ICS 35.040
L 80

中华人民共和国国家标准

GB/T 18238.2—2002
idt ISO/IEC FDIS 10118-2:2000

信息技术　安全技术　散列函数
第2部分:采用n位块密码的散列函数

Information technology—Security techniques—
Hash-functions—
Part 2:Hash-functions using an n-bit block cipher

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 FDIS 10118-2:2000《信息技术　安全技术　散列函数　第 2 部分:采用 n 位块密码的散列函数》。

本标准的附录 A、附录 B 和附录 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 FDIS 10118-2 是由 ISO/IEC JTC1“信息技术”联合技术委员会的 SC 27“IT 安全技术”分委会制定的。

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

本标准的附录 A 和附录 B 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2部分：采用n位块密码的散列函数

GB/T 18238.2—2002
idt ISO/IEC FDIS 10118-2:2000

Information technology—Security techniques—
Hash-functions—
Part 2:Hash-functions using an n-bit block cipher

1　范围

本标准规定了采用n位块密码算法的散列函数，这些函数适合于已实现这样一个算法的环境。

本标准规定了四种散列函数。第一种提供了长度小于或者等于n的散列代码，其中n是采用算法的块长度。第二种提供了长度小于或者等于$2n$的散列代码。第三种提供了长度等于$2n$的散列代码。第四种提供了长度等于$3n$的散列代码。本标准规定的全部四种散列函数符合ISO/IEC 10118-1中规定的通用模型。

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 17964—2000　信息技术　安全技术　n位块密码算法的操作方式(idt ISO/IEC 10116:1997)

ISO/IEC 10118-1:2000　信息技术　安全技术　散列函数　第1部分：概述

3　定义

本标准采用ISO/IEC 10118-1中给出的定义以及下列定义：

3.1　n位块密码　n-bit block cipher

明文块和密文块的长度均为n位的块密码。(见GB/T 17964)

4　符号和缩略语

本标准采用ISO/IEC 10118-1中给出的符号和缩略语以及下列符号和缩略语：

e	n位块加密算法(见GB/T 17964)。
K	算法e的密钥(见GB/T 17964)。
$e_K(P)$	对明文块P采用算法e和密钥K(见GB/T 17964)的密码操作。
u或者u'	把一个n位块转换为算法e的密钥的变换。
B^L	当n是偶数时，构成块B的最左边的$n/2$位的串。当n是奇数时，构成块B的最左边的$(n+1)/2$位的串。

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