ICS 35.040
L 80

# 中华人民共和国国家标准

GB/T 15852.1—2008/ISO/IEC 9797-1:1999
代替 GB 15852—1995

# 信息技术　安全技术　消息鉴别码
# 第1部分:采用分组密码的机制

**Information technology—Security techniques—
Message Authentication Codes(MACs)—
Part 1:Mechanisms using a block cipher**

(ISO/IEC 9797-1:1999,IDT)

2008-07-02 发布　　2008-12-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

# 目　　次

# 前　言

GB/T 15852《信息技术　安全技术　消息鉴别码》分为2个部分：

——第1部分：采用分组密码的机制；

——第2部分：采用专用杂凑函数的机制。

本部分是GB/T 15852的第1部分，等同采用ISO/IEC 9797-1:1999《信息技术　安全技术　消息鉴别码　第1部分：采用分组密码的机制》。除对国际标准中笔误做了修改外，也做了编辑性的修改并更新了参考文献。

本部分是GB 15852—1995《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》的修订版。本部分代替GB 15852—1995。与GB 15852—1995相比较，本部分增加了一种填充方法和三种消息鉴别码(MAC)算法。GB 15852—1995附录A中的可选进程，在本部分中被调整到标准主体内。

本部分的附录A和附录B是资料性附录。

本部分由全国信息安全标准化技术委员会提出并归口。

本部分修订单位：中国科学院软件研究所、信息安全国家重点实验室。

本部分主要修订人：吴文玲、王鹏、张立廷、陈华。

本部分所代替标准历次版本发布情况：

——GB 15852—1995。

# 引　言

本部分规定的前三种 MAC 算法通常称作 CBC-MAC。在 ANSI X9.9 中所规定的 MAC 算法是本部分中 MAC 算法的一种特例(当 $n=64$、$m=32$ 时,使用 MAC 算法 1、填充方法 1 和分组密码 DEA(见 ANSI X3.92:1981))。在 ANSI X9.19 中所规定的 MAC 算法也是本部分中 MAC 算法的一种特例(当 $n=64$、$m=32$ 时,使用 MAC 算法 1 或 3、填充方法 1 和分组密码 DEA(见 ANSI X3.92:1981))。

第 4 种 MAC 算法是 CBC-MAC 的一个变种,它使用了一个特殊的初始变换。当 MAC 算法的密钥长度是分组密码密钥长度两倍的时候,建议使用 MAC 算法 4。

第 5 种 MAC 算法并行使用 MAC 算法 1,然后把所得到的两个结果相异或。

第 6 种 MAC 算法并行使用 MAC 算法 4,然后把所得到的两个结果相异或。

本部分例子中提及的分组密码均为举例性说明,具体使用时均须采用国家密码管理部门批准的相应分组密码。

# 信息技术　安全技术　消息鉴别码
# 第1部分:采用分组密码的机制

## 1　范围

GB/T 15852的本部分规定了六种采用分组密码的消息鉴别码算法。这些消息鉴别码算法可用作数据完整性检验,检验数据是否被非授权地改变。同样这些消息鉴别码算法也可用作消息鉴别,保证消息源的合法性。数据完整性和消息鉴别的强度依赖于密钥的长度及其保密性、分组密码的算法强度以及分组长度、消息鉴别码的长度和具体的消息鉴别码算法。

本部分适用于任何安全体系结构、进程及应用的安全服务。

## 2　规范性引用文件

下列文件中的条款通过GB/T 15852的本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分,然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

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)

GB/T 15843.1—2008　信息技术　安全技术　实体鉴别　第1部分:概述(ISO/IEC 9798-1:1997,IDT)

GB/T 17964—2008　信息安全技术　分组密码算法的工作模式

## 3　术语和定义

下列术语和定义适用于本部分。

3.1　本部分采用GB/T 9387.2—1995中定义的如下术语。

3.1.1

**数据完整性　data integrity**

数据没有被非授权地修改或破坏的性质。

3.2　下列术语和定义适用于本部分。

3.2.1

**分组　block**

一种定义了长度的比特串。

3.2.2

**分组密码密钥　block cipher key**

控制分组密码运算的密钥。

3.2.3

**初始变换　initial transformation**

消息鉴别码算法起始时所应用的函数。

3.2.4

**消息鉴别码(MAC)算法密钥　MAC algorithm key**

一种用于控制消息鉴别码算法运算的密钥。

3.2.5

**消息鉴别码　message authentication code (MAC)**

利用对称密码技术和秘密密钥,由消息所导出的数据项。任何持有这一秘密密钥的实体,可利用消