ICS 35.040
L 80

中华人民共和国国家标准

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

信息技术　安全技术　散列函数
第2部分：采用n位块密码的散列函数

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

2002-07-18 发布　　2002-12-01 实施

中华人民共和国
国家质量监督检验检疫总局　发布

目　　次

前言 …… I
ISO/IEC 前言 …… II
1　范围 …… 1
2　引用标准 …… 1
3　定义 …… 1
4　符号和缩略语 …… 1
5　通用模型的使用 …… 2
6　散列函数 1 …… 2
7　散列函数 2 …… 3
8　散列函数 3 …… 4
9　散列函数 4 …… 6
附录 A(提示的附录)　数据加密算法的使用 …… 9
附录 B(提示的附录)　实例 …… 11
附录 C(提示的附录)　参考文献 …… 15

前　言

本标准等同采用国际标准 ISO/IEC FDIS 10118-2:2000《信息技术　安全技术　散列函数　第2部分:采用n位块密码的散列函数》。

本标准的附录A、附录B和附录C均为提示的附录。

本标准由中华人民共和国信息产业部提出。

本标准由中国电子技术标准化研究所归口。

本标准起草单位:中国电子技术标准化研究所。

本标准主要起草人:徐冬梅、张展新。

ISO/IEC 前言

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

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

国际标准 ISO/IEC FDIS 10118-2 是由 ISO/IEC JTC1"信息技术"联合技术委员会的 SC 27"IT 安全技术"分委会制定的。

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

——第 1 部分:概述

——第 2 部分:采用 n 位块密码的散列函数

——第 3 部分:专用散列函数

——第 4 部分:采用模运算的散列函数

本标准的附录 A 和附录 B 均为提示的附录。

中华人民共和国国家标准

信息技术　安全技术　散列函数
第2部分：采用n位块密码的散列函数

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

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

1　范围

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

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

2　引用标准

下列标准所包含的条文，通过在本标准中引用而构成为本标准的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB/T 1988—1998　信息技术　信息交换用七位编码字符集(eqv ISO 646:1991)

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

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

3　定义

本标准采用ISO/IEC 10118-1中给出的定义以及下列定义：

3.1　n位块密码　n-bit block cipher

明文块和密文块的长度均为n位的块密码。(见GB/T 17964)

4　符号和缩略语

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

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

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

B^R　　当 n 是偶数时，构成块 B 的最右边的 $n/2$ 位的串。当 n 是奇数时，构成块 B 的最右边的 $(n-1)/2$ 位的串。

B^x　　当 B 是 n 个 m 位块的串时，B^x 表示 B 的第 x 个 m 位块。

B^{x-y}　　当 B 是 n 个 m 位块的串时，B^{x-y} 表示 B 的第 x 个到第 y 个 m 位块。

5　通用模型的使用

下面四章中规定的散列函数提供了长度为 L_H 的散列代码 H。散列函数符合 ISO/IEC 10118-1 中规定的通用模型。对于下列四种散列函数中的每一种，因此它只需规定：

——参数 L_1、L_2；

——填充法；

——初始化值 IV；

——循环函数 ϕ；

——输出变换 T

使用通用模型定义的散列函数的用法也需要选择参数 L_H。

6　散列函数 1

6.1　参数选择

本章中规定的散列函数的参数 L_1、L_2 和 L_H 应满足 $L_1=L_2=n$，并且 L_H 小于或等于 n。

6.2　填充法

同该散列函数一起使用的填充法的选择超出本标准的范围。填充法举例如 ISO/IEC 10118-1 的附录 A 中所示。

6.3　初始化值

同该散列函数一起使用的 IV 的选择超出本标准的范围。IV 的值应由散列函数用户协商确定。

6.4　循环函数

循环函数 ϕ 把所填充的(长 $L_1=n$ 位)数据块 D_j 与(长 $L_2=n$ 位)H_{j-1} 组合起来，以产生 H_j，其中 H_{j-1} 是循环函数的前一步输出。作为循环函数的一部分，有必要选择函数 u，该函数把 n 位块变换成与块密码算法 e 一起使用的密钥。与该散列函数一起使用的函数 u 的选择超出本标准范围(指南见附录 A)。

循环函数本身定义如下：

$$\phi(D_j,H_{j-1}) = e_{K_j}(D_j) \oplus D_j$$

其中 $K_j=u(H_{j-1})$。循环函数如图 1 所示。

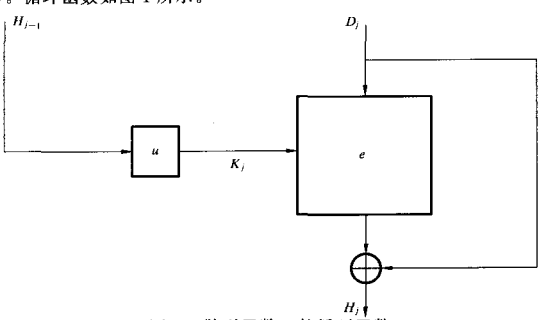

图 1　散列函数 1 的循环函数

6.5 输出变换

输出变换 T 是简单截短，即通过取最终输出块 H_q 的左边 L_H 位得到散列代码 H。

7 散列函数 2

7.1 参数选择

本章中规定的散列函数的参数 L_1、L_2 和 L_H 应满足 $L_1=n$，$L_2=2n$，且 L_H 小于或等于 $2n$。

7.2 填充法

同该散列函数一起使用的填充法的选择超出本标准的范围。填充法举例如 ISO/IEC 10118-1 的附录 A 中所示。

7.3 初始化值

同该散列函数一起使用的 IV（长度为 $2n$）的选择超出本标准的范围。IV 的值应由散列函数用户协商确定。然而，应这样选择 IV 以使 $u(IV^L)$ 和 $u'(IV^R)$ 是不同的。

7.4 循环函数

循环函数 ϕ 把所填充的（长 $L_1=n$ 位）数据块 D_i 与（长 $L_2=n$ 位）H_{i-1} 组合起来，以产生 H_i，其中 H_{i-1} 是循环函数的前一步输出。作为循环函数的一部分，有必要选择两种变换 u 和 u'。这两种变换用于把输出块变换成算法 e 的两个合适的 L_K 位密钥。u 和 u' 的规定超出本标准范围，然而，应当考虑到 u 和 u' 的选择对于散列函数的安全是重要的（见附录 A）。

设 H_0^L 和 H_0^R 分别等于 IV^L 和 IV^R。输出块以下列方式迭代计算，对 j 从 1 到 q 做：

$$\phi(D_j, H_{j-1}) = H_j$$

$$K_j^L = u(H_{j-1}^L) \text{ 和 } K_j^R = u'(H_{j-1}^R)$$

$$B_j = e_{K_j^L}(D_j) \oplus D_j \text{ 和 } B'_j = e_{K_j^R}(D_j) \oplus D_j$$

$$H_j^L = B_j^L \| B'^R_j \text{ 和 } H_j^R = B'^L_j \| B_j^R$$

循环函数如图 2 所示。

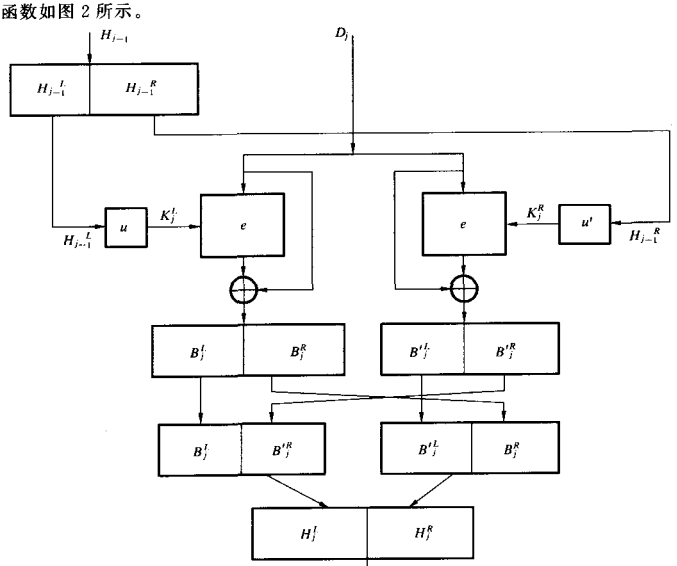

图 2 散列函数 2 的循环函数

7.5 输出变换

如果 L_H 是偶数，那么散列代码是 H_q^L 最左边 $L_H/2$ 位和 H_q^R 最左边 $L_H/2$ 位的串联。如果 L_H 是奇数，那么散列代码是 H_q^L 最左边 $(L_H+1)/2$ 位和 H_q^R 最左边 $(L_H-1)/2$ 位的串联。

8 散列函数 3

本章规定的散列函数提供了长度为 L_H 的散列代码，其中对偶数值 n 来说，L_H 等于 $2n$。

8.1 概述

以下是规定散列函数 3 所要求的某些特定的定义。

变换 u：

定义从密文空间到密钥空间的 r 个映射：$u_1, u_2, \cdots\cdots, u_r$，使得

对于任何 $i, j \in \{1,2,\cdots,r\}$，$j \neq i$，对于 C 的全部值都有 $u_i(C) \neq u_j(C)$。

这可通过固定特定的密钥位得到：例如，如果 $r=8$，我们可把 3 个密钥位固定到值 000，001，…，111 上。例如，为避免与弱密钥或块密码的补码特性相关的问题，可以对映射 u_i 施加附加的条件。

定义 r 个函数 f_i 如下：

$$f_i(X,Y) = e_{w_i(X)}(Y) \oplus Y, 1 \leqslant i \leqslant r$$

线性映射 β：

定义线性映射 β，输入一个 $2n$ 位串 $X=x_0 \| x_1 \| x_2 \| x_3$，它把该串映射为 $2n$ 位串 $Y=y_0 \| y_1 \| y_2 \| y_3$，如下述：

$y_0 := x_0 \oplus x_3$

$y_1 := x_0 \oplus x_1 \oplus x_3$

$y_2 := x_1 \oplus x_2$

$y_3 := x_2 \oplus x_3$

这里 x_i 和 y_i 是 $n/2$ 位串。

8.2 参数选择

本章中规定的散列函数的参数 L_1、L_2 和 L_H 应满足，$L_1=4n$，$L_2=8n$，且 L_H 等于 $2n$。

8.3 填充法

同该散列函数一起使用的填充法应按照 ISO/IEC 10118-1 的 A3 章中规定，以使 $r=n$。

8.4 初始化值

同该散列函数一起使用的 IV（其中长度为 $8n$）的选择超出本标准的范围。IV 的值应由散列函数用户协商确定。

8.5 循环函数

循环函数 ϕ 具有 8 个并行的加密过程，以及 8 个 n 位链接变量 H_j^{1-8}。

在每次迭代中，把 4 个 n 位（长 $L_1=4n$ 位）数据块 D_j^{1-4} 与（长 $L_2=8n$ 位）H_{j-1}^{1-8} 组合起来，以产生 H_j^{1-8}，其中（长 $L_2=8n$ 位）H_{j-1}^{1-8} 是循环函数前一步的输出。

循环函数基于线性映射 γ_1，输入 12 个 n 位串 l^{1-12}，并把它们映射为 8 个 n 位串 X^{1-8} 和 8 个 n 位串 Y^{1-8}。映射使用 8 个 $2n$ 位辅助串 $R^0, R^1, M^0, M^1, \cdots, M^5$。映射 γ_1 通过如下步骤定义：

a) for $i=0$ to 5 do $\{M^{iL} := l^{2i+1}; M^{iR} := l^{2i+2};\}$

$R^0 := 0; R^1 := 0;$

b) for $i=0$ to 5 do{

$B := R^1 \oplus M^i;$

$R^1 := R^0 \oplus \beta(B);$

$R^0 := B;\}$

c) for $i=0$ to 8 do$\{X^i := l^i;\}$

$Y^1 := R^{0L};$

$Y^2 := R^{0R};$

$Y^3:=R^{1L}$;

$Y^4:=R^{1R}$;

for $i=1$ to 4 do $\{Y^{4+i}:=I^{8+i};\}$

循环函数具有下列形式($1\leqslant j\leqslant q$):

$(X_j^{1-8},Y_j^{1-8}):=\gamma_1(H_{j-1}^{1-8},D_j^{1-4})$;

for $i=1$ to 8 do$\{H_j^i:=f_i(X_j^i,Y_j^i);\}$

循环函数如图 3a 所示,线性映射 γ_1 如图 3b 所示。

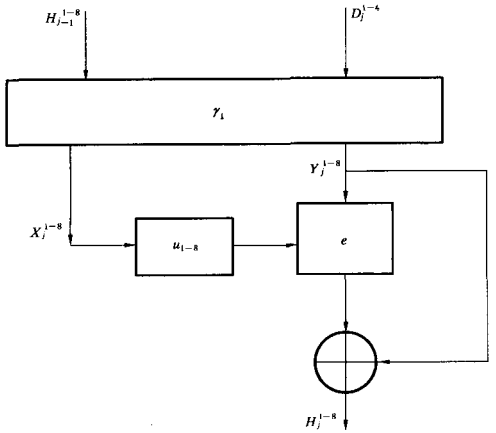

图 3a 散列函数 3 的循环函数

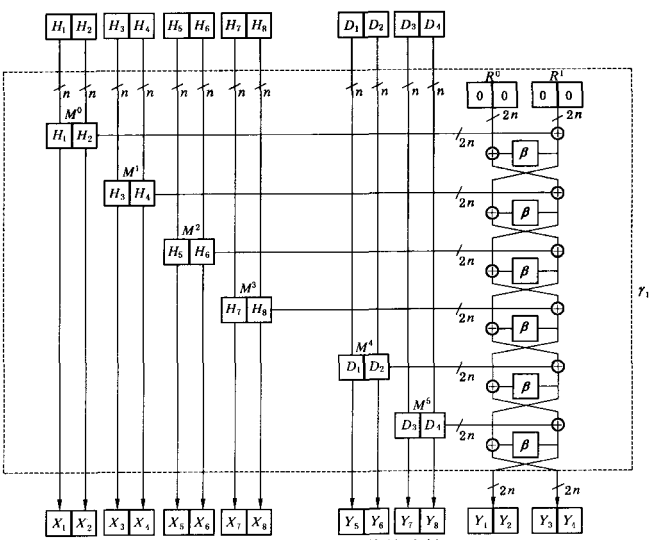

图 3b 散列函数 3 的线性映射 γ_1

8.6 输出变换

在处理所填充的消息后，链接变量具有值 H_q^{1-8}。执行 4 次附加的循环函数的迭代，其消息输入分别是：

$D_{q+1}^{1-4} = H_q^{1-4}$

$D_{q+2}^{1-4} = H_q^{5-8}$

$D_{q+3}^{1-4} = H_q^{1-4}$

$D_{q+4}^{1-4} = H_q^{5-8}$

这样散列函数的输出 L_H 包括 $H_{q+4}^1 \| H_{q+4}^2$。输出变换要求 26 次加密过程(在最后一次迭代中仅需要执行两次加密过程)。

9 散列函数 4

本章规定的散列函数提供长度为 L_H 的散列代码，其中对于偶数值 n 来说，L_H 等于 $3n$。

9.1 概述

关于与该散列函数相关的特定定义见 8.1。

9.2 参数选择

本章中规定的散列函数的参数 L_1、L_2 和 L_H 应满足 $L_1=3n$，$L_2=9n$，且 L_H 等于 $3n$。

9.3 填充法

同该散列函数一起使用的填充法应按照 ISO/IEC 10118-1:2000 条 A.3 中规定的，以使 $r=n$。

9.4 初始化值

同该散列函数一起使用的(长 $9n$)IV 的选择超出本标准的范围。IV 的值应由散列函数用户协商确定。

9.5 循环函数

循环函数 ϕ 具有 9 个并行的加密过程，以及 9 个 n 位链接变量 H_j^{1-9}。

在每次迭代中，把 3 个 n 位(长 $L_1=3n$ 位)数据块 D_j^{1-3} 与(长 $L_2=9n$ 位)H_{j-1}^{1-9}组合起来，以产生(长 $L_2=9n$ 位)H_j^{1-9}，其中 H_{j-1}^{1-9}是循环函数前一步的输出。

循环函数基于线性映射 γ_2，输入 12 个 n 位串 l^{1-12}，并把它们映射为 9 个 n 位串 X^{1-9}和 9 个 n 位串 Y^{1-9}。映射使用 9 个 2n 位辅助串 $R^0, R^1, R^2, M^0, M^1, \cdots, M^5$。映射 γ_2 通过下列步骤定义：

a) for $i=0$ to 5 do $\{M^{iL} := l^{2i+1}; M^{iR} := l^{2i+2};\}$

$R^0 := 0; R^1 := 0; R^2 := 0;$

b) for $i=0$ to 5 do{

$B := R^2 \oplus M^i;$

$U := \beta(B);$

$R^2 := R^1 \oplus U;$

$R^1 := R^0 \oplus U;$

$R^0 := B;\}$

c) for $i=0$ to 9 do$\{X^i := l^i;\}$

$Y^1 := R^{0L};$

$Y^2 := R^{0R};$

$Y^3 := R^{1L};$

$Y^4 := R^{1R};$

$Y^5 := R^{2L};$

$Y^6 := R^{2R};$

for $i=1$ to 3 do $\{Y^{6+i}:=l^{9+i};\}$

循环函数具有下列形式($1\leqslant j\leqslant q$)：

$(X_j^{1-9},Y_j^{1-9}):=\gamma_2(H_{j-1}^{1-9},D_j^{1-3})$；

for $i=1$ to 9 do$\{H_j^i:=f_i(X_j^i,Y_j^i);\}$

循环函数如图 4a 所示，线性映射 γ_2 如图 4b 所示。

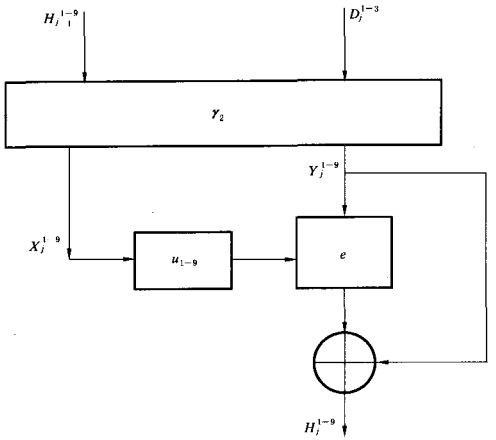

图 4a　散列函数 4 的循环函数

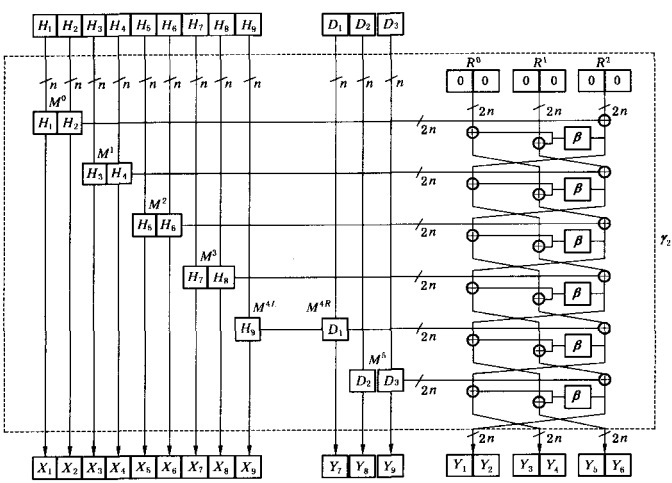

图 4b　散列函数 4 的线性映射 γ_2

9.6 输出变换

在处理所填充的消息后，链接变量具有值 H_q^{1-8}。执行 4 次附加的循环函数的迭代，其消息输入分别是：

$D_{q+1}^{1-3} = H_q^{1-3}$

$D_{q+2}^{1-3} = H_q^{4-6}$

$D_{q+3}^{1-3} = H_q^{7-9}$

$D_{q+4}^{1-2} = H_q^{1-3}$

这样散列函数的输出包括 $H_{q+4}^{1} \| H_{q+4}^{2} \| H_{q+4}^{3}$。输出变换要求 30 次加密过程(在最后一次迭代中仅需要执行 3 次加密过程)。

附 录 A
（提示的附录）
数据加密算法的使用

A1 概述

本附录提供了数据加密算法(DEA)(ANSI X3.92)与本标准中规定的散列操作一起使用的方法。DEA 名称为数据加密标准(DES)。

位的编号如附录 C 的[2]中 ANSI X3.92 所示。

这些方法在附录 C 的[3]中作了描述，DEA 的参数是 $n=64$ 及 $L_K=64$。

A2 散列函数 1

见第 6 章。

IV 应等于“5252525252525252”(用十六进制记法表示)。

变换 u 应按照如下选择。令 $X=x_1x_2\cdots x_{64}$是 64 位串 X 的二进制分解，则 $Y=u(X)$是让位 x_2 和位 x_3 的值分别为 1、0，并且以位 x_8'，x_{16}'，x_{24}'，x_{32}'，x_{40}'，x_{48}'，x_{56}'，x_{64}'分别取代位 x_8，x_{16}，x_{24}，x_{32}，x_{40}，x_{48}，x_{56}，x_{64}以后得到的字符串，其中 x_{8i}'表示 X 中紧接 x_{8i}'的前 7 位即 x_{8i-7}，x_{8i-6}，x_{8i-5}，x_{8i-4}，x_{8i-3}，x_{8i-2}，x_{8i-1}的奇偶校验位。结果是：$Y=x_1'10x_4x_5x_6x_7x_8'x_9x_{10}\cdots x_{63}x_{64}'$。固定 X 中的位 2 和位 3 的理由在与 IBM MDC-2 的算法相关的附录 C 的[7]中描述；然而，相同的理由也适用于此散列函数。

注：认为找出循环函数和散列函数的碰撞要求 2^{27}次 DES 加密过程。

A3 散列函数 2

见第 7 章。

IV^L 应等于“5252525252525252”(用十六进制记法表示)。

IV^R 应等于“2525252525252525”(用十六进制记法表示)。

变换 u 应与 A2 章中的相同，变换 u'应按照如下选择。令 $X=x_1x_2\cdots x_{64}$是 64 位字符串 X 的二进制分解，则 $Y=u'(X)$是在分别让位 x_2 和位 x_3 的值为 0、1，并且以 x_8'，x_{16}'，x_{24}'，x_{32}'，x_{40}'，x_{48}'，x_{56}'，x_{64}'分别取代位 x_8，x_{16}，x_{24}，x_{32}，x_{40}，x_{48}，x_{56}，x_{64}以后得到的串，其中 x_{8i}'表示 X 中紧接 x_{8i}'的前 7 位即：x_{8i-7}，x_{8i-6}，x_{8i-5}，x_{8i-4}，x_{8i-3}，x_{8i-2}，x_{8i-1}的奇偶校验位。结果是：$Y=x_1'01x_4x_5x_6x_7x_8'x_9x_{10}\cdots x_{63}x_{64}'$。固定 X 中的位 2 和位 3 的理由在与 IBM MDC-2 的算法相关的附录 C 的[7]中描述；然而，相同的理由也适用于该散列函数。

注：认为找出循环函数和散列函数的碰撞要求 2^{55}个 DES 加密过程。

A4 散列函数 3

见第 8 章。

IV^1，IV^2，…，IV^8 应等于“5252525252525252”(用十六进制记法表示)。

变换 u_1，u_2，…，u_8 应按照如下选择。令 $X=x_1x_2\cdots x_{64}$是 64 位串 X 的二进制分解，则 $Y=u_i(X)$是在分别让位 x_1，x_2，…，x_5 的值为表 A1 中给出的值，并且以 x_8'，x_{16}'，x_{24}'，x_{32}'，x_{40}'，x_{48}'，x_{56}'，x_{64}'分别取代位 x_8，x_{16}，x_{24}，x_{32}，x_{40}，x_{48}，x_{56}，x_{64}以后得到的串，其中 x_{8i}'表示 X 中紧接 x_{8i}'的前 7 位即 x_{8i-7}，x_{8i-6}，x_{8i-5}，x_{8i-4}，x_{8i-3}，x_{8i-2}，x_{8i-1}的奇偶校验位。

表 A1 散列函数 3:8 个子函数中密钥位 1、2、3、4 和 5 的值

子函数 i	子函数 i
1	00101
2	01001
3	10001
4	00110
5	01010
6	10010
7	01100
8	10100

注：认为找出循环函数和散列函数的碰撞要求 2^{51}次 DES 加密过程。

A5 散列函数 4

见第 9 章。

$IV^1, IV^2, \cdots, IV^9$ 应等于“5252525252525252”(用十六进制记法表示)。

变换 $u_1, u_2, \cdots, u_9$ 应按照如下选择。令 $X = x_1 x_2 \cdots x_{64}$是 64 位字符串 X 的二进制分解，则 $Y = u_i(X)$ 是在分别让位 $x_1, x_2, \cdots, x_5$ 的值为表 A2 中给出的值，并且以 $x_8', x_{16}', x_{24}', x_{32}', x_{40}', x_{48}', x_{56}', x_{64}'$分别取代位 $x_8, x_{16}, x_{24}, x_{32}, x_{40}, x_{48}, x_{56}, x_{64}$以后得到的串，其中 x_{8i}'表示 X 中紧挨 x_{8i}'的前 7 位即 $x_{8i-7}, x_{8i-6}, x_{8i-5}, x_{8i-4}, x_{8i-3}, x_{8i-2}, x_{8i-1}$的奇偶校验位。

表 A2 散列函数 4:9 个子函数中密钥位 1、2、3、4 和 5 的值

子函数 i	子函数 i
1	00101
2	01001
3	10001
4	00110
5	01010
6	10010
7	01100
8	10100
9	11000

注：认为找出循环函数和散列函数的碰撞要求 2^{76}次 DES 加密过程。

A6 动机

如果 DEA 用于散列构建中，它具有某些不期望的特性。首先，有 4 个弱密钥，其中加密函数等于解密函数。另外，这 4 个弱密钥中，有 2^{32}个不动点，即，对其加密为自身明文本值。其次，有 16 对半弱密钥，其中由某一个密钥所诱导出的加密函数等于另一个密钥的解密函数。DES 也具有补码特性：如果明文和密钥两者都取补码，那么密文也取补码。

对于散列函数 1 和 2，如上所述固定密钥的 2 个位的值，是避免弱密钥和半弱密钥的充分必要条件。散列函数 1 需要 1 个固定的值，散列函数 2 需要 2 个固定值。这些值必须具有下列特性：

——全部值必须是不同的。

——这些值中任何一个值都不允许使用弱密钥和半弱密钥。

对于散列函数 3 和 4，如上所述固定密钥的 5 个位的值，是避免弱密钥、半弱密钥和补码特性的充分必要条件。

散列函数 3 要求 8 个固定值，散列函数 4 要求 9 个固定值。这些值必须具有下列特性：

——全部值必须是不同的。

——这些值中任何一个值都不允许能使用弱密钥和半弱密钥。

——这些值中没有一个值是另一个值的补码值。

满足上述条件的事实可从下列观察中推出。考虑密钥的 5 个位：1、2、3、4 和 5，对于 DEA 的全部弱密钥和半弱密钥，这 5 位取下列值中的一个：00000，11111，00011，或者 11100。

附 录 B
（提示的附录）
实 例

B1 概述

本附录给出使用本标准附录 A 中规定的前两个散列函数的散列代码的计算的举例，以及 ISO/IEC 10118-1 的附录 B 中规定的填充法的举例。

对于“Now _ is _ the _ time _ for _ all _”来说，数据串是附录 C 的[8]中所描述的 7 位 GB 1988 代码（无奇偶校验），其中“_”表示空白，用十六进制记法表示：

‘4E6F772069732074686520746965D6520666F7220616C6C20’

B2 散列函数 1

见 A2。

填充法 1

j	D_j	H_{j-1}	H_j
1	4E6F772069732074	5252525252525252	858A260F7391482D
2	68652074696D6520	858A260f7391482D	BDE06E66A0454081
3	666F7220616C6C20	BDE06E66A0454081	FF87B67E29BB87B1

填充法 2

j	D_j	H_{j-1}	H_j
1	4E6F772069732074	5252525252525252	858A260F7391482D
2	68652074696D6520	858A260F7391482D	BDE06E66A0454081
3	666F7220616C6C20	BDE06E66A0454081	FF87B67E29BB87B1
4	80000000000000000	FF87B67E29BB87B1	D992E6CBDFD9BA81

B3 散列函数 2

见 A3。

填充法 1

j	D_j	H_{j-1}^{L}	H_{j-1}^{K}
1	4E6F772069732074	5252525252525252	2525252525252525

2	68652074696D6520	858A260FFD4873A8	49771DD37391482D
3	666F7220616C6C20	B002740352F7CF4F	CFE8087E1B93CCB2

j	H_j^L	H_j^R
1	858A260FFD4873A8	49771DD37391482D
2	B002740352F7CF4F	CFE8087E1B93CCB2
3	42E50CD224BACEBA	760BDD2BD409281A

填充法 2

j	D_j	H_{j-1}^L	H_{j-1}^R
1	4E6F772069732074	5252525252525252	858A260F7391482D
2	68652074696D6520	858A260F7391482D	BDE06E66A0454081
3	666F7220616C6C20	B002740352F7CF4F	CFE8087E1B93CCB2
4	8000000000000000	42E50CD224BACEBA	760BDD2BD409281A

j	H_j^L	H_j^R
1	858A260FFD4873A8	49771DD37391482D
2	B002740352F7CF4F	CFE8087E1B93CCB2
3	42E50CD224BACEBA	760BDD2BD409281A
4	2E4679B5ADD9CA75	35D87AFEAB33BEE2

B4 散列函数 3

见 A4。

填充法 3

M_1^{1-4}	H_0^{1-8}	H_1^{1-8}
4e6f772069732074	5252525252525250	3817bdae19b2225a
68652074696d6520	5252525252525250	e3d076623583d877
666f7220616c6c20	5252525252525250	49b40c792ef3a4c4
8000000000000000	5252525252525250	8a719789bd78110d
	5252525252525250	858a260f7391482d
	5252525252525250	24663b3c87d579f5
	5252525252525250	ae090bece542b395
	5252525252525250	828147754817b9d3

M_2^{1-4}	H_1^{1-8}	H_2^{1-8}
0000000000000000	3817bdae19b2225a	e707467a1f5346a0
0000000000000000	e3d076623583d877	bb5ee05a7169849b
0000000000000000	49b40c792ef3a4c4	1f8bf96576f3af2c
00000000000000c0	8a719789bd78110d	4c0f7b482d1315f2
	858a260f7391482d	d1f9b69c6e3ada6a
	24663b3c87d579f5	bd47cdf126206f86
	ae090bece542b395	91a3a27d96a760b4
	828147754817b9d3	52f0a65fa311abd9

M_3^{1-4}	H_2^{1-8}	H_3^{1-8}
e707467a1f5346a0	e707467a1f5346a0	1b1cb5b24f14bd5e
bb5ee05a7169849b	bb5ee05a7169849b	77c4fea88f17c659
1f8bf96576f3af2c	1f8bf96576f3af2c	84d0ab573184e7b8

4c0f7b482d1315f2	4c0f7b482d1315f2	04ad6d640ef3dd41
	d1f9b69c6e3ada6a	8c382ad7b2608680
	bd47cdf126206f86	440e7d6734aba3ad
	91a3a27d96a760b4	6c79fd354cebf488
	52f0a65fa311abd9	933baecdaefe96dd
M_4^{1-4}	H_3^{1-8}	H_4^{1-8}
d1f9b69c6e3ada6a	1b1cb5b24f14bd5e	14103e8e1371d79c
bd47cdf126206f86	77c4fea88f17c659	039d8adbc72e1b75
91a3a27d96a760b4	84d0ab573184e7b8	485480d68b15a8c1
52f0a65fa311abd9	04ad6d640ef3dd41	76ad4f338fa4626d
8c382ad7b2608680	c53cad3191b7294e	
440e7d6734aba3ad	fc1ab80fce4920f3	
6c79fd354cebf488	861f2b7c4a224f6e	
933baecdaefe96dd	4b96399b28f000d4	
M_5^{1-4}	H_4^{1-8}	H_5^{1-8}
e707467a1f5346a0	14103e8e1371d79c	fb6810eb1a7f3c8b
bb5ee05a7169849b	039d8adbc72e1b75	720441fd4d9c653c
1f8bf96576f3af2c	485480d68b15a8c1	815b516b2e25abd9
4c0f7b482d1315f2	76ad4f338fa4626d	1433b28ec0dfe04b
c53cad3191b7294e	f38221f40dc72976	
fc1ab80fce4920f34	561afdfc9279fa2	
861f2b7c4a224f6e	432023481ffa3998	
4b96399b28f000d4	c0579150f5b09d73	
M_6^{1-4}	H_5^{1-8}	H_6^{1-8}
d1f9b69c6e3ada6a	fb6810eb1a7f3c8b	701e6b65f31a6ddb
bd47cdf126206f86	720441fd4d9c653c	23d7d4c6c8d66715
91a3a27d96a760b4	815b516b2e25abd9	af57c481a50ad950
52f0a65fa311abd9	1433b28ec0dfe04b	aa692ba1d340203a
f38221f40dc72976	c42f680e5ce50575	
4561afdfc9279fa2	a1f7db3639418d8d	
432023481ffa3998	457804332a268880	
c0579150f5b09d73	a8f6d4077398b932	

B5 散列函数 4

见 A5。

填充法 3

M_1^{1-3}	H_0^{1-9}	H_1^{1-9}
4e6f772069732074	5252525252525250	4c94cc79cae77819
686520746 96d6520	5252525252525250	d29e99f5c68a6233
666f7220616c6c20	5252525252525250	4e887bd627992f6f
	5252525252525250	f49f29f403beb556
	5252525252525250	0d864de5c09ca081
	5252525252525250	8af58cd7aac38005

	5252525252525250	8cb3928bd36dc983
	5252525252525250	4d263c662e075af8
	5252525252525250	58fc2852cd3b3012
M_2^{1-3}	H_1^{1-9}	H_2^{1-9}
8000000000000000	4c94cc79cae77819	414cf3eb381277c7
0000000000000000	d29e99f5c68a6233	bd58a6176226bcc9
00000000000000c0	4e887bd627992f6f	0f7050105fcbc9d6
	f49f29f403beb556	85c8c35886441428
	0d864de5c09ca081	4ae14549dc5ba435
	8af58cd7aac38005	add8eadcf2b954c1
	8cb3928bd36dc983	968e8c4604d7d06e
	4d263c662e075af8	e1a291fa48ebf45a
	58fc2852cd3b3012	b2dd1fe8fdb34712
M_3^{1-3}	H_2^{1-9}	H_3^{1-9}
414cf3eb381277c7	414cf3eb381277c7	b76c32c73212fb32
bd58a6176226bcc9	bd58a6176226bcc9	54885ed14ffd1c1b
0f7050105fcbc9d6	0f7050105fcbc9d6	3e0a181f8f239845
	85c8c35886441428	8a3e93dd54caff45
	4ae14549dc5ba435	027fc8d2823deade
	add8eadcf2b954c1	2ba78ba7bc398e5e
	968e8c4604d7d06e	fadffa8c7d70d4e2
	e1a291fa48ebf45a	8ceaef44bbc1ab78
	b2dd1fe8fdb34712	aa5985d2bcac5f5b
M_4^{1-3}	H_3^{1-9}	H_4^{1-9}
85c8c35886441428	b76c32c73212fb32	4c0997a2ad69abf5
4ae14549dc5ba435	54885ed14ffd1c1b	b27994d84743a3c8
add8eadcf2b954c1	3e0a181f8f239845	5e0347b82ba1a6af
	8a3e93dd54caff45	db895422b6aa9d00
	027fc8d2823dead	e26a0a405cf180c8
	2ba78ba7bc398e5e	4c7aa1e6d50e03b9
	fadffa8c7d70d4e2	838ca9bf32f46e93
	8ceaef44bbc1ab78	c86773b042a59790
	aa5985d2bcac5f5b	56043d88183ec785
M_5^{1-3}	H_4^{1-9}	H_5^{1-9}
968e8c4604d7d06e	4c0997a2ad69abf5	b96a4f306ec9ca2a
e1a291fa48ebf45a	b27994d84743a3c8	1d35c007225c43f4
b2dd1fe8fdb34712	5e0347b82ba1a6af	6dfa8d6f7371a3a5
	db895422b6aa9d00	9d9e3f4a956b638e
	e26a0a405cf180c8	80eea45b14fe4d68
	4c7aa1e6d50e03b9	ea8e1ca53f197d7e
	838ca9bf32f46e93	dac6e66cd9e7100a
	c86773b042a59790	031598c70f3294b5
	56043d88183ec785	452fcbff98fe864b

M_6^{1-3}	H_5^{1-9}	H_6^{1-9}
414cf3eb381277c7	b96a4f306ec9ca2a	a53c5ffcd01d3b29
bd58a6176226bcc9	1d35c007225c43f4	7155c6869a8a1b28
0f7050105fcbc9d6	6dfa8d6f7371a3a5	16dd5634f47109b4
	9d9e3f4a956b638e	07aaf79ab9dbe8fd
	80eea45b14fe4d68	64bc2dc5b6be379b
	ea8e1ca53f197d7e	3d67e08e82e336fc
	dac6e66cd9e7100a	255ba6b94074363f
	031598c70f3294b5	fea159a050fdeb4d
	452fcbff98fe864b	7253b8ff11830261

附 录 C
（提示的附录）
参 考 文 献

[1] ISO/IEC 9979:1999 信息技术 安全技术 加密算法的登记规程

[2] ANSI X3.92:1981 数据加密算法

[3] S. M. MATYAS. 带控制矢量的密钥处理(Key Processing with Control Vectors)。*J. of Cryptology*, Vol. 2, 1991, pp. 113-136.

[4] L. R. KNUDSEN, B. PRENEEL. 基于块密码和四进制代码的散列函数(Hash-functions based on block ciphers and quaternary codes)。*Advances in Cryptology*, Proc. AsiaCrypt'96, LNCS 1163. K. Kim, T. Matsumoto, Eds., Springer-Verlag, 1996, pp. 77-90.

[5] L. R. KNUDSEN, B. PRENEEL. 基于代码的快速、安全的散列(Fast and secure hashing based on codes)。*Advances in Cryptology*, Proc. Crypto'97, LNCS 1294. B. Kaliski, Ed., Springer-Verlag, 1997, pp. 485-498.

[6] US patent 4,908,861, 使用基于公开单向加密函数更正检测代码的数据鉴别(*Data Authentication Using Modification Detection Codes based on A Public One way Encryption Function*)。Issued March 13, 1990.

[7] Don Coppersmith, Stephen M. Matyas, Mohammed Peyravian. MDC-2 算法中位固定的基本原理(*Rationale for Bit Fixing in the MDC-2 Algorithm*)。IBM T. J. Watson Research Center, Yorktown Heights, N. Y., 10598. Research Report RC21471, May 7 1999.

[8] GB/T 1988—1998 信息技术 信息交换用七位编码字符集(eqv ISO 646:1991)。