第 8 章：存储器系统　　作者：希赛教育软考学院　来源：希赛网　2014年01月27日

主存储器

8.1.1 主要知识点

主存储器也就是我们简称的主存或内存，根据工艺和技术不同，可分为下列几种。

RAM（Random Access Memory）：RAM存储器既可以写入也可以读出，但断电后信息无法保存，因此只能用于暂存数据。RAM又可分为 DRAM和 SRAM两种。

?DRAM（Dynamic RAM）：信息会随时间逐渐消失，因此需要定时　　刷新，维持信息不丢失。

?SRAM（Static RAM）：在不断电的情况下信息能够一直保持而不会丢失。

DRAM的密度大于 SRAM且更加便宜，但 SRAM速度快，电路简单（无须刷新电路），然而容量小，价格高。

ROM（Read Ony Memory）：只读存储器，信息已固化在存储器中。ROM出厂时其内容由厂家用掩膜技术（Mask）写好，只可读出，但无法改写。一般用于存放系统程序BIOS和用于微程序控制。

PROM（Programmabe ROM）：可编程 ROM,只能进行一次写入操作（与 ROM相同），但是可以在出厂后，由用户使用特殊电子设备进行写入。

EPROM（Erasabe PROM）：可擦除的 PROM,其中的内容既可以读出，也可以写入。但是在一次写操作之前必须用紫外线照射 15~20分钟以擦去所有信息，然后再写入，可以写多次。

E2PROM（Eectricay EPROM）：电可擦除EPROM,与 EPROM相似，可以读出也可写入，而且在写操作之前，不需要把以前内容先擦去。能够直接对寻址的字节或块进行修改，只不过写操作所需的时间远远大于读操作所需时间（每字节需几百ms），其集成度也较低。

闪速存储器（Fash Memory）：其性能介于 EPROM与 E2PROM之间。与E2PROM相似，可使用电信号进行删除操作。整块闪速存储器可以在数秒内删除，速度远快于EPROM;而且可以选择删除某一块而非整块芯片的内容，但还不能进行字节级别的删除操作。集成度与 EPROM相当，高于E2PROM.闪速存储器有时也简称为闪存。

相联存储器（Content Addressabe Memory,CAM）：CAM是一种特殊的存储器，是一种基于数据内容进行访问的存储设备 CAM.当对其写入数据时，CAM能够自动选择一个未用的空单元进行存储；当要读出数据时，不是给出其存储单元的地址，而是直接给出该数据或者该数据的一部分内容，CAM对所有的存储单元中的数据同时进行比较并标记符合条件的所有数据以供读取。由于比较是同时、并行进行的，所以这种基于数据内容进行读写的机制，其速度比基于地址进行读写的方式要快许多。

辅助存储器

8.2 辅助存储器

辅助存储器用于存放当前不需要立即使用的信息，一旦需要，再和主机成批交换数据，是主存储器的后备，因此称之为辅助存储器；它又是主机的外围设备，又称之为"外存储器".辅助存储器的最大特点是存储器容量大、可靠性高、价格低。常用的辅助存储器有磁带存储器、磁盘存储器和光盘存储器。

上一节 本书简介 下一节

磁带存储器

8.2.1 磁带存储器

磁带存储设备是一种顺序存取的设备，存取时间较长，但存储容量大，便于携带，价格便宜，所以也是一种主要的辅助存储器。磁带的内容由磁带机进行读写（最便宜也最慢）。按磁带机的读写方式主要可以分为两种，启停式和数据流。

启停式磁带机按带宽可以分为1/4英寸、1/2英寸和1英寸3种。磁带上的信息以文件块的形式存放。整盘磁带的开始有一卷标标明，然后有一初始空白块，用以适应磁带从静止到稳定带速所需的时间。文件记录以文件头标志和文件尾标志标识，一个文件由若干数据块组成，每一数据块又由若干记录组成（一个数据块所包括的记录条数叫块因子）。数据块之间以空白块进行分隔，文件之间也存在一段空隙。所有的文件都顺序地排列在磁带上，一个文件的长度不仅包括记录信息，也包括块间间隔。磁带机每一次读写信息的位数与磁带表面并行记录信息的磁道数有关：如7道、9道和16道，则分别有7、9、16个磁头并列，一次可以读写7位、9位或16位。

数据流磁带机结构简单，价格低，数据传输速率快。其记录格式是串行逐道记录信息，每次读写1位信息，数据连续地写在磁带上，数据块之间以空隙分隔。磁带机不能在块间启停。读写顺序如下：（4个磁道）先从0道的首端（BOT）开始，到其末端（EOT）；然后第1道反向记录从EOT到BOT,而2道又正向从 BOT到 EOT,3道再反向。

上一节 本书简介 下一节

磁盘存储器

8.2.2 磁盘存储器

磁盘上的数据都存放于磁道上。磁道就是磁盘上的一组同心圆，其宽度与磁头的宽度相同。为了避免减小干扰，磁道与磁道之间要保持一定的间隔（inter-track gap），沿磁盘半径方向，单位长度内磁道的数目称之为道密度（道/英寸，TPI），最外层为0道。

沿磁道方向，单位长度内存储二进制信息的个数叫位密度。为了简化电路设计，每个磁道存储的位数都是相同的，所以其位密度也随着从外向内而增加。磁盘的数据传输是以块为单位的，所以磁盘上的数据也以块的形式进行存放。这些块就称为扇区（sector），每个磁道通常包括10~100个扇区。同样为了避免干扰，扇区之间也相互留有空隙（inter–sector gap）。柱面是若干个磁盘组成的磁盘组，所有盘面上相同位置的磁道组称为一个柱面（每个柱面有n个磁道）；若每个磁盘有m个磁道，则该磁盘组共有m个柱面。

磁盘的非格式化容量为Cn=w×3.14×d×m×n,其中w为位密度，d为最内圈直径（内径，本题为200mm），m为记录面数，n为每面磁道数。

磁盘格式化后能够存储有用信息的总量。存储容量=n×t×s×b,其中：n为保存数据的总盘面数；t为每面磁道数；s为每道的扇区数；b为每个扇区存储的字节数。

磁盘的存取时间包括寻道时间和等待时间。寻道时间（查找时间，Seek Time）为磁头移动到目标磁道所需的时间（movabe–head disk），对于固定磁头磁盘而言，无须移动磁头，只需选择目标磁道对应的磁头即可。等待时间为等待读写的扇区旋转到磁头下方所用的时间。一般选用磁道旋转一周所用时间的一半作为平均等待时间。寻道时间由磁盘机的性能决定，目前主流硬盘典型的AST（Average Seek Time）一般在10ms左右，而转速则有2400rpm,5400rpm,7200rpm,等等。软盘转速较慢，一般只有360rpm（因为磁头与盘面接触性读写）。

磁盘的数据传输速率是指磁头找到地址后，单位时间写入或读出的字节数。R=TB/T,其中：TB为一个磁道上记录的字节数，T为磁盘每转一圈所需的时间，R为数据传输速率。

上一节　本书简介　下一节

作者：希赛教育软考学院　来源：希赛网　2014年01月27日

RAID存储器

8.2.3 RAID存储器

廉价磁盘冗余阵列（Redundant Array Of Inexpensive Disks,RAID）技术旨在缩小日益扩大的CPU速度和磁盘存储器速度之间的差距。其策略是用多个较小的磁盘驱动器替换单一的大容量磁盘驱动器，同时合理地在多个磁盘上分布存放数据以支持同时从多个磁盘进行读写，从而改善了系统的 I/O性能。小容量驱动器阵列与大容量驱动器相比，具有成本低，功耗小，性能好等优势；低代价的编码容错方案在保持阵列的速度与容量优势的同时保证了极高的可靠性。同时也较容易扩展容量。但是由于允许多个磁头同时进行操作以提高I/O数据传输速度，因此不可避免地提高了出错的概率。

为了补偿可靠性方面的损失，RAID使用存储的校验信息（Stored Parity Information）来从错误中恢复数据。最初，inexpensive一词主要针对当时另一种技术（Singe arge Expensive

Disk,SED）而言，但随着技术的发展，SED已是昨日黄花，RAID和non-RAID皆采用了类似的磁盘技术。因此，RAID现在代表独立磁盘冗余阵列（redundant array of independent disks），用independent来强调RAID技术所带来的性能改善和更高的可靠性。

RAID机制中共分6个级别，工业界公认的标准分别为RAID0~RAID5,RAID应用的主要技术有分块技术、交叉技术和重聚技术。

RAID0级（无冗余和无校验的数据分块）：具有最高的I/O性能和最高的磁盘空间利用率，易管理，但系统的故障率高，属于非冗余系统，主要应用于那些关注性能、容量和价格而不是可靠性的应用程序。

RAID1级（磁盘镜像阵列）：由磁盘对组成，每一个工作盘都有其对应的镜像盘，上面保存着与工作盘完全相同的数据拷贝，具有最高的安全性，但磁盘空间利用率只有50%.RAID1主要用于存放系统软件、数据，以及其他重要文件。它提供了数据的实时备份，一旦发生故障，所有的关键数据即刻就可使用。

RAID2级（采用纠错海明码的磁盘阵列）：采用了海明码纠错技术，用户需增加校验盘来提供单纠错和双验错功能。对数据的访问涉及到阵列中的每一个盘。大量数据传输时I/O性能较高，但不利于小批量数据传输，实际应用中很少使用。

RAID3和RAID4级（采用奇偶校验码的磁盘阵列）：把奇偶校验码存放在一个独立的校验盘上。如果有一个盘失效，其上的数据可以通过对其他盘上的数据进行异或运算得到。读数据很快，但因为写入数据时要计算校验位，速度较慢。

RAID5（无独立校验盘的奇偶校验码磁盘阵列）：与RAID4类似，但没有独立的校验盘，校验信息分布在组内所有盘上，对于大、小批量数据读写性能都很好。RAID4和RAID5使用了独立存取（Independent Access）技术，阵列中每一个磁盘都相互独立地操作，所以I/O请求可以并行处理。所以，该技术非常适合于I/O请求率高的应用而不太适应于要求高数据传输率的应用。与其他方案类似，RAID4、RAID5也应用了数据分块技术，但块的尺寸相对大一点。

　作者：希赛教育软考学院　来源：希赛网　2014年01月27日

光盘存储器

8.2.4 光盘存储器

光盘存储器是利用激光束在记录表面存储信息，根据激光束的反射光来读出信息。光盘存储器主要有CD、CD-ROM、CD-I、DVI、WORM、DVD,以及EOD（Erasable Optical Disk）。

CD-ROM的读取目前有3种方式：恒定角速度、恒定线速度和部分恒定角速度。

CD-ROM非常适用于把大批量数据分发给大量的用户。与传统磁盘存储器相比，有以下优点：具有更大的容量，可靠性高，光盘的复制更简易，可更换，便于携带；其缺点是只读，存取时间比较长。

DVD-ROM技术类似于CD-ROM技术，但是可以提供更高的存储容量。DVD可以分为单面单层、单面双层、双面单层和双面双层四种物理结构。DVD与CD/VCD的主要技术参数比较如表8-1所

示。

表8-1 DVD于CD/VCD的主要技术参数比较

技 术 手 段	CD/VCD	DVD
镜数值孔径 na	0.45	0.6
影像质量	240 线	540～720 线
影音质量	16 比特	24 比特，96kHz
纠错编码冗余度	31%	15.4%
通道码调制方式	8/17 调制	8/16 调制
激光波长λ	780nm	650nm/635nm
光斑直径	1.74μm	1.08μm
道间距	1.6μm	0.74μm
技 术 手 段	CD/VCD	DVD
凹坑最小长度	0.83μm	0.4μm
凹坑宽度	0.6μm	0.4μm
容量	650MB	17GB（单层单面）

上一节 本书简介 下一节

作者：希赛教育软考学院 来源：希赛网 2015年08月17日

Cache存储器

8.3.1 主要知识点

Cache（高速缓冲存储器）的功能是提高CPU数据输入/输出的速率，突破所谓的"冯·诺依曼瓶颈",即CPU与存储系统间数据传送带宽限制。高速存储器能以极高的速率进行数据的访问，但因其价格高昂，如果计算机的主存储器完全由这种高速存储器组成则会大大增加计算机的成本。通常在CPU和主存储器之间设置小容量的高速存储器 Cache.Cache容量小但速度快，主存储器速度较低但容量大，通过优化调度算法，系统的性能会大大改善，其存储系统容量与主存相当，而访问速度近似Cache.在计算机的存储系统体系中，Cache是访问速度最快的层次。

使用Cache改善系统性能的依据是程序的局部性原理（有关此原理的详细情况，请读者阅读"操作系统"相关章节）。依据局部性原理，把主存储器中访问概率高的内容存放在Cache中，当CPU需要读取数据时就首先在Cache中查找是否有所需内容，如果有则直接从cache中读取；若没有再从主存中读取该数据，然后同时送往CPU和Cache.如果CPU需要访问的内容大多都能在Cache中找到（称为访问命中，hit），则可以大大提高系统性能。

如果以p代表对 Cache的访问命中率，t1表示 cache的周期时间，t2表示主存储器周期时间，以读操作为例，使用"Cache+主存储器"的系统的平均周期为t3,则：t3=p×t1+（1–p）×t2.其中，（1–p）又称为失效率（未命中率）。

系统的平均存储周期与命中率有很密切的关系，命中率的提高即使很小，也能导致性能上的较大改善。

当CPU发出访问请求后，存储器地址先被送到Cache控制器以确定所需数据是否已在Cache中，若命中则直接对Cache进行访问。这个过程称为Cache的地址映射。常见的映射方法有直接映射、全相联映射和组相联映射。

当Cache存储器产生了一次访问未命中之后，相应的数据应同时读入CPU和Cache.但是当Cache已存满数据后，新数据必须淘汰Cache中的某些旧数据。最常用的淘汰算法有随机淘汰法、先

进先出法（FIFO）和近期最少使用淘汰法（RU）。

因为需要保证缓存在Cache中的数据与主存中的内容一致，相对读操作而言，Cache的写操作比较复杂，常用的有以下几种方法。

写直达（write through）：当要写Cache时，数据同时写回主存储器，有时也称为写通。

写回（write back）：CPU修改Cache的某一行后，相应的数据并不立即写入主存储器单元。而是当该行从Cache中被淘汰时，才把数据写回到主存储器中。

标记法：对Cache中的每一个数据设置一个有效位。当数据进入Cache后，有效位置1;而当CPU要对该数据进行修改时，数据只需写入主存储器并同时将该有效位清0。当要从Cache中读取数据时需要测试其有效位：若为1 则直接从Cache中取数，否则从主存中取数。

第 8 章：存储器系统　作者：希赛教育软考学院　来源：希赛网　2014年01月27日

例题分析

8.4 例题分析

例题1（2002年试题56）

设某流水线计算机主存的读/写时间为 00ns,有一个指令和数据合一的 Cache,已知该Cache的读/写时间为 0ns,取指令的命中率为 98%,取数的命中率为 95%.在执行某类程序时，约有 1/5 指令需要存/取一个操作数。假设指令流水线在任何时候都不阻塞，则设置Cache 后，每条指令的平均访存时间约为 （56）.

（56）A.12ns B.15ns C.18ns D.120ns

例题分析：

这其实是一道简单的数学计算题。根据题意，98%的取指令操作需10ns,2%的取指令操作需100ns;取指令操作数时95%需10ns,5%的存/取操作数需要100ns,并且只有1/5（20%）的指令需要存/取一个操作数。因此，设置Cache后，每条指令的平均访存时间为：

（2%×100+98%×10）+ 1/5×（5%×100+95%×10）= 14.7ns

例题答案：（56）B

例题2（2006年5月试题3~4）

高速缓存Cache与主存间采用全相联地址映像方式，高速缓存的容量为4MB,分为4块，每块1MB,主存容量为256MB.若主存读写时间为30ns,高速缓存的读写时间为3ns,平均读写时间为3.27ns,则该高速缓存的命中率为 （3） %.若地址变换表如下所示，则主存地址为8888888H时，高速缓存地址为 （4） H.

（3）A.90　B.95　C.97　D.99

（4）A.488888　B.388888　C.288888　D.188888

例题分析：

第（3）空是一个简单的计算题。我们设高速缓存的命中率为（t）。

则：

30×（1-t）+3×t=3.27

解方程得：t=0.99.所以高速缓存的命中率为99%.

接下来看第（4）空，由于高速缓存的容量为：4MB,分为4块。所以把高速缓存的22位长地址划分为两部分，块号为2位，而块内地址为20位。主存容量为：256MB,所以主存地址长度为：28位。这样主存的块号为：8位，块内地址为20位。此时我们先将主存地址8888 888H化为二进制数：1000 1000 1000 1000 1000 1000 1000,其中斜体为块号：88H,加粗部分为块内地址：88888.查表得到Cache对应块号为：1H,所以高速缓存地址为：188888H.所以答案为D.

例题答案：（3）D（4）D

例题3（2002年试题58~60）

假设一个有3个盘片的硬盘，共有4个记录面，转速为7200转/分，盘面有效记录区域的外直径为30cm,内直径为 0cm,记录位密度为 250位/mm,磁道密度为 8道/mm,每磁道分16个扇区，每扇区512字节，则该硬盘的非格式化容量和格式化容量约为 （58），数据传输速率约为（59）.若一个文件超出一个磁道容量，剩下的部分（60）。

（58）A.120MB和1OOMB B.30MB和25MB

C.60MB和50MB D.22.5MB 和 25MB

（59）A.2 356Kb/s B. 3534Kb/s C.7 069Kb/s D. 1178Kb/s

（60）A.存于同一盘面的其他编号的磁道上 B.存于其他盘面的同一编号的磁道上

C.存于其他盘面的其他编号的磁道上 D.存放位置随机

例题分析：

对于这类试题，需要考生记住几个公式：

总磁道数 = 记录面数×磁道密度×（外直径–内直径）/2

非格式化容量 = 位密度×3.14×最内圈直径×总磁道数

格式化容量 = 每道扇区数×扇区容量×总磁道数

平均数据传输速率 =位密度×3.14×最内圈直径×盘片转速

另外，做这类试题时，一定要注意单位的换算。根据题目给定条件，我们可计算如下：

总磁道数 = 4×8×（30–10）/2×10 = 3200,（因为直径是以厘米为单位的，而道密度是以毫米为单位的，所以需要乘以10）。

非格式化容量=（250×3.14×10×10×3200）/8/1024/1024 = 29.95MB（因为括号中求出的单位是位，而8位为1字节，1MB=1024KB）。

格式化容量 =（16×512×3200）/1024/1024 = 25.07MB（因为括号中求出的单位是字节）。

平均数据传输速率 =（250×3.14×10×10） ×7200/60=1178Kb/s（因为括号中求出的单位是字节）。

根据硬盘存放数据的规则，在向磁盘记录一个文件时，应将文件尽可能记录在同一柱面（不同记录面上的同号磁道构成一个柱面）上，当一个柱面记录不下时，再记录到相邻柱面上。因此，当一个文件超出一个磁道容量时，剩下的部分应存于其他盘面的同一编号的磁道上，即同一柱面的其他磁道上。

例题答案：（58）B （59）D （60）B

例题4（2005年5月试题17）

页式存储系统的逻辑地址是由页号和页内地址两部分组成的。假定页面的大小为4KB,地址变换

过程如图8-1所示，图中逻辑地址用十进制数表示。

	地址变换表
0	38H
1	88H
2	59H
3	67H

图8-1 地址变换过程

图中有效地址经过变换后，十进制数物理地址a应为 （17） .

（17）A.33220 B.8644 C.4548 D.2500

例题分析：

此题考查的是虚拟存储中的页式存储，题目已知页面大小为4KB,因为4K=212,所以页内地址有12位。现在把逻辑地址8644转换成二进制数得：10 0001 1100 0100,这里的低12位为页内偏移量，最高两位则为页号，所以逻辑地址8644的页号为10,即十进制数的2,所以物理块号为8,化为二进制数得：1000.把物理块号和页内偏移地址拼合得：1000 0001 1100 0100,化为十进制得：33220.所以正确答案是A.

例题答案：A

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01月27日

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。

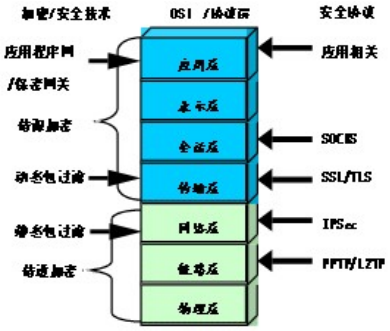

图9-1 网络安全技术层次结构图

上一节 本书简介 下一节

 作者：希赛教育软考学院 来源：希赛网 2014年03月13日

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。