ICS 35.040
L 80

中华人民共和国国家标准

GB/T 18238.3—2002
idt ISO/IEC 10118-3:1998

信息技术　安全技术　散列函数
第3部分:专用散列函数

Information technology—Security techniques—Hash-functions—Part 3:Dedicated hash-functions

2002-07-18 发布　　2002-12-01 实施

中华人民共和国
国家质量监督检验检疫总局　发布

目　　次

前　言

本标准等同采用国际标准ISO/IEC 10118-3:1998《信息技术 安全技术 散列函数 第3部分:专用散列函数》。

本标准附录A、附录B、附录C均为提示的附录。

本标准由中华人民共和国信息产业部提出。

本标准由中国电子技术标准化研究所归口。

本标准起草单位:中国电子技术标准化研究所。

本标准主要起草人:徐冬梅、张展新。

ISO/IEC 前言

ISO(标准化组织)和IEC(国际电工委员会)是世界性的标准化机构。国家成员体(都是ISO或IEC的成员国)通过国际组织建立的各个技术委员会参与制定针对特定技术领域的标准。ISO和IEC的各技术委员会在共同感兴趣的领域内进行合作。与ISO和IEC有联系的其他官方和非官方国际组织也可参与标准的制定工作。

对于信息技术领域,ISO和IEC建立了一个联合技术委员会,即ISO/IEC JTC1。由联合技术委员会提出的标准草案需分发给国家成员体进行表决。发布一项标准,至少需要75%的参与表决的国家成员体投票赞成。

国际标准ISO/IEC 10118-3是由ISO/IEC JTC1“信息技术”联合技术委员会的SC27“信息技术 安全技术”分委员会制定的。

ISO/IEC 10118在总标题“信息技术 安全技术 散列函数”下包含以下几个部分:

——第1部分:概述

——第2部分:采用n位块密码的散列函数

——第3部分:专用散列函数

——第4部分:采用模运算的散列函数

可能还会有后续部分。

本标准的附录A、附录B和附录C均为提示的附录。

中华人民共和国国家标准

信息技术　安全技术　散列函数
第3部分：专用散列函数

GB/T 18238.3—2002
idt ISO/IEC 10118-3:1998

Information technology—Security techniques—Hash-functions—Part 3:Dedicated hash-functions

1　范围

本标准规定了专用散列函数，即专门设计的散列函数。本标准的散列函数基于循环函数的迭代使用。本标准规定了三种不同的循环函数，从而产生了不同的专用散列函数。第一种和第三种提供了长度达160位的散列码，第二种提供了长度达128位的散列码。

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为本标准的条文。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 1988—1998　信息技术　信息交换用七位编码字符集(eqv ISO 646:1991)

GB/T 18238.1—2000　信息技术　安全技术　散列函数　第1部分：概述(idt ISO/IEC 10118-1:1994)

3　定义

GB/T 18238.1中给出的定义以及下列定义适用于本标准：

3.1　块　block

长度为L_1的位串，即送往循环函数的第一个输入的长度。

3.2　散列函数标识符　hash-function identifier

标识特定散列函数的字节。

3.3　循环函数　round-function

把长度为L_1和L_2的两个二进制串变换成长度为L_2的一个二进制串的函数$\phi(.\ ,.)$。它作为散列函数的一部分迭代使用，其中它把长度为L_1的数据串与前一步输出的长度为L_2的数据串组合起来。

3.4　字　word

一个32位的串。

4　符号和记法

本标准采用GB/T 18238.1中定义的符号和记法。

D	输入到散列函数的数据串。
H	散列码。
IV	初始化值。

中华人民共和国国家质量监督检验检疫总局2002-07-18批准　　2002-12-01实施