

# 1.3安全性、可靠性与系统性能评测基础知识

## 1.3.1计算机安全概述

**计算机安全：**是一个**涵盖非常广的课题。它包括如下内容：**

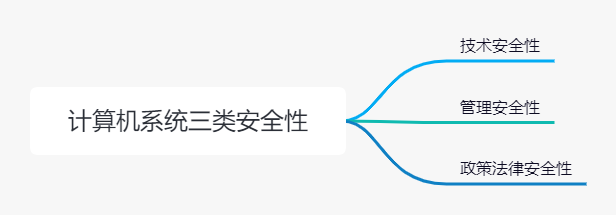
1. 硬件、软件和技术、安全规划、安全管理和安全监督。
2. 安全管理、通信与网络安全、密码学、安全体系及模型、容错与容灾、涉及安全的应用程序
3. 系统开发、法律、犯罪及道德规范等领域。

**安全管理**是其中非常重要的一块。

作为信息系统的管理部门应根据**管理原则**和该**系统处理数据的保密性**，制定相应的**管理制度或规范**。

### 1.计算机的安全等级

计算机系统中安全性共有三类，分别是**技术安全性**、**管理安全性**、**政策法律安全性**。



一些重要的安全评估准则如下：

**（1）**美国国防部和国家标准局推出的《可信计算机系统评估准则》（TCSEC）。

**（2）**加拿大的《可信计算机产品评估准则》（CTCPEC）。

**（3）**美国制定的《联邦（最低安全要求）评估准则》（FC）。

**（4）**欧洲英、法、德、荷四国国防部门信息安全机构联合指定的《信息技术安全评估准则》（ITSEC），该准则事实上已成为欧盟各国使用的共同评估标准。

**（5）**美国制定的《信息技术安全通过评估准则》（简称CC标准），国际标准组织（ISO）于1996年批准CC标准以ISO/IEC15408-1999名称正式列入国际标准系列。

其中，美国国防部和国家标准局的《可信计算机系统评测标准》TCSEC/TDI将系统划分为4组7个等级。

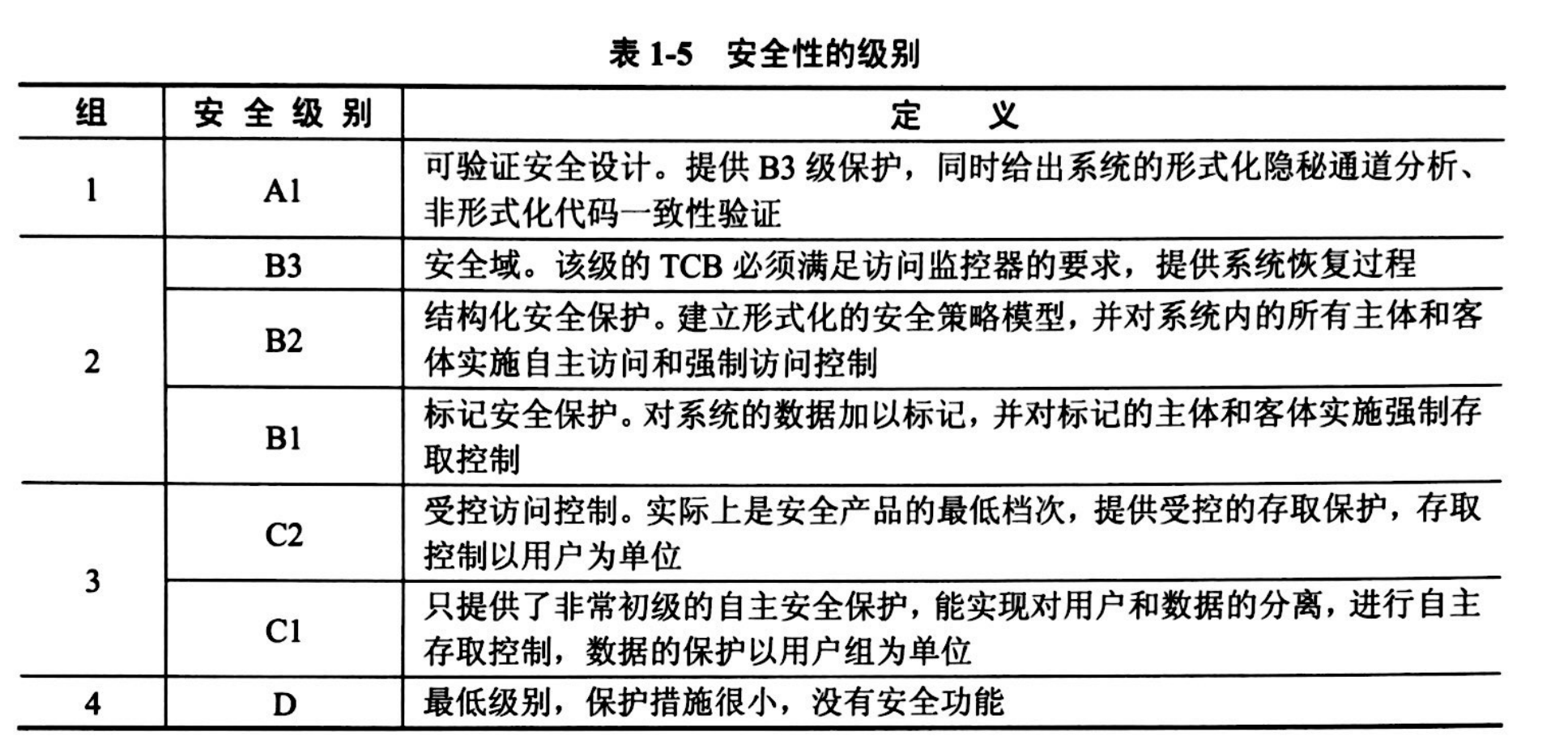
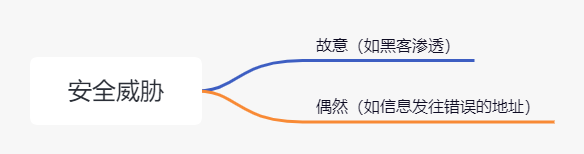


图 1安全性的级别

### 2.安全威胁

**安全威胁：**指某个人、物、事件对某一资源的机密性、完整性、可用性或合法性所造成的的危害。

**威胁的具体实现：**某种攻击。



**安全威胁分为两类：故意**（如黑客渗透）、**偶然**（信息发往错误的地址）

### 3.影响数据安全的因素

分为**内部**和**外部**两类。

**1)内部因素**

(1).可采用多种技术对数据加密。

(2).制定数据安全规划。

(3).建立安全存储体系，包括容量、容错数据保护和数据备份等。

(4).建立事故应急计划和容灾措施。

(5).重视安全管理，制定数据安全管理规范。

**1)外部因素**

(1).可将数据分成不同的密级，规定外部使用人员的权限。

(2).设置身份认证、密码、设置口令、设置指纹和声纹笔迹等多种认证。

(3).设置防火墙，为计算机建立一道屏障，防止外部入侵破坏数据。

(4).建立入侵检测、审计和追踪，对计算机进行防卫。

(5).包括计算机物理环境的保障、防辐射、防水和防火等外部防灾措施。

## 1.3.2加密技术和认证技术

### 1.加密技术

加密技术是最常用的**安全保密手段**。

**加密技术关键：**加密/解密算法和密钥管理。

**加密基本过程：**对原来为明文的文件或数据按某种加密算法进行处理，使其成为不可读的一段代码，通常称为**“密文”。**只有输入相应的密钥之后，才能显示出原来的内容。

**数据加密与解密过程关系：**一对逆关系。

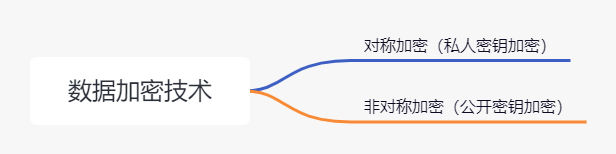
数据加密是用加密算法E和加密密钥K1将明文P变换成密文C，记为：

**C=EK1（P）**

数据解密是数据加密的逆过程，解密算法D和解密密钥K2将密文变换成明文P，记为：

**P=DK2（C）**

数据加密技术分为两类，即**对称加密（私人密钥加密）**和**非对称加密（公开密钥加密）**。



#### 1)对称加密技术

**对称加密采用技术：**对称密码编码技术

**对称加密特点：**文件加密和解密使用相同的密钥

常用的对称加密算法有以下几种。

**（1）数据加密标准算法（Digital Encryption Standard,DES）**

**主要采用方法：**替换和移位。

**实现原理：**它用56位密钥对64位二进制数据块进行加密，每次加密可对64位的输入数据进行16轮编码，经一系列替换和移位后，输入的64位原始数据转换成完全不同的64位输出数据。

**优点：**DES算法运算速度快，密钥生产容易，适合于在当前大多数计算机上用软件方法实现，同时也适合于在专用芯片上实现。

**（2）三重DES（3DES，或称TDEA）**

**与DES的关系：**在DES的基础上采用三重DES。

**实现原理：**用两个56位的密钥K1和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。

**（3）RC-5（Rivest Cipher5）**

RC-5是在RCF2040中定义的。

**（4）国际数据加密算法（International Data Encryption Adleman,IDEA）**

**与DES的关系：**IDEA是在DES算法的基础上发展起来的，类似于三重DES。

IDEA的密钥为128位

**实现原理：**它设计了一系列加密轮次，每轮加密都使用从完整的加密密钥中生成的一个子密钥。

1. **高级加密标准（Advanced Encryption Standard，AES）算法**

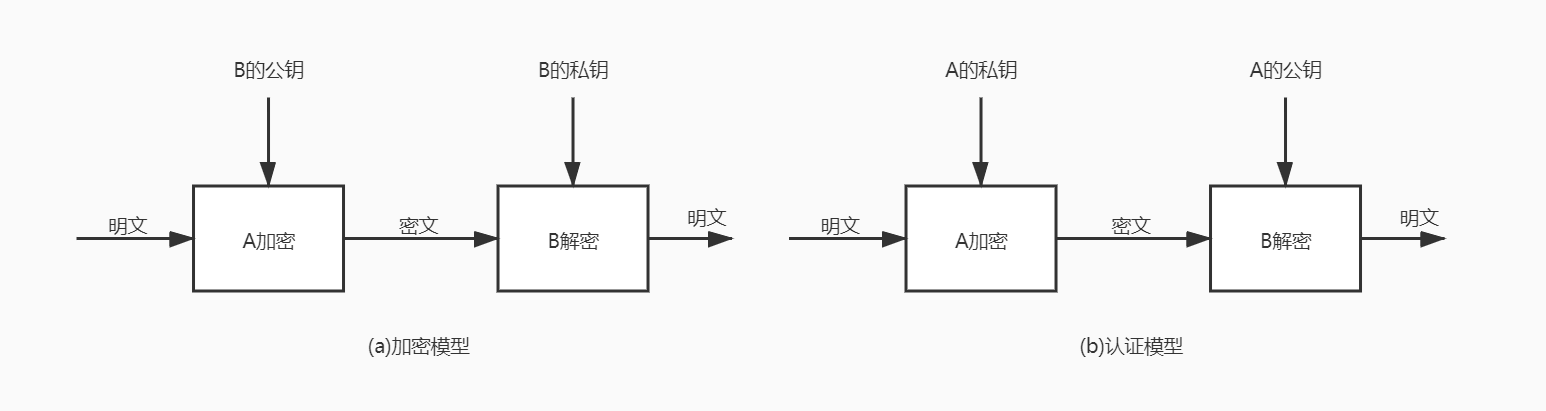
**基于算法：**AES算法基于排列和置换运算。

**实现原理：**AES使用几种不同的方法来执行排列和置换运算。

**特点：**它是一个**迭代**、**对称密钥分组的密码**，它可以使用128、192和256位密钥，并且用128位（16字节）分组加密和解密数据。

#### 2)非对称加密技术（公钥加密技术）

**与对称算法区别：**非对称算法需要两个密钥，公开密钥（Publickey）和私有密钥（Privatekey）。**公开密钥与私有密钥关系：**它们是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。非对称密钥有两种体制。



图：非对称加密体制模型

**非对称加密算法实现机密信息交换的基本过程：**

1. 甲方生成一对密钥并将其中的一把作为公用密钥向其他方公开。
2. 得到该公用密钥的乙方使用该密钥对机密信息进行加密后再发送给甲方。
3. 甲方再用自己保存的另一把专用密钥对加密后的信息进行解密。甲方只能用其专用密钥解密由其公用密钥加密后的任何信息。

**非对称加密算法优点：**保密性较好，消除了最终用户交换密钥的需要。

**非对称加密算法缺点：**加密和解密花费的时间长、速度慢，不适合于对文件加密，而只适用于对少量数据进行加密。

**RSA算法：**它是一种公钥加密算法。

**RSA实现过程：**

1. 选择大素数p和q（大于10100）。
2. 令n=p×q和z=(p-1)×(q-1)。
3. 选择d与z互质。
4. 选择e，使e×d=1（mod z）。

明文P被分成k位的块，k是满足2k<n的最大整数，于是有0≤P＜n。加密时计算，

C=Pe(mod n)

这样公钥为（e，n）。解密时计算

P=Cd（mod n）

即私钥为（d，n）。

例如，设p=3，q=11，n=33，z=20，d=7，e=3，C=P3(mod 33),P=C7(mod 33)，则有

C=23(mod 33)=8(mod 33)=8

P=87(mod 33)=2097152(mod 33)=2

**不对称与对称密码学的比较**

（1）对称密码是指在加密和解密时使用同一个密钥的方式，不对称密码则是指在加密和解密时使用不同密钥的方式。

（2）[对称密钥加密](https://www.wanweibaike.com/wiki-%E5%AF%B9%E7%A7%B0%E5%AF%86%E9%92%A5%E5%8A%A0%E5%AF%86)牵涉到[密钥管理](https://www.wanweibaike.com/wiki-%E5%AF%86%E9%92%A5%E7%AE%A1%E7%90%86)的问题，尤其是[密钥交换](https://www.wanweibaike.com/wiki-%E5%AF%86%E9%92%A5%E4%BA%A4%E6%8D%A2)，它需要通信双方在通信之前先透过另一个安全的渠道交换共享的密钥，才可以安全地把密文透过不安全的渠道发送；对称密钥一旦被窃，其所作的加密将即时失效；而在[互联网](https://www.wanweibaike.com/wiki-%E4%BA%92%E8%81%94%E7%BD%91)，如果通信双方分隔异地而素未谋面，则对称加密事先所需要的“安全渠道”变得不可行；非对称加密则容许加密公钥随便散布，解密的私钥不发往任何用户，只在单方保管；如此，即使公钥在网上被截获，如果没有与其匹配的私钥，也无法解密，极为适合在互联网上使用。另一方面，不对称密码的公钥解密的特性可以形成[数字签名](https://www.wanweibaike.com/wiki-%E6%95%B8%E4%BD%8D%E7%B0%BD%E7%AB%A0)，使数据和文件受到保护并可信赖；如果公钥透过数字证书认证机构签授成为电子证书，更可作为数字身份的认证，这都是[对称密钥加密](https://www.wanweibaike.com/wiki-%E5%AF%B9%E7%A7%B0%E5%AF%86%E9%92%A5%E5%8A%A0%E5%AF%86)无法实现的。不过，不对称密码的钥加密[在计算上相当复杂](https://www.wanweibaike.com/wiki-%E8%A8%88%E7%AE%97%E8%A4%87%E9%9B%9C%E6%80%A7%E7%90%86%E8%AB%96)，性能欠佳、远远不比对称加密；因此，在一般实际情况下，往往通过公钥加密来[随机](https://www.wanweibaike.com/wiki-%E5%AF%86%E7%A0%81%E5%AD%A6%E5%AE%89%E5%85%A8%E4%BC%AA%E9%9A%8F%E6%9C%BA%E6%95%B0%E7%94%9F%E6%88%90%E5%99%A8)[创建临时的对称秘钥](https://www.wanweibaike.com/wiki-%E8%BF%AA%E8%8F%B2-%E8%B5%AB%E7%88%BE%E6%9B%BC%E5%AF%86%E9%91%B0%E4%BA%A4%E6%8F%9B)，亦即[对话键](https://www.wanweibaike.com/wiki-%E5%B0%8D%E8%A9%B1%E9%8D%B5)，然后才通过对称加密来传输大量、主体的数据。

#### 3)密钥管理

**密钥包括：**密钥是有生命周期的，密钥和证书的有效时间，以及已撤销密钥和证书的维护时间等。

**密钥管理包括：**密钥管理主要指密钥对的安全管理，包括密钥产生、密钥备份和恢复、密钥更新等。

**（1）密钥产生**

密钥对的产生是证书申请过程中重要的一步，其中产生的私钥由用户保留，公钥和其他信息则交给CA中心进行签名，从而产生证书。根据证书类型和应用的不同，密钥对的产生也有不同的形式和方法。对于普通证书和测试证书，一般由浏览器或固定的终端应用来产生，这样产生的密钥强度较小，不适合应用于比较重要的安全网络交易。而对于比较重要的证书，如商家证书和服务器证书等，密钥对一般由专用应用程序或CA中心直接产生，这样产生的密钥强度大，适合于重要的应用场合。

**数字证书（CA中心颁发的证书）：**数字证书是指在互联网通讯中标志通讯各方身份信息的一个数字认证，人们可以在网上用它来识别对方的身份。因此数字证书又称为数字标识。数字证书对网络用户在[计算机网络](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%BD%91%E7%BB%9C/18763)交流中的信息和数据等以[加密](https://baike.baidu.com/item/%E5%8A%A0%E5%AF%86/752748)或[解密](https://baike.baidu.com/item/%E8%A7%A3%E5%AF%86/18611004)的形式保证了信息和数据的完整性和安全性。**数字证书就相当于社会中的**[**身份证**](https://baike.baidu.com/item/%E8%BA%AB%E4%BB%BD%E8%AF%81/113951)**，用户在进行**[**电子商务**](https://baike.baidu.com/item/%E7%94%B5%E5%AD%90%E5%95%86%E5%8A%A1/98106)**活动时可以通过数字证书来证明自己的身份，并识别对方的身份。又称公开密钥认证（英语：Public key certificate）或身份证书（identity certificate）。是用于公开密钥基础建设的电子文件，用来证明公开密钥拥有者的身份。证书实际是由证书签证机关（CA）签发的对用户的公钥的认证。它将**[**公钥**](https://baike.baidu.com/item/%E5%85%AC%E9%92%A5/6447788)**的值绑定到持有对应**[**私钥**](https://baike.baidu.com/item/%E7%A7%81%E9%92%A5/8973452)**的个人、设备或服务的身份。简而言之，认证机构用自己的私钥对需要认证的人（或组织机构）的公钥施加数字签名并生成证书，即证书的本质就是对公钥施加数字签名。**

CA中心：CA中心又称CA机构，即[证书授权中心](https://baike.baidu.com/item/%E8%AF%81%E4%B9%A6%E6%8E%88%E6%9D%83%E4%B8%AD%E5%BF%83/123838)(Certificate Authority )，或称证书授权机构，作为电子商务交易中受信任的第三方，承担公钥体系中公钥的合法性检验的责任。

**（2）密钥备份和恢复**

在一个PKI(Public Key Infrastructure，公开密钥体系）系统中，维护密钥对的备份至关重要，如果没有这种措施，当密钥丢失后，将意味着加密数据的完全丢失，对于一些重要数据，这将是灾难性的。所以，密钥的备份和恢复也是PKI密钥管理中重要的一环。换句话说，即使密钥丢失，使用PKI的企业和组织必须仍能够得到确认，受密钥加密保护的重要信息也必须能够恢复。当然，这不能让一个独立的个人完全控制最重要的主密钥，否则将引起严重后果。

PKI：公开密钥基础建设（英语：Public Key Infrastructure，[缩写](https://www.wanweibaike.com/wiki-%E7%B8%AE%E5%AF%AB)：PKI），又称公开密钥基础架构、公钥基础建设、公钥基础设施、公开密码匙基础建设或公钥基础架构，是一组由硬件、软件、参与者、管理政策与流程组成的基础架构，其目的在于创造、管理、分配、使用、存储以及撤销[数字证书](https://www.wanweibaike.com/wiki-%E6%95%B8%E4%BD%8D%E6%86%91%E8%AD%89)。

PKI的组成要素主要有:用户（使用PKI的人或机构）；[认证机构](https://www.wanweibaike.com/wiki-%E8%AA%8D%E8%AD%89%E6%A9%9F%E6%A7%8B)（Certification Authority,CA）（颁发证书的人或机构）；仓库（保存证书的[数据库](https://www.wanweibaike.com/wiki-%E6%95%B0%E6%8D%AE%E5%BA%93)）。用户和认证机构称之为实体。[[2]](https://www.wanweibaike.com/wiki-%E5%85%AC%E9%96%8B%E9%87%91%E9%91%B0%E5%9F%BA%E7%A4%8E%E5%BB%BA%E8%A8%AD#cite_note-2)

**（3）密钥更新**

如果用户可以一次又一次地使用同样的密钥与别人交换信息，那么密钥也同其他任何密码一样存在着一定的安全性，虽然说用户的私钥是不对外公开的，但是也很难保证私钥长期的保密性，很难保证长期以来不被泄露。

对每一个由CA颁发的证书都会有有效期，密钥对生命周期的长短由签发证书的CA中心来确定，各CA系统的证书的有效期限有所不同，一般为2-3年。当用户的私钥被泄露或证书的有效期快到时，用户应该更新私钥。这时用户可以废除证书，产生新的密钥对，申请新的证书。

**（4）多密钥的管理**

Kerberos建立了一个安全的、可信任的密钥分发中心（Key Distribution Center,KDC）,每个用户只要知道一个和KDC进行会话的密钥就可以了，而不需要知道成百上千个不同的密钥。

### 2.认证技术

**解决问题：**认证技术主要解决网络通信过程中通信双方的身份认可。

**认证过程：**涉及加密和密钥交换。

**加密使用方法：**通常加密可使用对称加密、不对称加密及两种加密方法的混合方法。

**认证方：**一般有账户名/口令认证、使用摘要算法认证和基于PKI的认证。

**PKI：**是一种遵循既定标准的密钥管理平台，能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系。简单来说，PKI就是利用公钥理论和技术建立的提供安全服务的基础设施。

**数字签名：**数字签名（又称[公钥](https://baike.baidu.com/item/%E5%85%AC%E9%92%A5)数字签名）是只有信息的发送者才能产生的别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。它是一种类似写在纸上的普通的物理签名，但是使用了[公钥加密](https://baike.baidu.com/item/%E5%85%AC%E9%92%A5%E5%8A%A0%E5%AF%86/6245950)领域的技术来实现的，用于鉴别数字信息的方法。简单地说，所谓数字签名就是**附加在**[**数据单元**](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%8D%95%E5%85%83)**上的一些数据**，或是对数据单元所作的[密码](https://baike.baidu.com/item/%E5%AF%86%E7%A0%81)变换。这种数据或变换允许[数据单元](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%8D%95%E5%85%83)的接收者用以确认数据单元的来源和数据单元的完整性并保护数据，防止被人(例如接收者)进行伪造。

**PKI基础技术：**包括加密、数字签名、数据完整性机制、数字信封和双重数字签名等

**完整的PKI系统基本构成部分：**权威认证机构（CA）、数字证书库、密钥备份及恢复系统、证书作废系统、应用接口等

**（1）认证机构**

即数字证书的申请及签发机关，CA必须具备权威性的特征。

**（2）数字证书库**

用于存储已签发的数字证书及公钥，用户可由此获得所需的其他用户的证书及公钥。

**（3）密钥备份及恢复系统**

如果用户丢失了用于解密数据的密钥，则数据将无法被解密，这将造成合法数据丢失。为了避免这种情况，PKI提供了备份与恢复密钥的机制。但须注意，密钥的备份与恢复必须由可信的机构来完成。并且，密钥备份与恢复**只能针对解密密钥**，签名私钥为确保其唯一性而不能够作备份。

**（4）证书作废系统**

证书作废处理系统是PKI的一个必备组件。与日常生活中的各种身份证件一样，证书在有效期内也可能需要作废，原因可能是密钥介质丢失或用户身份变更等。为实现这一点，PKI必须提供作废证书的一系列机制。

**（5）应用接口**

PKI的价值在于使用户能够方便地使用加密、数字签名等安全服务，因此一个完整的PKI必须提供良好的应用接口系统，使得各种各样的应用能够以安全、一致、可信的方式与PKI交互，确保安全网络环境的完整性和易用性。

从大的方面来说，所有提供公钥加密和数字签名服务的系统都可归结为PKI系统的一部分，PKI的主要目的是通过自动管理密钥和证书为用户建立起一个安全的网络运行环境，使用户可以在多种应用环境下方便地使用加密和数字签名技术，从而保证网上数据的机密性、完整性和有效性。

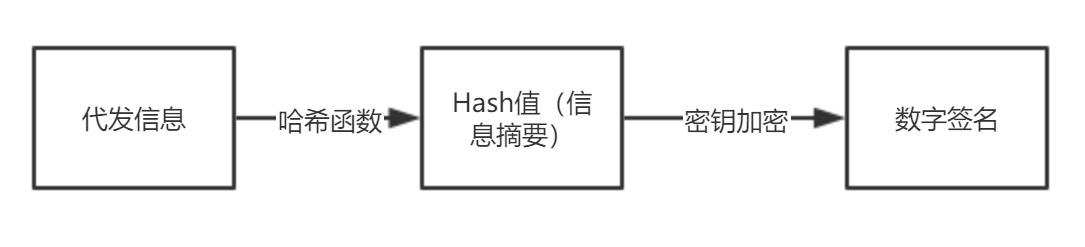


图 2hash值与数字签名

#### 1)Hash函数与信息摘要

**Hash函数提供了这样一种计算过程：**输入一个长度不固定的字符串，返回一串固定长度的字符串，又称Hash值。单向Hash函数用于产生信息摘要。

**Hash函数解决问题：一、**在某一特定的时间内，无法查找经Hash操作后生成特定Hash值的原报文。**二、**无法查找两个经Hash操作后生成相同Hash值的不同报文。

这样，在数字签名中就可以解决验证签名和用户身份验证、不可抵赖性的问题。

**信息摘要：**简要地描述了一份较长的信息或文件，它可以被看作一份长文件的“数字指纹”。信息摘要用于创建数字签名，对于特定的文件而言，信息摘要是唯一的。信息摘要可以被公开，它不会透露相应文件的任何内容。

**MD5（MD表示信息摘要）：**是专门用于加密处理的并被广泛使用的Hash函数。它以512位分组来处理输入的信息，且每一分组又被划分为16个32位子分组，经过了一系列的处理后，算法的输出由四个32位分组组成，将这四个32位分组级联后将生成一个128位散列值。

**MD5算法的特点：**

1. **压缩性：**任意长度的数据，算出的MD5值长度都是固定的。
2. **容易计算：**从原数据计算出MD5值很容易。
3. **抗修改性：**对原数据进行任何改动，即使只修改1个字节，所得到的MD5值都有很大区别。
4. **强抗碰撞：**已知原数据和其MD5值，想找到一个具有相同MD5值的数据（即伪造数据）是非常困难的。

#### 2)数字签名

数字签名经过以下几个过程：

1. 信息发送者使用一个单向散列函数（Hash函数）对信息生成信息摘要。
2. 信息发送者使用自己的私钥签名信息摘要。
3. 信息发送者把信息本身和已签名的信息摘要一起发送出去。
4. 信息接收者通过使用与信息发送者使用的同一个单向散列函数（Hash函数）对接收的信息本身生成新的信息摘要，再使用信息发送者的公钥对信息摘要进行验证，以确认信息发送者的身份和信息是否被修改过。

数字加密经过以下几个过程。

（1）当信息发送者需要发送信息时，首先生成一个对称密钥，用该对称密钥加密要发送的报文。

（2）信息发送者用信息接收者的公钥加密上述对称密钥。

（3）信息发送者将第（1）步和第(2）步的结果结合在一起传给信息接收者，称为数字信封。

（4）信息接收者使用自己的私钥解密被加密的对称密钥，再用此对称密钥解密被发送方加密的密文，得到真正的原文。

**数字签名和数字加密：**它们的过程虽然都使用公开密钥体系，但实现的过程正好相反，使用的密钥对也不同。数字签名使用的是发送方的密钥对，发送方用自己的私有密钥进行加密，接收方用发送方的公开密钥进行解密，这是一个一对多的关系，任何拥有发送方公开密钥的人都可以验证数字签名的正确性。数字加密则使用的是接收方的密钥对，这是多对一的关系，任何知道接收方公开密钥的人都可以向接收方发送加密信息，只有唯一拥有接收方私有密钥的人才能对信息解密。另外，数字签名只采用了非对称密钥加密算法；而数字加密采用了对称密钥加密算法和非对称密钥加密算法相结合的方法。

#### 3)SSL协议

**SSL协议作用：**用于提高应用程序之间数据的安全系数。

**SSL协议整体概念总结：**一个保证任何安装了安全套接字的客户和服务器间事务安全的协议，它涉及所有TCP/IP应用程序。

**TCP/IP协议族：**是应用最广泛的通信协议集合，包括大量的Internet应用中的标准协议支持跨网络架构、跨操作系统平台的通信

**SSL协议主要提供以下三方面的服务：**

1. 用户和服务器的合法性认证。
2. 加密数据以隐藏被传送的数据。
3. 保护数据的完整性。

**安全套接层协议：**是一个保证计算机通信安全的协议，对通信对话过程进行安全保护。

**安全套接层协议过程：**

1. 接通阶段。客户端通过网络向服务器打招呼，服务器回应。
2. 密码交换阶段。客户端与服务器之间交换双方认可的密码，一般选送RSA密码算法，也有的选用Diffie-Hellmanf和Fortezza-KEA密码算法。
3. 会谈密码阶段。客户端与服务器间产生彼此交谈的会谈密码。
4. 检验阶段。客户端检验服务器取得的密码。
5. 客户认证阶段。服务器验证客户端的可信度。
6. 结束阶段。客户端与服务器之间相互交换结束的信息。

当上述动作完成之后，两者间的资料传送就会加密，另外一方收到资料后，再将编码资料还原。

发送时，信息用对称密钥加密，对称密钥用非对称算法加密，再把两个包绑在一起传送过去。接受的过程与发送正好相反，先打开有对称密钥的加密包，再用对称密钥解锁。

#### 4)数字时间戳技术

数字时间戳是数字签名技术的一种变种应用。在电子商务交易文件中，时间是十分重要的信息。在书面合同中，文件签署的日期和签名一样均是十分重要的防止文件被伪造和篡改的关键性内容。

**数字时间戳服务（Digital Time Stamp Service，DTS）：**是网上电子商务安全服务项目之一，能提供电子文件的日期和时间信息的安全保护。

时间戳是一个经加密后形成的凭证文档，包括如下3个部分：

1. 需加时间戳的文件的摘要（Digest）。
2. DTS收到文件的日期和时间。
3. DTS的数字签名。

**时间戳产生过程：**用户首先将需要加时间戳的文件用Hash编码加密形成摘要，然后将该摘要发送到DTS，DTS在加入了收到文件摘要的日期和时间信息后再对该文件加密（数字签名），然后送回用户。

书面签署文件的时间是由签署人自己写上的，而数字时间戳则是由认证单位DTS来加入的，以DTS收到文件的时间为依据。

## 1.3.3计算机可靠性

### 1.计算机可靠性概述

**计算机系统硬件故障原因：**通常是由元器件的失效引起的。

**元器件可靠性分为三个阶段：**

1. 开始阶段，元器件的工作处于不稳定期，失效率较高。
2. 第二阶段，元器件进入正常工作期，失效率最低，基本保持常数。
3. 第三阶段，元器件开始老化，失效率又重新提高。

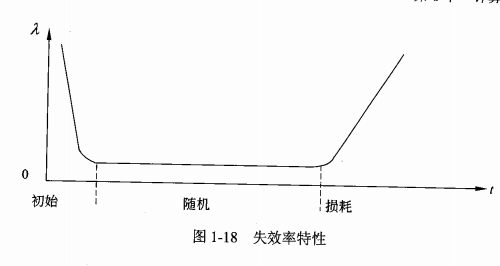
因此，应保证在计算机中使用的元器件处于第二阶段。在第一阶段应对元器件进行老化筛选，而到了第三个阶段，则淘汰该计算机。

**计算机系统的可靠性：**指从它开始运行（t=0）到某时刻t这段时间内能正常运行的概率，用R(t)表示。

**失效率：**是指单位时间内失效的元件数与元件总数的比例，用λ表示，当λ为常数时，可靠性与失效率的关系为：

R（t）=e-λt

典型的失效率与时间的关系曲线如图所示。



两次故障之间系统能正常工作的时间的平均值称为平均无故障时间（MTBF），即

MTBF=1/λ

通常用平均修复时间（MTRF）来表示计算机的可维修性，即计算机的维修效率，指从故障发生到机器修复平均所需要的时间。计算机的可用性是指计算机的使用效率，它以系统在执行任务的任意时刻能正常工作的概率A来表示，即

A=

计算机的RAS是指用可靠性R、可用性A和可维修性S这3个指标衡量一个计算机系统。

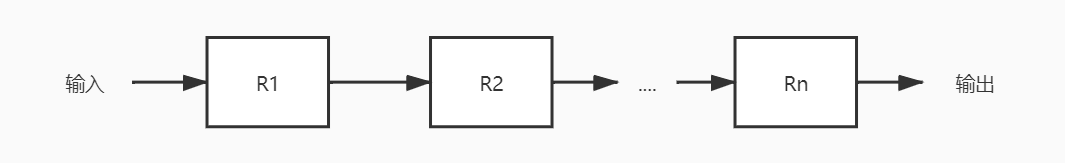
实际应用中，引起计算机故障的原因除了元器件以外还有组装工艺、逻辑设计等因素。因此，不同厂家生产的兼容机即使采用相同的元器件，其可靠性及MTBF也可能相差很大。

### 2.计算机可靠性模型

**常见的系统可靠性数学模型有以下三种：**

#### 1)串联系统

**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。



图：串联系统的可靠性模型

设系统中各个子系统的可靠性分别用R1,R2，...,Rn来表示，则系统的可靠性R可由下式求得。

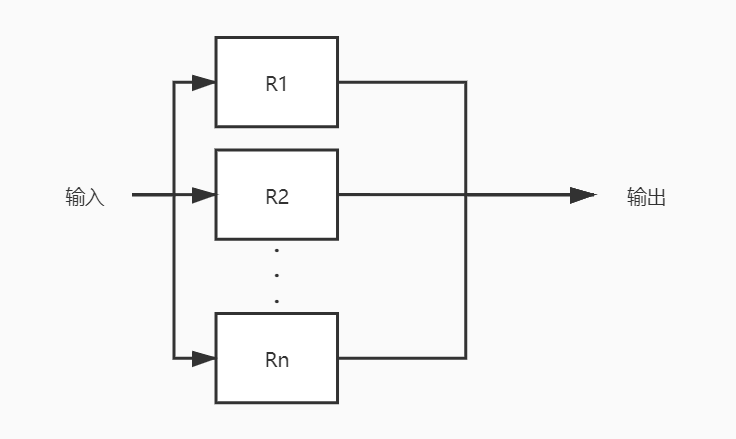
R=R1R2…Rn

如果各个系统的子系统的失效率分别用λ1，λ2，...，λn来表示，则系统的失效率λ可由下式求得。

λ=λ1+λ2+…+λn

#### 2)并联系统

**并联系统：**假如一个系统由N个子系统组成，只要有一个子系统正常工作，系统就能正常工作，这样的系统称为并联系统，如图所示。



图：并联系统的可靠性模型

设每个系统的可靠性分别为R1，R2，…，Rn表示，整个系统的可靠性可由下式求得。

R=1-(1-R1)(1-R2)…(1-Rn)

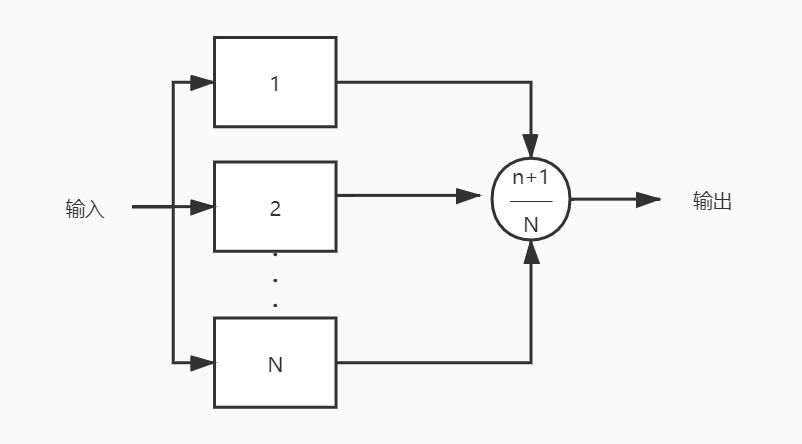
假设所有子系统的失效率均为λ，则系统的失效率μ为：

μ=

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)N模冗余系统

N模冗余系统由N个（N=2n+1）相同的子系统和一个表决器组成，表决器把N个子系统中占多数相同结果的输出作为系统的输出，如图所示。



图：N模冗余系统

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

R=Ri0（1-R0）N-i

其中，

**提高计算机的可靠性一般有两项措施：**

1. 提高元器件质量，改进加工工艺与工艺结构，完善电路设计。
2. 发展容错技术，使得在计算机硬件有故障的情况下，计算机仍能继续运行，得出正确的结果。

## 1.3.4计算机系统的性能评价

### 1.性能评测的常用方法

#### 1)时钟频率

**特点：**计算机的时钟频率在一定程度上反映了机器速度，一般来讲，主频越多，速度越快。**局限性：**相同频率、不同体系结构的机器，其速度可能会相差很多，因此还需要用其他方法来测定机器性能。

#### 2)指令执行速度

在计算机发展初期，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以反映出乘法、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被设计成与加法指令相同，因此加法指令的运算速度有一定的代表性。当时表征机器运算速度的单位是KIPS（每秒千条指令），后来随着机器运算速度的提高，计量单位发展到MIPS（每秒百万条指令）。

另一种描述计算机指令执行速度的指标是每秒钟执行浮点数的百万次操作的数量MELOPS。

#### 3)等效指令速度法

**诞生原因：**随着计算机指令系统的发展，指令的种类大大增加，用单种指令的MIPS值来表征机器的运算速度的局限性日益暴露，因此出现了吉普森混合法或等效指令速度法等改进的办法。

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在程序中所占的比例为wi，执行时间为ti，则等效指令的执行时间为：

T=

其中，n为指令的种类数。

#### 4)数据处理速度（Processing Data Rate，PDR）法

**诞生原因：**因为在不同程序中，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、流水线和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，而且与指令的执行顺序与地址分布有关。

PDR法采用计算PDR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以及每条指令的平均运算速度有关，其计算方法如下：

PDR=L/R

其中，L=0.85G+0.15H+0.4J+0.15K,R=0.85M+0.09N+0.06P。

式中：G——每条定点指令的位数；

M——平均定点加法时间；

H——每条浮点指令的位数；

N——平均浮点加法时间；

J——定点操作数的位数；

P——平均浮点乘法时间；

K——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、多功能部件等技术对性能的影响。

#### 5)核心程序法

**诞生原因：**上述性能评价方法主要是针对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，但是核心程序各部分之间的联系较小。

### 2.基准测试程序

**基准程序法中的基准程序：**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。

#### 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及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。

Dhrystone程序测试的结果由每秒多少个Dhrystones来表示机器的性能，这个数值越大，性能越好。

#### 2)浮点测试程序

在科学计算和工程应用领域内，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，而大部分工作站则标出用Linpack和Whetstone基准程序测得的浮点性能。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。

##### 理论峰值浮点速度

巨型机和小巨型机在说明书中经常给出“理论峰值速度”的MELOPS值，它不是机器实际执行程序时的速度，而是机器在理论上最大能完成的浮点处理速度。它不仅与处理机时钟周期有关，而且还与一个处理机里能并行执行操作的流水线功能部件数目和处理机的数目有关。多个CPU机器的峰值速度是单个CPU的峰值速度与CPU个数的乘积。

##### Linpack基准测试程序

Linpack基准程序是一个用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。

##### （3）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。

#### 3)SPEC基准程序

SPEC原来主要测试CPU性能，现在则强调开发能反映真实应用的基准测试程序集，并已推广至测试高性能计算机系统、网络服务器上商业应用服务器等。

#### 4)TPC基准程序

用于评测计算机在事务处理、数据库处理、企业管理与决策支持系统等方面的性能。

TPC基准测试程序在商业界范围内建立了用于衡量机器性能以及性能价格比的标准。但是，任何一种测试程序都有一定的适用范围，TPC也不例外。