发展。

广域网一般用电话线路，当然也可以用其他的媒介如光纤、卫星来建立。目前经常采用的几种电话线路技术如下。

公用交换电话网（PSTN）：在大多数家庭中使用。

综合业务数字网（ISDN）：最常用的是基带ISDN,被分为三条信道，两条用于数据传输，一条用于控制，称为2B+D,每条B信道速率为64Kb/s,而D信道则为16Kb/s.

T1线路：主要用于商业应用，其传输速率达到1.544Mbps.

广域网在平时的经济、政治活动中充当着越来越重要的角色，随着全球经济的进一步发展，对文件远程传输的要求越来越多。不仅是参与远程联网的结点数据量在膨胀，而且传输的流量也在日

益增大，从早期的文本文件的传输发展到了现在的音频、视频文件的传输需求。这也无形地鞭策着广域网技术的进一步发展。

随着ISDN（综合业务数字网）、FR（帧中继）、ATM（异步转移模式）、SMDS（交换式多兆位数据服务等高速广域网技术的出现和发展，广域网不再是过去"老牛拉破车"一样的低传输速率，而是成为了信息时代的生命线--信息高速公路。

3.城域网

伴着进军信息时代的号角，世界各地纷纷掀起了建设信息化新都市的热潮。为了更好地进行信息化都市的建设，一个范围为一个城市的计算机网络架设的具体技术研究工作分离出来。许多科研机构纷纷开始投身于研究如何整合现有的网络技术，让都市网络化、信息化。这就是城域网技术（MAN）。这是一个年轻而且富有极大潜力的新技术。

城域网的覆盖范围介于局域网和广域网之间，城域网的主要技术是DQDB--分布式队列双总线。