



# 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 .....	■
ISO/IEC 前言 .....	IV
1 范围 .....	1
2 引用标准 .....	1
3 定义 .....	1
4 符号和记法 .....	1
5 要求 .....	2
6 专用散列函数模型 .....	3
7 专用散列函数 1 .....	4
8 专用散列函数 2 .....	7
9 专用散列函数 3 .....	9
附录 A(提示的附录) 实例 .....	11
附录 B(提示的附录) 形式规范 .....	36
附录 C(提示的附录) 参考文献 .....	48

## 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的的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  $\phi(\cdot, \cdot)$ 。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。

$L_X$	位串 $X$ 的长度(按位表示)。
$X \oplus Y$	位串 $X$ 和 $Y$ 的异或。
下列符号和记法适用于本标准:	
$a_i, a'_i$	用于规定循环函数的索引序列。
$B_i$	字节。
$C_i, C'_i$	循环函数中使用的常数字。
$D_i$	填充处理后从数据串导出的块。
$f_i, g_i$	采用三个字作为输入并产生单个字作为输出,用于规定循环函数的函数。
$H_i$	在散列操作中用于存储中间结果的长 $L_2$ 位的串。
$L_1$	送往循环函数 $\phi$ 的两个输入串中的第一个输入串的长度(按位表示)
$L_2$	送往循环函数 $\phi$ 的两个输入串中的第二个输入串的长度(按位表示),循环函数的输出串的长度(按位表示),以及 $IV$ 的长度(按位表示)。
$q$	填充和分离过程后数据串中的块数。
$S^n()$	“循环左移” $n$ 位操作,即,如果 $A$ 是一个字并且 $n$ 是一个非负整数,那么 $S^n(A)$ 表示将字 $A$ 经过 $n$ 次左循环移位而得到的字。
$t_i, t'_i$	用于规定循环函数的移位值。
$W, X_i, X'_i, Y_i, Z_i$	用来存储中间计算结果的字。
$\phi$	一个循环函数,即,如果 $X, Y$ 是长度分别为 $L_1$ 和 $L_2$ 的位串,那么 $\phi(X, Y)$ 是通过把 $\phi$ 应用于 $X, Y$ 所得到的串。
$\wedge$	位串的逐位逻辑“与”操作,即,如果 $A, B$ 是字,那么 $A \wedge B$ 是等于 $A$ 和 $B$ 逐位逻辑“与”得到的字。
$\vee$	位串的逐位逻辑“或”操作,即,如果 $A, B$ 是字,那么 $A \vee B$ 是等于 $A$ 和 $B$ 逐位逻辑“或”得到的字。
$\neg$	位字符串的逐位逻辑非操作,即如果 $A$ 是字,那么 $\neg A$ 是 $A$ 逐位逻辑“非”得到的字
$\uplus$	模 $2^{32}$ 加法操作,即,如果 $A, B$ 是字,那么 $A \uplus B$ 是通过把 $A$ 和 $B$ 视为整数的二进制表示并计算它们的模 $2^{32}$ 和而得到的字,其中结果被限制在 $0$ 和 $2^{32}-1$ 之间,包括 $0$ 和 $2^{32}-1$ 。
$:=$	表示在循环函数过程描述中所使用的“置等于”操作的符号,其中它表示符号左边的字应与符号右边表达的值相等。

## 5 要求

想要使用本标准中的散列函数的用户应选择:

- 以下规定的专用散列函数之一;以及
- 散列码  $H$  的长度  $L_H$ 。

注

- 1 定义了第一种和第二种专用散列函数以利于“小结尾”计算机软件的实现,也就是字中最低访问字节被解释为最低有效位;相反,第三种循环函数的定义便于“大结尾”计算机软件的实现,就是字的最低访问字节被解释为最高有效位。然而,通过适当地调整定义,任何循环函数都能够在“小结尾”计算机或者在“大结尾”计算机上实现。本文定义的全部散列函数把一个位串作为输入并且给出一个输出位串;这不依赖于每个散列函数内所使用的内部字节排序约定。
- 2  $L_H$  的选择影响散列函数的安全性。在进行  $2^{L_H}$  散列码计算时被认为在计算上是不可行的环境中本标准所规定的全部散列函数被认为是无碰撞散列函数。

## 6 专用散列函数模型

### 6.1 概述

本标准中规定的散列函数要求使用循环函数 $\phi$ 。后续各章规定了三种可替换函数 $\phi$ 。

本标准中规定的散列函数提供长度为 $L_H$ 的散列码,其中对于所使用的循环函数 $\phi$ 来说, $L_H$ 的值小于或者等于 $L_2$ 。

在本标准散列函数的规范中,假设输入到散列函数的填充数据串是以字节序列形式表示的。如果所填充的数据串以 $8n$ 位序列形式, $x_0, x_1, \dots, x_{8n-1}$ 表示,那么它将以以下的方式被解释为 $n$ 字节的序列, $B_0, B_1, \dots, B_{n-1}$ 。每组8个连续位被认为是一个字节,每组第一个位是该字节的最高有效位。因此,对任何 $i(0 \leq i < n)$ :

$$B_i = 2^7 x_{8i} + 2^6 x_{8i+1} + \dots + x_{8i+7}$$

对于本标准规定的三种专用散列函数中的每一种均定义了标识符。在第7、8和9章中规定的专用散列函数的散列函数标识符分别等于31、32和33(十六进制)。34到3F(十六进制)之间的值保留作为以后的散列函数标识符使用。

### 6.2 散列操作

设 $\phi$ 为循环函数, $IV$ 是长度为 $L_2$ 的初始化值。对于本标准规定的散列函数,对给定的循环函数 $\phi$ , $IV$ 的值应是固定的。

数据 $D$ 的散列码 $H$ 按照以下四步计算。

#### 6.2.1 第1步(填充)

填充数据串 $D$ 是以确保其长度是 $L_1$ 的倍数。本标准后续各章中规定了填充法的特定实例。

#### 6.2.2 第2步(分离)

数据串 $D$ 的填充版被分离成 $L_1$ 位的块 $D_1, D_2, \dots, D_q$ ,其中 $D_1$ 表示 $D$ 填充后的第1个 $L_1$ 位, $D_2$ 表示第2个 $L_1$ 位,依次类推。填充和分离过程如图1所示。

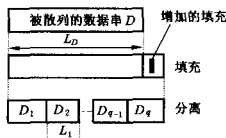


图1 填充和分离过程

#### 6.2.3 第3步(迭代)

设 $D_1, D_2, \dots, D_q$ 经填充和分离后,成为长度是 $L_1$ 位的数据块。设 $H_0$ 为与 $IV$ 相等的位串。 $L_2$ 位串 $H_1, H_2, \dots, H_q$ 用以下方法迭代计算:

对于 $i$ 从1到 $q$ :

$$H_i = \phi(D_i, H_{i-1})$$

迭代过程如图2所示。

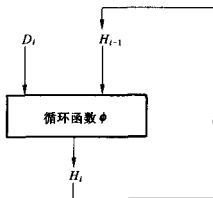


图2 迭代过程

## 6.2.4 第4步(截短)

通过取最后长度为  $L_2$  位的输出串  $H_q$  的最左边的  $L_H$  位而导出散列码  $H$ 。

## 7 专用散列函数 1

注：本章包含循环函数的描述、初始化值以及附录 C 中[3]的 RIPEMD-160 填充法。

## 7.1 概述

本章规定了填充法、初始化值和循环函数,用于本标准描述的一般模型。这里规定的填充法、初始化值和循环函数,当用于上述一般模型时,要同时定义专用散列函数 1。该专用散列函数可用于包含至多  $2^{64}$ -1 位的所有数据串  $D$ 。

用于专用散列函数 1 的 ISO/IEC 散列函数标识符等于 31(16 进制)。

## 7.2 参数、函数和常数

## 7.2.1 参数

该散列函数中,  $L_1=512, L_2=160$ 。

## 7.2.2 字节排序约定

在第 7 章循环函数描述中,假定输入到循环函数中的块以字节序列形式表示,每个 512 位的块由 16 个字组成。一个 64 个字节序列,  $B_0, B_1, \dots, B_{63}$ , 应按下述方法解释为 16 个字的序列,  $Z_0, Z_1, \dots, Z_{15}$ 。每组 4 个连续字节作为一个字,字的第 1 个字节是该字的最低有效字节。因此

$$Z_i = 2^{24}B_{4i+3} + 2^{16}B_{4i+2} + 2^8B_{4i+1} + B_{4i} \quad (0 \leq i \leq 15)$$

把散列码从字序列转换到字节序列,应遵照相反的过程。

注：这里规定的字节排序与 9.2.2 中规定的字节排序不同。

## 7.2.3 函数

为便于软件实现,根据字操作来描述循环函数  $\phi$ 。在本循环函数中使用一序列函数:  $g_0, g_1, \dots, g_{79}$ , 其中函数  $g_i$  ( $0 \leq i \leq 79$ ), 以三个字  $X_0, X_1$  和  $X_2$  作为输入, 并产生单个字作为输出。

函数  $g_i$  定义如下:

$$g_i(X_0, X_1, X_2) = X_0 \oplus X_1 \oplus X_2 \quad (0 \leq i \leq 15);$$

$$g_i(X_0, X_1, X_2) = (X_0 \wedge X_1) \vee (\neg X_0 \wedge X_2) \quad (16 \leq i \leq 31);$$

$$g_i(X_0, X_1, X_2) = (X_0 \vee \neg X_1) \oplus X_2 \quad (32 \leq i \leq 47);$$

$$g_i(X_0, X_1, X_2) = (X_0 \wedge X_2) \vee (X_1 \wedge \neg X_2) \quad (48 \leq i \leq 63);$$

$$g_i(X_0, X_1, X_2) = X_0 \oplus (X_1 \vee \neg X_2) \quad (64 \leq i \leq 79)$$

## 7.2.4 常数

本循环函数中使用两个常数字序列  $C_0, C_1, \dots, C_{79}$  和  $C'_0, C'_1, \dots, C'_{79}$ 。用十六进制表示(其中最高有效位对应于最左边的位)定义如下:

$$C_i = 00000000 \quad (0 \leq i \leq 15);$$

$$C_i = 5A827999 \quad (16 \leq i \leq 31);$$

$$C_i = 6ED9EBA1 \quad (32 \leq i \leq 47);$$

$$C_i = 8F1BBCDC \quad (48 \leq i \leq 63);$$

$$C_i = A953FD4E \quad (64 \leq i \leq 79);$$

$$C'_i = 50A28BE6 \quad (0 \leq i \leq 15);$$

$$C'_i = 5C4DD124 \quad (16 \leq i \leq 31);$$

$$C'_i = 6D703EF3 \quad (32 \leq i \leq 47);$$

$$C'_i = 7A6D76E9 \quad (48 \leq i \leq 63);$$

$$C'_i = 00000000 \quad (64 \leq i \leq 79)。$$



本循环函数中使用了80个移位值组成的两个序列,其中每个移位值在5和15之间,用 $(t_0, t_1, \dots, t_{79})$ 和 $(t'_0, t'_1, \dots, t'_{79})$ 表示这两个序列。循环函数还使用80个索引组成的两个序列,其中每个序列中的每个值在0和15之间,用 $(a_0, a_1, \dots, a_{79})$ 和 $(a'_0, a'_1, \dots, a'_{79})$ 表示这两个序列。所有四个序列在下表中定义:

$i$	0	1	2	3	4	5	6	7
$t_i$	11	14	15	12	5	8	7	9
$t'_i$	8	9	9	11	13	15	15	5
$a_i$	0	1	2	3	4	5	6	7
$a'_i$	5	14	7	0	9	2	11	4
$i$	8	9	10	11	12	13	14	15
$t_i$	11	13	14	15	6	7	9	8
$t'_i$	7	7	8	11	14	14	12	6
$a_i$	8	9	10	11	12	13	14	15
$a'_i$	13	6	15	8	1	10	3	12
$i$	16	17	18	19	20	21	22	23
$t_i$	7	6	8	13	11	9	7	15
$t'_i$	9	13	15	7	12	8	9	11
$a_i$	7	4	13	1	10	6	15	3
$a'_i$	6	11	3	7	0	13	5	10
$i$	24	25	26	27	28	29	30	31
$t_i$	7	12	15	9	11	7	13	12
$t'_i$	7	7	12	7	6	15	13	11
$a_i$	12	0	9	5	2	14	11	8
$a'_i$	14	15	8	12	4	9	1	2
$i$	32	33	34	35	36	37	38	39
$t_i$	11	13	6	7	14	9	13	15
$t'_i$	9	7	15	11	8	6	6	14
$a_i$	3	10	14	4	9	15	8	1
$a'_i$	15	5	1	3	7	14	6	9
$i$	40	41	42	43	44	45	46	47
$t_i$	14	8	13	6	5	12	7	5
$t'_i$	12	13	5	14	13	13	7	5
$a_i$	2	7	0	6	13	11	5	12
$a'_i$	11	8	12	2	10	0	4	13

$i$	48	49	50	51	52	53	54	55
$t_i$	11	12	14	15	14	15	9	8
$t'_i$	15	5	8	11	14	14	6	14
$a_i$	1	9	11	10	0	8	12	4
$a'_i$	8	6	4	1	3	11	15	0

$i$	56	57	58	59	60	61	62	63
$t_i$	9	14	5	6	8	6	5	12
$t'_i$	6	9	12	9	12	5	15	8
$a_i$	13	3	7	15	14	5	6	2
$a'_i$	5	12	2	13	9	7	10	14

$i$	64	65	66	67	68	69	70	71
$t_i$	9	15	5	11	6	8	13	12
$t'_i$	8	5	12	9	12	5	14	6
$a_i$	4	0	5	9	7	12	2	10
$a'_i$	12	15	10	4	1	5	8	7

$i$	72	73	74	75	76	77	78	79
$t_i$	5	12	13	14	11	8	5	6
$t'_i$	8	13	6	5	15	13	11	11
$a_i$	14	1	3	8	11	6	15	13
$a'_i$	6	2	13	14	0	3	9	11

### 7.2.5 初始化值

对于该循环函数来说,初始化值  $IV$  应该总是下列 160 位的串,在这里表示为十六进制的 5 个字  $Y_0$ 、 $Y_1$ 、 $Y_2$ 、 $Y_3$  和  $Y_4$  的序列,其中  $Y_0$  表示 160 位中最左边的 32 位。

$Y_0 = 67452301$

$Y_1 = \text{EFCDAB89}$

$Y_2 = 98BADCFE$

$Y_3 = 10325476$

$Y_4 = \text{C3D2E1F0}$

### 7.3 填充法

需要填充数据串  $D$ ,使它具有 512 的整数倍位数。填充过程操作如下:

a)  $D$  连接上单个“1”。

b) 上一步所得的结果再连接上 0~511 个“0”位,以使结果串的(按位)长度与 448 模 512 同余。更确切地说,如果  $D$  的原始长度为  $L_D$ ,并设  $r$  为  $L_D$  除以 512 的余数,那么要连接的“0”的数目等于  $447-r$  (当  $r \leq 447$ ) 或  $959-r$  (当  $r > 447$ )。这样所得到的位串长度将比 512 位的整数倍少 64 位。

c) 把以 64 位二进制表示的  $L_D$  分成两个 32 位串,一个表示  $L_D$  的“最高有效串”,另一个表示“最低有效串”。把这两个 32 位的串(“最低有效串”在前)与前一步得到的字串相连接。

在以下对循环函数的描述中,每个 512 位数据块  $D_i$  ( $1 \leq i \leq q$ ) 视为作为一个 16 个字的序列,  $Z_0, Z_1, \dots, Z_{15}$ , 其中  $Z_0$  对应  $D_i$  最左边的 32 位。

## 7.4 循环函数的描述

循环函数  $\phi$  操作如下。注意,在以下的描述中,使用符号  $W, X_0, X_1, X_2, X_3, X_4, X'_0, X'_1, X'_2, X'_3, X'_4$  来表示 11 个不同的字,这些字包含计算中要求的值。

a) 假定  $\phi$  的 512 位(第一次)输入包含在  $Z_0, Z_1, \dots, Z_{15}$  中,其中  $Z_0$  是 512 位的最左边 32 位,同样假定  $\phi$  的 160 位第二次输入包含在 5 个字  $Y_0, Y_1, Y_2, Y_3$  和  $Y_4$  中。

b) 置  $X_0 := Y_0$   $X_1 := Y_1$   $X_2 := Y_2$   $X_3 := Y_3$   $X_4 := Y_4$

c) 置  $X'_0 := Y_0$   $X'_1 := Y_1$   $X'_2 := Y_2$   $X'_3 := Y_3$   $X'_4 := Y_4$

d) 按照规定的次序执行以下四步,  $i := 0$  到 79:

(1)  $W := S^5(X_0 \oplus_{g_i}(X_1, X_2, X_3) \oplus Z_m \oplus C_i) \oplus X_4$

(2)  $X_0 := X_4$   $X_4 := X_3$   $X_3 := S^{10}(X_2)$   $X_2 := X_1$   $X_1 := W$

(3)  $W := S^5(X'_0 \oplus_{g_{79-i}}(X'_1, X'_2, X'_3) \oplus Z_m \oplus C'_i) \oplus X'_4$

(4)  $X'_0 := X'_4$   $X'_4 := X'_3$   $X'_3 := S^{10}(X'_2)$   $X'_2 := X'_1$   $X'_1 := W$

e) 设

$W := Y_0$

$Y_0 := Y_1 \oplus X_2 \oplus X'_3$

$Y_1 := Y_2 \oplus X_3 \oplus X'_4$

$Y_2 := Y_3 \oplus X_4 \oplus X'_0$

$Y_3 := Y_4 \oplus X_0 \oplus X'_1$

$Y_4 := W \oplus X_1 \oplus X'_2$

f) 5 个字  $Y_0, Y_1, Y_2, Y_3, Y_4$  表示循环函数  $\phi$  的输出。循环函数最终迭代后,通过使用 7.2.2 中规定的相反的过程,5 个字  $Y_0, Y_1, Y_2, Y_3, Y_4$  应转换成一个 20 个字节的序列,其中由  $Y_0$  产生前 4 个字节,  $Y_1$  产生下 4 个字节,依次类推。这样,首(最左边的)字节对应于  $Y_0$  的最低有效字节,第 20 个(最右边的)字节对应于  $Y_4$  的最高有效字节。通过使用 6.1 中规定的相反的过程,这 20 个字节应转换成 160 个位的串,即首(最左边的)位对应于首(最左边的)字节的最高有效位,第 160(最右边的)位对应于第 20 个(最右边的)字节的最低有效位。

## 8 专用散列函数 2

本散列函数应仅用于当散列码包含小于或等于 128 位时就认为足够安全的应用中。

注:本章包含循环函数的描述、初始化值以及附录 C 中 [3] 的 RIPEMD-128 的填充法。

### 8.1 概述

本章规定了填充法、初始化值和循环函数,它们用于本标准描述的一般模型。这里规定的填充法、初始化值和循环函数,当它们用于上述一般模型时,要同时定义专用散列函数 2。该专用散列函数可适用于包含最多  $2^{64} - 1$  位的全部数据串 D。

用于专用散列函数 2 的 ISO/IEC 散列函数标识符等于 32(16 进制)。

### 8.2 参数、函数和常数

#### 8.2.1 参数

本散列函数中,  $L_1 = 512$ ,  $L_2 = 128$ 。

#### 8.2.2 字节排序约定

本散列函数的字节排序约定与第 7 章散列函数的约定相同。

#### 8.2.3 函数

为便于软件实现,根据字操作来描述循环函数  $\phi$ 。在本循环函数中使用一序列函数:  $g_0, g_1, \dots, g_{63}$ , 其中每个函数  $g_i$  ( $0 \leq i \leq 63$ ), 以三个字  $X_0, X_1$  和  $X_2$  作为输入,并产生单个字作为输出。

函数  $g_i$  与 7.2.3 中前 64 个函数的定义相同。

### 8.2.4 常数

本循环函数使用了两个常数字序列  $C_0, C_1, \dots, C_{63}$  和  $C'_0, C'_1, \dots, C'_{63}$ 。用十六进制表示(其中最高有效位对应于最左边的位)它们定义如下:

$$C_i = 00000000 \quad (0 \leq i \leq 15);$$

$$C_i = 5A827999 \quad (16 \leq i \leq 31);$$

$$C_i = 6ED9EBA1 \quad (32 \leq i \leq 47);$$

$$C_i = 8F1BBCDC \quad (48 \leq i \leq 63);$$

$$C'_i = 50A28BE6 \quad (0 \leq i \leq 15);$$

$$C'_i = 5C4DD124 \quad (16 \leq i \leq 31);$$

$$C'_i = 6D703EF3 \quad (32 \leq i \leq 47);$$

$$C'_i = 00000000 \quad (48 \leq i \leq 63);$$

本循环函数也使用了两个 64 个移位值序列,其中每个移位值在 5 和 15 之间,用  $(t_0, t_1, \dots, t_{63})$  和  $(t'_0, t'_1, \dots, t'_{63})$  表示这些序列,它们的定义与 7.2.4 中相应序列的前 64 个值相同。

最后,本循环函数还使用两个 64 个索引序列,其中每个序列中的每个值在 0 和 15 之间,用  $(a_0, a_1, \dots, a_{63})$  和  $(a'_0, a'_1, \dots, a'_{63})$  表示这些序列,它们的定义与 7.2.4 中相应序列的前 64 个值相同。

### 8.2.5 初始值

对于本循环函数来说,初始值  $IV$  应总是下列 128 位的字符串,在这里表示为十六进制的 4 个字节序列  $Y_0, Y_1, Y_2$  和  $Y_3$ ,其中  $Y_0$  表示 128 位中的最左边 32 位。

$$Y_0 = 67452301$$

$$Y_1 = EFCDA89$$

$$Y_2 = 98BADCFE$$

$$Y_3 = 10325476$$

### 8.3 填充法

本散列函数使用的填充法与 7.3 中定义的填充法相同。

### 8.4 循环函数的描述

循环函数  $\phi$  操作如下。注意,在以下的描述中,使用符号  $W, X_0, X_1, X_2, X_3, X'_0, X'_1, X'_2, X'_3$  来表示 9 个不同的字,这些字包含计算中要求的值。

a) 假定  $\phi$  的 512 位第一次输入到中包含在  $Z_0, Z_1, \dots, Z_{15}$  中,其中  $Z_0$  是 512 位的最左边 32 位,同样假定第二次输入到  $\phi$  中的 128 位包含在 4 个字  $Y_0, Y_1, Y_2$  和  $Y_3$  中。

$$b) \text{ 置 } X_0 := Y_0 \quad X_1 := Y_1 \quad X_2 := Y_2 \quad X_3 := Y_3$$

$$c) \text{ 置 } X'_0 := Y_0 \quad X'_1 := Y_1 \quad X'_2 := Y_2 \quad X'_3 := Y_3$$

d) 按照规定的次序执行以下四步,  $i := 0$  到 63:

$$(1) W := S^i(X_0 \uplus_{g_i}(X_1, X_2, X_3) \uplus Z_i \uplus C_i)$$

$$(2) X_0 := X_3 \quad X_3 := X_2 \quad X_2 := X_1 \quad X_1 := W$$

$$(3) W := S^i(X'_0 \uplus_{g'_{63-i}}(X'_1, X'_2, X'_3) \uplus Z'_i \uplus C'_i)$$

$$(4) X'_0 := X'_3 \quad X'_3 := X'_2 \quad X'_2 := X'_1 \quad X'_1 := W$$

e) 置

$$W := Y_0$$

$$Y_0 := Y_1 \uplus X_2 \uplus X'_3$$

$$Y_1 := Y_2 \uplus X_3 \uplus X'_0$$

$$Y_2 := Y_3 \uplus X_0 \uplus X'_1$$

$$Y_3 := W \uplus X_1 \uplus X'_2$$

f) 4 个字  $Y_0, Y_1, Y_2, Y_3$  表示循环函数  $\phi$  的输出。循环结束后,通过使用 7.2.2 中规定的相反的转换过程,4 个字  $Y_0, Y_1, Y_2, Y_3$  应转换成 16 个字节的序列,其中  $Y_0$  应产生得到前四个字节,  $Y_1$  应产生下面 4 个字节,依次类推。这样首(最左边的)字节对应于  $Y_0$  的最低有效字节,第 16 个(最右边的)字节对应于  $Y_4$  的最高有效字节。通过使用 6.1 中规定的相反的转换过程,这 16 个字节应转换成 128 个位的串,即首(最左边的)位对应于首(最左边的)字节的最高有效位,第 128(最右边的)位对应于第 16 个(最右边的)字节的最低有效位。

## 9 专用散列函数 3

注:本章包含循环函数的描述、初始化值以及 SHA-1 的填充法。

### 9.1 概述

本条规定了填充法、初始化值和循环函数,用于本标准描述的一般模型。这里规定的填充法、初始化值和循环函数,当它们用于上述一般模型时,要同时定义专用散列函数 3。该专用散列函数可适用于包含最多  $2^{64}-1$  位的全部数据串  $D$ 。

用于专用散列函数 3 的 ISO/IEC 散列函数标识符等于 33(16 进制)。

### 9.2 参数、函数和常数

#### 9.2.1 参数

该散列函数中,  $L_1=512, L_2=160$ 。

#### 9.2.2 字节排序约定

在第 9 章循环函数的描述中,假定输入到循环函数的块以字节序列形式表示,每个 512 位的块由 16 个这样的字组成。一个 64 个字节序列:  $B_0, B_1, \dots, B_{63}$ , 应按照下列方法,被解释为 16 个字节序列:  $Z_0, Z_1, \dots, Z_{15}$ 。每组 4 个连续字节作为一个字,字的第 2 个字节是该字的最高有效字节。因此

$$Z_i = 2^{24} B_{4i} + 2^{16} B_{4i+1} + 2^8 B_{4i+2} + B_{4i+3} \quad (0 \leq i \leq 15)$$

把散列码从字节序列转换到字节序列,应遵照相反的转换过程。

注:这里规定的字节次序与 7.2.2 中规定的字节次序不同。

#### 9.2.3 函数

为便于软件实现,根据字操作来描述循环函数  $\phi$ 。在循环函数中使用一序列函数:  $f_0, f_1, \dots, f_{63}$ , 其中每个函数  $f_i (0 \leq i \leq 79)$ , 以三个字  $X_0, X_1$  和  $X_2$  作为输入,产生单个字作为输出。

函数  $f_i$  定义如下:

$$f_i(X_0, X_1, X_2) = (X_0 \wedge X_1) \vee (\neg X_0 \wedge X_2) \quad (0 \leq i \leq 19);$$

$$f_i(X_0, X_1, X_2) = X_0 \oplus X_1 \oplus X_2 \quad (20 \leq i \leq 39);$$

$$f_i(X_0, X_1, X_2) = (X_0 \wedge X_1) \vee (X_0 \wedge X_2) \vee (X_1 \wedge X_2) \quad (40 \leq i \leq 59);$$

$$f_i(X_0, X_1, X_2) = X_0 \oplus X_1 \oplus X_2 \quad (60 \leq i \leq 79);$$

#### 9.2.4 常数

该循环函数使用常数字序列  $C'_0, C'_1, \dots, C'_{79}$ 。用十六进制表示(其中最高有效位对应于最左边的位)定义如下:

$$C'_i = 5A827999 \quad (0 \leq i \leq 19);$$

$$C'_i = 6ED9EBA1 \quad (20 \leq i \leq 39);$$

$$C'_i = 8F1BBCDC \quad (40 \leq i \leq 59);$$

$$C'_i = CA62C1D6 \quad (60 \leq i \leq 79)。$$

#### 9.2.5 初始化值

对于该循环函数来说,初始化值  $IV$  应总是 160 位的字符串,在这里表示为十六进制的 5 个字  $Y_0, Y_1, Y_2, Y_3$  和  $Y_4$ , 其中  $Y_0$  表示 160 位中最左边的 32 位。

$$Y_0 = 67452301$$

$$Y_1 = \text{EFCDAB89}$$

$$Y_2 = \text{98BADCFE}$$

$$Y_3 = \text{10325476}$$

$$Y_4 = \text{C3D2E1F0}$$

### 9.3 填充法

需要填充数据串  $D$ , 使它具有 512 整数倍位数。填充过程操作如下:

a)  $D$  连接上单个“1”。

b) 上一步所得的结果再连接上  $0 \sim 511$  个“0”位, 以使结果串的(按位)长度与 448 模 512 同余。更确切地说, 如果  $D$  的原始长度为  $L_D$ , 并设  $r$  为  $L_D$  除以 512 的余数, 那么要连接的“0”的数目等于  $447 - r$  (当  $r \leq 447$ ) 或  $959 - r$  (当  $r > 447$ )。这样所得到的位串长度比 512 位的整数倍少 64 位。

c) 连接上一步结果串与 64 位二进制表示的  $L_D$ , 最高位在前。

在以下对循环函数的描述中, 每个 512 位数据块  $D_i$  ( $1 \leq i \leq q$ ) 作为一个 16 个字序列:  $Z_0, Z_1, \dots, Z_{15}$ , 其中  $Z_0$  对应于  $D_i$  最左边的 32 位。

### 9.4 循环函数的描述

循环函数  $\phi$  操作如下。注意, 在以下的描述中, 使用符号  $W, X_0, X_1, X_2, X_3, X_4, Z_0, Z_1, \dots, Z_{79}$  来表示 86 个不同的字, 这些字包含计算中要求的值。

a) 假定  $\phi$  的 512 位(第一次)输入包含在  $Z_0, Z_1, \dots, Z_{15}$  中, 其中  $Z_0$  是 512 位的最左边 32 位, 同样假定  $\phi$  的 160 位(第二次)输入包含在 5 个字  $Y_0, Y_1, Y_2, Y_3$  和  $Y_4$  中。

b) 对于  $i = 16 \sim 79$  置

$$Z_i := S^1(Z_{i-3} \oplus Z_{i-8} \oplus Z_{i-14} \oplus Z_{i-16})$$

c) 置  $X_0 := Y_0$   $X_1 := Y_1$   $X_2 := Y_2$   $X_3 := Y_3$   $X_4 := Y_4$

d) 执行以下两步,  $i := 0 \sim 79$ :

(1)  $W := S^5(X_0) \uplus f_i(X_1, X_2, X_3) \uplus X_4 \uplus Z_i \uplus C_i$

(2)  $X_4 := X_3$   $X_3 := X_2$   $X_2 := S^{30}(X_1)$   $X_1 := X_0$   $X_0 := W$

e) 置

$$Y_0 := Y_0 \uplus X_0$$

$$Y_1 := Y_1 \uplus X_1$$

$$Y_2 := Y_2 \uplus X_2$$

$$Y_3 := Y_3 \uplus X_3$$

$$Y_4 := Y_4 \uplus X_4$$

f) 5 个字  $Y_0, Y_1, Y_2, Y_3, Y_4$  表示循环函数  $\phi$  的输出。循环结束后, 通过使用 9.2.2 中规定的相反的转换过程, 5 个字  $Y_0, Y_1, Y_2, Y_3, Y_4$  应转换成一个 20 个字节的序列, 其中  $Y_0$  应产生前 4 个字节,  $Y_1$  应产生下面 4 个字节, 依次类推。这样首(最左边的)字节对应于  $Y_0$  的最高有效字节, 第 20 个(最右边的)字节对应于  $Y_4$  的最低有效字节。通过使用 6.1 中规定的相反的转换过程, 这 20 个字节应转换成 160 个位的串, 即首(最左边的)位对应于首(最左边的)字节的最高有效位, 第 160(最右边的)位对应于第 20 个(最右边的)字节的最低有效位。

附 录 A  
(提示的附录)  
实 例

## A1 概述

本附录给出了专用散列函数 1、2 和 3 的计算实例。对于每个散列函数都给出了散列码计算的九个例子。而且每个散列函数的例 3 和例 8 还给出了散列函数操作过程中得到的中间值。

## A2 专用散列函数 1

本附录引用 GB 1988 编码的数据串。

注：附录 C 中的[3]含有专用散列函数 1 的伪码描述。

### A2.1 例 1

本例中数据串为空串，即零长度串。

散列码是下列 160 位串：

9C 11 85 A5 C5 E9 FC 54 61 28 08 97 7E E8 F5 48 B2 25 8D 31

### A2.2 例 2

本例中数据串由单个字节串组成，即字母“a”的 GB 1988 编码版本。散列码是下列 160 位串：

0B DC 9D 2D 25 6B 3E E9 DA AE 34 7B E6 F4 DC 83 5A 46 7F FE

### A2.3 例 3

本例中数据串由“abc”GB 1988 编码版本的 3 字节串组成。它等同于位串：“01100001 01100010 01100011”。

经过填充过程后，由该数据串推导出的单个 16 字的块如下：

80636261 00000000 00000000 00000000 00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000 00000018 00000000

下列是变量  $X_0, X_1, X_2, X_3, X_4, X'_0, X'_1, X'_2, X'_3, X'_4$  的连续值(用 16 进制表示)：

67452301, EFCDAB89, 98BADCFE, 10325476, C3D2E1F0, 67452301, EFCDAB89,

98BADCFE, 10325476, C3D2E1F0

C3D2E1F0, 3115FC67, EFCDAB89, EB73FA62, 10325476, C3D2E1F0, DDD63FB8,

EFCDAB89, EB73FA62, 10325476

10325476, B41192D5, 3115FC67, 36AE27BF, EB73FA62, 10325476, 322E7AE3, DDD63FB8,

36AE27BF, EB73FA62

EB73FA62, 3A35DC50, B41192D5, 57F19CC4, 36AE27BF, EB73FA62, 883EE903,

322E7AE3, 58FEE377, 36AE27BF

36AE27BF, D3786413, 3A35DC50, 464B56D0, 57F19CC4, 36AE27BF, 92B2B79B, 883EE903,

B9EB8CC8, 58FEE377

57F19CC4, 0E946720, D3786413, D77140E8, 464B56D0, 58FEE377, F9091FF2, 92B2B79B,

FBA40E20, B9EB8CC8

464B56D0, D52BF632, 0E946720, E1904F4D, D77140E8, B9EB8CC8, E5B09992, F9091FF2,

CADE6E4A, FBA40E20

D77140E8, 150BD8A8, D52BF632, 519C803A, E1904F4D, FBA40E20, 8B2D9FB3, E5B09992,

247FCBE4, CADE6E4A

E1904F4D, 3D6F601F, 150BD8A8, AFD8CB54, 519C803A, CADE6E4A, E755F422, 8B2D9FB3, C2664B96, 247FCBE4

519C803A, B7B60384, 3D6F601F, 2F62A054, AFD8CB54, 247FCBE4, 5922D09E, E755F422, B67ECE2C, C2664B96

AFD8CB54, B85A0A3F, B7B60384, BD807CF5, 2F62A054, C2664B96, CF24E72C, 5922D09E, 57D08B9D, B67ECE2C

2F62A054, 7F8B38E5, B85A0A3F, D80E12DE, BD807CF5, B67ECE2C, CA6A1C75, CF24E72C, 8B427964, 57D08B9D

BD807CF5, 9DACA495, 7F8B38E5, 6828FEE1, D80E12DE, 57D08B9D, 227F6D84, CA6A1C75, 939CB33C, 8B427964

D80E12DE, BC05F46F, 9DACA495, 2CE395FE, 6828FEE1, 8B427964, 5D801685, 227F6D84, A871D729, 939CB33C

6828FEE1, 1494F053, BC05F46F, B2925676, 2CE395FE, 939CB33C, B3C3F4D5, 5D801685, FDB61089, A871D729

2CE395FE, 85861D02, 1494F053, 17D1BEF0, B2925676, A871D729, 3D16242D, B3C3F4D5, 005A1576, FDB61089

B2925676, 597BF629, 85861D02, 53C14C52, 17D1BEF0, FDB61089, FF459078, 3D16242D, 0FD356CF, 005A1576

17D1BEF0, 6347EF78, 597BF629, 18740A16, 53C14C52, 005A1576, 927E40A8, FF459078, 5890B4F4, 0FD356CF

53C14C52, 45C8FA44, 6347EF78, EFD8A565, 18740A16, 0FD356CF, ACBB994E, 927E40A8, 1641E3FD, 5890B4F4

18740A16, AD2956AF, 45C8FA44, 1FBDE18D, EFD8A565, 5890B4F4, AD30AD24, ACBB994E, F902A249, 1641E3FD

EFD8A565, 5EAF16B7, AD2956AF, 23E91117, 1FBDE18D, 1641E3FD, 6261732E, AD30AD24, EE653AB2, F902A249

1FBDE18D, 41730D4B, 5EAF16B7, A55ABEB4, 23E91117, F902A249, 45ED27AF, 6261732E, C2B492B4, EE653AB2

23E91117, FC0CCBD3, 41730D4B, BC5ADD7A, A55ABEB4, EE653AB2, 243C5668, 45ED27AF, 85CCB989, C2B492B4

A55ABEB4, 042ECC93, FC0CCBD3, CC352D05, BC5ADD7A, C2B492B4, 82F89BD1, 243C5668, B49EBD17, 85CCB989

BC5ADD7A, 4D4D4377, 042ECC93, 332F4FF0, CC352D05, 85CCB989, 5FC74686, 82F89BD1, F159A090, B49EBD17

CC352D05, 5207002B, 4D4D4377, BB324C10, 332F4FF0, B49EBD17, B2720031, 5FC74686, E26F460B, F159A090

332F4FF0, 388278F5, 5207002B, 350DDD35, BB324C10, F159A090, 58A100F8, B2720031, 1D1A197F, E26F460B

BB324C10, 62879D70, 388278F5, 1C00AD48, 350DDD35, E26F460B, 5992068B, 58A100F8, C800C6C9, 1D1A197F

350DDD35, A30A1FD9, 62879D70, 09E3D4E2, 1C00AD48, 1D1A197F, CC290DCA, 5992068B, 8403E162, C800C6C9

1C00AD48, BDA2B31B, A30A1FD9, 1E75C18A, 09E3D4E2, C800C6C9, 863D625E,



CC290DCA, 481A2D66, 8403E162

09E3D4E2, F7211DEE, BDA2B31B, 287F668C, 1E75C18A, 8403E162, 6061B5A5, 863D625E, A4372B30, 481A2D66

1E75C18A, B6A665C6, F7211DEE, 8ACC6EF6, 287F668C, 481A2D66, AA98ADB5, 6061B5A5, F5897A18, A4372B30

287F668C, 2D30FA02, B6A665C6, 8477BBDC, 8ACC6EF6, A4372B30, 2999255A, AA98ADB5, 86D69581, F5897A18

8ACC6EF6, C76D12F9, 2D30FA02, 99971ADA, 8477BBDC, F5897A18, 98237631, 2999255A, 62B6D6AA, 86D69581

8477BBDC, 516F84DF, C76D12F9, C3E808B4, 99971ADA, 86D69581, 6C472A90, 98237631, 649568A6, 62B6D6AA

99971ADA, F3FA5B05, 516F84DF, B44BE71D, C3E808B4, 62B6D6AA, 2EAD5672, 6C472A90, 8DD8C660, 649568A6

C3E808B4, D539625E, F3FA5B05, BE137D45, B44BE71D, 649568A6, C5CB48BA, 2EAD5672, 1CAA41B1, 8DD8C660

B44BE71D, D8500C99, D539625E, E96C17CF, BE137D45, 8DD8C660, 05286DFB, C5CB48BA, B559C8BA, 1CAA41B1

BE137D45, 7ECDE5B2, D8500C99, E5897B54, E96C17CF, 1CAA41B1, 88396DD2, 05286DFB, 2D22EB17, B559C8BA

E96C17CF, 681D30B9, 7ECDE5B2, 40326761, E5897B54, B559C8BA, 333F2212, 88396DD2, A1B7EC14, 2D22EB17

E5897B54, 960F7BFD, 681D30B9, 3796C9FB, 40326761, 2D22EB17, C699295B, 333F2212, E5B74A20, A1B7EC14

40326761, 6770E498, 960F7BFD, 74C2E5A0, 3796C9FB, A1B7EC14, BFD68874, C699295B, FC8848CC, E5B74A20

3796C9FB, 75EB06C5, 6770E498, 3DEFF658, 74C2E5A0, E5B74A20, BDDF3474, BFD68874, 64A56F1A, FC8848CC

74C2E5A0, 14FA827A, 75EB06C5, C392619D, 3DEFF658, FC8848CC, 8CBC87E9, BDDF3474, 5A21D2FF, 64A56F1A

3DEFF658, 804B0068, 14FA827A, AC1B15D7, C392619D, 64A56F1A, CDDA6EBF, 8CBC87E9, 7CD1D2F7, 5A21D2FF

C392619D, 475BA81B, 804B0068, EA09E853, AC1B15D7, 5A21D2FF, 656C7DA3, CDDA6EBF, F21FA632, 7CD1D2F7

AC1B15D7, D26BC25D, 475BA81B, 2C01A201, EA09E853, 7CD1D2F7, 76D66CA3, 656C7DA3, 69BAFF37, F21FA632

EA09E853, DBC5A2CB, D26BC25D, 6EA06D1D, 2C01A201, F21FA632, C9B17F72, 76D66CA3, B1F68D95, 69BAFF37

2C01A201, 77367F5E, DBC5A2CB, AF097749, 6EA06D1D, 69BAFF37, 65A60151, C9B17F72, 59B28DDB, B1F68D95

6EA06D1D, 8155A6B4, 77367F5E, 168B2F6F, AF097749, B1F68D95, 33F3AC81, 65A60151, C5FDCB26, 59B28DDB

AF097749, C90C4D38, 8155A6B4, D9FD79DC, 168B2F6F, 59B28DDB, 9BFB827D, 33F3AC81, 98054596, C5FDCB26

168B2F6F, 9762713B, C90C4D38, 569AD205, D9FD79DC, C5FDCB26, DDC8130E, 9BFB827D, CEB204CF, 98054596

D9FD79DC, 7EBF9C32, 9762713B, 3134E324, 569AD205, 98054596, C24C2C79, DDC8130E, EE09F66F, CEB204CF

569AD205, 20EFA01, 7EBF9C32, 89C4EE5D, 3134E324, CEB204CF, F255847E, C24C2C79, 204C3B77, EE09F66F

3134E324, 75B7117F, 20EFA01, FE70C9FA, 89C4EE5D, EE09F66F, DCD63949, F255847E, 30B1E709, 204C3B77

89C4EE5D, A96BE4C7, 75B7117F, BFE80483, FE70C9FA, 204C3B77, 5B99238D, DCD63949, 5611FBC9, 30B1E709

FE70C9FA, 5E3201FC, A96BE4C7, DC45FDD6, BFE80483, 30B1E709, B43484F4, 5B99238D, 58E52773, 5611FBC9

BFE80483, 2CF95A98, 5E3201FC, AF931EA5, DC45FDD6, 5611FBC9, 52325A09, B43484F4, 648E356E, 58E52773

DC45FDD6, 1393F0C3, 2CF95A98, C807F178, AF931EA5, 58E52773, D015577D, 52325A09, D213D2D0, 648E356E

AF931EA5, BB49CCF7, 1393F0C3, E56A60B3, C807F178, 648E356E, BB9C87C4, D015577D, C9682548, D213D2D0

C807F178, 6A330EB4, BB49CCF7, 4FC30C4E, E56A60B3, D213D2D0, B1BB1A2E, BB9C87C4, 555DF740, C9682548

E56A60B3, 14E58204, 6A330EB4, 2733DEED, 4FC30C4E, C9682548, AC77F96D, B1BB1A2E, 721F12EE, 555DF740

4FC30C4E, 79AAF53E, 14E58204, CC3AD1A8, 2733DEED, 555DF740, 1774D326, AC77F96D, EC68BAC6, 721F12EE

2733DEED, 210769B3, 79AAF53E, 96081053, CC3AD1A8, 721F12EE, A625F112, 1774D326, DFE5B6B1, EC68BAC6

CC3AD1A8, F44B53A7, 210769B3, ABD4F9E6, 96081053, EC68BAC6, 5DCA4D12, A625F112, D34C985D, DFE5B6B1

96081053, 7C1E3640, F44B53A7, 1DA6CC84, ABD4F9E6, DFE5B6B1, EBC4D9C6, 5DCA4D12, 97C44A98, D34C985D

ABD4F9E6, 06B59EE8, 7C1E3640, 2D4E9FD1, 1DA6CC84, D34C985D, 095F37FD, EBC4D9C6, 29344977, 97C44A98

1DA6CC84, C422C3CD, 06B59EE8, 78D901F0, 2D4E9FD1, 97C44A98, 5BBEE487, 095F37FD, 13671BAF, 29344977

2D4E9FD1, AD864025, C422C3CD, D67BA01A, 78D901F0, 29344977, BF5B2529, 5BBEE487, 7CDF425, 13671BAF

78D901F0, 29A83BB5, AD864025, 8B0F3710, D67BA01A, 13671BAF, FB5747C5, BF5B2529, FB921D6E, 7CDF425

D67BA01A, 626E3910, 29A83BB5, 190096B6, 8B0F3710, 7CDF425, DD935A5F, FB5747C5, 6C94A6FD, FB921D6E

8B0F3710, A719D8BC, 626E3910, A0EED4A6, 190096B6, FB921D6E, 27754F3A, DD935A5F, 5D1F17ED, 6C94A6FD

190096B6, BA84C782, A719D8BC, B8E44189, A0EED4A6, 6C94A6FD, 4F5CA4A5,

27754F3A, 4D697F76, 5D1F17ED

A0EED4A6, 9F6887A9, BA84C782, 6762F29C, B8E44189, 5D1F17ED, 325AFE7E,  
4F5CA4A5, D53CE89D, 4D697F76

B8E44189, 3A88288C, 9F6887A9, 131E0AEA, 6762F29C, 4D697F76, 86AFE021, 325AFE7E,  
7292953D, D53CE89D

6762F29C, AB23F78F, 3A88288C, A21EA67D, 131E0AEA, D53CE89D, C97F9EA1,  
86AFE021, 6BF9F8C9, 7292953D

131E0AEA, 7299044A, AB23F78F, 20A230EA, A21EA67D, 7292953D, 9F60751C,  
C97F9EA1, BF80861A, 6BF9F8C9

A21EA67D, 6A3F10CF, 7299044A, 8FDE3EAC, 20A230EA, 6BF9F8C9, 1E9CE713,  
9F60751C, FE7A8725, BF80861A

20A230EA, 1A1B904D, 6A3F10CF, 641129CA, 8FDE3EAC, BF80861A, C13F038A,  
1E9CE713, 81D4727D, FE7A8725

8FDE3EAC, 0B2CDC01, 1A1B904D, FC433DA8, 641129CA, FE7A8725, BF627814,  
C13F038A, 739C4C7A, 81D4727D

641129CA, D563BFDC, 0B2CDC01, 6E413468, FC433DA8, 81D4727D, 5FCCBADE,  
BF627814, FC0E2B04, 739C4C7A

散列码是下列 160 位串:

8E B2 08 F7 E0 5D 98 7A 9B 04 4A 8E 98 C6 B0 87 F1 5A 0B FC

#### A.2.4 例 4

本例中数据串是 14 字节串,由“message digest”的 GB 1988 编码版本组成。

散列码是下列 160 位串:

5D 06 89 EF 49 D2 FA E5 72 B8 81 B1 23 A8 5F FA 21 59 5F 36

#### A.2.5 例 5

本例中数据串是 26 字节串,由“abcdefghijklmnopqrstuvwxy z”的 GB 1988 编码版本组成。

散列码是下列 160 位串:

F7 1C 27 10 9C 69 2C 1B 56 BB DC EB 5B 9D 28 65 B3 70 8D BC

#### A.2.6 例 6

本例中数据串是 62 字节串,

散列码是下列 160 位串:

B0 E2 0B 6E 31 16 64 02 86 ED 3A 87 A5 71 30 79 B2 1F 51 89

#### A.2.7 例 7

本例中数据串是 80 字节串,由 8 次重复“1234567890”的 GB 1988 编版本组成。

散列码是下列 160 位串:

9B 75 2E 45 57 3D 4B 39 F4 DB D3 32 3C AB 82 BF 63 32 6B FB

#### A.2.8 例 8

本例中数据串是 56 字节串,由“abcdcbcdcedefgefghfghighijhijkijklklmklmnl  
mnomnopnopq”的 GB 1988 编码版本组成。

经过填充过程后,由数据串推导出来的两个 16 字的块如下:

64636261 65646362 66656463 67666564 68676665 69686766 6A696867 6B6A6968

6C6B6A69 6D6C6B6A 6E6D6C6B 6F6E6D6C 706F6E6D 71706F6E 00000080 00000000

00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000 000001C0 00000000

下列是变量  $X_0, X_1, X_2, X_3, X_4, X'_0, X'_1, X'_2, X'_3, X'_4$  的连续值(用 16 进制表示), 它们在处理第 1 块过程中获得。

67452301, EFCDAB89, 98BADCFE, 10325476, C3D2E1F0, 67452301, EFCDAB89, 98BADCFE, 10325476, C3D2E1F0

C3D2E1F0, 3115FB87, EFCDAB89, EB73FA62, 10325476, C3D2E1F0, 463DA521, E-FCDAB89, EB73FA62, 10325476

10325476, CC21EC2E, 3115FB87, 36AE27BF, EB73FA62, 10325476, DB247A12, 463DA521, 36AE27BF, EB73FA62

EB73FA62, DFEB9B7A, CC21EC2E, 57EE1CC4, 36AE27BF, EB73FA62, 1D166A23, DB247A12, F6948518, 36AE27BF

36AE27BF, 2363912E, DFEB9B7A, 87B0BB30, 57EE1CC4, 36AE27BF, CE7A12F6, 1D166A23, 91E84B6C, F6948518

57EE1CC4, A1B60DC7, 2363912E, AE6DEB7F, 87B0BB30, F6948518, 57FF19DD, CE7A12F6, 59A88C74, 91E84B6C

87B0BB30, 96AC7C1E, A1B60DC7, 8E44B88D, AE6DEB7F, 91E84B6C, 01A9FEFA, 57FF19DD, E84BDB39, 59A88C74

AE6DEB7F, 6AE46154, 96AC7C1E, D8371E86, 8E44B88D, 59A88C74, 5D9A609C, 01A9FEFA, FC67755F, E84BDB39

8E44B88D, 3CF61F09, 6AE46154, B1F07A5A, D8371E86, E84BDB39, 030F7FE7, 5D9A609C, A7FBE806, FC67755F

D8371E86, 696F0D9A, 3CF61F09, 918551AB, B1F07A5A, FC67755F, 7456C8E3, 030F7FE7, 69827176, A7FBE806

B1F07A5A, AB957B91, 696F0D9A, D87C24F3, 918551AB, A7FBE806, F64C4453, 7456C8E3, 3DF9C0C, 69827176

918551AB, 9FF4A064, AB957B91, BC3669A5, D87C24F3, 69827176, 22A5FE6E, F64C4453, 5B238DD1, 3DF9C0C

D87C24F3, 912FE998, 9FF4A064, 55EE46AE, BC3669A5, 3DF9C0C, 8D7E53E4, 22A5FE6E, 31114FD9, 5B238DD1

BC3669A5, C45F164E, 912FE998, D281927F, 55EE46AE, 5B238DD1, 695B23B7, 8D7E53E4, 97F9B88A, 31114FD9

55EE46AE, 2211A508, C45F164E, BFA66244, D281927F, 31114FD9, 6FAA776F, 695B23B7, F94F9235, 97F9B88A

D281927F, 80B1F3DE, 2211A508, 7C593B11, BFA66244, 97F9B88A, 4D94F720, 6FAA776F, 6C8EDDA5, F94F9235

BFA66244, 3AA6A8F5, 80B1F3DE, 46942088, 7C593B11, F94F9235, D81C6137, 4D94F720, A9DDBDBE, 6C8EDDA5

7C593B11, 9E4C4BF6, 3AA6A8F5, C7CF7A02, 46942088, 6C8EDDA5, B2ECCABD, D81C6137, 53DC8136, A9DDBDBE

46942088, F929216E, 9E4C4BF6, 9AA3D4EA, C7CF7A02, A9DDBDBE, A96B1820, B2ECCABD, 7184DF60, 53DC8136

C7CF7A02, D9AEEFAF, F929216E, 312FDA79, 9AA3D4EA, 53DC8136, 5A5E09B3, A96B1820, B32AF6CB, 7184DF60

9AA3D4EA, 8BB34505, D9AEFFAF, A485BBE4, 312FDA79, 7184DF60, 616711FA, 5A5E09B3, AC6082A5, B32AF6CB  
312FDA79, 07067302, 8BB34505, BBEBEF66, A485BBE4, B32AF6CB, F4F47116, 616711FA, 7826CD69, AC6082A5  
A485BBE4, 51997747, 07067302, CD14162E, BBEBEF66, AC6082A5, FAE97297, F4F47116, 9C47E985, 7826CD69  
BBEBEF66, C213132C, 51997747, 19CC081C, CD14162E, 7826CD69, 887E5A3F, FAE97297, D1C45BD3, 9C47E985  
CD14162E, 29D001F0, C213132C, 65DD1D46, 19CC081C, 9C47E985, 187068EF, 887E5A3F, A5CA5FEB, D1C45BD3  
19CC081C, 2B59B58A, 29D001F0, 4C4CB308, 65DD1D46, D1C45BD3, 56C66FD3, 187068EF, F968FE21, A5CA5FEB  
65DD1D46, C45681A6, 2B59B58A, 4007C0A7, 4C4CB308, A5CA5FEB, D718432A, 56C66FD3, C1A3BC61, F968FE21  
4C4CB308, 2E32CA16, C45681A6, 66D628AD, 4007C0A7, F968FE21, 775BA27D, D718432A, 19BF4D5B, C1A3BC61  
4007C0A7, 5C712D51, 2E32CA16, 5A069B11, 66D628AD, C1A3BC61, 6243D22F, 775BA27D, 610CAB5C, 19BF4D5B  
66D628AD, 989BC126, 5C712D51, CB2858B8, 5A069B11, 19BF4D5B, 44DCD35A, 6243D22F, 6E89F5DD, 610CAB5C  
5A069B11, 9EE4CA1F, 989BC126, C4B54571, CB2858B8, 610CAB5C, 8FBE3F7E, 44DCD35A, 0F48BD89, 6E89F5DD  
CB2858B8, F417F849, 9EE4CA1F, 6F049A62, C4B54571, 6E89F5DD, DA718428, 8FBE3F7E, 734D6913, 0F48BD89  
C4B54571, 75239882, F417F849, 93287E7B, 6F049A62, 0F48BD89, 91573E0A, DA718428, F8FDFA3E, 734D6913  
6F049A62, 3AC6B69F, 75239882, 5FE127D0, 93287E7B, 734D6913, 2A5224A6, 91573E0A, C610A369, F8FDFA3E  
93287E7B, 0B7C24AC, 3AC6B69F, 8E6209D4, 5FE127D0, F8FDFA3E, 8128FFB7, 2A5224A6, 5CF82A45, C610A369  
5FE127D0, 2854DCE0, 0B7C24AC, 1ADA7CEB, 8E6209D4, C610A369, FF374DFD, 8128FFB7, 489298A9, 5CF82A45  
8E6209D4, 267080E2, 2854DCE0, F092B02D, 1ADA7CEB, 5CF82A45, C5E0CCD7, FF374DFD, A3FEDE04, 489298A9  
1ADA7CEB, 7806D96F, 267080E2, 537380A1, F092B02D, 489298A9, 31860C44, C5E0CCD7, DD37F7FC, A3FEDE04  
F092B02D, 52638496, 7806D96F, C2038899, 537380A1, A3FEDE04, CEE7092B, 31860C44, 83335F17, DD37F7FC  
537380A1, 59FC5CDB, 52638496, 1B65BDE0, C2038899, DD37F7FC, 46827AAE, CEE7092B, 183110C6, 83335F17  
C2038899, 8AE30FBE, 59FC5CDB, 8E125949, 1B65BDE0, 83335F17, A757A907, 46827AAE, 9C24AF3B, 183110C6  
1B65BDE0, 4F4AEBED, 8AE30FBE, F1736D67, 8E125949, 183110C6, E90F38FC,

A757A907, 09EAB91A, 9C24AF3B  
8E125949, 65BBCCCC, 4F4AEBED, 8C3EFA2B, F1736D67, 9C24AF3B, EC65CB85,  
E90F38FC, 5EA41E9D, 09EAB91A  
F1736D67, 0B3B88C1, 65BBCCCC, 2BAFB53D, 8C3EFA2B, 09EAB91A, 54B06FBD,  
EC65CB85, 3CE3F3A4, 5EA41E9D  
8C3EFA2B, 6DF30989, 0B3B88C1, EF333196, 2BAFB53D, 5EA41E9D, D8D6F0E3,  
54B06FBD, 972E17B1, 3CE3F3A4  
2BAFB53D, 156421AC, 6DF30989, EE23042C, EF333196, 3CE3F3A4, B30DA892,  
D8D6F0E3, C1BEF552, 972E17B1  
EF333196, 6F54F9CA, 156421AC, CC2625B7, EE23042C, 972E17B1, F526A85A, B30DA892,  
5BC38F63, C1BEF552  
EE23042C, A5D28921, 6F54F9CA, 9086B055, CC2625B7, C1BEF552, 5F5587DB, F526A85A,  
36A24ACC, 5BC38F63  
CC2625B7, 2959D915, A5D28921, 53E729BD, 9086B055, 5BC38F63, 9FABAC24, 5F5587DB,  
9AA16BD4, 36A24ACC  
9086B055, 4EFF0384, 2959D915, 4A248697, 53E729BD, 36A24ACC, 52E4FB9B, 9FABAC24,  
561F6D7D, 9AA16BD4  
53E729BD, 17292945, 4EFF0384, 676454A5, 4A248697, 9AA16BD4, E13C3BDA, 52E4FB9B,  
AEB0927E, 561F6D7D  
4A248697, 5FE71F22, 17292945, FC0E113B, 676454A5, 561F6D7D, 71244E49, E13C3BDA,  
93EE6D4B, AEB0927E  
676454A5, DC06A80F, 5FE71F22, A4A5145C, FC0E113B, AEB0927E, AA49234C,  
71244E49, F0EF6B84, 93EE6D4B  
FC0E113B, 5BD21FC5, DC06A80F, 9C7C897F, A4A5145C, 93EE6D4B, 42532D95,  
AA49234C, 913925C4, F0EF6B84  
A4A5145C, 5587BC4F, 5BD21FC5, 1AA03F70, 9C7C897F, F0EF6B84, CDA86FD0,  
42532D95, 248D32A9, 913925C4  
9C7C897F, A1755F6B, 5587BC4F, 487F156F, 1AA03F70, 913925C4, 69C12F76, CDA86FD0,  
4CB65509, 248D32A9  
1AA03F70, 100A6B19, A1755F6B, 1EF13D56, 487F156F, 248D32A9, 44272219, 69C12F76,  
A1BF4336, 4CB65509  
487F156F, AA2CFD07, 100A6B19, D57DAE85, 1EF13D56, 4CB65509, CBD360C3, 44272219,  
04BDD9A7, A1BF4336  
1EF13D56, 28246D22, AA2CFD07, 29AC6440, D57DAE85, A1BF4336, 27A64C2D,  
CBD360C3, 9C886510, 04BDD9A7  
D57DAE85, 4909C2BD, 28246D22, B3F41EA8, 29AC6440, 04BDD9A7, CCB70B88,  
27A64C2D, 4D830F2F, 9C886510  
29AC6440, 9020271B, 4909C2BD, 91B488A0, B3F41EA8, 9C886510, 2020C0FC, CCB70B88,  
9930B49E, 4D830F2F  
B3F41EA8, A557D838, 9020271B, 270AF524, 91B488A0, 4D830F2F, 7541E108, 2020C0FC,  
DC2E2332, 9930B49E  
91B488A0, F879D1F8, A557D838, 809C6E40, 270AF524, 9930B49E, 0A66EBF9, 7541E108,  
8303F080, DC2E2332

270AF524, 39BAC08A, F879D1F8, 5F60E295, 809C6E40, DC2E2332, A0AB24D8, 0A66EBF9, 078421D5, 8303F080

809C6E40, DF212B9C, 39BAC08A, E747E3E1, 5F60E295, 8303F080, 44C068DD, A0AB24D8, 9BAFE429, 078421D5

5F60E295, 46F2CD86, DF212B9C, EB0228E6, E747E3E1, 078421D5, 3F8B3B48, 44C068DD, AC936282, 9BAFE429

E747E3E1, A17766F4, 46F2CD86, 84AE737C, EB0228E6, 9BAFE429, 873A41C4, 3F8B3B48, 01A37513, AC936282

EB0228E6, FC20AA01, A17766F4, CB36191B, 84AE737C, AC936282, A2969EB4, 873A41C4, 2CED20FE, 01A37513

84AE737C, 93A30DD9, FC20AA01, DD9BD285, CB36191B, 01A37513, 7B345F4F, A2969EB4, E907121C, 2CED20FE

CB36191B, 98554E1C, 93A30DD9, 82A807F0, DD9BD285, 2CED20FE, 07B2EA78, 7B345F4F, 5A7AD28A, E907121C

DD9BD285, 79D46BD1, 98554E1C, 8C37664E, 82A807F0, E907121C, 93451653, 07B2EA78, D17D3DEC, 5A7AD28A

82A807F0, 5FBC55DB, 79D46BD1, 55387261, 8C37664E, 5A7AD28A, AA0DF949, 93451653, CBA9E01E, D17D3DEC

8C37664E, DEF23A3B, 5FBC55DB, 51AF45E7, 55387261, D17D3DEC, 030FFB9A, AA0DF949, 14594E4D, CBA9E01E

55387261, 287DB1EB, DEF23A3B, F1576D7E, 51AF45E7, CBA9E01E, 0D9CD217, 030FFB9A, 37E526A8, 14594E4D

51AF45E7, CF955B8E, 287DB1EB, C8E8EF7B, F1576D7E, 14594E4D, BECE1BBD, 0D9CD217, 3FEE680C, 37E526A8

F1576D7E, 83B6B7E8, CF955B8E, F6C7ACA1, C8E8EF7B, 37E526A8, D97CFEEC, BECE1BBD, 73485C36, 3FEE680C

C8E8EF7B, 7943C443, 83B6B7E8, 556E3B3E, F6C7ACA1, 3FEE680C, DBEA79F5, D97CFEEC, 386EF6FB, 73485C36

F6C7ACA1, F336AA45, 7943C443, DADFA20E, 556E3B3E, 73485C36, 91704BDB, DBEA79F5, F3FBB365, 386EF6FB

556E3B3E, 2FF847D6, F336AA45, 0F110DE5, DADFA20E, 386EF6FB, 40CBA97D, 91704BDB, A9E7D76F, F3FBB365

DADFA20E, 33FE64C9, 2FF847D6, DAA917CC, 0F110DE5, F3FBB365, B0BD2456, 40CBA97D, C12F6E45, A9E7D76F

0F110DE5, 78378FE9, 33FE64C9, E11F58BF, DAA917CC, A9E7D76F, CA09D415, B0BD2456, 2EA5F503, C12F6E45

下列是变量  $X_0, X_1, X_2, X_3, X_4, X'_0, X'_1, X'_2, X'_3, X'_4$  的连续值(用 16 进制表示), 它们在处理第 2 块过程中获得。

52720555, 3B09A402, 94C343B1, 9CEDC3EA, 9039D740, 52720555, 3B09A402, 94C343B1, 9CEDC3EA, 9039D740

9039D740, 59874B6C, 3B09A402, 0D0EC653, 9CEDC3EA, 9039D740, 7FA6C9AF, 3B09A402, 0D0EC653, 9CEDC3EA

9CEDC3EA, 1D0D43D8, 59874B6C, 269008EC, 0D0EC653, 9CEDC3EA, 149F92B4,

7FA6C9AF, 269008EC, 0D0EC653  
0D0EC653, EF3045D6, 1D0D43D8, 1D2DB166, 269008EC, 0D0EC653, 0E887E05, 149F92B4,  
9B26BDFF, 269008EC  
269008EC, 1E6BC8AD, EF3045D6, 350F6074, 1D2DB166, 269008EC, 6E8757AC, 0E887E05,  
7E4AD052, 9B26BDFF  
1D2DB166, 79CC70E3, 1E6BC8AD, C1175BBC, 350F6074, 9B26BDFF, 32C1290B,  
6E8757AC, 21F8143A, 7E4AD052  
350F6074, 13A4B937, 79CC70E3, AF22B479, C1175BBC, 7E4AD052, 8EB02C5A, 32C1290B,  
1D5EB1BA, 21F8143A  
C1175BBC, EE066CB9, 13A4B937, 31C38DE7, AF22B479, 21F8143A, 719EB9D9,  
8EB02C5A, 04A42CCB, 1D5EB1BA  
AF22B479, A08AFF93, EE066CB9, 92E4DC4E, 31C38DE7, 1D5EB1BA, 3D5B8A9A,  
719EB9D9, C0B16A3A, 04A42CCB  
31C38DE7, 89E27A43, A08AFF93, 19B2E7B8, 92E4DC4E, 04A42CCB, 47DEA0A3,  
3D5B8A9A, 7AE765C6, C0B16A3A  
92E4DC4E, 50EEC8A1, 89E27A43, 2BFE4E82, 19B2E7B8, C0B16A3A, A6AACEE1,  
47DEA0A3, 6E2A68F5, 7AE765C6  
19B2E7B8, 0FDE892D, 50EEC8A1, 89E90E27, 2BFE4E82, 7AE765C6, 4456D048,  
A6AACEE1, 7A828D1F, 6E2A68F5  
2BFE4E82, 47B046C8, 0FDE892D, BB228543, 89E90E27, 6E2A68F5, 072D166E, 4456D048,  
AB3B869A, 7A828D1F  
89E90E27, 5C8F582E, 47B046C8, 7A24B43F, BB228543, 7A828D1F, B37A11D1, 072D166E,  
5B412111, AB3B869A  
BB228543, 3D7F05B8, 5C8F582E, C11B211E, 7A24B43F, AB3B869A, 654CBE94, B37A11D1,  
B459B81C, 5B412111  
7A24B43F, 962BCAF7, 3D7F05B8, 3D60B972, C11B211E, 5B412111, 6AFF9ABA,  
654CBE94, E84746CD, B459B81C  
C11B211E, 1A459D2E, 962BCAF7, FC16E0F5, 3D60B972, B459B81C, EE0E390E,  
6AFF9ABA, 32FA5195, E84746CD  
3D60B972, 1622907A, 1A459D2E, AF2BDE58, FC16E0F5, E84746CD, 569023C2, EE0E390E,  
FE6AE9AB, 32FA5195  
FC16E0F5, B75B2E49, 1622907A, 1674B869, AF2BDE58, 32FA5195, 5C2944E8, 569023C2,  
38E43BB8, FE6AE9AB  
AF2BDE58, 6F16D4C4, B75B2E49, 8A41E858, 1674B869, FE6AE9AB, 103CE067, 5C2944E8,  
408F095A, 38E43BB8  
1674B869, 46FDEE89, 6F16D4C4, 6CB926DD, 8A41E858, 38E43BB8, AB641473, 103CE067,  
A513A170, 408F095A  
8A41E858, E9F89F50, 46FDEE89, 5B5311BC, 6CB926DD, 408F095A, 25643DBF, AB641473,  
F3819C40, A513A170  
6CB926DD, EC9A614C, E9F89F50, F7BA251B, 5B5311BC, A513A170, E60A5336,  
25643DBF, 9051CEAD, F3819C40  
5B5311BC, D525F69D, EC9A614C, E27D43A7, F7BA251B, F3819C40, FF4D318D,  
E60A5336, 90F6FC95, 9051CEAD



F7BA251B, EDFBF331, D525F69D, 698533B2, E27D43A7, 9051CEAD, 6D5A28DD, FF4D318D, 294CDB98, 90F6FC95

E27D43A7, 93C5E732, EDFBF331, 97DA7754, 698533B2, 90F6FC95, 855C140A, 6D5A28DD, 34C637FD, 294CDB98

698533B2, 24907FDF, 93C5E732, EFCCC7B7, 97DA7754, 294CDB98, 79C1BC35, 855C140A, 68A375B5, 34C637FD

97DA7754, E2193F3E, 24907FDF, 179CCA4F, EFCCC7B7, 34C637FD, B2D5EF34, 79C1BC35, 70502A15, 68A375B5

EFCCC7B7, D3AD6006, E2193F3E, 41FF7C92, 179CCA4F, 68A375B5, DB87209A, B2D5EF34, 06F0D5E7, 70502A15

179CCA4F, 6B8BFAB4, D3AD6006, 64FCFB88, 41FF7C92, 70502A15, 4DEC84F2, DB87209A, 57BCD2CB, 06F0D5E7

41FF7C92, 5052D6EF, 6B8BFAB4, B5801B4E, 64FCFB88, 06F0D5E7, D4F6A30D, 4DEC84F2, 1C826B6E, 57BCD2CB

64FCFB88, FF36EBC8, 5052D6EF, 2FEAD1AE, B5801B4E, 57BCD2CB, 0191C9F0, D4F6A30D, B213C937, 1C826B6E

B5801B4E, 5A010C53, FF36EBC8, 4B5BBD41, 2FEAD1AE, 1C826B6E, 20FBAB36, 0191C9F0, DA8C3753, B213C937

2FEAD1AE, 952BFB5D, 5A010C53, DBAF23FC, 4B5BBD41, B213C937, 7E796493, 20FBAB36, 4727C006, DA8C3753

4B5BBD41, FE05BEE3, 952BFB5D, 04314D68, DBAF23FC, DA8C3753, C9EABB3E, 7E796493, EEACD883, 4727C006

DBAF23FC, 2256AF69, FE05BEE3, AFED7654, 04314D68, 4727C006, B44977A5, C9EABB3E, E5924DF9, EEACD883

04314D68, 5285B0D3, 2256AF69, 16FB8FF8, AFED7654, EEACD883, 287580C6, B44977A5, AAECFB27, E5924DF9

AFED7654, 1DFB856C, 5285B0D3, 5ABDA489, 16FB8FF8, E5924DF9, 1E1DBD16, 287580C6, 25DE96D1, AAECFB27

16FB8FF8, 32974404, 1DFB856C, 16C34D4A, 5ABDA489, AAECFB27, FBEB21BA, 1E1DBD16, D60318A1, 25DE96D1

5ABDA489, 90AC71CE, 32974404, EE15B077, 16C34D4A, 25DE96D1, B74BF3E2, FBEB21BA, 76F45878, D60318A1

16C34D4A, 849CCC12, 90AC71CE, 5D1010CA, EE15B077, D60318A1, 755BEDDF, B74BF3E2, AC86EBEF, 76F45878

EE15B077, 340EBE92, 849CCC12, B1C73A42, 5D1010CA, 76F45878, 3CD099C6, 755BEDDF, 2FCF8ADD, AC86EBEF

5D1010CA, F531E5F5, 340EBE92, 73304A12, B1C73A42, AC86EBEF, A19BBAA2, 3CD099C6, 6FB77DD5, 2FCF8ADD

B1C73A42, 27528557, F531E5F5, 3AFA48D0, 73304A12, 2FCF8ADD, EFC554F1, A19BBAA2, 426718F3, 6FB77DD5

73304A12, E4AFA69F, 27528557, C797D7D4, 3AFA48D0, 6FB77DD5, F56F1485, EFC554F1, 6EEA8A86, 426718F3

3AFA48D0, E3462C93, E4AFA69F, 4A155C9D, C797D7D4, 426718F3, E0A1480A,

F56F1485, 1553C7BF, 6EEA8A86  
C797D7D4, 3CF5CD85, E3462C93, BE9A7F92, 4A155C9D, 6EEA8A86, 9F80007D,  
E0A1480A, BC5217D5, 1553C7BF  
4A155C9D, B6C756F9, 3CF5CD85, 18B24F8D, BE9A7F92, 1553C7BF, 090898BE, 9F80007D,  
85202B82, BC5217D5  
BE9A7F92, CC2AB627, B6C756F9, D73614F3, 18B24F8D, BC5217D5, A0CD75A2,  
090898BE, 0001F67E, 85202B82  
18B24F8D, E5471921, CC2AB627, 1D5BE6DB, D73614F3, 85202B82, 95FE46E6, A0CD75A2,  
2262F824, 0001F67E  
D73614F3, E8FEFBC6, E5471921, AAD89F30, 1D5BE6DB, 0001F67E, 4B55D832, 95FE46E6,  
35D68A83, 2262F824  
1D5BE6DB, 788FFBE7, E8FEFBC6, 1C648795, AAD89F30, 2262F824, 681302D4, 4B55D832,  
F91B9A57, 35D68A83  
AAD89F30, FA97F1BB, 788FFBE7, FBEF1BA3, 1C648795, 35D68A83, 860F8E32,  
681302D4, 5760C92D, F91B9A57  
1C648795, 2FE154B4, FA97F1BB, 3FEF9DE2, FBEF1BA3, F91B9A57, CA3DDAC0,  
860F8E32, 4C0B51A0, 5760C92D  
FBEF1BA3, D884695B, 2FE154B4, 5FC6EFEA, 3FEF9DE2, 5760C92D, 7E790793,  
CA3DDAC0, 3E38CA18, 4C0B51A0  
3FEF9DE2, A09357E9, D884695B, 8552D0BF, 5FC6EFEA, 4C0B51A0, 4E0DF927,  
7E790793, F76B0328, 3E38CA18  
5FC6EFEA, 019B9791, A09357E9, 11A56F62, 8552D0BF, 3E38CA18, 311DFB90, 4E0DF927,  
E41E4DF9, F76B0328  
8552D0BF, 70DB6FDF, 019B9791, 4D5FA682, 11A56F62, 7F6B0328, 24FA9DC7, 311DFB90,  
37E49D38, E41E4DF9  
11A56F62, 82F104B4, 70DB6FDF, 6E5E4406, 4D5FA682, E41E4DF9, CE45E142,  
24FA9DC7, 77EE40C4, 37E49D38  
4D5FA682, BFAB29F8, 82F104B4, 6DBF7DC3, 6E5E4406, 37E49D38, 9C4F267F, CE45E142,  
EA771C93, 77EE40C4  
6E5E4406, 880198A9, BFAB29F8, C412D20B, 6DBF7DC3, 77EE40C4, 06880805, 9C4F267F,  
17850B39, EA771C93  
6DBF7DC3, 917C197C, 880198A9, ACA7E2FE, C412D20B, EA771C93, 7625BD09, 06880805,  
3C99FE71, 17850B39  
C412D20B, 03E7992A, 917C197C, 0662A620, ACA7E2FE, 17850B39, 8720C8E7, 7625BD09,  
2020141A, 3C99FE71  
ACA7E2FE, 824CEF7A, 03E7992A, F065F245, 0662A620, 3C99FE71, CBB7DA7A,  
8720C8E7, 96F425D8, 2020141A  
0662A620, AF16F218, 824CEF7A, 9E64A80F, F065F245, 2020141A, 88851068, CBB7DA7A,  
83239E1C, 96F425D8  
F065F245, EFC8943D, AF16F218, 33BDEA09, 9E64A80F, 96F425D8, C85C4EB8, 88851068,  
DF69EB2E, 83239E1C  
9E64A80F, C8OFF53B, EFC8943D, 5BC862BC, 33BDEA09, 83239E1C, 57BF18E2,  
C85C4EB8, 1441A222, DF69EB2E

33BDEA09, 28DF9E36, C80FF53B, 2250F7BF, 5BC862BC, DF69EB2E, 48932C1A, 57BF18E2, 713AE321, 1441A222

5BC862BC, 6E1D8950, 28DF9E36, 3FD4EF20, 2250F7BF, 1441A222, 15C7B0BD, 48932C1A, FC63895E, 713AE321

2250F7BF, 21EEE621, 6E1D8950, 7E78D8A3, 3FD4EF20, 713AE321, FCBC9E78, 15C7B0BD, 4CB06922, FC63895E

3FD4EF20, 561379BA, 21EEE621, 762541B8, 7E78D8A3, FC63895E, DD28EA60, FCBC9E78, 1EC2F457, 4CB06922

7E78D8A3, 4D0255C5, 561379BA, BB988487, 762541B8, 4CB06922, CF1BB810, DD28EA60, F279E3F2, 1EC2F457

762541B8, 966845EC, 4D0255C5, 4DE6E958, BB988487, 1EC2F457, 5D899D62, CF1BB810, A3A98374, F279E3F2

BB988487, D922DEB8, 966845EC, 09571534, 4DE6E958, F279E3F2, F1144141, 5D899D62, 6EE0433C, A3A98374

4DE6E958, B919B2A3, D922DEB8, A117B259, 09571534, A3A98374, 940BBA12, F1144141, 26758976, 6EE0433C

09571534, D3CF80F9, B919B2A3, 8B7AE364, A117B259, 6EE0433C, 33DDA9B5, 940BBA12, 510507C4, 26758976

A117B259, F548EA98, D3CF80F9, 66CA8EE4, 8B7AE364, 26758976, DCE0B562, 33DDA9B5, 2EE84A50, 510507C4

8B7AE364, A1D3372D, F548EA98, 3E03E74F, 66CA8EE4, 510507C4, C103FBE9, DCE0B562, 76A6D4CF, 2EE84A50

66CA8EE4, 6578D66C, A1D3372D, 23AA63D5, 3E03E74F, 2EE84A50, 832961D9, C103FBE9, 82D58B73, 76A6D4CF

3E03E74F, 57C29604, 6578D66C, 4CDCB687, 23AA63D5, 76A6D4CF, B183744E, 832961D9, 0FEFA704, 82D58B73

23AA63D5, 27F5E937, 57C29604, E359B195, 4CDCB687, 82D58B73, E710A112, B183744E, A587660C, 0FEFA704

散列码是下列 160 位串:

12 A0 53 38 4A 9C 0C 88 E4 05 A0 6C 27 DC F4 9A DA 62 EB 2B

#### A2.9 例 9

本例数据串是 1000000 字节串,由字母“a”重复  $10^6$  次的 GB 1988 编码版本组成。

散列码是下列 160 位串:

52 78 32 43 C1 69 7B DB E1 6D 37 F9 7F 68 F0 83 25 DC 15 28

### A3 专用散列函数 2

散列函数 2。

#### A3.1 例 1

本例中数据串为空串,即零长度串。

散列码是下列 128 位串:

CD F2 62 13 A1 50 DC 3E CB 61 0F 18 F6 B3 8B 46

#### A3.2 例 2

本例中数据串由单个字节的数据串组成,即字母“a”的 GB 1988 编码版本。散列码是下列 128 位串:

86 BE 7A FA 33 9D 0F C7 CF C7 85 E7 2F 57 8D 33

### A.3.3 例 3

本例中数据串由“abc”的 GB 1988 编码版本的 3 字节串组成。它等同于位串：“01100001 01100010 01100011”。

经过填充过程后,由该数据串推导出的单个 16 字的块如下:

80636261 00000000 00000000 00000000 00000000 00000000 00000000 00000000  
00000000 00000000 00000000 00000000 00000000 00000000 00000018 00000000

下列是变量  $X_0, X_1, X_2, X_3, X'_0, X'_1, X'_2, X'_3$  的连续值(用 16 进制表示):

67452301, EFCDAB89, 98BADCFE, 10325476, 67452301, EFCDAB89, 98BADCFE, 10325476  
10325476, 6D431A77, EFCDAB89, 98BADCFE, 10325476, 70376F40, EFCDAB89, 98BADCFE  
98BADCFE, B05D8A99, 6D431A77, EFCDAB89, 98BADCFE, 989F6BB0, 70376F40, EFCDAB89  
EFCDAB89, 0C32E5C7, B05D8A99, 6D431A77, EFCDAB89, 39B14904, 989F6BB0, 70376F40  
6D431A77, A20B2C0F, 0C32E5C7, B05D8A99, 70376F40, 671C03CC, 39B14904, 989F6BB0  
B05D8A99, 74EBB911, A20B2C0F, 0C32E5C7, 989F6BB0, BFD55C42, 671C03CC, 39B14904  
0C32E5C7, 2FFB728B, 74EBB911, A20B2C0F, 39B14904, A12F346F, BFD55C42, 671C03CC  
A20B2C0F, A766AE02, 2FFB728B, 74EBB911, 671C03CC, 989C2210, A12F346F, BFD55C42  
74EBB911, 03234F3D, A766AE02, 2FFB728B, BFD55C42, 0F95FBEA, 989C2210, A12F346F  
2FFB728B, 52662805, 03234F3D, A766AE02, A12F346F, 068D5115, 0F95FBEA, 989C2210  
A766AE02, E778A4C3, 52662805, 03234F3D, 989C2210, AFCD27FC, 068D5115, 0F95FBEA  
03234F3D, 1C7F5769, E778A4C3, 52662805, 0F95FBEA, CBD1F3F8, AFCD27FC, 068D5115  
52662805, 95765642, 1C7F5769, E778A4C3, 068D5115, CFFE405F, CBD1F3F8, AFCD27FC  
E778A4C3, 35F37B70, 95765642, 1C7F5769, AFCD27FC, 2B55C9C3, CFFE405F, CBD1F3F8  
1C7F5769, 398F8F52, 35F37B70, 95765642, CBD1F3F8, DD6A43FB, 2B55C9C3, CFFE405F  
95765642, 13F3C36B, 398F8F52, 35F37B70, CFFE405F, 049B909E, DD6A43FB, 2B55C9C3  
35F37B70, 058D8BB5, 13F3C36B, 398F8F52, 2B55C9C3, 3713BFFD, 049B909E, DD6A43FB  
398F8F52, FCBE3664, 058D8BB5, 13F3C36B, DD6A43FB, 82ADB53, 3713BFFD, 049B909E  
13F3C36B, 7F7306A6, FCBE3664, 058D8BB5, 049B909E, CC1D8105, 82ADB53, 3713BFFD  
058D8BB5, 34CC3963, F7F306A6, FCBE3664, 3713BFFD, BE09159A, CC1D8105, 82ADB53  
FCBE3664, 416E8BA0, 34CC3963, F7F306A6, 82ADB53, 541AE568, BE09159A, CC1D8105  
F7F306A6, EDE91870, 416E8BA0, 34CC3963, CC1D8105, 27D40F94, 541AE568, BE09159A  
34CC3963, C352C547, EDE91870, 416E8BA0, BE09159A, 675C363A, 27D40F94, 541AE568  
416E8BA0, 5D5EEE28, C352C547, EDE91870, 541AE568, 77F3A38B, 675C363A, 27D40F94  
EDE91870, 6CC4BEF2, 5D5EEE28, C352C547, 27D40F94, 84D73C44, 77F3A38B, 675C363A  
C352C547, E140970B, 6CC4BEF2, 5D5EEE28, 675C363A, D2958F37, 84D73C44, 77F3A38B  
5D5EEE28, 79F631A9, E140970B, 6CC4BEF2, 77F3A38B, FC39C927, D2958F37, 84D73C44  
6CC4BEF2, 038E0E91, 79F631A9, E140970B, 84D73C44, E3A5A4DE, FC39C927, D2958F37  
E140970B, 1B942D52, 038E0E91, 79F631A9, D2958F37, 4BA3A889, E3A5A4DE, FC39C927  
79F631A9, 496AECFD, 1B942D52, 038E0E91, FC39C927, A964BA74, 4BA3A889, E3A5A4DE  
038E0E91, FE6CD56F, 496AECFD, 1B942D52, E3A5A4DE, 7AF9DDB0, A964BA74, 4BA3A889  
1B942D52, 2E94F501, FE6CD56F, 496AECFD, 4BA3A889, 7DA68EA9, 7AF9DDB0, A964BA74  
496AECFD, 584E8E58, 2E94F501, FE6CD56F, A964BA74, 9C7247E5, 7DA68EA9, 7AF9DDB0  
FE6CD56F, 41A17EFA, 584E8E58, 2E94F501, 7AF9DDB0, 0130312B, 9C7247E5, 7DA68EA9  
2E94F501, 8981C6CD, 41A17EFA, 584E8E58, 7DA68EA9, 90552232, 0130312B, 9C7247E5

584E8E58, 400A93E1, 8981C6CD, 41A17EFA, 9C7247E5, 99C1FBA4, 90552232, 0130312B  
 41A17EFA, 841F817F, 400A93E1, 8981C6CD, 0130312B, 9D481CD2, 99C1FBA4, 90552232  
 8981C6CD, 659379BE, 841F817F, 400A93E1, 90552232, F5AABE07, 9D481CD2, 99C1FBA4  
 400A93E1, AB3D9A70, 659379BE, 841F817F, 99C1FBA4, C3AFB7E6, F5AABE07, 9D481CD2  
 841F817F, D3D21DC8, AB3D9A70, 659379BE, 9D481CD2, 473E2B79, C3AFB7E6, F5AABE07  
 659379BE, 38C8D29D, D3D21DC8, AB3D9A70, F5AABE07, C4CAFF99, 473E2B79, C3AFB7E6  
 AB3D9A70, 738B9B0F, 38C8D29D, D3D21DC8, C3AFB7E6, A2879AA4, C4CAFF99, 473E2B79  
 D3D21DC8, 8528B83E, 738B9B0F, 38C8D29D, 473E2B79, 56565EDB, A2879AA4, C4CAFF99  
 38C8D29D, 7345AF18, 8528B83E, 738B9B0F, C4CAFF99, E7A4BD86, 56565EDB, A2879AA4  
 738B9B0F, FFCC52B, 7345AF18, 8528B83E, A2879AA4, 974B9E10, E7A4BD86, 56565EDB  
 8528B83E, A77E902B, FFCC52B, 7345AF18, 56565EDB, 96CC5AE1, 974B9E10, E7A4BD86  
 7345AF18, CB9C6C83, A77E902B, FFCC52B, E7A4BD86, 57E6A772, 96CC5AE1, 974B9E10  
 FFCC52B, 38A2DA83, CB9C6C83, A77E902B, 974B9E10, F10B6CF5, 57E6A772, 96CC5AE1  
 A77E902B, 487F9401, 38A2DA83, CB9C6C83, 96CC5AE1, 90426E6B, F10B6CF5, 57E6A772  
 CB9C6C83, C7184576, 487F9401, 38A2DA83, 57E6A772, 0066E6BE, 90426E6B, F10B6CF5  
 38A2DA83, 56D619B1, C7184576, 487F9401, F10B6CF5, 22D17257, 0066E6BE, 90426E6B  
 487F9401, 3A35A3C5, 56D619B1, C7184576, 90426E6B, 016777A4, 22D17257, 0066E6BE  
 C7184576, B5517538, 3A35A3C5, 56D619B1, 0066E6BE, 9A8DC5A0, 016777A4, 22D17257  
 56D619B1, 4609C4C2, B5517538, 3A35A3C5, 22D17257, A9C46E68, 9A8DC5A0, 016777A4  
 3A35A3C5, D5C2B699, 4609C4C2, B5517538, 016777A4, 13B0D540, A9C46E68, 9A8DC5A0  
 B5517538, 342AF741, D5C2B699, 4609C4C2, 9A8DC5A0, 983D8B08, 13B0D540, A9C46E68  
 4609C4C2, 38286DDA, 342AF741, D5C2B699, A9C46E68, 96084F4E, 983D8B08, 13B0D540  
 D5C2B699, 9BCEEC0A, 38286DDA, 342AF741, 13B0D540, D25FDBB1, 96084F4E, 983D8B08  
 342AF741, 5803DF3A, 9BCEEC0A, 38286DDA, 983D8B08, 35EA6FE0, D25FDBB1, 96084F4E  
 38286DDA, E1B026EB, 5803DF3A, 9BCEEC0A, 96084F4E, B862709F, 35EA6FE0, D25FDBB1  
 9BCEEC0A, 31587C22, E1B026EB, 5803DF3A, D25FDBB1, C02839EB, B862709F, 35EA6FE0  
 5803DF3A, 9B25E1DC, 31587C22, E1B026EB, 35EA6FE0, 00245200, C02839EB, B862709F  
 E1B026EB, 2205379E, 9B25E1DC, 31587C22, B862709F, CB116A95, 00245200, C02839EB  
 31587C22, 5E3334A3, 2205379E, 9B25E1DC, C02839EB, B90EE1BF, CB116A95, 00245200  
 9B25E1DC, 56F80FA9, 5E3334A3, 2205379E, 00245200, 64132D32, B90EE1BF, CB116A95

散列码是下列 128 位串：

C1 4A 12 19 9C 66 E4 BA 84 63 6B 0F 69 14 4C 77

#### A3.4 例 4

本例中数据串是 14 字节串，由“message digest”GB 1988 编码版本组成。

散列码是下列 128 位串：

9E 32 7B 3D 6E 52 30 62 AF C1 13 2D 7D F9 D1 B8

#### A3.5 例 5

本例中数据串是 26 字节串，由“abcdefghijklmnopqrstuvwxy”GB 1988 编码版本组成。

散列码是以下 128 位串：

FD 2A A6 07 F7 1D C8 F5 10 71 49 22 B3 71 83 4E

#### A3.6 例 6

本例中数据串是 62 字节串，由“ABCDEFGHJKLMNPQRSTUVWXYZ Zabcdefghijklmnop

jklmnopqrstuvwxyz0123456789”的 GB 1988 编码版本组成。

散列码是下列 128 位串：

B0 E2 0B 6E 31 16 64 02 86 ED 3A 87 A5 71 30 79 B2 1F 51 89

### A3.7 例 7

本例中数据串是 80 字节串，由 8 次重复“1234567890”的 GB1988 编码版本组成。

散列码是下列 160 位串：

D1 E9 59 EB 17 9C 91 1F AE A4 62 4C 60 C5 C7 02

### A3.8 例 8

本例中数据串是 56 字节串，由“abcdcbcdcedefdefgefghfghijhijhijklklmklmlnlnomnopnopq”的 GB 1988 编码版本组成。

经过填充过程后，由数据串推导出来的两个 16 字的块如下：

64636261 65646362 66656463 67666564 68676665 69686766 6A696867 6B6A6968  
6C6B6A69 6D6C6B6A 6E6D6C6B 6F6E6D6C 706F6E6D 71706F6E 00000080 00000000

00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000  
00000000 00000000 00000000 00000000 00000000 00000000 000001C0 00000000

下列是变量  $X_0, X_1, X_2, X_3, X'_0, X'_1, X'_2, X'_3$  的连续值(用 16 进制表示)，它们在处理第 1 块过程中获得。

67452301, EFCDAB89, 98BADCFE, 10325476, 67452301, EFCDAB89, 98BADCFE, 10325476  
10325476, 6D431997, EFCDAB89, 98BADCFE, 10325476, D89ED5A9, EFCDAB89, 98BADCFE  
98BADCFE, C9AE23F2, 6D431997, EFCDAB89, 98BADCFE, 69B10AC1, D89ED5A9, EFCDAB89  
EFCDAB89, 69A6A520, C9AE23F2, 6D431997, EFCDAB89, B661DB9C, 69B10AC1, D89ED5A9  
6D431997, FB032247, 69A6A520, C9AE23F2, D89ED5A9, ABACC2AF, B661DB9C, 69B10AC1  
C9AE23F2, 16C49226, FB032247, 69A6A520, 69B10AC1, D412CAD1, ABACC2AF, B661DB9C  
69A6A520, 77A099B7, 16C49226, FB032247, B661DB9C, E2DEDf22, D412CAD1, ABACC2AF  
FB032247, 3B9BAEB7, 77A099B7, 16C49226, ABACC2AF, CFB03688, E2DEDf22, D412CAD1  
16C49226, DA61AB82, 3B9BAEB7, 77A099B7, D412CAD1, 72599389, CFB03688, E2DEDf22  
77A099B7, 54C888CC, DA61AB82, 3B9BAEB7, E2DEDf22, CF3CD682, 72599389, CFB03688  
3B9BAEB7, F2635347, 54C888CC, DA61AB82, CFB03688, B235784E, CF3CD682, 72599389  
DA61AB82, E2CAC9B4, F2635347, 54C888CC, 72599389, 881678DF, B235784E, CF3CD682  
54C888CC, 9596C718, E2CAC9B4, F2635347, CF3CD682, E815373B, 881678DF, B235784E  
F2635347, 9DD54912, 9596C718, E2CAC9B4, B235784E, BD994B56, E815373B, 881678DF  
E2CAC9B4, 2E8539A7, 9DD54912, 9596C718, 881678DF, B0055655, BD994B56, E815373B  
9596C718, 2303C213, 2E8539A7, 9DD54912, E815373B, CC87EF5A, B0055655, BD994B56  
9DD54912, EA79BE25, 2303C213, 2E8539A7, BD994B56, 6B24384D, CC87EF5A, B0055655  
2E8539A7, 23D7CB45, EA79BE25, 2303C213, B0055655, 93E7329F, 6B24384D, CC87EF5A  
2303C213, F028EF04, 23D7CB45, EA79BE25, CC87EF5A, 35B95AE7, 93E7329F, 6B24384D  
EA79BE25, 48863F19, F028EF04, 23D7CB45, 6B24384D, 06C6536D, 35B95AE7, 93E7329F  
23D7CB45, 514C81B6, 48863F19, F028EF04, 93E7329F, FF1C5DC7, 06C6536D, 35B95AE7  
F028EF04, 6102CE67, 514C81B6, 48863F19, 35B95AE7, D0D541F1, FF1C5DC7, 06C6536D  
48863F19, 330485FD, 6102CE67, 514C81B6, 06C6536D, A94C0DD9, D0D541F1, FF1C5DC7  
514C81B6, 289E8C82, 330485FD, 6102CE67, FF1C5DC7, DEDC1E39, A94C0DD9, D0D541F1  
6102CE67, 13CC3A1D, 289E8C82, 330485FD, D0D541F1, 12D926C0, DEDC1E39, A94C0DD9

330485FD, 40A226A6, 13CC3A1D, 289E8C82, A94C0DD9, ED7EDA63, 12D926C0, DEDC1E39  
 289E8C82, 70BFB1A8, 40A226A6, 13CC3A1D, DEDC1E39, 9E52219C, ED7EDA63, 12D926C0  
 13CC3A1D, CE1D1A37, 70BFB1A8, 40A226A6, 12D926C0, F5D22339, 9E52219C, ED7EDA63  
 40A226A6, EC9F7830, CE1D1A37, 70BFB1A8, ED7EDA63, 0BC5B4FC, F5D22339, 9E52219C  
 70BFB1A8, 3CF2D6EE, EC9F7830, CE1D1A37, 9E52219C, FCFBD391, 0BC5B4FC, F5D22339  
 CE1D1A37, F0C1F95C, 3CF2D6EE, EC9F7830, F5D22339, 2B6A389B, FCFBD391, 0BC5B4FC  
 EC9F7830, 9A351A9D, F0C1F95C, 3CF2D6EE, 0BC5B4FC, FBF85B05, 2B6A389B, FCFBD391  
 3CF2D6EE, 138B0685, 9A351A9D, F0C1F95C, FCFBD391, F7BBBE8B, FBF85B05, 2B6A389B  
 F0C1F95C, EA3574D1, 138B0685, 9A351A9D, 2B6A389B, C8592ACC, F7BBBE8B, FBF85B05  
 9A351A9D, 4719C849, EA3574D1, 138B0685, FBF85B05, FE2D3EFA, C8592ACC, F7BBBE8B  
 138B0685, 57F52A13, 4719C849, EA3574D1, F7BBBE8B, 5411CC34, FE2D3EFA, C8592ACC  
 EA3574D1, 4751F880, 57F52A13, 4719C849, C8592ACC, DC8ED546, 5411CC34, FE2D3EFA  
 4719C849, 80605BAF, 4751F880, 57F52A13, FE2D3EFA, 55C1E317, DC8ED546, 5411CC34  
 57F52A13, 1E53AD4A, 80605BAF, 4751F880, 5411CC34, 0B92E4F0, 55C1E317, DC8ED546  
 4751F880, 1ABEED79, 1E53AD4A, 80605BAF, DC8ED546, 5E192900, 0B92E4F0, 55C1E317  
 80605BAF, 75EACBB7, 1ABEED79, 1E53AD4A, 55C1E317, 186EBOCF, 5E192900, 0B92E4F0  
 1E53AD4A, 08AC1056, 75EACBB7, 1ABEED79, 0B92E4F0, 8F3A64E3, 186EBOCF, 5E192900  
 1ABEED79, 9BDB7A88, 08AC1056, 75EACBB7, 5E192900, 3701E7B3, 8F3A64E3, 186EBOCF  
 75EACBB7, ADF32F05, 9BDB7A88, 08AC1056, 186EBOCF, 6CE969E9, 3701E7B3, 8F3A64E3  
 08AC1056, 2277B80D, ADF32F05, 9BDB7A88, 8F3A64E3, EE7224D5, 6CE969E9, 3701E7B3  
 9BDB7A88, 535DBB9A, 2277B80D, ADF32F05, 3701E7B3, 3E849D0F, EE7224D5, 6CE969E9  
 ADF32F05, 2A494EC5, 535DBB9A, 2277B80D, 6CE969E9, DDBD8EE7, 3E849D0F, EE7224D5  
 2277B80D, 693C7A09, 2A494EC5, 535DBB9A, EE7224D5, C3DDAC40, DDBD8EE7, 3E849D0F  
 535DBB9A, 148A5796, 693C7A09, 2A494EC5, 3E849D0F, 5E0E10B9, C3DDAC40, DDBD8EE7  
 2A494EC5, D2932448, 148A5796, 693C7A09, DDBD8EE7, ICCB75AF, 5E0E10B9, C3DDAC40  
 693C7A09, 39CA97B6, D2932448, 148A5796, C3DDAC40, 27F81499, ICCB75AF, 5E0E10B9  
 148A5796, 770BCE98, 39CA97B6, D2932448, 5E0E10B9, 82843491, 27F81499, ICCB75AF  
 D2932448, 8C4DC6AF, 770BCE98, 39CA97B6, ICCB75AF, 4E4E13E9, 82843491, 27F81499  
 39CA97B6, 048CC517, 8C4DC6AF, 770BCE98, 27F81499, 03BD1BD9, 4E4E13E9, 82843491  
 770BCE98, 419960CF, 048CC517, 8C4DC6AF, 82843491, 6FA999B7, 03BD1BD9, 4E4E13E9  
 8C4DC6AF, 407700EE, 419960CF, 048CC517, 4E4E13E9, 37B18629, 6FA999B7, 03BD1BD9  
 048CC517, E60ABEC4, 407700EE, 419960CF, 03BD1BD9, 9EA44395, 37B18629, 6FA999B7  
 419960CF, 0E248A8B, E60ABEC4, 407700EE, 6FA999B7, F877D28C, 9EA44395, 37B18629  
 407700EE, 10667792, 0E248A8B, E60ABEC4, 37B18629, F63EA862, F877D28C, 9EA44395  
 E60ABEC4, 646BB7A8, 10667792, 0E248A8B, 9EA44395, 424072F0, F63EA862, F877D28C  
 0E248A8B, 625CCE22, 646BB7A8, 10667792, F877D28C, 3B7642B8, 424072F0, F63EA862  
 10667792, 8E0E1101, 625CCE22, 646BB7A8, F63EA862, CD620F4E, 3B7642B8, 424072F0  
 646BB7A8, C23D3583, 8E0E1101, 625CCE22, 424072F0, BFAA1A02, CD620F4E, 3B7642B8  
 625CCE22, 81DE3DC5, C23D3583, 8E0E1101, 3B7642B8, 1BA7FD36, BFAA1A02, CD620F4E  
 8E0E1101, D24E4181, 81DE3DC5, C23D3583, CD620F4E, E62BB2A4, 1BA7FD36, BFAA1A02

下列是变量  $X_0, X_1, X_2, X_3, X'_0, X'_1, X'_2, X'_3$  的连续值(用 16 进制表示), 它们在处理第 2 块过程中获得。

31560350, 285A21CF, 846C181B, 553B61B8, 31560350, 285A21CF, 846C181B, 553B61B8

553B61B8, 1ADDE153, 285A21CF, 846C181B, 553B61B8, 56C8C102, 285A21CF, 846C181B  
846C181B, CE8FC309, 1ADDE153, 285A21CF, 846C181B, 702249A4, 56C8C102, 285A21CF  
285A21CF, 0DD8403A, CE8FC309, 1ADDE153, 285A21CF, 22CB0A97, 702249A4, 56C8C102  
1ADDE153, 4842F01E, 0DD8403A, CE8FC309, 56C8C102, 35B2DCDF, 22CB0A97, 702249A4  
CE8FC309, BE6A9014, 4842F01E, 0DD8403A, 702249A4, D2EFFB4A, 35B2DCDF, 22CB0A97  
0DD8403A, 7FE339CA, BE6A9014, 4842F01E, 22CB0A97, 59EA6C60, D2EFFB4A, 35B2DCDF  
4842F01E, D1CCFD4B, 7FE339CA, BE6A9014, 35B2DCDF, 82DEA3AE, 59EA6C60, D2EFFB4A  
BE6A9014, 108966B1, D1CCFD4B, 7FE339CA, D2EFFB4A, 4481FDE2, 82DEA3AE, 59EA6C60  
7FE339CA, 899223E8, 108966B1, D1CCFD4B, 59EA6C60, 13BB8F73, 4481FDE2, 82DEA3AE  
D1CCFD4B, 5E3B9917, 899223E8, 108966B1, 82DEA3AE, 946BD478, 13BB8F73, 4481FDE2  
108966B1, 7666663B, 5E3B9917, 899223E8, 4481FDE2, BD0605EA, 946BD478, 13BB8F73  
899223E8, A1BAD92C, 7666663B, 5E3B9917, 13BB8F73, 36F99153, BD0605EA, 946BD478  
5E3B9917, DE527A04, A1BAD92C, 7666663B, 946BD478, EB4AE872, 36F99153, BD0605EA  
7666663B, E52F1533, DE527A04, A1BAD92C, BD0605EA, 7C346442, EB4AE872, 36F99153  
A1BAD92C, 5C3C2C22, E52F1533, DE527A04, 36F99153, AFA320AD, 7C346442, EB4AE872  
DE527A04, FC1C4108, 5C3C2C22, E52F1533, EB4AE872, B4905651, AFA320AD, 7C346442  
E52F1533, 0A03E84B, FC1C4108, 5C3C2C22, 7C346442, 02E94FA1, B4905651, AFA320AD  
5C3C2C22, FB74BD26, 0A03E84B, FC1C4108, AFA320AD, E08D1799, 02E94FA1, B4905651  
FC1C4108, C78DC5C4, FB74BD26, 0A03E84B, B4905651, 69AFAA80, E08D1799, 02E94FA1  
0A03E84B, ACF60434, C78DC5C4, FB74BD26, 02E94FA1, FA665E46, 69AFAA80, E08D1799  
FB74BD26, 58F751E0, ACF60434, C78DC5C4, E08D1799, 269AB7E3, FA665E46, 69AFAA80  
C78DC5C4, EB75C7CB, 58F751E0, ACF60434, 69AFAA80, 0F06388B, 269AB7E3, FA665E46  
ACF60434, 83C0A8B7, EB75C7CB, 58F751E0, FA665E46, FD44FBD5, 0F06388B, 269AB7E3  
58F751E0, 27C87178, 83C0A8B7, EB75C7CB, 269AB7E3, DBBC0190, FD44FBD5, 0F06388B  
EB75C7CB, B7B9163F, 27C87178, 83C0A8B7, 0F06388B, D0E3FC2B, DBBC0190, FD44FBD5  
83C0A8B7, 0FA1C6DC, B7B9163F, 27C87178, FD44FBD5, 7D87B4BA, D0E3FC2B, DBBC0190  
27C87178, 2CC60316, 0FA1C6DC, B7B9163F, DBBC0190, 68367FDB, 7D87B4BA, D0E3FC2B  
B7B9163F, 08029C44, 2CC60316, 0FA1C6DC, D0E3FC2B, 53AB5439, 68367FDB, 7D87B4BA  
0FA1C6DC, F693A10E, 08029C44, 2CC60316, 7D87B4BA, E78B75B5, 53AB5439, 68367FDB  
2CC60316, 356224B9, F693A10E, 08029C44, 68367FDB, 830530DF, E78B75B5, 53AB5439  
08029C44, 669F7869, 356224B9, F693A10E, 53AB5439, 67FCB1AC, 830530DF, E78B75B5  
F693A10E, 7B70C168, 669F7869, 356224B9, E78B75B5, 757BB243, 67FCB1AC, 830530DF  
356224B9, 037FB19C, 7B70C168, 669F7869, 830530DF, F0CA8878, 757BB243, 67FCB1AC  
669F7869, 9B0A10B3, 037FB19C, 7B70C168, 67FCB1AC, FA10CB33, F0CA8878, 757BB243  
7B70C168, 9D015956, 9B0A10B3, 037FB19C, 757BB243, 5487E56C, FA10CB33, F0CA8878  
037FB19C, 6A7DE5F4, 9D015956, 9B0A10B3, F0CA8878, A5D33699, 5487E56C, FA10CB33  
9B0A10B3, E522D913, 6A7DE5F4, 9D015956, FA10CB33, BEB495BC, A5D33699, 5487E56C  
9D015956, 0EFD42E5, E522D913, 6A7DE5F4, 5487E56C, 05202F93, BEB495BC, A5D33699  
6A7DE5F4, 7902100B, 0EFD42E5, E522D913, A5D33699, BACE7DD9, 05202F93, BEB495BC  
E522D913, 1ACEFABC, 7902100B, 0EFD42E5, BEB495BC, 08D045DD, BACE7DD9, 05202F93  
0EFD42E5, E07378FF, 1ACEFABC, 7902100B, 05202F93, 5448A3A0, 08D045DD, BACE7DD9  
7902100B, 489C7A1A, E07378FF, 1ACEFABC, BACE7DD9, D98BE3AA, 5448A3A0, 08D045DD  
1ACEFABC, C02A45A5, 489C7A1A, E07378FF, 08D045DD, 12EC982F, D98BE3AA, 5448A3A0



E07378FF, 3068DDE8, C02A45A5, 489C7A1A, 5448A3A0, 4A1EB2B2, 12EC982F, D98BE3AA  
 489C7A1A, D5DD5018, 3068DDE8, C02A45A5, D98BE3AA, D677AAA8, 4A1EB2B2, 12EC982F  
 C02A45A5, B9D75D76, D5DD5018, 3068DDE8, 12EC982F, 5AA89133, D677AAA8, 4A1EB2B2  
 3068DDE8, 51A9B2DD, B9D75D76, D5DD5018, 4A1EB2B2, 49BCE169, 5AA89133, D677AAA8  
 D5DD5018, 36F589C4, 51A9B2DD, B9D75D76, D677AAA8, CF4FA8D2, 49BCE169, 5AA89133  
 B9D75D76, B5C60EAF, 36F589C4, 51A9B2DD, 5AA89133, C1985969, CF4FA8D2, 49BCE169  
 51A9B2DD, 725DF80C, B5C60EAF, 36F589C4, 49BCE169, 427440B4, C1985969, CF4FA8D2  
 36F589C4, 3F7A2507, 725DF80C, B5C60EAF, CF4FA8D2, 60927896, 427440B4, C1985969  
 B5C60EAF, 9D539EB6, 3F7A2507, 725DF80C, C1985969, 7050ED96, 60927896, 427440B4  
 725DF80C, 5A249895, 9D539EB6, 3F7A2507, 427440B4, CBC74513, 7050ED96, 60927896  
 3F7A2507, A7CECDCD, 5A249895, 9D539EB6, 60927896, 8431C75E, CBC74513, 7050ED96  
 9D539EB6, F8DCD12B, A7CECDCD, 5A249895, 7050ED96, 0E3A1C68, 8431C75E, CBC74513  
 5A249895, 3E30DB2A, F8DCD12B, A7CECDCD, CBC74513, 62EEEC87, 0E3A1C68, 8431C75E  
 A7CECDCD, A25D36CE, 3E30DB2A, F8DCD12B, 8431C75E, 2B1F312D, 62EEEC87, 0E3A1C68  
 F8DCD12B, A92CF759, A25D36CE, 3E30DB2A, 0E3A1C68, FB124197, 2B1F312D, 62EEEC87  
 3E30DB2A, 0CD0BA66, A92CF759, A25D36CE, 62EEEC87, DB8A5C11, FB124197, 2B1F312D  
 A25D36CE, AF62D775, 0CD0BA66, A92CF759, 2B1F312D, EC3264DC, DB8A5C11, FB124197  
 A92CF759, 69D4E1DF, AF62D775, 0CD0BA66, FB124197, 9AA87F7C, EC3264DC, DB8A5C11  
 0CD0BA66, 0EE66339, 69D4E1DF, AF62D775, DB8A5C11, 04512915, 9AA87F7C, EC3264DC  
 AF62D775, 5C5B5FBD, 0EE66339, 69D4E1DF, EC3264DC, C763272A, 04512915, 9AA87F7C  
 69D4E1DF, 0D80E8CF, 5C5B5FBD, 0EE66339, 9AA87F7C, CCD7DF45, C763272A, 04512915

散列码是下列 128 位串:

A1 AA 06 89 D0 FA FA 2D DC 22 E8 8B 49 13 3A 06

#### A3.9 例 9

本例数据串是 1000000 字节串,由字母“a”的重复  $10^6$  次的 GB1988 编码版本组成。

散列码是下列 128 位串:

4A 7F 57 23 F9 54 EB A1 21 6C 9D 8F 63 20 43 1F

#### A4 专用散列函数 3

散列函数 3。

##### A4.1 例 1

本例中数据串为空串,即零长度串。

散列码是下列 160 位串:

DA 39 A3 EE 5E 6B 4B 0D 32 55 BF EF 95 60 18 90 AF D8 07 09

##### A4.2 例 2

本例中数据串含有单个字节串,即字母“a”的 GB 1988 编码版本。散列码是下列 160 位串:

86 F7 E4 37 FA A5 A7 FC E1 5D 1D DC B9 EA EA EA 37 76 67 B8

##### A4.3 例 3

本例中数据串是含有“abc”的 GB 1988 编码的 3 字节串。它等同于位串:“01100001 01100010 01100011”。

经过填充过程后,由此数据串推导出的单个 16 字的块如下:

61626380 00000000 00000000 00000000 00000000 00000000 00000000 00000000  
 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000018

下列是变量  $X_0, X_1, X_2, X_3, X_4$  的连续值(用 16 进制表示):

0116FC33, 67452301, 7BF36AE2, 98BADCFE, 10325476  
8990536D, 0116FC33, 59D148C0, 7BF36AE2, 98BADCFE  
A1390F08, 8990536D, C045BF0C, 59D148C0, 7BF36AE2  
CDD8E11B, A1390F08, 626414DB, C045BF0C, 59D148C0  
CFD499DE, CDD8E11B, 284E43C2, 626414DB, C045BF0C  
3FC7CA40, CFD499DE, F3763846, 284E43C2, 626414DB  
993E30C1, 3FC7CA40, B3F52677, F3763846, 284E43C2  
9E8C07D4, 993E30C1, 0FF1F290, B3F52677, F3763846  
4B6AE328, 9E8C07D4, 664F8C30, 0FF1F290, B3F52677  
8351F929, 4B6AE328, 27A301F5, 664F8C30, 0FF1F290  
FBDA9E89, 8351F929, 12DAB8CA, 27A301F5, 664F8C30  
63188FE4, FBDA9E89, 60D47E4A, 12DAB8CA, 27A301F5  
4607B664, 63188FE4, 7EF6A7A2, 60D47E4A, 12DAB8CA  
9128F695, 4607B664, 18C623F9, 7EF6A7A2, 60D47E4A  
196BEE77, 9128F695, 1181ED99, 18C623F9, 7EF6A7A2  
20BDD62F, 196BEE77, 644A3DA5, 1181ED99, 18C623F9  
4E925823, 20BDD62F, C65AFB9D, 644A3DA5, 1181ED99  
82AA6728, 4E925823, C82F758B, C65AFB9D, 644A3DA5  
DC64901D, 82AA6728, D3A49608, C82F758B, C65AFB9D  
FD9E1D7D, DC64901D, 20AA99CA, D3A49608, C82F758B  
1A37B0CA, FD9E1D7D, 77192407, 20AA99CA, D3A49608  
33A23BFC, 1A37B0CA, 7F67875F, 77192407, 20AA99CA  
21283486, 33A23BFC, 868DEC32, 7F67875F, 77192407  
D541F12D, 21283486, 0CE88EFF, 868DEC32, 7F67875F  
C7567DC6, D541F12D, 884A0D21, 0CE88EFF, 868DEC32  
48413BA4, C7567DC6, 75507C4B, 884A0D21, 0CE88EFF  
BE35FBD5, 48413BA4, B1D59F71, 75507C4B, 884A0D21  
4AA84D97, BE35FBD5, 12104EE9, B1D59F71, 75507C4B  
8370B52E, 4AA84D97, 6F8D7EF5, 12104EE9, B1D59F71  
C5FBAF5D, 8370B52E, D2AA1365, 6F8D7EF5, 12104EE9  
1267B407, C5FBAF5D, A0DC2D4B, D2AA1365, 6F8D7EF5  
3B845D33, 1267B407, 717EEBD7, A0DC2D4B, D2AA1365  
046FAA0A, 3B845D33, C499ED01, 717EEBD7, A0DC2D4B  
2C0EBC11, 046FAA0A, CEE1174C, C499ED01, 717EEBD7  
21796AD4, 2C0EBC11, 811BEA82, CEE1174C, C499ED01  
DCBB0CB, 21796AD4, 4B03AF04, 811BEA82, CEE1174C  
0F511FD8, DCBB0CB, 085E5AB5, 4B03AF04, 811BEA82  
DC63973F, 0F511FD8, F72EEC32, 085E5AB5, 4B03AF04  
4C986405, DC63973F, 03D447F6, F72EEC32, 085E5AB5  
32DE1CBA, 4C986405, F718E5CF, 03D447F6, F72EEC32  
FC87DEDf, 32DE1CBA, 53261901, F718E5CF, 03D447F6  
970A0D5C, FC87DEDf, 8CB7872E, 53261901, F718E5CF

7F193DC5, 970A0D5C, FF21F7B7, 8CB7872E, 53261901  
 EE1B1AAF, 7F193DC5, 25C28357, FF21F7B7, 8CB7872E  
 40F28E09, EE1B1AAF, 5FC64F71, 25C28357, FF21F7B7  
 1C51E1F2, 40F28E09, FB86C6AB, 5FC64F71, 25C28357  
 A01B846C, 1C51E1F2, 503CA382, FB86C6AB, 5FC64F71  
 BEAD02CA, A01B846C, 8714787C, 503CA382, FB86C6AB  
 BAF39337, BEAD02CA, 2806E11B, 8714787C, 503CA382  
 120731C5, BAF39337, AFAB40B2, 2806E11B, 8714787C  
 641DB2CE, 120731C5, EEBCE4CD, AFAB40B2, 2806E11B  
 3847AD66, 641DB2CE, 4481CC71, EEBCE4CD, AFAB40B2  
 E490436D, 3847AD66, 99076CB3, 4481CC71, EEBCE4CD  
 27E9F1D8, E490436D, 8E11EB59, 99076CB3, 4481CC71  
 7B71F76D, 27E9F1D8, 792410DB, 8E11EB59, 99076CB3  
 5E6456AF, 7B71F76D, 09FA7C76, 792410DB, 8E11EB59  
 C846093F, 5E6456AF, 5EDC7DDB, 09FA7C76, 792410DB  
 D262FF50, C846093F, D79915AB, 5EDC7DDB, 09FA7C76  
 09D785FD, D262FF50, F211824F, D79915AB, 5EDC7DDB  
 3F52DE5A, 09D785FD, 3498BFD4, F211824F, D79915AB  
 D756C147, 3F52DE5A, 4275E17F, 3498BFD4, F211824F  
 548C9CB2, D756C147, 8FD4B796, 4275E17F, 3498BFD4  
 B66C020B, 548C9CB2, F5D5B051, 8FD4B796, 4275E17F  
 6B61C9E1, B66C020B, 9523272C, F5D5B051, 8FD4B796  
 19DFA7AC, 6B61C9E1, ED9B0082, 9523272C, F5D5B051  
 101655F9, 19DFA7AC, 5AD87278, ED9B0082, 9523272C  
 0C3DF2B4, 101655F9, 0677E9EB, 5AD87278, ED9B0082  
 78DD4D2B, 0C3DF2B4, 4405957E, 0677E9EB, 5AD87278  
 497093C0, 78DD4D2B, 030F7CAD, 4405957E, 0677E9EB  
 3F2588C2, 497093C0, DE37534A, 030F7CAD, 4405957E  
 C199F8C7, 3F2588C2, 125C24F0, DE37534A, 030F7CAD  
 39859DE7, C199F8C7, 8FC96230, 125C24F0, DE37534A  
 EDB42DE4, 39859DE7, F0667E31, 8FC96230, 125C24F0  
 11793F6F, EDB42DE4, CE616779, F0667E31, 8FC96230  
 5EE76897, 11793F6F, 3B6D0B79, CE616779, F0667E31  
 63F7DAB7, 5EE76897, C45E4FDB, 3B6D0B79, CE616779  
 A079B7D9, 63F7DAB7, D7B9DA25, C45E4FDB, 3B6D0B79  
 860D21CC, A079B7D9, D8FDF6AD, D7B9DA25, C45E4FDB  
 5738D5E1, 860D21CC, 681E6DF6, D8FDF6AD, D7B9DA25  
 42541B35, 5738D5E1, 21834873, 681E6DF6, D8FDF6AD

散列码是下列 160 位串:

8E B2 08 F7 E0 5D 98 7A 9B 04 4A 8E 98 C6 B0 87 F1 5A 0B FC

#### A4.4 例 4

本例中数据串是 14 字节串,由“message digest”的 GB 1988 编码版本组成。

散列码是下列 160 位串：

C1 22 52 CE DA 8B E8 99 4D 5F A0 29 0A 47 23 1C 1D 16 AA E3

#### A4.5 例 5

本例中数据串是 26 字节串，由“abcdefghijklmnopqrstuvwxyz”的 GB 1988 编码版本组成。

散列码是下列 160 位串：

32 D1 0C 7B 8C F9 65 70 CA 04 CE 37 F2 A1 9D 84 24 0D 3A 89

#### A4.6 例 6

本例中数据串是 62 字节串，由“ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789”的 GB 1988 编码版本组成。

散列码是下列 160 位串：

76 1C 45 7B F7 3B 14 D2 7E 9E 92 65 C4 6F 4B 4D DA 11 F9 40

#### A4.7 例 7

本例中数据串是 80 字节串，由“1234567890”的 GB 1988 编码版本组成。

散列码是下列 160 位串：

50 AB F5 70 6A 15 09 90 A0 8B 2C 5E A4 0F A0 E5 85 55 47 32

#### A4.8 例 8

本例中数据串是 56 字节串，由“abcdcbcedefdefefghfghfghijhijhijklklmklmlnlnomnopnopq”的 GB 1988 编码版本组成。

经过填充过程后，由数据串推导出来的两个 16 字的块如下：

61626364 62636465 63646566 64656667 65666768 66676869 6768696A 68696AA6B  
696AA6B6C 6A6B6C6D 6B6C6D6E 6C6D6E6F 6D6E6F70 6E6F7071 80000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000 00000000 000001C0

下列是变量  $X_0, X_1, X_2, X_3, X_4$  的连续值(用 16 进制表示)，它们在处理第 1 块过程中获得。

0116FC17, 67452301, 7BF36AE2, 98BADCFE, 10325476  
EBF3B452, 0116FC17, 59D148C0, 7BF36AE2, 98BADCFE  
5109913A, EBF3B452, C045BF05, 59D148C0, 7BF36AE2  
2C4F6EAC, 5109913A, BAFCE14, C045BF05, 59D148C0  
33F4AE5B, 2C4F6EAC, 9442644E, BAFCE14, C045BF05  
96B85189, 33F4AE5B, 0B13DBAB, 9442644E, BAFCE14  
DB04CB58, 96B85189, CCFD2B96, 0B13DBAB, 9442644E  
45833F0F, DB04CB58, 65AE1462, CCFD2B96, 0B13DBAB  
C565C35E, 45833F0F, 36C132D6, 65AE1462, CCFD2B96  
6350AFDA, C565C35E, D160CFC3, 36C132D6, 65AE1462  
8993EA77, 6350AFDA, B15970D7, D160CFC3, 36C132D6  
E19ECAAA2, 8993EA77, 98D42BF6, B15970D7, D160CFC3  
8603481E, E19ECAAA2, E264FA9D, 98D42BF6, B15970D7  
32F94A85, 8603481E, B867B2A8, E264FA9D, 98D42BF6  
B2E7A8BE, 32F94A85, A180D207, B867B2A8, E264FA9D  
42637E39, B2E7A8BE, 4CBE52A1, A180D207, B867B2A8  
6B068048, 42637E39, ACB9EA2F, 4CBE52A1, A180D207  
426B9C35, 6B068048, 5098DF8E, ACB9EA2F, 4CBE52A1

944B1BD1, 426B9C35, 1AC1A012, 5098DF8E, ACB9EA2F  
6C445652, 944B1BD1, 509AE70D, 1AC1A012, 5098DF8E  
95836DA5, 6C445652, 6512C6F4, 509AE70D, 1AC1A012  
09511177, 95836DA5, 9B111594, 6512C6F4, 509AE70D  
E2B92DC4, 09511177, 6560DB69, 9B111594, 6512C6F4  
FD224575, E2B92DC4, C254445D, 6560DB69, 9B111594  
EEB82D9A, FD224575, 38AE4B71, C254445D, 6560DB69  
5A142C1A, EEB82D9A, 7F48915D, 38AE4B71, C254445D  
2972F7C7, 5A142C1A, BBAE0B66, 7F48915D, 38AE4B71  
D526A644, 2972F7C7, 96850B06, BBAE0B66, 7F48915D  
E1122421, D526A644, CA5CBDF1, 96850B06, BBAE0B66  
05B457B2, E1122421, 3549A991, CA5CBDF1, 96850B06  
A9C84BEC, 05B457B2, 78448908, 3549A991, CA5CBDF1  
52E31F60, A9C84BEC, 816D15EC, 78448908, 3549A991  
5AF3242C, 52E31F60, 2A7212FB, 816D15EC, 78448908  
31C756A9, 5AF3242C, 14B8C7D8, 2A7212FB, 816D15EC  
E9AC987C, 31C756A9, 16BCC90B, 14B8C7D8, 2A7212FB  
AB7C32EE, E9AC987C, 4C71D5AA, 16BCC90B, 14B8C7D8  
5933FC99, AB7C32EE, 3A6B261F, 4C71D5AA, 16BCC90B  
43F87AE9, 5933FC99, AADF0CBB, 3A6B261F, 4C71D5AA  
24957F22, 43F87AE9, 564CFF26, AADF0CBB, 3A6B261F  
ADEB7478, 24957F22, 50FE1EBA, 564CFF26, AADF0CBB  
D70E5010, ADEB7478, 89255FC8, 50FE1EBA, 564CFF26  
79BCFB08, D70E5010, 2B7ADD1E, 89255FC8, 50FE1EBA  
F9BCB8DE, 79BCFB08, 35C39404, 2B7ADD1E, 89255FC8  
63E9561, F9BCB8DE, 1E6F3EC2, 35C39404, 2B7ADD1E  
98C1EA64, 63E9561, BE6F2E37, 1E6F3EC2, 35C39404  
C6EA241E, 98C1EA64, 58CFA558, BE6F2E37, 1E6F3EC2  
A2AD4F02, C6EA241E, 26307A99, 58CFA558, BE6F2E37  
C8A69090, A2AD4F02, B1BA8907, 26307A99, 58CFA558  
88341600, C8A69090, A8AB53C0, B1BA8907, 26307A99  
7E846F58, 88341600, 3229A424, A8AB53C0, B1BA8907  
86E358BA, 7E846F58, 220D0580, 3229A424, A8AB53C0  
8D2E76C8, 86E358BA, 1FA11BD6, 220D0580, 3229A424  
CE892E10, 8D2E76C8, A1B8D62E, 1FA11BD6, 220D0580  
EDEA95B1, CE892E10, 234B9DB2, A1B8D62E, 1FA11BD6  
36D1230A, EDEA95B1, 33A24B84, 234B9DB2, A1B8D62E  
776C3910, 36D1230A, 7B7AA56C, 33A24B84, 234B9DB2  
A681B723, 776C3910, 8DB448C2, 7B7AA56C, 33A24B84  
AC0A794F, A681B723, 1DDB0E44, 8DB448C2, 7B7AA56C  
F03D3782, AC0A794F, E9A06DC8, 1DDB0E44, 8DB448C2  
9EF775C3, F03D3782, EB029E53, E9A06DC8, 1DDB0E44  
36254B13, 9EF775C3, BC0F4DE0, EB029E53, E9A06DC8

4080D4DC, 36254B13, E7BDDD70, BC0F4DE0, EB029E53  
 2BFAF7A8, 4080D4DC, CD8952C4, E7BDDD70, BC0F4DE0  
 513F9CA0, 2BFAF7A8, 10203537, CD8952C4, E7BDDD70  
 E5895C81, 513F9CA0, 0AFEBDEA, 10203537, CD8952C4  
 1037D2D5, E5895C81, 144FE728, 0AFEBDEA, 10203537  
 14A82DA9, 1037D2D5, 79625720, 144FE728, 0AFEBDEA  
 6D17C9FD, 14A82DA9, 440DF4B5, 79625720, 144FE728  
 2C7B07BD, 6D17C9FD, 452A0B6A, 440DF4B5, 79625720  
 FDF6EFFF, 2C7B07BD, 5B45F27F, 452A0B6A, 440DF4B5  
 112B96E3, FDF6EFFF, 4B1EC1EF, 5B45F27F, 452A0B6A  
 84065712, 112B96E3, FF7DBBFF, 4B1EC1EF, 5B45F27F  
 AB89FB71, 84065712, C44AE5B8, FF7DBBFF, 4B1EC1EF  
 C5210E35, AB89FB71, A10195C4, C44AE5B8, FF7DBBFF  
 352D9F4B, C5210E35, 6AE27EDC, A10195C4, C44AE5B8  
 1A0E0E0A, 352D9F4B, 7148438D, 6AE27EDC, A10195C4  
 D0D47349, 1A0E0E0A, CD4B67D2, 7148438D, 6AE27EDC  
 AD38620D, D0D47349, 86838382, CD4B67D2, 7148438D  
 D3AD7C25, AD38620D, 74351CD2, 86838382, CD4B67D2  
 8CE34517, D3AD7C25, 6B4E1883, 74351CD2, 86838382

下列是变量  $X_0, X_1, X_2, X_3, X_4$  的连续值(用 16 进制表示), 它们在处理第 2 块过程中获得。

2DF257E9, F4286818, B0DEC9EB, 0408F581, 84677148  
 4D3DC58F, 2DF257E9, 3D0A1A06, B0DEC9EB, 0408F581  
 C352BB05, 4D3DC58F, 4B7C95FA, 3D0A1A06, B0DEC9EB  
 EE7743C6, C352BB05, D34F7163, 4B7C95FA, 3D0A1A06  
 41E34277, EE7743C6, 70D4AEC1, D34F7163, 4B7C95FA  
 5443915C, 41E34277, BBBDD0F1, 70D4AEC1, D34F7163  
 E7FA0377, 5443915C, D078D09D, BBBDD0F1, 70D4AEC1  
 C6946813, E7FA0377, 1510E457, D078D09D, BBBDD0F1  
 FDDE1DE1, C6946813, F9FE80DD, 1510E457, D078D09D  
 B8538ACA, FDDE1DE1, F1A51A04, F9FE80DD, 1510E457  
 6BA94F63, B8538ACA, 7F778778, F1A51A04, F9FE80DD  
 43A2792F, 6BA94F63, AE14E2B2, 7F778778, F1A51A04  
 FECD7BBF, 43A2792F, DAEA53D8, AE14E2B2, 7F778778  
 A2604CA8, FECD7BBF, D0E89E4B, DAEA53D8, AE14E2B2  
 258B0BAA, A2604CA8, FFB35EEF, D0E89E4B, DAEA53D8  
 D9772360, 258B0BAA, 2898132A, FFB35EEF, D0E89E4B  
 5507DB6E, D9772360, 8962C2EA, 2898132A, FFB35EEF  
 A51B58BC, 5507DB6E, 365DC8D8, 8962C2EA, 2898132A  
 C2EB709F, A51B58BC, 9541F6DB, 365DC8D8, 8962C2EA  
 D8992153, C2EB709F, 2946D62F, 9541F6DB, 365DC8D8  
 37482F5F, D8992153, F0BADC27, 2946D62F, 9541F6DB  
 EE8700BD, 37482F5F, F6264854, F0BADC27, 2946D62F

9AD594B9, EE8700BD, CDD20BD7, F6264854, F0BAD27  
8FBAA5B9, 9AD594B9, 7BA1C02F, CDD20BD7, F6264854  
88FB5867, 8FBAA5B9, 66B5652E, 7BA1C02F, CDD20BD7  
EEC50521, 88FB5867, 63EEA96E, 66B5652E, 7BA1C02F  
50BCE434, EEC50521, E23ED619, 63EEA96E, 66B5652E  
5C416DAF, 50BCE434, 7BB14148, E23ED619, 63EEA96E  
2429BE5F, 5C416DAF, 142F390D, 7BB14148, E23ED619  
0A2FB108, 2429BE5F, D7105B6B, 142F390D, 7BB14148  
17986223, 0A2FB108, C90A6F97, D7105B6B, 142F390D  
8A4AF384, 17986223, 028BEC42, C90A6F97, D7105B6B  
6B629993, 8A4AF384, C5E61888, 028BEC42, C90A6F97  
F15F04F3, 6B629993, 2292BCE1, C5E61888, 028BEC42  
295CC25B, F15F04F3, DAD8A664, 2292BCE1, C5E61888  
696DA404, 295CC25B, FC57C13C, DAD8A664, 2292BCE1  
CEF5AE12, 696DA404, CA573096, FC57C13C, DAD8A664  
87D5B80C, CEF5AE12, 1A5B6901, CA573096, FC57C13C  
84E2A5F2, 87D5B80C, B3BD6B84, 1A5B6901, CA573096  
03BB6310, 84E2A5F2, 21F56E03, B3BD6B84, 1A5B6901  
C2D8F75F, 03BB6310, A138A97C, 21F56E03, B3BD6B84  
BFB25768, C2D8F75F, 00EED8C4, A138A97C, 21F56E03  
28589152, BFB25768, F0B63DD7, 00EED8C4, A138A97C  
EC1D3D61, 28589152, 2FEC95DA, F0B63DD7, 00EED8C4  
3CAED7AF, EC1D3D61, 8A162454, 2FEC95DA, F0B63DD7  
C3D033EA, 3CAED7AF, 7B074F58, 8A162454, 2FEC95DA  
7316056A, C3D033EA, CF2BB5EB, 7B074F58, 8A162454  
46F93B68, 7316056A, B0F40CFA, CF2BB5EB, 7B074F58  
DC8E7F26, 46F93B68, 9CC5815A, B0F40CFA, CF2BB5EB  
850D411C, DC8E7F26, 11BE4EDA, 9CC5815A, B0F40CFA  
7E4672C0, 850D411C, B7239FC9, 11BE4EDA, 9CC5815A  
89FBD41D, 7E4672C0, 21435047, B7239FC9, 11BE4EDA  
1797E228, 89FBD41D, 1F919CB0, 21435047, B7239FC9  
431D65BC, 1797E228, 627EF507, 1F919CB0, 21435047  
2BDBB8CB, 431D65BC, 05E5F88A, 627EF507, 1F919CB0  
6DA72E7F, 2BDBB8CB, 10C7596F, 05E5F88A, 627EF507  
A8495A9B, 6DA72E7F, CAF6EE32, 10C7596F, 05E5F88A  
E785655A, A8495A9B, DB69CB9F, CAF6EE32, 10C7596F  
5B086C42, E785655A, EA1256A6, DB69CB9F, CAF6EE32  
A65818F7, 5B086C42, B9E15956, EA1256A6, DB69CB9F  
7AAB101B, A65818F7, 96C21B10, B9E15956, EA1256A6  
93614C9C, 7AAB101B, E996063D, 96C21B10, B9E15956  
F66D9BF4, 93614C9C, DEAAAC06, E996063D, 96C21B10  
D504902B, F66D9BF4, 24D85327, DEAAAC06, E996063D  
60A9DA62, D504902B, 3D9B66FD, 24D85327, DEAAAC06

8B687819, 60A9DA62, F541240A, 3D9B66FD, 24D85327  
 083E90C3, 8B687819, 982A7698, F541240A, 3D9B66FD  
 F6226BBF, 083E90C3, 62DA1E06, 982A7698, F541240A  
 76C0563B, F6226BBF, C20FA430, 62DA1E06, 982A7698  
 989DD165, 76C0563B, FD889AEF, C20FA430, 62DA1E06  
 8B2C7573, 989DD165, DDB0158E, FD889AEF, C20FA430  
 AE1B8E7B, 8B2C7573, 66277459, DDB0158E, FD889AEF  
 CA1840DE, AE1B8E7B, E2CB1D5C, 66277459, DDB0158E  
 16F3BABB, CA1840DE, EB86E39E, E2CB1D5C, 66277459  
 D28D83AD, 16F3BABB, B2861037, EB86E39E, E2CB1D5C  
 6BC02DFE, D28D83AD, C5BCEEAE, B2861037, EB86E39E  
 D3A6E275, 6BC02DFE, 74A360EB, C5BCEEAE, B2861037  
 DA955482, D3A6E275, 9AF00B7F, 74A360EB, C5BCEEAE  
 58C0AAC0, DA955482, 74E9B89D, 9AF00B7F, 74A360EB  
 906FD62C, 58C0AAC0, B6A55520, 74E9B89D, 9AF00B7F  
 散列码是下列 160 位串:

84 98 3E 44 1C 3B D2 6E BA AE 4A A1 F9 51 29 E5 E5 46 70 F1

#### A4.9 例 9

本例数据串是 1000000 字节串,由字母“a”的重复  $10^6$  次的 GB 1988 编码版本组成。

散列码是下列 160 位串:

34 AA 97 3C D4 C4 DA A4 F6 1E EB 2B DB AD 27 31 65 34 01 6F

## 附 录 B

(提示的附录)

### 形 式 规 范

#### B0 引言

下列各条是用称为 Z 的规范语言表示的专用散列函数 1、2 和 3 的完整规范。Z 的记法是指附录 C [1]中描述的记法。

Z 保留了在本标准正文中使用的命名、结构等中的大部分。

Z 完全按 Z 写成,包括注释部分。注释针对本标准正文文本中的各部分,而 Z 是由此推导出的。

Z 把消息建模成自然数 0 和 1 的序列(串)。

#### B1 专用散列函数 1 规范

##### #3 定义

##### #3.2 循环函数

$Bit = \{0, 1\}$

$String = seqBit$

$L_1: N$

$L_2: N$

$String\_L_1 = \{s: String \mid \#s = L_1\}$



$$\text{String\_}L_2 = \{s; \text{String} \mid \#s = L_2\}$$

$$\mid O; \text{String\_}L_1 \times \text{String\_}L_2 \rightarrow \text{String\_}L_2$$

### #3.3 字

$$\text{Word} = \{w; \text{String} \mid \#w = 32\}$$

$$\text{Word\_capacity} = 2 \uparrow 32$$

$$\text{Word\_capacity\_m\_1} = (2 \uparrow 32) - 1$$

$$I\text{Word} = 0.. \text{Word\_capacity\_m\_1}$$

### #4 符号和记法

$S^*(\ )$  只需按照 Z 中定义  $S^*$ (关系迭代) 的方式定义  $S$

$$\mid S; \text{Word} \rightarrow \text{Word}$$

$$\mid \forall A; \text{Word} \cdot$$

$$\quad (\text{let } I = W\_to\_I(A) \cdot$$

$$\quad (\text{let } Shift\_I = (I * 2) + (I \text{ div } (2 \uparrow 31))) \text{ mod } (2 \uparrow 32) \cdot$$

$$\quad S(A) = I\_to\_W(Shift\_I))$$

$\wedge \vee \oplus$  只定义需要定义的那些字

$$BO = \text{Bit} \times \text{Bit} \rightarrow \text{Bit}$$

$$\mid LO; \text{Word} \times \text{Word} \times BO \rightarrow \text{Word}$$

$$\mid \forall p, q; \text{Word}; bo; BO \cdot$$

$$LO(p, q, bo) = \{n; 1.. \#p \cdot n \rightarrow bo(p(n), q(n))\}$$

$$\mid \_xor\_ , \_or\_ , \_and\_ ; BO$$

$$0 \text{ xor } 1 = 1$$

$$0 \text{ xor } 0 = 0$$

$$1 \text{ xor } 0 = 1$$

$$1 \text{ xor } 1 = 0$$

$$0 \text{ or } 1 = 1$$

$$0 \text{ or } 0 = 0$$

$$1 \text{ or } 0 = 1$$

$$1 \text{ or } 1 = 1$$

$$0 \text{ and } 1 = 0$$

$$0 \text{ and } 0 = 0$$

$$1 \text{ and } 0 = 0$$

$$1 \text{ and } 1 = 1$$

$$\mid \_XOR\_ , \_OR\_ , \_AND\_ ; \text{Word} \times \text{Word} \rightarrow \text{Word}$$

$$\mid \forall A, B; \text{Word} \cdot$$

$$A \text{ XOR } B = LO(A, B, (\_xor\_)) \wedge$$

$$A \text{ OR } B = LO(A, B, (\_or\_)) \wedge$$

$$A \text{ AND } B = LO(A, B, (\_and\_))$$

$$\text{NOT}; \text{Word} \rightarrow \text{Word}$$

$$\forall A; \text{Word} \cdot$$

$$\text{NOT } A = A \text{ XOR } \{n: 1.. \#A \cdot n \rightarrow 1\}$$

出

$$\_ \text{出} \_; \text{Word} \times \text{Word} \rightarrow \text{Word}$$

$$\forall A, B; \text{Word} \cdot$$

$$A \text{ 出 } B = I\_to\_W((W\_to\_I(A) + W\_to\_I(B)) \bmod \text{Word\_capacity})$$

#5 要求

#6 专用散列函数模型

#6.1 概述

$$L_H; \mathbf{N}_1$$

$$L_H \leq L_2$$

$$\text{Byte} = \{b; \text{String} \mid \#b = 8\}$$

$$I \text{ Byte} = 0..255$$

$$B\_to\_I; \text{Byte} \rightarrow I \text{ Byte}$$

$$\forall x; \text{Byte} \cdot B\_to\_I(x) =$$

$$x(1) \times 2 \uparrow 7 + x(2) \times 2 \uparrow 6 + x(3) \times 2 \uparrow 5 + x(4) \times 2 \uparrow 4 +$$

$$x(5) \times 2 \uparrow 3 + x(6) \times 2 \uparrow 2 + x(7) \times 2 + x(8)$$

#6.2 散列操作

$$IV; \text{String} \_ L_2$$

$$\text{Maximum\_Length\_of\_String}; \mathbf{N}$$

$$\text{hash}; \text{String} \leftrightarrow \text{String} \_ L_H$$

$$\forall D; \text{String} \mid \#D \leq \text{Maximum\_Length\_of\_String} \cdot$$

$$\text{hash}(D) =$$

$$(\text{let } PD = \text{pad}(D) \cdot$$

$$(\text{let } SD = \text{split}(PD) \cdot$$

$$(\text{let } H_q = \text{iterate}(SD, IV) \cdot$$

$$\text{truncate}(H_q)))$$

#6.2.1 第1步(填充)

$$\text{StringMultiple} \_ L_1 = \{s; \text{String} \mid \#s \bmod L_1 = 0\}$$

$$pad: String \rightarrow StringMultiple\_L_1$$

## # 6.2.2 第 2 步(分离)

$$StringBlocks == seq\ String\_L_1$$

$$split: StringMultiple\_L_1 \rightarrow StringBlocks$$

$$split =$$

$$\{sml\ 1: StringMultiple\_L_1; Sb: StringBlocks \mid sml\ 1 = \wedge / sb \cdot sml\ 1 \mapsto sb\}$$

## # 6.2.3 第 3 步(迭代)

$$iterate: StringBlocks \times String\_L_2 \mapsto String\_L_2$$

$$\forall sb: StringBlocks; H_{i-1}: String\_L_2 \mid \#sb \geq 1 \cdot$$

$$iterate(sb, H_{i-1}) =$$

$$(\text{let } D_i = sb(1) \cdot$$

$$(\text{let } H_i = \phi(D_i, H_{i-1}) \cdot$$

$$\text{if } \#sb = 1$$

$$\text{then } H_i$$

$$\text{else } iterate(\text{tail } sb, H_i))$$

## # 6.2.4 第 4 步(截短)

$$String\_L_H = \{s: String \mid \#s = L_H\}$$

$$truncate: String\_L_2 \rightarrow String\_L_H$$

$$\forall sy: String\_L_2 \cdot$$

$$truncate(sy) = (1..L_H) \uparrow sy$$

## # 7 专用散列函数 1

## # 7.1 概述

$$Maximum\_Length\_of\_String = (2 \uparrow 64) - 1$$

## # 7.2 参数、函数和常数

## # 7.2.1 参数

$$L_1 = 512$$

$$L_2 = 160$$

$$L_H = 160$$

## # 7.2.2 字节排序约定

$$W\_to\_I: Word \rightarrow IWord$$

$$\forall w: Word \cdot$$

$$W\_to\_I(w) =$$

$$(\text{let } B_0 = B\_to\_I((1..8) \uparrow w) \cdot$$

$$(\text{let } B_1 = B\_to\_I((9..16) \uparrow w) \cdot$$

$$(\text{let } B_2 = B\_to\_I((17..24) \uparrow w) \cdot$$

$$(\text{let } B_3 = B\_to\_I((25..32) \uparrow w) \cdot$$

$$B_3 * 2 \uparrow 24 + B_2 * 2 \uparrow 16 + B_1 * 2 \uparrow 8 + B_0)))$$

$$I\_to\_W: IWord \rightarrow Word$$

$$I\_to\_W = W\_to\_I$$

## #7.2.3 函数

$$Indexed\_g = \{g; seq(Word \times Word \times Word \rightarrow Word) \mid \#g = 80\}$$

$$g; Indexed\_g$$

$$\forall X_0, X_1, X_2; Word \cdot$$

$$(\forall i; 1..16 \cdot$$

$$g(i)(X_0, X_1, X_2) = X_0 \text{ XOR } X_1 \text{ XOR } X_2) \wedge$$

$$(\forall i; 17..32 \cdot$$

$$g(i)(X_0, X_1, X_2) = (X_0 \text{ AND } X_1) \text{ OR } (\text{NOT } X_0 \text{ AND } X_2)) \wedge$$

$$(\forall i; 33..48 \cdot$$

$$g(i)(X_0, X_1, X_2) = (X_0 \text{ OR } \text{NOT } X_1) \text{ XOR } X_2 \wedge$$

$$(\forall i; 49..64 \cdot$$

$$g(i)(X_0, X_1, X_2) = (X_0 \text{ AND } X_2) \text{ OR } (X_1 \text{ AND } \text{NOT } X_2)) \wedge$$

$$(\forall i; 65..80 \cdot$$

$$g(i)(X_0, X_1, X_2) = X_0 \text{ XOR } (X_1 \text{ OR } \text{NOT } X_2))$$

## #7.2.4 常数

$$x00000000 = 0$$

$$x5A827999 = 1518500249$$

$$x6ED9EBA1 = 1859775393$$

$$x8F1BBCDC = 2400959708$$

$$xA953FD4E = 2840853838$$

$$x50A28BE6 = 1352829926$$

$$x5C4DD124 = 1548603684$$

$$x6D703EF3 = 1836072691$$

$$x7A6D76E9 = 2053994217$$

$$Constants = \{c; StringWord \mid \#c = 80\}$$

$$C, C'; Constants$$

$$(\forall i; 1..16 \cdot$$

$$C(i) = I\_to\_W(x00000000)) \wedge$$

$$(\forall i; 17..32 \cdot$$

$$C(i) = I\_to\_W(x5A827999)) \wedge$$

$$(\forall i; 33..48 \cdot$$

$$C(i) = I\_to\_W(x6ED9EBA1)) \wedge$$

$$(\forall i; 49..64 \cdot$$

$$C(i) = I\_to\_W(x8F1BBCDC)) \wedge$$

$$(\forall i; 65..80 \cdot$$

$$C'(i) = I\_to\_W(xA953FD4E)) \wedge$$

```

(∀ i:1..16 •
  C'(i)=I_to_W(x50A28BE6)) ∧
(∀ i:17..32 •
  C'(i)=I_to_W(x5C4DD124)) ∧
(∀ i:33..48 •
  C'(i)=I_to_W(x6D703EF3)) ∧
(∀ i:49..64 •
  C'(i)=I_to_W(x7A6D76E9)) ∧
(∀ i:65..80 •
  C'(i)=I_to_W(x00000000))

```

t==

```

<11,14,15,12,5,8,7,9,11,13,14,15,6,7,9,8,
7,6,8,13,11,9,7,15,7,12,15,9,11,7,13,12,
11,13,6,7,14,9,13,15,14,8,13,6,5,12,7,5,
11,12,14,15,14,15,9,8,9,14,5,6,8,6,5,12,
9,15,5,11,6,8,13,12,5,12,13,14,11,8,5,6>

```

t'==

```

<8,9,9,11,13,15,15,5,7,7,8,11,14,14,12,6,
9,13,15,7,12,8,9,11,7,7,12,7,6,15,13,11,
9,7,15,11,8,6,6,14,12,13,5,14,13,13,7,5
15,5,8,11,14,14,6,14,6,9,12,9,12,5,15,8,
8,5,12,9,12,5,14,6,8,13,6,5,15,13,11,11>

```

注意用 Z 表示以 1 开始的序列中  $a$  和  $a'$  的值比常规文本中的值大 1。

a==

```

<1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,
8,5,14,2,11,7,16,4,13,1,10,6,3,15,12,9,
4,11,15,5,10,16,9,2,3,8,1,7,14,12,6,13,
2,10,12,11,1,9,13,5,14,4,8,16,15,6,7,3,
5,1,6,10,8,13,3,11,15,2,4,9,12,7,16,14>

```

a'==

```

<6,15,8,1,10,3,12,5,14,7,16,9,2,11,4,13,
7,12,4,8,1,14,6,11,15,16,9,13,5,10,2,3,
16,6,2,4,8,15,7,10,12,9,13,3,11,1,5,14,
9,7,5,2,4,12,16,1,6,13,3,14,10,8,11,15,
13,16,11,5,2,6,9,8,7,3,14,15,1,4,10,12>

```

#### #7.2.5 初始化值

x67452301==1732584193

Y<sub>0</sub>=I\_to\_W(x67452301)

xEFCDAB89==4023233417

$Y_1 = I\_to\_W(xEFCDAB89)$   
 $x98BADCFE = 2562383102$   
 $Y_2 = I\_to\_W(x98BADCFE)$   
 $x10325476 = 271733878$   
 $Y_3 = I\_to\_W(x10325476)$   
 $xC3D2E1F0 = 3285377520$   
 $Y_4 = I\_to\_W(xC3D2E1F0)$

$IV = Y_0 \wedge Y_1 \wedge Y_2 \wedge Y_3 \wedge Y_4$

### # 7.3 填充法

$\forall D: String \bullet$

$pad(D) =$

(let  $L_D = \#D \bullet$

(let  $Zeros = (n: 1..((447 - L_D) \bmod 512) \bullet n \rightarrow 0) \bullet$

(let  $Length\_D\_LSH = I\_to\_W(L_D \bmod (2 \uparrow 32)) \bullet$

(let  $Length\_D\_MSH = I\_to\_W(L_D \text{ div } (2 \uparrow 32)) \bullet$

$D \wedge \langle 1 \rangle \wedge Zeros \wedge Length\_D\_LSH \wedge Length\_D\_MSH)))$

### # 7.4 循环函数的描述

$StringWord = seq\ Word$

$Split\_String\_to\_StringWord: String \rightarrow StringWord$

$Split\_String\_to\_StringWord =$

$\{s: String; sw: StringWord \mid s = \wedge /sw \bullet s \rightarrow sw\}$

$L80: StringWord \times StringWord \times$

$Indexed\_g \times seq\ \mathbf{N} \times seq\ \mathbf{N} \times$

$Constants \times 1..80 \rightarrow StringWord$

$\forall Z, X: StringWord; g: Indexed\_g; t, a: seq\ \mathbf{N};$

$C: Constants; i: 1..80 \mid \#Z = 16 \wedge \#X = 5 \bullet$

$L80(Z, X, g, t, a, C, i) =$

(let  $X0 = X(1); X1 = X(2); X2 = X(3); X3 = X(4); X4 = (X)5 \bullet$

(let  $W = S^{(i)}(X_0 \boxplus g(i)(X1, X2, X3)) \boxplus Z(a(i)) \boxplus C(i)) \boxplus X4 \bullet$

(let  $Y = \langle X4, W, X1, S^{10}(X2), X3 \rangle \bullet$

if  $(i = 80)$

then  $Y$

else  $L80(Z, Y, g, t, a, C, i+1)))$

$\forall sx: String\_L_1; sy: String\_L_2 \bullet$

$\phi(sx, sy) =$

(let  $Z = Split\_String\_to\_StringWord(sx) \bullet$

(let  $Y = Split\_String\_to\_StringWord(sy) \bullet$

(let  $X = L80(Z, Y, g, t, a, C, 1) \bullet$

```

(let X' == L80(Z, Y, revg, s', a', C', 1) •
  (let Y0 == Y(2) 出 X(3) 出 X'(4) •
    (let Y1 == Y(3) 出 X(4) 出 X'(5) •
      (let Y2 == Y(4) 出 X(5) 出 X'(1) •
        (let Y3 == Y(5) 出 X(1) 出 X'(2) •
          (let Y4 == Y(1) 出 X(2) 出 X'(3) •
            Y0 ^ Y1 ^ Y2 ^ Y3 ^ Y4)))))))))

```

## B1.1 辅助函数

$\_ \uparrow \_ : \mathbf{N} \times \mathbf{N} \rightarrow \mathbf{N}$ $\forall p : \mathbf{N} \cdot$ $p \uparrow 0 = 1 \wedge$ $(\forall n : \mathbf{N}_1 \cdot p \uparrow n = p * (p \uparrow (n-1)))$
--

## B2 专用散列函数 2 规范

重复#3、#4、#5、#6各部分以及附录B1的B1.1。

## #8 专用散列函数 2

## #8.1 概述

$$\text{Maximum\_Length\_of\_String} = (2 \uparrow 64) - 1$$

## #8.2 参数、函数和常数

## #8.2.1 参数

$$L_1 = 512$$

$$L_2 = 128$$

$$L_H = 128$$

## #8.2.2 字节排序约定

重复附录B1的#7.2.2

## #8.2.3 函数

重复附录B1的#7.2.3

$$g2 == (1..64)1g$$

## #8.2.4 Constants

$$x00000000 == 0$$

$$x5A827999 == 1518500249$$

$$x6ED9EBA1 == 1859775393$$

$$x8F1BBCDC == 2400959708$$

$$x50A28BE6 == 1352829926$$

$$x5C4DD124 == 1548603684$$

$$x6D703EF3 == 1836072691$$

$$\text{Constants} == \{c : \text{StringWord} \mid \#c = 64\}$$

$C, C' : \text{Constants}$
----------------------------

$(\forall i : 1..16 \cdot$
----------------------------

$$\begin{aligned}
& C(i) = I\_to\_W(x00000000) \wedge \\
& (\forall i; 17..32 \cdot \\
& \quad C(i) = I\_to\_W(x5A827999) \wedge \\
& (\forall i; 33..48 \cdot \\
& \quad C(i) = I\_to\_W(x6ED9EBA1) \wedge \\
& (\forall i; 49..64 \cdot \\
& \quad C(i) = I\_to\_W(x8F1BBCDC) \wedge \\
& \\
& (\forall i; 1..16 \cdot \\
& \quad C'(i) = I\_to\_W(x50A28BE6) \wedge \\
& (\forall i; 17..32 \cdot \\
& \quad C'(i) = I\_to\_W(x5C4DD124) \wedge \\
& (\forall i; 33..48 \cdot \\
& \quad C'(i) = I\_to\_W(x6D703EF3) \wedge \\
& (\forall i; 49..64 \cdot \\
& \quad C'(i) = I\_to\_W(x00000000)
\end{aligned}$$

重复附录 B1 的 #7.2.4 中的  $a, a', t, t'$  中。

$$t2 = (1..64) \uparrow t$$

$$t2' = (1..64) \uparrow t'$$

$$a2 = (1..64) \uparrow a$$

$$a2' = (1..64) \uparrow a'$$

#### #8.2.5 初始化值

$$x67452301 = 1732584193$$

$$Y_0 = I\_to\_W(x67452301)$$

$$xEFCDAB89 = 4023233417$$

$$Y_1 = I\_to\_W(xEFCDAB89)$$

$$x98BADCFE = 2562383102$$

$$Y_2 = I\_to\_W(x98BADCFE)$$

$$x10325476 = 271733878$$

$$Y_3 = I\_to\_W(x10325476)$$

$$IV = Y_0 \cap Y_1 \cap Y_2 \cap Y_3$$

#### #8.3 填充法

重复附录 B1 的 #7.3

#### #8.4 循环函数的描述

重复附录 B1 的 #7.4 中 *StringWord* 和 *Split\_String\_to\_StringWord* 定义。

$$L64; StringWord \times StringWord \times$$

$$Indexed\_g \times seq \mathbf{N} \times seq \mathbf{N} \times$$

$$Constants \times 1..64 \rightarrow StringWord$$

$$\forall Z, X; StringWord; g; Indexed\_g; t; a; seq \mathbf{N};$$



```

C; Constants; i: 1..64 | #Z=16 ∧ #X=5 •
L64(Z, X, g, t, a, C, i) =
  (let X0 == X(1); X1 == X(2); X2 == X(3); X3 == X(4) •
  (let W == S(6)(X0 出g(i)(X1, X2, X3) 出Z(a(i)) 出C(i))) •
  (let Y == <X3, W, X1, X2> •
  if (i=64)
  then Y
  else L64(Z, Y, g, t, a, C, i+1))))

```

∀ *sx*; String <sub>L<sub>1</sub></sub>; *sy*; String <sub>L<sub>2</sub></sub> •

```

φ(sx, sy) =
  (let Z == Split_String_to_StringWord(sx) •
  (let Y == Split_String_to_StringWord(sy) •
  (let X == L64(Z, Y, g2, t2, a2, C, 1) •
  (let X' == L64(Z, Y, rev g2, t2', a2', C', 1) •
  (let Y0 == Y(2) 出 X(3) 出 X'(4) •
  (let Y1 == Y(3) 出 X(4) 出 X'(1) •
  (let Y2 == Y(4) 出 X(1) 出 X'(2) •
  (let Y3 == Y(1) 出 X(2) 出 X'(3) •
  Y0 ∧ Y1 ∧ Y2 ∧ Y3))))))

```

### B3 专用散列函数3规范

重复#3、#4、#5、#6各部分以及附录B1的B1.1。

#### #9 专用散列函数3

##### #9.1 概述

*Maximum\_Length\_of\_String* = (2 ↑ 64) - 1

##### #9.2 参数、函数和常数

###### #9.2.1 参数

*L<sub>1</sub>* = 512

*L<sub>2</sub>* = 160

*L<sub>H</sub>* = 160

###### #9.2.2 字节排序约定

*W\_to\_I*: Word → IWord

∀ *w*; Word • *W\_to\_I*(*w*) =

(let *B<sub>0</sub>* == *B\_to\_I*((1..8) ↑ *w*) •

(let *B<sub>1</sub>* == *B\_to\_I*((9..16) ↑ *w*) •

(let *B<sub>2</sub>* == *B\_to\_I*((17..24) ↑ *w*) •

(let *B<sub>3</sub>* == *B\_to\_I*((25..32) ↑ *w*) •

*B<sub>3</sub>* + *B<sub>2</sub>* \* 2 ↑ 8 + *B<sub>1</sub>* \* 2 ↑ 16 + *B<sub>0</sub>* \* 2 ↑ 24

*I\_to\_W*: IWord → Word

$$\overline{I\_to\_W=W\_to\_I}$$

## #9.2.3 函数

$$Indexed\_f == \{f; seq(Word \times Word \times Word \rightarrow Word) \mid \#f = 80\}$$

$$f; Indexed\_f$$

$$\forall X_0, X_1, X_2: Word \cdot$$

$$(\forall i; 1..20 \cdot$$

$$f(i)(X_0, X_1, X_2) = (X_0 \text{ AND } X_1) \text{ OR } (\text{NOT } X_0 \text{ AND } X_2) \wedge$$

$$(\forall i; 21..40 \cdot$$

$$f(i)(X_0, X_1, X_2) = X_0 \text{ XOR } X_1 \text{ XOR } X_2 \wedge$$

$$(\forall i; 41..60 \cdot$$

$$f(i)(X_0, X_1, X_2) = (X_0 \text{ AND } X_1) \text{ OR } (X_0 \text{ AND } X_2) \text{ OR } (X_1 \text{ AND } X_2) \wedge$$

$$(\forall i; 61..80 \cdot$$

$$f(i)(X_0, X_1, X_2) = X_0 \text{ XOR } X_1 \text{ XOR } X_2)$$

## #9.2.4 常数

$$x5A827999 == 1518500249$$

$$x6ED9EBA1 == 1859775393$$

$$x8F1BBCDC == 2400959708$$

$$xCA62C1D6 == 3395469782$$

$$Constants == \{c; StringWord \mid \#c = 80\}$$

$$C; Constants$$

$$(\forall i; 1..20 \cdot$$

$$C(i) = I\_to\_W(x5A827999) \wedge$$

$$(\forall i; 21..40 \cdot$$

$$C(i) = I\_to\_W(x6ED9EBA1) \wedge$$

$$(\forall i; 41..60 \cdot$$

$$C(i) = I\_to\_W(x8FABBCDC) \wedge$$

$$(\forall i; 61..80 \cdot$$

$$C(i) = I\_to\_W(xCA62C1D6))$$

## #9.2.5 初始化值

$$x67452301 == 1732584193$$

$$Y_0 == I\_to\_W(x67452301)$$

$$xEFCDAB89 == 4023233417$$

$$Y_1 == I\_to\_W(xEFCDAB89)$$

$$x98BADCFE == 2562383102$$

$$Y_2 == I\_to\_W(x98BADCFE)$$

$$x10325476 == 271733878$$

$$Y_3 == I\_to\_W(x10325476)$$

$$xC3D2E1F0 == 3285377520$$

$$Y_4 == I\_to\_W(xC3D2E1F0)$$

$$IV = Y_0 \wedge Y_1 \wedge Y_2 \wedge Y_3 \wedge Y_4$$

## #9.3 填充法

 $\forall D; \text{String} \bullet$ 
 $\text{pad}(D) =$ 
 $(\text{let } L_D = \#D \bullet$ 
 $(\text{let } \text{Zeros} = \langle n; 1..((447 - L_D) \bmod 512) \bullet n^{\wedge} \rightarrow 0 \rangle \bullet$ 
 $(\text{let } \text{Length\_D\_MSH} = I\_to\_W(L_D \text{ div } (2 \uparrow 32)) \bullet$ 
 $(\text{let } \text{Length\_D\_LSH} = I\_to\_W(L_D \bmod (2 \uparrow 32)) \bullet$ 
 $D \wedge \langle 1 \rangle \wedge \text{Zeros} \wedge \text{Length\_D\_MSH} \wedge \text{Length\_D\_LSH} \rangle \rangle \rangle$ 

## #9.4 循环函数的描述

 $\text{StringWord} = \text{seq Word}$ 
 $\text{Split\_String\_to\_StringWord}; \text{String} \rightarrow \text{StringWord}$ 
 $\text{Strlit\_String\_to\_StringWord} =$ 
 $\{s; \text{String}; sw; \text{StringWord} \mid s = \wedge / sw \bullet s \rightarrow sw\}$ 
 $L80; \text{StringWord} \times \text{StringWord} \times 1..80 \leftrightarrow \text{StringWord}$ 
 $\forall X, Z; \text{StringWord}; i; 1..80 \mid \#X = 5 \wedge \#Z = 80 \bullet$ 
 $L80(X, Z, i) =$ 
 $(\text{let } W = S^6(X(1)) \text{ 出 } f(i)(X(2), X(3), X(4)) \text{ 出 } X(5) \text{ 出 } Z(i) \text{ 出 } C(i) \bullet$ 
 $(\text{let } X0 = W \bullet$ 
 $(\text{let } X1 = X(1) \bullet$ 
 $(\text{let } X2 = S^{30}(X(2)) \bullet$ 
 $(\text{let } X3 = X(3) \bullet$ 
 $(\text{let } X4 = X(4) \bullet$ 
 $(\text{let } Y = \langle X0, X1, X2, X3, X4 \rangle \bullet$ 
 $\text{if } (i = 80)$ 
 $\text{then } Y$ 
 $\text{else } L80(Y, Z, i+1) \rangle \rangle \rangle \rangle \rangle$ 
 $\text{XOR\_Z}; \text{StringWord} \leftrightarrow \text{StringWord}$ 
 $\forall Z1\_16; \text{StringWord} \mid \#Z1\_16 = 16 \bullet$ 
 $(\forall i; 1..16 \bullet$ 
 $\text{XOR\_Z}(Z1\_16)(i) = Z1\_16(i) \wedge$ 
 $(\forall i; 17..80 \bullet$ 
 $\text{XOR\_Z}(Z1\_16)(i) = S^1(\text{XOR\_Z}(Z1\_16)(i-3) \text{ XOR}$ 
 $\text{XOR\_Z}(Z1\_16)(i-8) \text{ XOR}$ 
 $\text{XOR\_Z}(Z1\_16)(i-14) \text{ XOR}$ 
 $\text{XOR\_Z}(Z1\_16)(i-16)) \bullet$ 
 $\forall sm; \text{String\_L}_1; sm; \text{String\_L}_2 \bullet$

```

 $\phi(sm, sn) =$ 
  (let Z1_16 == Split_String_to_StringWord(sm) •
  (let Y == Split_String_to_StringWord(sn) •
  (let Z == XOR_Z(Z1_16) •
  (let X == L80(Y, Z, 1) •
  (let Y0 == Y(1) 出 X(1) •
  (let Y1 == Y(2) 出 X(2) •
  (let Y2 == Y(3) 出 X(3) •
  (let Y3 == Y(4) 出 X(4) •
  (let Y4 == Y(5) 出 X(5) •
  Y0 ^ Y1 ^ Y2 ^ Y3 ^ Y4))))))))))

```

### 附 录 C

(提示的附录)

#### 参 考 文 献

- [1] J. M. Spivey, Z 记法——参考手册, Prentice-Hall, 1992(第 2 版)
- [2] 美国商业部/标准和技术国家研究所. 安全散列标准. 联邦信息处理标准出版物(FIPS PUB) 180-1, 1995 年 4 月 17 日
- [3] A. Bosselaers, H. Dobbertin 和 B. Preneel. 新的加密散列函数 RIPEMD-160. Dr. Dobbs, (1997 年 1 月) Vol. 22 No. 1 p24-28.