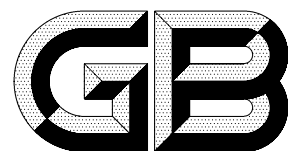


ICS 35.040  
L 80



# 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 的成员体)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 的各个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。