ICS 35.040
L 80

中华人民共和国国家标准

GB/T 18238.1—2000
idt ISO/IEC 10118-1:1994

信息技术　安全技术　散列函数　第1部分：概述

Information technology—Security techniques—Hash-function—Part 1:General

2000-10-17 发布　　2001-08-01 实施

国家质量技术监督局　发布

前　言

本标准等同采用国际标准 ISO/IEC 10118-1:1994《信息技术　安全技术　散列函数　第 1 部分：概述》。

本标准描述 GB/T 18238 各个部分所共用的定义、符号、缩略语和要求。

本标准的附录 A、附录 B 和附录 C 均是提示的附录。

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：罗韧鸿、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范围的标准。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 10118-1 是由 ISO/IEC JTC1"信息技术"联合技术委员会的 SC27"信息安全技术"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 位块密码算法的散列函数

——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、附录 B 和附录 C 均为提示的附录。

引　言

散列函数将任意位串映射到一个给定的范围内。这些散列函数能用来：

——将一条消息缩减成一个短的印记，作为一个数字签名机制的输入；

——将用户定义到一个给定的位串而不透露此位串的内容。

GB/T 18238 提供适用于各种安全技术的各种散列函数。散列函数可以用于本标准范畴之外的其他用途，如模拟一个随机数产生器。

中华人民共和国国家标准

信息技术　安全技术　散列函数
第1部分：概述

GB/T 18238.1—2000
idt ISO/IEC 10118-1:1994

Information technology—Security techniques—Hash-function—Part 1:General

1　范围

GB/T 18238规定了散列函数，它可用于提供鉴别、完整性和抗抵赖服务。

注：散列码的产生不牵涉到秘密密钥，这不同于消息鉴别码(MAC)的计算，计算MAC要利用一个秘密密钥来确保对一条消息的鉴别。有关MAC计算的内容可参见GB 15852。

本标准包含GB/T 18238各个部分所共用的定义、符号、缩略语和要求。

2　定义

下列定义适用于GB/T 18238。

2.1　无碰撞散列函数　collision-resistant hash-function

满足下列特性的散列函数：

——找出能映射到同一个输出的任何两个不同的输入在计算上是不可行的。

注：计算可行性依赖于用户的特定安全要求和环境。

2.2　数据串(数据)　data string(data)

作为一个散列函数的输入的位串。

2.3　散列码　hash-code

作为一个散列函数的输出的位串。

注：在该领域的文献中，有多个术语具有与散列码相同或相似的含义。例如：篡改检测码(Modification Detection Code)、操纵检测码(Manipulation Detection Code)、摘要、散列结果、散列值和印记。

2.4　散列函数　hash-function

将任意位串映射到固定长度位串的函数，它满足下面两个特性：

——为一个给定的输出找出能映射到该输出的一个输入在计算上是不可行的；

——为一个给定的输入找出能映射到同一个输出的另一个输入在计算上是不可行的。

注

1　在这一技术领域中，有多个术语具有与散列函数相同或相似的含义。例如：压缩编码(compressed encoding)和压缩函数(condensing function)。

2　计算可行性依赖于用户的特定安全要求和环境。

2.5　初始化值　initializing value

定义一个散列函数的起始点时所使用的值。

2.6　填充　padding

给一个数据串添加额外的位。

国家质量技术监督局2000-10-17批准　　2001-08-01实施

3 符号和记法

GB/T 18238 使用下列符号和缩略语：

D	数据
H	散列码
IV	初始化值
L_X	位串 X 的长度(按位数)
X ‖ Y	位串 X 和 Y 以 X 在前 Y 在后的顺序连接的结果
X⊕Y	位串 X 和 Y 的异或

所有位串的最左边为第一个位。如果在上下文中使用了术语“最高有效位/字节”和“最低有效位/字节”，例如将位串看作数字值，则块的最左边的位是最高有效位。

4 要求

虽然在每个实体的环境中数据的表示可能不同，但要求使用散列函数的有关各方所操作的数据应完全相同，这就有可能要求一个或多个实体在应用散列函数之前将数据转换成各方同意的表示形式。

GB/T 18238 中规定的某些散列函数使用一个(或多个)初始化值。在这种情况下，应确保产生散列码的实体和进行校验的实体使用相同的初始化值。附录 A 给出了这方面的例子。

GB/T 18238 中规定的某些散列函数要求进行填充，以使数据串具有所要求的长度。填充方法可以在 GB/T 18238 中需要填充的各个部分中规定。附录 B 给出了这种方法的例子。

附 录 A
（提示的附录）
关于初始化值的指南

初始化值可以用多种方式来选择；例如，它可能是：

——一个固定值；

——每次使用散列函数时随机选择的一个值；

——依赖于要进行散列运算的数据的一种或多种特性（长度、类型等）的一个值。

本标准第4章中指出应确保产生散列码的实体和进行校验的实体使用相同的初始化值，这可通过使用一个固定值来实现。如果校验实体事前不知道初始化值，就要以一种能确保其完整性的方式来传送这个值。例如，IV可以与散列码连接，并输入到数字签名机制中。

附 录 B
（提示的附录）
填 充 方 法

GB/T 18238其他部分规定的散列码计算可能要求选择某种填充方法。本附录列出了两种方法。如果散列码的验证者不知道需要计算散列码的数据的长度，建议使用填充方法2。填充位（若有）无需与数据一起存储或发送。验证者应知道填充位是否已被存储或发送，以及使用了哪种填充方法。

B1 方法1

在需要计算散列码的数据上附加必要但尽可能少的“0”（可能一个也不加），以达到所要求的长度。

B2 方法2

在需要计算散列码的数据上附加一个“1”。再在所生成的数据上附加必要但尽可能少的“0”（可能一个也不加），以达到所要求的长度。

注：方法2总是要求附加至少一个填充位。

附 录 C
（提示的附录）
参 考 标 准

[1] 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 (idt ISO/IEC 9797:1994)