INTERNATIONAL STANDARD

ISO/IEC 10118-2

Second edition
2000-12-15

Information technology — Security techniques — Hash-functions —

Part 2: Hash-functions using an *n*-bit block cipher

Technologies de l'information — Techniques de sécurité — Fonctions de brouillage —

Partie 2: Fonctions de brouillage utilisant un chiffrement par blocs de n *bits*

Reference number
ISO/IEC 10118-2:2000(E)

© ISO/IEC 2000

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO/IEC 2000

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

© ISO/IEC 2000 – All rights reserved

Not for Resale

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Symbols and abbreviated terms 1

5 Use of the general model 2

6 Hash-function one 2
6.1 Parameter selection 2
6.2 Padding method 2
6.3 Initializing value 2
6.4 Round-function 2
6.5 Output transformation 3

7 Hash-function two 3
7.1 Parameter selection 3
7.2 Padding method 3
7.3 Initializing value 3
7.4 Round-function 4
7.5 Output transformation 5

8 Hash-function three 5
8.1 General 5
8.2 Parameter selection 5
8.3 Padding method 5
8.4 Initializing value 6
8.5 Round-function 6
8.6 Output transformation 8

9 Hash-function four 8
9.1 General 8
9.2 Parameter selection 8
9.3 Padding method 8
9.4 Initializing value 8
9.5 Round-function 8
9.6 Output transformation 10

Annex A (informative) **Use of DEA** 11

Annex B (informative) **Examples** 14

Bibliography 19

© ISO/IEC 2000 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 10118-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 10118-2:1994), which has been technically revised to conform to the general model described in ISO/IEC 10118-1, and to add two additional hash-functions. Note, however, that implementations which comply with ISO/IEC 10118-2:1994 will be compliant with this edition of ISO/IEC 10118-2.

ISO/IEC 10118 consists of the following parts, under the general title *Information technology — Security techniques — Hash-functions*:

— *Part 1: General*

— *Part 2: Hash-functions using an n-bit block cipher*

— *Part 3: Dedicated hash-functions*

— *Part 4: Hash-functions using modular arithmetic*

Annexes A and B of this part of ISO/IEC 10118 are for information only.

© ISO/IEC 2000 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Introduction

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) draw attention to the fact that it is claimed that compliance with this part of ISO/IEC 10118 may involve the use of a patent concerning the “Data Authentication Using Modification Detection Codes Based on a Public One Way Encryption Function,” (U.S. Patent 4,908,861 issued 1990-03-13).

ISO and IEC take no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured ISO and IEC that he is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO and IEC. Information may be obtained from:

Director of Licensing
International Business Machnies Corporation
500 Columbus Avenue
Thornwood, NY 10594
U.S.A.

Attention is drawn to the possibility that some of the elements of this part of ISO/IEC 10118 may be the subject of patent rights other than those identified above. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

© ISO/IEC 2000 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

Information technology — Security techniques — Hash-functions —

Part 2: Hash-functions using an *n*-bit block cipher

1 Scope

This part of ISO/IEC 10118 specifies hash-functions which make use of an *n*-bit block cipher algorithm. They are therefore suitable for an environment in which such an algorithm is already implemented.

Four hash-functions are specified. The first provides hash-codes of length smaller than or equal to *n*, where *n* is the block-length of the algorithm used. The second provides hash-codes of length less than or equal to 2*n*; the third provides hash-codes of length equal to 2*n*; and the fourth provides hash-codes of length 3*n*. All four of the hash-functions specified in this part of ISO/IEC 10118 conform to the general model specified in ISO/IEC 10118-1.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of ISO/IEC 10118. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this part of ISO/IEC 10118 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO/IEC 10116:1997, *Information technology — Security techniques — Modes of operation for an n-bit block cipher.*

ISO/IEC 10118-1:2000, *Information technology — Security techniques — Hash-functions — Part 1: General.*

3 Terms and definitions

For the purposes of this part of ISO/IEC 10118, the terms and definitions given in ISO/IEC 10118-1 and the following apply.

3.1
***n*-bit block cipher**
a block cipher with the property that plaintext blocks and ciphertext blocks are *n* bits in length (see ISO/IEC 10116)

4 Symbols and abbreviated terms

For the purposes of this part of ISO/IEC 10118, the symbols and abbreviations given in ISO/IEC 10118-1 and the following apply:

e *n*-bit block cipher algorithm (see ISO/IEC 10116)

K Key for the algorithm *e* (see ISO/IEC 10116)

© ISO/IEC 2000 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

$e_K(P)$ Operation of encipherment using the algorithm e and the key K (see ISO/IEC 10116) on plaintext P

u or u' Transformation of one n-bit block into a key for the algorithm e

B^L When n is even, the string composed of the $n/2$ leftmost bits of the block B. When n is odd, the string composed of the $(n+1)/2$ leftmost bits of the block B

B^R When n is even, the string composed of the $n/2$ rightmost bits of the block B. When n is odd, the string composed of the $(n-1)/2$ rightmost bits of the block B

B^x When B is a string of n m-bit blocks, B^x represents the x-th m-bit block of B

B^{x-y} When B is a string of n m-bit blocks, B^{x-y} represents the x-th through the y-th m-bit blocks of B

5 Use of the general model

The hash-functions specified in the next four clauses provide hash-codes H of length L_H. The hash-function conforms to the general model specified in ISO/IEC 10118-1. For each of the four hash-functions that follow, it is therefore only necessary to specify:

— the parameters L_1, L_2;

— the padding method;

— the initializing value IV;

— the round-function ϕ;

— the output transformation T.

The use of a hash-function defined using the general model will also require the selection of the parameter L_H.

6 Hash-function one

6.1 Parameter selection

The parameters L_1 and L_2 and L_H for the hash-function specified in this clause shall satisfy $L_1 = L_2 = n$, and L_H is less than or equal to n.

6.2 Padding method

The selection of the padding method for use with this hash-function is beyond the scope of this part of ISO/IEC 10118. Examples of padding methods are presented in annex A of ISO/IEC 10118-1:2000.

6.3 Initializing value

The selection of the IV for use with this hash-function is beyond the scope of this part of ISO/IEC 10118. The value of the IV shall be agreed upon and fixed by the users of the hash-function.

6.4 Round-function

The round-function ϕ combines a padded data block D_i (of $L_1 = n$-bits) with H_{i-1}, the previous output of the round-function (of $L_2 = n$ bits), to yield H_i. As part of the round-function it is necessary to choose a function u, which transforms an n-bit block into a key for use with the block cipher algorithm e. The selection of the function u for use with this hash-function is outside the scope of this part of ISO/IEC 10118 (see annex A for guidance).

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2000 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The round-function itself is defined as follows:

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

where $K_j = u\,(H_{j-1})$. The round-function is shown in Figure 1.

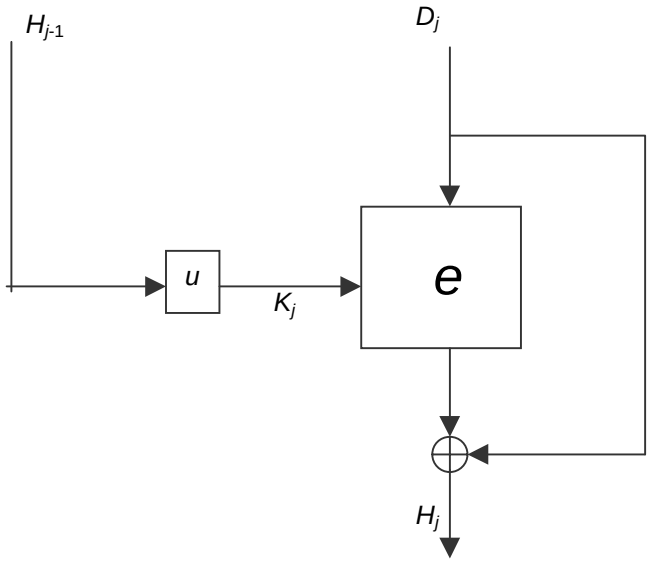

Figure 1 — Round-function of hash-function one

6.5 Output transformation

The output transformation T is simply truncation, i.e., the hash-code H is derived by taking the leftmost L_H bits of the final output block H_q.

7 Hash-function two

7.1 Parameter selection

The parameters L_1 and L_2 and L_H for the hash-function specified in this clause shall satisfy $L_1 = n$, $L_2 = 2n$, and L_H is less than or equal to $2n$.

7.2 Padding method

The selection of the padding method for use with this hash-function is beyond the scope of this part of ISO/IEC 10118. Examples of padding methods are presented in annex A of ISO/IEC 10118-1:2000.

7.3 Initializing value

The selection of the IV (of length $2n$) for use with this hash-function is beyond the scope of this part of ISO/IEC 10118. The value of the IV shall be agreed upon and fixed by the users of the hash-function. However, the IV shall be selected such that $u(IV^L)$ and $u'(IV^R)$ are different.

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2000 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.4 Round-function

The round-function ϕ combines a padded data block D_i (of $L_1 = n$ bits) with H_{i-1}, the previous output of the round-function (of $L_2 = 2n$ bits), to yield H_i. As part of the round-function it is necessary to choose two transformations u and u'. These transformations are used to transform an output block into two suitable L_K bit keys for the algorithm e. The specification of u and u' is beyond the scope of this part of ISO/IEC 10118. However, it should be taken into consideration that the selection of u and u' is important for the security of the hash-function (see annex A).

Set H_0^L and H_0^R equal to IV^L and IV^R respectively. The output blocks are calculated iteratively in the following way, for $j = 1$ to q:

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

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

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

$H_j^L = B_j^L \,||\, B'^R_j$ and $H_j^R = B'^L_j \,||\, B_j^R$

The round-function is shown in Figure 2.

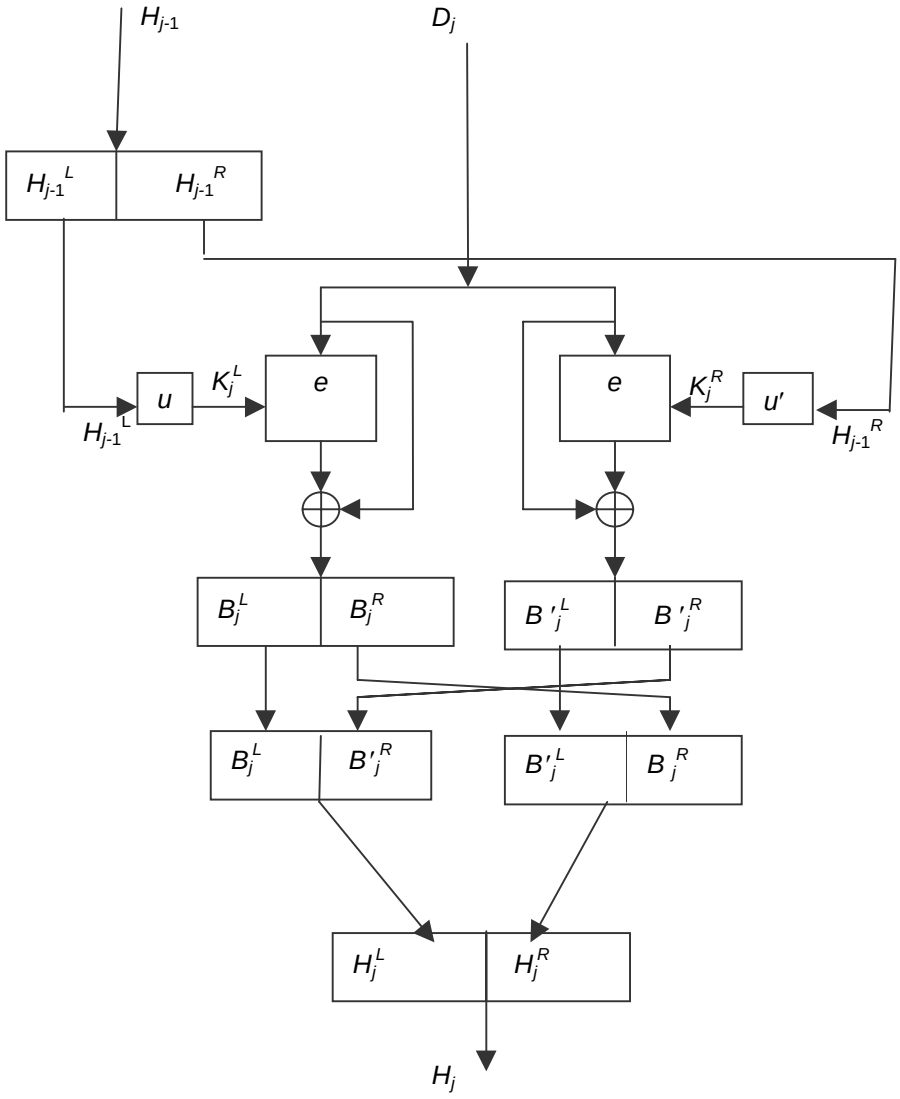

Figure 2 — Round-function of hash-function two

© ISO/IEC 2000 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

7.5 Output transformation

If L_H is even, the hash-code is the concatenation of the $L_H/2$ leftmost bits of H_q^L and the $L_H/2$ leftmost bits of H_q^R. If L_H is odd, the hash-code is the concatenation of the $(L_H+1)/2$ leftmost bits of H_q^L and the $(L_H-1)/2$ leftmost bits of H_q^R.

8 Hash-function three

The hash-function specified in this clause provides hash-codes of length L_H, where L_H is equal to $2n$ for even values of n.

8.1 General

Some specific definitions that are required to specify hash-function three follow.

Transformation u:

Define r mappings $u_1, u_2, \ldots, u_r$ from the ciphertext space to the key space, such that,

For all i, j from the set $\{1,2,\ldots,r\}$, $j \neq i$, $u_i(C) \neq u_j(C)$ for all values of C.

This can be achieved by fixing specific key bits: e.g., if $r = 8$ one can fix three key bits to the values 000, 001, ..., 111. Additional conditions might be imposed upon the mappings u_i, for example, to avoid the problems related to weak keys or complementation properties of the block cipher.

Function f_i:

Define the r functions f_i as follows:

$f_i(X,Y) = e_{ui(X)}(Y) \oplus Y$, $1 \leq i \leq r$.

Linear mapping β:

Define the linear mapping β that takes as input a $2n$-bit string $X = x_0||x_1||x_2||x_3$ and maps it to a $2n$-bit string $Y = y_0||y_1||y_2||y_3$ as follows:

$y_0 := x_0 \oplus x_3$

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

$y_2 := x_1 \oplus x_2$

$y_3 := x_2 \oplus x_3$

Here x_i and y_j are $n/2$ bit strings.

8.2 Parameter selection

The parameters L_1 and L_2 and L_H for the hash-function specified in this clause shall satisfy $L_1 = 4n$, $L_2 = 8n$, and L_H is equal to $2n$.

8.3 Padding method

The padding method for use with this hash-function shall be that specified in clause A.3 of ISO/IEC 10118-1:2000, such that $r = n$.

© ISO/IEC 2000 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

8.4 Initializing value

The selection of the *IV* (of length 8*n*) for use with this hash-function is beyond the scope of this part of ISO/IEC 10118. The value of the *IV* shall be agreed upon and fixed by the users of the hash-function.

8.5 Round-function

The round-function ϕ has 8 parallel encryptions, and 8 *n*-bit chaining variables $H_j^{1\text{-}8}$.

In every iteration, 4 *n*-bit data blocks, $D_j^{1\text{-}4}$ (of length $L_1 = 4n$ bits) are combined with $H_{j\text{-}1}{}^{1\text{-}8}$, the previous output of the round-function (of length $L_2 = 8n$ bits), to yield $H_j^{1\text{-}8}$ (of length $L_2 = 8n$ bits).

The round-function is based on a linear mapping γ_1, that takes as input 12 *n*-bit strings $I^{1\text{-}12}$ and maps them to 8 *n*-bit strings $X^{1\text{-}8}$ and to 8 *n*-bit strings $Y^{1\text{-}8}$. The mapping uses 8 2*n*-bit auxiliary strings R^0, R^1, M^0, M^1, ..., M^5. The mapping γ_1 is defined by the following steps:

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

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

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

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

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

$R^0 := B$; }

iii) for $i = 1$ to 8 do { $X^i := I^i$;}

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

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

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

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

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

The round-function has the following form ($1 \le j \le q$).

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

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

The round-function is illustrated in Figure 3a and the linear mapping γ_1 in Figure 3b.

© ISO/IEC 2000 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

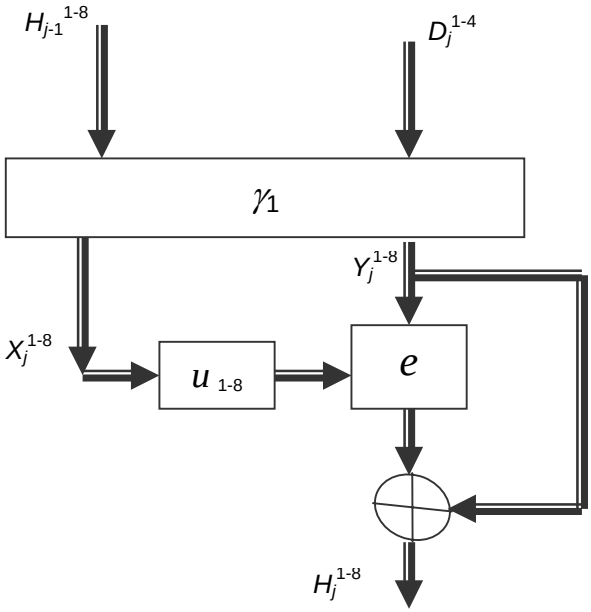

Figure 3a — Round-function of hash-function three

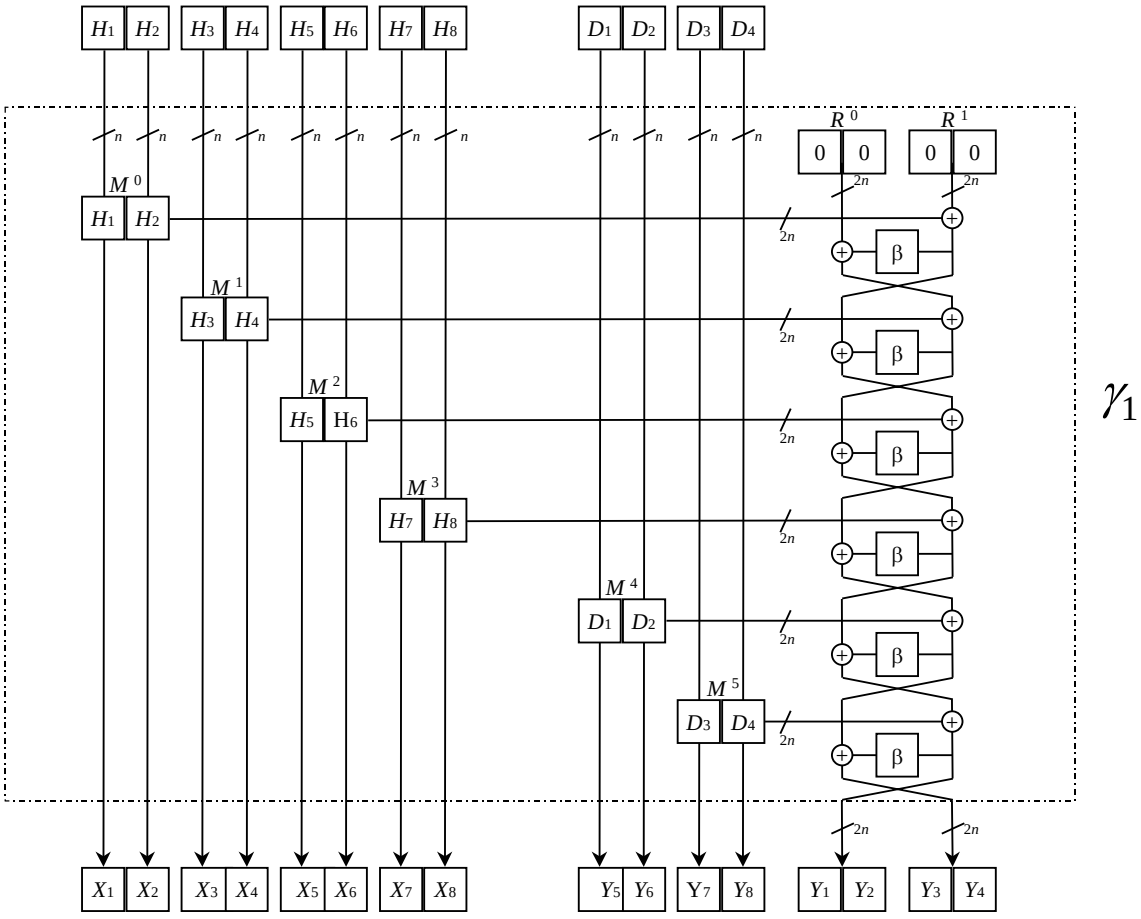

Figure 3b — Linear mapping γ_1 of hash-function three

© ISO/IEC 2000 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

8.6 Output transformation

After processing of the padded message, the chaining variables have the values $H_q^{1\text{-}8}$. Perform four additional iterations of the round-function with the data inputs

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

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

$D_{q+3}^{1\text{-}4} = H_q^{1\text{-}4}$, and

$D_{q+4}^{1\text{-}4} = H_q^{5\text{-}8}$, respectively.

The output L_H of the hash-function then consists of $H_{q+4}^{1} \,||\, H_{q+4}^{2}$. The output transformation requires 26 encryptions (in the last iteration only two encryptions need to be performed).

9 Hash-function four

The hash-function specified in this clause provides hash-codes of length L_H, where L_H is equal to $3n$ for even values of n.

9.1 General

See 8.1 for specific definitions relevant to this hash-function.

9.2 Parameter selection

The parameters L_1 and L_2 and L_H for the hash-function specified in this clause shall satisfy $L_1 = 3n$, $L_2 = 9n$, and L_H is equal to $3n$.

9.3 Padding method

The padding method for use with this hash-function shall be that specified in clause A.3 of ISO/IEC 10118-1:2000, such that $r = n$.

9.4 Initializing value

The selection of the *IV* (of length $9n$) for use with this hash-function is beyond the scope of this part of ISO/IEC 10118. The value of the *IV* shall be agreed upon and fixed by the users of the hash-function.

9.5 Round-function

The round-function ϕ has 9 parallel encryptions, and 9 n-bit chaining variables $H_j^{1\text{-}9}$.

In every iteration, 3 n-bit data blocks, $D_j^{1\text{-}3}$ (of length $L_1 = 3n$ bits) are combined with $H_{j\text{-}1}^{1\text{-}9}$, the previous output of the round-function (of length $L_2 = 9n$ bits), to yield $H_j^{1\text{-}9}$ (of length $L_2 = 9n$ bits).

The round-function is based on a linear mapping γ_2, that takes as input 12 n-bit strings $I^{1\text{-}12}$ and maps them to 9 n-bit strings $X^{1\text{-}9}$ and to 9 n-bit strings $Y^{1\text{-}9}$. The mapping uses 9 $2n$-bit auxiliary strings R^0, R^1, R^2,M^0, M^1, …, M^5. The mapping γ_2 is defined by the following steps:

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

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

© ISO/IEC 2000 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ii) for i = 0 to 5 do {

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

$U := \beta(B)$;

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

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

$R^0 := B$; }

iii) for i = 1 to 9 do { $X^i := I^i$;}

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

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

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

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

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

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

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

The round-function has the following form ($1 \le j \le q$).

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

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

The round-function is illustrated in Figure 4a and the linear mapping γ_2 in Figure 4b.

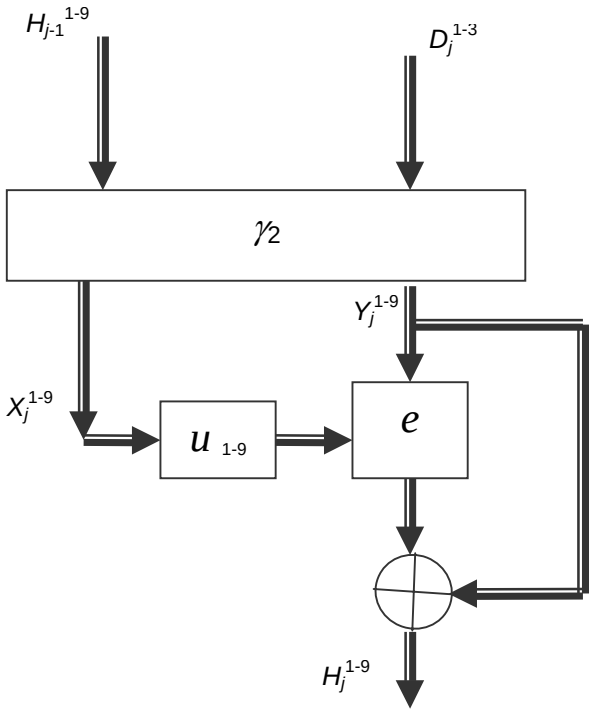

Figure 4a — Round-function of hash-function four

© ISO/IEC 2000 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

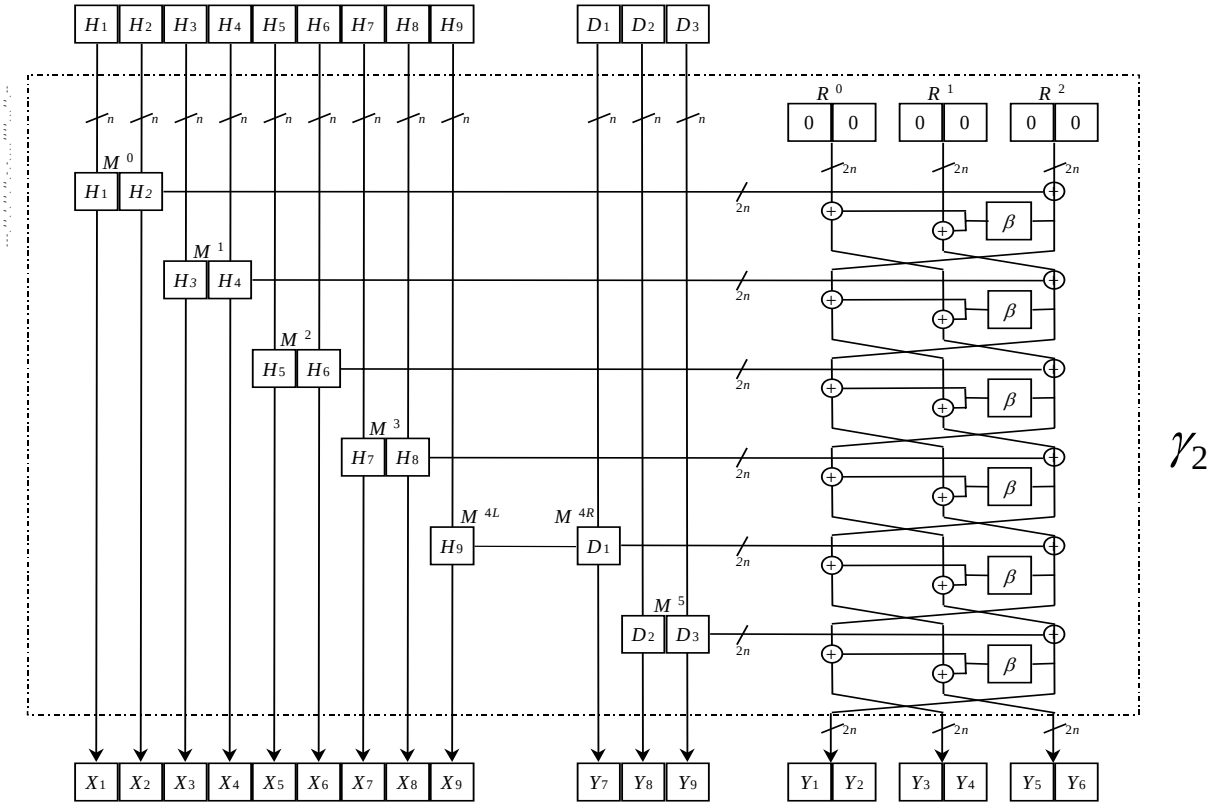

Figure 4b — Linear mapping γ_2 of hash-function four

9.6 Output transformation

After processing of the padded message, the chaining variables have the values $H_q^{1\text{-}9}$. Perform four additional iterations of the round-function with the message inputs

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

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

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

$D_{q+4}^{1\text{-}3} = H_q^{1\text{-}3}$ respectively.

The output of the hash-function then consists of $H_{q+4}^{1} || H_{q+4}^{2} || H_{q+4}^{3}$ The output transformation requires 30 encryptions (in the last iteration only three encryptions need to be performed).

© ISO/IEC 2000 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex A
(informative)

Use of DEA

A.1 General

This annex presents a way of using the DEA (ANSI X3.92) in conjunction with the hashing operations specified in this part of ISO/IEC 10118. The DEA is also known under the name DES.

The numbering of the bits is as in ANSI X3.92 [2].

These methods have been described in [3]. The parameters for DEA are $n = 64$ and $L_K = 64$.

A.2 Hash-function one

See clause 6.

IV should be equal to '5252525252525252' (in hexadecimal notation).

The transformation *u* should be chosen as follows. Let $X = x_1x_2\ldots x_{64}$ be the binary decomposition of a 64-bit string *X*. Then $Y = u(X)$ is the string obtained after forcing the bits x_2 and x_3 to the values '10', and replacing the bits x_8, x_{16}, x_{24}, x_{32}, x_{40}, x_{48}, x_{56}, x_{64} with x_8', x_{16}', x_{24}', x_{32}', x_{40}', x_{48}', x_{56}', x_{64}' respectively, where x_{8i}' represents the parity bit for the preceding 7 bits of *X*, namely, x_{8i-7}, x_{8i-6}, x_{8i-5}, x_{8i-4}, x_{8i-3}, x_{8i-2}, x_{8i-1}. The result is: $Y = x_1'\ 10\ x_4\ x_5\ x_6\ x_7\ x_8'\ x_9\ x_{10}\ldots\ x_{63}\ x_{64}'$. The justification for fixing bits 2 and 3 of *X* is described in [7] with respect to the IBM MDC-2 algorithm; however, the same justification applies to this hash-function.

NOTE It is believed that finding collisions for the round-function and for the hash-function requires 2^{27} DES encryptions.

A.3 Hash-function two

See clause 7.

IV^L should be equal to '5252525252525252' (in hexadecimal notation).

IV^R should be equal to '2525252525252525' (in hexadecimal notation).

The transformation *u* should be the same as in clause A.2. The transformation *u'* should be chosen as follows. Let $X = x_1x_2\ldots x_{64}$ be the binary decomposition of a 64-bit string *X*. Then $Y = u'(X)$ is the string obtained after forcing the bits x_2 and x_3 to the values '01', and replacing the bits x_8, x_{16}, x_{24}, x_{32}, x_{40}, x_{48}, x_{56}, x_{64} with x_8', x_{16}', x_{24}', x_{32}', x_{40}', x_{48}', x_{56}', x_{64}' respectively, where x_{8i}' represents the parity bit for the preceding 7 bits of *X*, namely, x_{8i-7}, x_{8i-6}, x_{8i-5}, x_{8i-4}, x_{8i-3}, x_{8i-2}, x_{8i-1}. The result is: $Y = x_1'\ 01\ x_4\ x_5\ x_6\ x_7\ x_8'\ x_9\ x_{10}\ldots\ x_{63}\ x_{64}'$. The justification for fixing bits 2 and 3 of *X* is described in [7] with respect to the IBM MDC-2 algorithm; however, the same justification applies to this hash-function.

NOTE It is believed that finding collisions for the round-function and for the hash-function requires 2^{55} DES encryptions.

A.4 Hash-function three

See clause 8.

© ISO/IEC 2000 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

IV^1, IV^2, ... IV^8 shall be equal to `5252525252525252' (in hexadecimal notation).

The transformations u_1, u_2, ..., u_8 shall be chosen as follows. Let $X = x_1\ x_2\ ...\ x_{64}$ be the binary decomposition of the 64-bit string X. Then $Y = u_i(X)$ is the string obtained after forcing the bits x_1, x_2, ... x_5 to the values given in Table A.1, and replacing the bits x_8, x_{16}, x_{24}, x_{32}, x_{40}, x_{48}, x_{56}, x_{64} with x_8', x_{16}', x_{24}', x_{32}', x_{40}', x_{48}', x_{56}', x_{64}' respectively, where x_{8i}' represents the parity bit for the preceding 7 bits of X, namely, x_{8i-7}, x_{8i-6}, x_{8i-5}, x_{8i-4}, x_{8i-3}, x_{8i-2}, x_{8i-1}.

Table A.1 — Hash-function three: Values of key bits No. 1, 2, 3, 4 and 5 in the eight subfunctions

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

NOTE It is believed that finding collisions for the round-function and for the hash-function requires 2^{51} DES encryptions.

A.5 Hash-function four

See clause 9.

IV^1, IV^2, ... IV^9 shall be equal to `5252525252525252' (in hexadecimal notation).

The transformations u_1, u_2, ..., u_9 shall be chosen as follows. Let $X = x_1\ x_2\ ...\ x_{64}$ be the binary decomposition of the 64-bit string X. Then $Y = u_i(X)$ is the string obtained after forcing the bits x_1, x_2, ... x_5 to the values given in Table A.2, and replacing the bits x_8, x_{16}, x_{24}, x_{32}, x_{40}, x_{48}, x_{56}, x_{64} with x_8', x_{16}', x_{24}', x_{32}', x_{40}', x_{48}', x_{56}', x_{64}' respectively, where x_{8i}' represents the parity bit for the preceding 7 bits of X, namely, x_{8i-7}, x_{8i-6}, x_{8i-5}, x_{8i-4}, x_{8i-3}, x_{8i-2}, x_{8i-1}.

Table A.2 — Hash-function four: Values of key bits No. 1, 2, 3, 4 and 5 in the nine subfunctions

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

NOTE It is believed that finding collisions for the round-function and for the hash-function requires 2^{76} DES encryptions.

© ISO/IEC 2000 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.6 Motivation

The DEA has some properties that are known to be undesirable, if the algorithm is used in hashing constructions. First of all, there are 4 weak keys, where the encryption function equals the decryption function. In addition, for these 4 weak keys there are 2^{32} fixed points, that is, values of plaintext which encrypt to themselves. Second, there are 16 pairs of semi-weak keys, for which the encryption function induced by one key equals the decryption function of the other key. DES also has the complementation property: if both plaintext and key are complemented, the ciphertext will be complemented as well.

For hash-function one and two, fixing 2 bits of the key as indicated above is a necessary and sufficient condition to avoid weak and semi-weak keys. Hash-function one needs one fixed value and hash-function two needs two fixed values. These values must have the following properties:

— All values must be different.

— None of the values must enable the use of a weak nor a semi-weak key.

For hash-function three and four, fixing 5 bits of the key as indicated above is a necessary and sufficient condition to avoid weak keys, semi-weak keys, and the complementation property.

Hash-function three requires 8 fixed values and hash-function four requires 9 fixed values. These values must have the following properties:

— All values must be different.

— None of the values must enable the use of a weak nor a semi-weak key.

— None of the values is the complemented value of another value.

The fact that the above conditions are met can be derived from the following observation. Consider the 5 key bits in positions 1, 2, 3, 4 and 5. For all weak and semi-weak keys of DEA, these 5 bits take one of the following values: 00000, 11111, 00011, or 11100.

© ISO/IEC 2000 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex B
(informative)

Examples

B.1 General

This annex gives examples for the computation of a hash-code using the first two hash-functions specified in annex A of this part of ISO/IEC 10118 and the padding methods specified in annex A of ISO/IEC 10118-1:2000.

The data string is the 7-bit ASCII code as described in [8] (no parity) for “Now_is_the_time_for_all_”, where ”_” denotes a blank, in hexadecimal notation:

‘4E6F77206973207468652074696D6520666F7220616C6C20’

B.2 Hash-function one

See A.2.

Padding method 1

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

Padding method 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

B.3 Hash-function two

See A.3.

Padding method 1

j	D_j	H_{j-1}^{L}	H_{j-1}^{R}
1	4E6F77206973274	5252525252525252	2525252525252525
2	68652074696D6520	858A260FFD4873A8	49771DD37391482D
3	666F7220616C620	B002740352F7CF4F	CFE8087E1B93CCB2

© ISO/IEC 2000 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

Padding method 2

j	D_j	H_{j-1}^L	H_{j-1}^R
1	4E6F772069732074	5252525252525252	2525252525252525
2	68652074696D6520	858A260FFD4873A8	49771DD37391482D
3	666F7220616C6C20	B002740352F7CF4F	CFE8087E1B93CCB2
4	80000000000000000	42E50CD224BACEBA	760BDD2BD409281A

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

B.4 Hash-function three

See A.4.

Padding method 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

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2000 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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
	fc1ab80fce4920f3	4561afdfc9279fa2
	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

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale
© ISO/IEC 2000 – All rights reserved

B.5 Hash-function four

See A.5.

Padding method 3

M_1^{1-3}	H_0^{1-9}	H_1^{1-9}
4e6f772069732074	5252525252525250	4c94cc79cae77819
68652074696d6520	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	bd58a6176226bcc90
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

© ISO/IEC 2000 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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
	452fcbff98fe864b7	253b8ff11830261

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2000 – All rights reserved
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Bibliography

[1] ISO/IEC 9979:1999, *Information technology — Security techniques — Procedures for the registration of cryptographic algorithms.*

[2] ANSI X3.92:1981, *Data Encryption Algorithm.*

[3] S.M. MATYAS. Key Processing with Control Vectors. *J. of Cryptology,* Vol. 2, 1991, pp. 113-136.

[4] L.R. KNUDSEN, B. PRENEEL. 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. 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, *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. *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] ISO 646:1991, *Information technology — ISO 7-bit coded character set for information interchange.*

© ISO/IEC 2000 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ICS 35.040

Price based on 19 pages

© ISO/IEC 2000 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale