ICS 35.020
L 80

中华人民共和国国家标准

GB 15852—1995
idt ISO/IEC 9797:1994

信息技术　安全技术　用块密码算法作密码校验函数的数据完整性机制

Information technology—Security techniques —Data integrity mechanism using a cryptographic check function employing a block cipher algorithm

1995-12-13发布　　1996-08-01实施

国家技术监督局　发布

前　言

本标准等同采用国际标准 ISO/IEC 9797:1994《信息技术　安全技术　用块密码算法作密码校验函数的数据完整性机制》。

该国际标准规定的用块密码算法作密码校验函数的数据完整性机制，适合于我国使用。

本标准的附录 A 是标准的附录。

本标准的附录 B 和附录 C 是提示的附录。

本标准由中华人民共和国电子工业部提出。

本标准由电子工业部标准化研究所归口。

本标准起草单位：电子工业部第三十研究所。

本标准主要起草人：龚奇敏、黄月江、吴世忠、杜明钰。

ISO/IEC 前言

ISO(国际标准化组织)和IEC(国际电工委员会)形成了一个世界范围内的标准化专门系统。ISO或IEC的成员国,通过由处理特殊技术活动领域的各个组织所建立的技术委员会来参与国际标准的开发。ISO和IEC的技术委员会在共同感兴趣的领域内合作,其他与ISO和IEC有联络的官方和非官方国际性组织,也参与这项工作。

在信息技术领域内,ISO和IEC已建立了一个联合技术委员会ISO/IEC JTC1。被联合技术委员会接受的国际标准草案分送给各成员国表决。一个国际标准的发布,需要至少75%的成员国投赞成票。

国际标准ISO/IEC 9797是由信息技术联合技术委员会ISO/IEC JTC1的IT安全技术SC 27分委员会制定的。

第二版取代其第一版(ISO/IEC 9797:1989),第一版已经过修改和扩充,增加了一种填充方法和一种可选进程,同时还增加了一个包含若干例子的新附录。

附录A是本国际标准的组成部分,附录B、C仅仅是一种信息。

引　言

本标准中规定的机制除了用 n 比特数据块的算法、m 比特的校验值和规定了一种附加的填充方法外，与 ISO 8731-1、ISO 9807 和 ANSI X9.9 标准中所用的相同。

ISO 8731-1、ANSI X9.9 和 ANSI X9.19 中叙述的密码校验值的计算方法是本标准的一种特殊情况，即当 $n=64$，$m=32$，采用 5.1 中规定的填充方法 1 以及使用 DEA（见 ANSI X3.92:1981）数据加密算法。

中华人民共和国国家标准

信息技术　安全技术　用块密码算法作密码校验函数的数据完整性机制

GB 15852—1995
idt ISO/IEC 9797:1994

Information technology—Security techniques —Data integrity mechanism using a cryptographic check function employing a block cipher algorithm

1　范围

本标准规定了一种使用密钥和 n 比特块密码算法计算 m 比特密码校验值的方法。这种方法可用作数据完整性机制，以检测数据是否已被非授权地改变。这种数据完整性机制的强度依赖于密钥的长度及其保密性，依赖于密码算法的特性以及校验值的长度 m。

本标准适用于任何安全体系结构、进程或应用的安全服务。

2　引用标准

下列标准所包含的条文，通过在本标准中引用而构成本标准的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB/T 9387.2—1995　信息处理系统　开放系统互连基本参考模型　第2部分：安全体系结构(idt ISO 7498—2:1989)

ISO/IEC 10116:1991　信息技术　n 位块密码算法的工作方式

3　定义和记法

3.1　定义

本标准使用了 GB/T 9387.2 和 ISO/IEC 10116 中定义的术语。

3.1.1　密码校验值　cryptographic check value

对数据单元进行加密变换所得到的信息。

3.1.2　数据完整性　data integrity

指数据没有被非授权地改变或破坏的性质。

3.1.3　n 比特块密码算法　n-bit block cipher algorithm

明文块和密文块长度均是 n 比特的块密码算法。

3.2　记法

本标准将密码校验值称作消息鉴别码(MAC)。

在本标准上下文中，当术语“最高有效位/字节”和“最低有效位/字节”具有某种含义时，例如，把比特串看成是数值，则一个块的最左边若干比特便是最高有效位。

4　要求

MAC 的长度(m)应小于或等于块的长度(n)，计算的结果和任何可选进程的结果都是长度为 n 的一个信息块，而最后 n 比特块的最左边 m 比特便形成了 MAC。

国家技术监督局1995-12-13批准　　1996-08-01实施