INTERNATIONAL STANDARD

ISO/IEC 10118-3

Third edition
2004-03-01

AMENDMENT 1
2006-02-15

Information technology — Security techniques — Hash-functions —

Part 3: Dedicated hash-functions

AMENDMENT 1: Dedicated Hash-Function 8 (SHA-224)

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

Partie 3: Fonctions de brouillage dédiées

AMENDEMENT 1: Fonction de brouillage dédiée 8 (SHA-224)

Reference number
ISO/IEC 10118-3:2004/Amd.1:2006(E)

© ISO/IEC 2006

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 2006

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.org
Web www.iso.org

Published 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 2006 – All rights reserved

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. 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.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Amendment 1 to ISO/IEC 10118-3:2004 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Amendment 1 to ISO/IEC 10118-3:2004 was written to serve two purposes.

First, with the inclusion of Dedicated Hash-Function 8 (SHA-224), ISO/IEC 10118-3:2004 now includes the complete family of SHA hash-functions. The description of SHA-224 is given in Clause 14. Test vectors for SHA-224 are given in A.8.

Second, it was noted that there were implementations of SHA-384 and SHA-512 in the field which correctly reproduced the test vector examples in ISO/IEC 10118-3:2004, yet still failed for inputs containing bytes that were not standard ASCII codes. In order to perform comprehensive testing of the SHA-224, SHA-256, SHA-384 and SHA-512 hash-functions, an extended set of test vectors is included for ISO/IEC 10118-3:2004 as a part of this amendment. This additional test vector information is given in A.9.

--`,,```,,,,````-`-`,,`,,`,`,,`---
© ISO/IEC 2006 – 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 3: Dedicated hash-functions

AMENDMENT 1: Dedicated Hash-Function 8 (SHA-224)

Page 22

Add the following after Figure 6.

14 Dedicated Hash-Function 8 (SHA-224)

In this clause we specify a padding method, an initialising value, and a round-function for use in the general model for hash-functions described in ISO/IEC 10118-1:2000. The padding method, initialising value and round-function specified here, when used in the above general model, together define Dedicated Hash-Function 8. This dedicated hash-function can be applied to all data strings D containing at most 2^{64}-1 bits.

The ISO/IEC hash-function identifier for Dedicated Hash-Function 8 is equal to 38 (hexadecimal).

NOTE Dedicated Hash-Function 8 defined in this clause is commonly called SHA-224, [2].

14.1 Parameters, functions and constants

14.1.1 Parameters

For this hash-function $L_1 = 512$, $L_2 = 256$ and $L_H = 224$.

14.1.2 Byte ordering convention

The byte ordering convention for this hash-function is the same as that for the hash-function of clause 10.

14.1.3 Functions

The functions for this hash-function are the same as those for the hash-function of clause 10.

14.1.4 Constants

The constants for this hash-function are the same as those for the hash-function of clause 10.

© ISO/IEC 2006 – 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

14.1.5 Initialising value

For this round-function the initialising value, *IV*, shall always be the following 256-bit string, represented here as a sequence of eight words Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6, Y_7 in a hexadecimal representation, where Y_0 represents the left-most 32 of the 256 bits:

Y_0 = c1059ed8
Y_1 = 367cd507
Y_2 = 3070dd17
Y_3 = f70e5939
Y_4 = ffc00b31
Y_5 = 68581511
Y_6 = 64f98fa7
Y_7 = befa4fa4

NOTE These values are the low order 32-bits of the values specified in 12.1.5.

14.2 Padding method

The padding method to be used with this hash-function shall be the same as the padding method defined in 10.2.

14.3 Description of the round-function

The round-function to be used with this hash-function shall be the same as the round-function defined in 10.3.

The final 224-bit hash is obtained by truncating the SHA-256-based hash output to its left-most 224 bits.

Page 23, Annex A

In the first line, replace “Dedicated Hash-Functions 1-7” by “Dedicated Hash-Functions 1-8”.

Page 77

Add the following after A.7.9.

A.8 Dedicated Hash-Function 8

A.8.1 Example 1

In this example the data-string is the empty string, i.e., the string of length zero.

The hash-code is the following 224-bit string.

d14a028c 2a3a2bc9 476102bb 288234c4 15a2b01f 828ea62a c5b3e42f

© ISO/IEC 2006 – 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.8.2 Example 2

In this example the data-string consists of a single byte, namely the ASCII-coded version of the letter 'a'.

The hash-code is the following 224-bit string.

```
abd37534 c7d9a2ef b9465de9 31cd7055 ffdb8879 563ae980 78d6d6d5
```

A.8.3 Example 3

In this example the data-string is the three-byte string consisting of the ASCII-coded version of 'abc'. This is equivalent to the bit-string: '01100001 01100010 01100011'.

After the padding process, the single 16-word block derived from the data-string is as follows.

```
61626380 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000018
```

The following are (hexadecimal representations of) the successive values of the variables Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6, Y_7.

```
init: c1059ed8 367cd507 3070dd17 f70e5939 ffc00b31 68581511 64f98fa7 befa4fa4
    0 0e96b2da c1059ed8 367cd507 3070dd17 0434225e ffc00b31 68581511 64f98fa7
    1 c20dab6b 0e96b2da c1059ed8 367cd507 9cab416f 0434225e ffc00b31 68581511
    2 ab113b7a c20dab6b 0e96b2da c1059ed8 82177fe8 9cab416f 0434225e ffc00b31
    3 8253cc1a ab113b7a c20dab6b 0e96b2da 8346b27d 82177fe8 9cab416f 0434225e
    4 08a0dc0c 8253cc1a ab113b7a c20dab6b 05b557db 8346b27d 82177fe8 9cab416f
    5 b2ca3a91 08a0dc0c 8253cc1a ab113b7a 898dc7bb 05b557db 8346b27d 82177fe8
    6 0b6b9023 b2ca3a91 08a0dc0c 8253cc1a a2e49147 898dc7bb 05b557db 8346b27d
    7 f09d116d 0b6b9023 b2ca3a91 08a0dc0c 7a84120d a2e49147 898dc7bb 05b557db
    8 ed6fa633 f09d116d 0b6b9023 b2ca3a91 c037faad 7a84120d a2e49147 898dc7bb
    9 55e6a367 ed6fa633 f09d116d 0b6b9023 aae50091 c037faad 7a84120d a2e49147
   10 0817e82b 55e6a367 ed6fa633 f09d116d c8c53a2c aae50091 c037faad 7a84120d
   11 17142334 0817e82b 55e6a367 ed6fa633 dd4c7be9 c8c53a2c aae50091 c037faad
   12 fc4f023e 17142334 0817e82b 55e6a367 87bea51a dd4c7be9 c8c53a2c aae50091
   13 be316902 fc4f023e 17142334 0817e82b 65141125 87bea51a dd4c7be9 c8c53a2c
   14 1d80d178 be316902 fc4f023e 17142334 4545f53a 65141125 87bea51a dd4c7be9
   15 9f341a45 1d80d178 be316902 fc4f023e 6a61c411 4545f53a 65141125 87bea51a
   16 0f324db9 9f341a45 1d80d178 be316902 06c80d6a 6a61c411 4545f53a 65141125
   17 ffe7012b 0f324db9 9f341a45 1d80d178 b7b601f4 06c80d6a 6a61c411 4545f53a
   18 62932ab8 ffe7012b 0f324db9 9f341a45 763b627a b7b601f4 06c80d6a 6a61c411
   19 5207d867 62932ab8 ffe7012b 0f324db9 7fbba936 763b627a b7b601f4 06c80d6a
   20 07d55ccb 5207d867 62932ab8 ffe7012b 9ba5a6ea 7fbba936 763b627a b7b601f4
   21 dece98a4 07d55ccb 5207d867 62932ab8 293ffb5d 9ba5a6ea 7fbba936 763b627a
   22 e62a812e dece98a4 07d55ccb 5207d867 28fe0fd9 293ffb5d 9ba5a6ea 7fbba936
   23 57206fb8 e62a812e dece98a4 07d55ccb c76084ea 28fe0fd9 293ffb5d 9ba5a6ea
   24 6a6abcf0 57206fb8 e62a812e dece98a4 b2614c5e c76084ea 28fe0fd9 293ffb5d
   25 937514f0 6a6abcf0 57206fb8 e62a812e b42ec21c b2614c5e c76084ea 28fe0fd9
   26 82af3ffb 937514f0 6a6abcf0 57206fb8 be6f6760 b42ec21c b2614c5e c76084ea
   27 eca3bcd5 82af3ffb 937514f0 6a6abcf0 1dccbb10 be6f6760 b42ec21c b2614c5e
   28 2d1576c4 eca3bcd5 82af3ffb 937514f0 01641929 1dccbb10 be6f6760 b42ec21c
   29 fe3c8658 2d1576c4 eca3bcd5 82af3ffb fc4b36c5 01641929 1dccbb10 be6f6760
   30 0d7cce07 fe3c8658 2d1576c4 eca3bcd5 a4a4a3a4 fc4b36c5 01641929 1dccbb10
   31 cce1951d 0d7cce07 fe3c8658 2d1576c4 4be9475c a4a4a3a4 fc4b36c5 01641929
   32 09b76257 cce1951d 0d7cce07 fe3c8658 0ccddd86 4be9475c a4a4a3a4 fc4b36c5
   33 f827767e 09b76257 cce1951d 0d7cce07 db116db7 0ccddd86 4be9475c a4a4a3a4
   34 e4a0bb48 f827767e 09b76257 cce1951d 994e2bac db116db7 0ccddd86 4be9475c
   35 d8bb1041 e4a0bb48 f827767e 09b76257 5b730abb 994e2bac db116db7 0ccddd86
```

© ISO/IEC 2006 – 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

```
36 2a2e32f4 d8bb1041 e4a0bb48 f827767e 22e15c59 5b730abb 994e2bac db116db7
37 0d275ca8 2a2e32f4 d8bb1041 e4a0bb48 f6c39382 22e15c59 5b730abb 994e2bac
38 7902369c 0d275ca8 2a2e32f4 d8bb1041 d9f8c2e0 f6c39382 22e15c59 5b730abb
39 f3c80288 7902369c 0d275ca8 2a2e32f4 00e3a7bb d9f8c2e0 f6c39382 22e15c59
40 483bba4d f3c80288 7902369c 0d275ca8 f0a8198c 00e3a7bb d9f8c2e0 f6c39382
41 d75d4d26 483bba4d f3c80288 7902369c fcecdcd4 f0a8198c 00e3a7bb d9f8c2e0
42 0744b618 d75d4d26 483bba4d f3c80288 03186faa fcecdcd4 f0a8198c 00e3a7bb
43 9cce9f01 0744b618 d75d4d26 483bba4d a56f6bbf 03186faa fcecdcd4 f0a8198c
44 a3701bd9 9cce9f01 0744b618 d75d4d26 af1bef5f a56f6bbf 03186faa fcecdcd4
45 131d4c09 a3701bd9 9cce9f01 0744b618 ecb77e1b af1bef5f a56f6bbf 03186faa
46 fb3777d9 131d4c09 a3701bd9 9cce9f01 1d601f44 ecb77e1b af1bef5f a56f6bbf
47 847ea00e fb3777d9 131d4c09 a3701bd9 503a7b95 1d601f44 ecb77e1b af1bef5f
48 aaa69347 847ea00e fb3777d9 131d4c09 5eeb9930 503a7b95 1d601f44 ecb77e1b
49 505caf28 aaa69347 847ea00e fb3777d9 ce695893 5eeb9930 503a7b95 1d601f44
50 675e0b02 505caf28 aaa69347 847ea00e c22dd75f ce695893 5eeb9930 503a7b95
51 abd26099 675e0b02 505caf28 aaa69347 1409c3f8 c22dd75f ce695893 5eeb9930
52 0df9857a abd26099 675e0b02 505caf28 2d864d9f 1409c3f8 c22dd75f ce695893
53 308b8799 0df9857a abd26099 675e0b02 02524f02 2d864d9f 1409c3f8 c22dd75f
54 909cc059 308b8799 0df9857a abd26099 6f2a444a 02524f02 2d864d9f 1409c3f8
55 8d25bd94 909cc059 308b8799 0df9857a 1273c622 6f2a444a 02524f02 2d864d9f
56 f32141da 8d25bd94 909cc059 308b8799 1771ed3f 1273c622 6f2a444a 02524f02
57 8ce24395 f32141da 8d25bd94 909cc059 f52f66a6 1771ed3f 1273c622 6f2a444a
58 07bcd846 8ce24395 f32141da 8d25bd94 149db547 f52f66a6 1771ed3f 1273c622
59 622d5e5b 07bcd846 8ce24395 f32141da b6f4c630 149db547 f52f66a6 1771ed3f
60 c693fc7a 622d5e5b 07bcd846 8ce24395 13dfb889 b6f4c630 149db547 f52f66a6
61 55d1c760 c693fc7a 622d5e5b 07bcd846 7e730e00 13dfb889 b6f4c630 149db547
62 fd89031b 55d1c760 c693fc7a 622d5e5b 55489ee6 7e730e00 13dfb889 b6f4c630
63 6203de4a fd89031b 55d1c760 c693fc7a 2aedb1b3 55489ee6 7e730e00 13dfb889
```

The following eight words Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6, Y_7 represent the output of the final iteration of the round-function.

$$Y_0 = c1059ed8 \boxplus 6203de4a = 23097d22$$
$$Y_1 = 367cd507 \boxplus fd89031b = 3405d822$$
$$Y_2 = 3070dd17 \boxplus 55d1c760 = 8642a477$$
$$Y_3 = f70e5939 \boxplus c693fc7a = bda255b3$$
$$Y_4 = ffc00b31 \boxplus 2aedb1b3 = 2aadbce4$$
$$Y_5 = 68581511 \boxplus 55489ee6 = bda0b3f7$$
$$Y_6 = 64f98fa7 \boxplus 7e730e00 = e36c9da7$$
$$Y_7 = befa4fa4 \boxplus 13dfb889 = ad25f72d$$

The hash value is the following 224-bit string.

```
23097d22 3405d822 8642a477 bda255b3 2aadbce4 bda0b3f7 e36c9da7
```


Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
© ISO/IEC 2006 – All rights reserved
Not for Resale

A.8.4 Example 4

In this example the data-string is the 14-byte string consisting of the ASCII-coded version of

‘message digest’

The hash-code is the following 224-bit string.

```
2cb21c83 ae2f004d e7e81c3c 7019cbcb 65b71ab6 56b22d6d 0c39b8eb
```

A.8.5 Example 5

In this example the data-string is the 62-byte string consisting of the ASCII-coded version of

‘ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789’

The hash-code is the following 224-bit string.

```
bff72b4f cb7d75e5 632900ac 5f90d219 e05e97a7 bde72e74 0db393d9
```

A.8.6 Example 6

In this example the data-string is the 80-byte string consisting of the ASCII-coded version of eight repetitions of

‘1234567890’

The hash-code is the following 224-bit string.

```
b50aecbe 4e9bb0b5 7bc5f3ae 760a8e01 db24f203 fb3cdcd1 3148046e
```

A.8.7 Example 7

In this example the data-string is the 56-byte string consisting of the ASCII-coded version of

‘abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq’

After the padding process, the following two 16-word blocks are derived from the data-string.

```
61626364 62636465 63646566 64656667 65666768 66676869 6768696a 68696a6b
696a6b6c 6a6b6c6d 6b6c6d6e 6c6d6e6f 6d6e6f70 6e6f7071 80000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 000001c0
```

The following are (hexadecimal representations of) the successive values of the variables Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6, Y_7 in the first block process.

```
init:  c1059ed8 367cd507 3070dd17 f70e5939 ffc00b31 68581511 64f98fa7 befa4fa4
     0  0e96b2be c1059ed8 367cd507 3070dd17 04342242 ffc00b31 68581511 64f98fa7
     1  51d17d7b 0e96b2be c1059ed8 367cd507 2f8ea3d4 04342242 ffc00b31 68581511
     2  ff1cbd7f 51d17d7b 0e96b2be c1059ed8 79a896fa 2f8ea3d4 04342242 ffc00b31
     3  24bcc047 ff1cbd7f 51d17d7b 0e96b2be 1f60795a 79a896fa 2f8ea3d4 04342242
     4  7d56a6ac 24bcc047 ff1cbd7f 51d17d7b de395286 1f60795a 79a896fa 2f8ea3d4
     5  745beb11 7d56a6ac 24bcc047 ff1cbd7f d863d132 de395286 1f60795a 79a896fa
     6  0dd41573 745beb11 7d56a6ac 24bcc047 2e60d323 d863d132 de395286 1f60795a
     7  9a2541fd 0dd41573 745beb11 7d56a6ac 08d2b348 2e60d323 d863d132 de395286
```

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

© ISO/IEC 2006 – 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	3140e909	9a2541fd	0dd41573	745beb11	95dfd707	08d2b348	2e60d323	d863d132
9	b2954925	3140e909	9a2541fd	0dd41573	05ef5e3d	95dfd707	08d2b348	2e60d323
10	b2a874fb	b2954925	3140e909	9a2541fd	9dcaf118	05ef5e3d	95dfd707	08d2b348
11	116ce44d	b2a874fb	b2954925	3140e909	0e6d566a	9dcaf118	05ef5e3d	95dfd707
12	5ff9349a	116ce44d	b2a874fb	b2954925	08eb3305	0e6d566a	9dcaf118	05ef5e3d
13	7fa9d65d	5ff9349a	116ce44d	b2a874fb	4657cf17	08eb3305	0e6d566a	9dcaf118
14	006b1b16	7fa9d65d	5ff9349a	116ce44d	08d09e8d	4657cf17	08eb3305	0e6d566a
15	b301c98a	006b1b16	7fa9d65d	5ff9349a	6fbefa1d	08d09e8d	4657cf17	08eb3305
16	e623ecc0	b301c98a	006b1b16	7fa9d65d	2b3f859c	6fbefa1d	08d09e8d	4657cf17
17	d9244a78	e623ecc0	b301c98a	006b1b16	e66d8d9c	2b3f859c	6fbefa1d	08d09e8d
18	99c72726	d9244a78	e623ecc0	b301c98a	b26a409c	e66d8d9c	2b3f859c	6fbefa1d
19	ab0cbed2	99c72726	d9244a78	e623ecc0	010d7c65	b26a409c	e66d8d9c	2b3f859c
20	78062878	ab0cbed2	99c72726	d9244a78	5678a949	010d7c65	b26a409c	e66d8d9c
21	d7c5c5d5	78062878	ab0cbed2	99c72726	b280360c	5678a949	010d7c65	b26a409c
22	bad2ee72	d7c5c5d5	78062878	ab0cbed2	0d4cd0c4	b280360c	5678a949	010d7c65
23	bcf47346	bad2ee72	d7c5c5d5	78062878	d6a19dc8	0d4cd0c4	b280360c	5678a949
24	5ecc417b	bcf47346	bad2ee72	d7c5c5d5	3337a11c	d6a19dc8	0d4cd0c4	b280360c
25	e15bfa57	5ecc417b	bcf47346	bad2ee72	0ce15173	3337a11c	d6a19dc8	0d4cd0c4
26	fae6167b	e15bfa57	5ecc417b	bcf47346	73dbe5c7	0ce15173	3337a11c	d6a19dc8
27	991c3f99	fae6167b	e15bfa57	5ecc417b	8602a31f	73dbe5c7	0ce15173	3337a11c
28	7055843b	991c3f99	fae6167b	e15bfa57	eb4de5f8	8602a31f	73dbe5c7	0ce15173
29	08dcfb6d	7055843b	991c3f99	fae6167b	4606d126	eb4de5f8	8602a31f	73dbe5c7
30	2964b340	08dcfb6d	7055843b	991c3f99	213b3e63	4606d126	eb4de5f8	8602a31f
31	5b3677d0	2964b340	08dcfb6d	7055843b	c9689cb0	213b3e63	4606d126	eb4de5f8
32	1ee0fe7d	5b3677d0	2964b340	08dcfb6d	14318a4d	c9689cb0	213b3e63	4606d126
33	6b918d6e	1ee0fe7d	5b3677d0	2964b340	216054a8	14318a4d	c9689cb0	213b3e63
34	a6710d0d	6b918d6e	1ee0fe7d	5b3677d0	bc823a58	216054a8	14318a4d	c9689cb0
35	5e198fed	a6710d0d	6b918d6e	1ee0fe7d	c49933fe	bc823a58	216054a8	14318a4d
36	136c320a	5e198fed	a6710d0d	6b918d6e	75687ccb	c49933fe	bc823a58	216054a8
37	40ee0c43	136c320a	5e198fed	a6710d0d	f1c2caf6	75687ccb	c49933fe	bc823a58
38	aa96d78c	40ee0c43	136c320a	5e198fed	f48b4ceb	f1c2caf6	75687ccb	c49933fe
39	27c97b86	aa96d78c	40ee0c43	136c320a	b556216a	f48b4ceb	f1c2caf6	75687ccb
40	b07bd327	27c97b86	aa96d78c	40ee0c43	30ec2d76	b556216a	f48b4ceb	f1c2caf6
41	d88d56bd	b07bd327	27c97b86	aa96d78c	dc2fa5a4	30ec2d76	b556216a	f48b4ceb
42	5c775077	d88d56bd	b07bd327	27c97b86	5fad6db5	dc2fa5a4	30ec2d76	b556216a
43	1526cca3	5c775077	d88d56bd	b07bd327	da8a0b1c	5fad6db5	dc2fa5a4	30ec2d76
44	c09dda14	1526cca3	5c775077	d88d56bd	d98ec23a	da8a0b1c	5fad6db5	dc2fa5a4
45	f885e124	c09dda14	1526cca3	5c775077	e4f23e41	d98ec23a	da8a0b1c	5fad6db5
46	5447f0ad	f885e124	c09dda14	1526cca3	bfb7497c	e4f23e41	d98ec23a	da8a0b1c
47	e6227061	5447f0ad	f885e124	c09dda14	5b09619b	bfb7497c	e4f23e41	d98ec23a
48	009cebea	e6227061	5447f0ad	f885e124	59ecab46	5b09619b	bfb7497c	e4f23e41
49	92b0d169	009cebea	e6227061	5447f0ad	9a572b85	59ecab46	5b09619b	bfb7497c
50	8d224e54	92b0d169	009cebea	e6227061	32144602	9a572b85	59ecab46	5b09619b
51	c1fcac71	8d224e54	92b0d169	009cebea	4e98a8b7	32144602	9a572b85	59ecab46
52	8e6ce843	c1fcac71	8d224e54	92b0d169	2c1823be	4e98a8b7	32144602	9a572b85
53	000f54de	8e6ce843	c1fcac71	8d224e54	f32cf2a8	2c1823be	4e98a8b7	32144602
54	2fe2af3a	000f54de	8e6ce843	c1fcac71	20f763ee	f32cf2a8	2c1823be	4e98a8b7
55	1fd539af	2fe2af3a	000f54de	8e6ce843	5acdbd62	20f763ee	f32cf2a8	2c1823be
56	7f86644e	1fd539af	2fe2af3a	000f54de	9fc10216	5acdbd62	20f763ee	f32cf2a8
57	0e08dc77	7f86644e	1fd539af	2fe2af3a	2a4ea749	9fc10216	5acdbd62	20f763ee
58	0b9f4851	0e08dc77	7f86644e	1fd539af	18b1dfb9	2a4ea749	9fc10216	5acdbd62
59	dbce97c3	0b9f4851	0e08dc77	7f86644e	6ec6ba5b	18b1dfb9	2a4ea749	9fc10216
60	3cd78fe1	dbce97c3	0b9f4851	0e08dc77	3e1ca2f1	6ec6ba5b	18b1dfb9	2a4ea749
61	35f4bf1c	3cd78fe1	dbce97c3	0b9f4851	ba1a8a1b	3e1ca2f1	6ec6ba5b	18b1dfb9
62	86795a7d	35f4bf1c	3cd78fe1	dbce97c3	2ce11258	ba1a8a1b	3e1ca2f1	6ec6ba5b
63	c14b4785	86795a7d	35f4bf1c	3cd78fe1	1108ac7f	2ce11258	ba1a8a1b	3e1ca2f1

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

© ISO/IEC 2006 – 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 following eight words Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6, Y_7 represent the output of the round-function in the first block process.

$$Y_0 = c1059ed8 \boxplus c14b4785 = 8250e65d$$
$$Y_1 = 367cd507 \boxplus 86795a7d = bcf62f84$$
$$Y_2 = 3070dd17 \boxplus 35f4bf1c = 66659c33$$
$$Y_3 = f70e5939 \boxplus 3cd78fe1 = 33e5e91a$$
$$Y_4 = ffc00b31 \boxplus 1108ac7f = 10c8b7b0$$
$$Y_5 = 68581511 \boxplus 2ce11258 = 95392769$$
$$Y_6 = 64f98fa7 \boxplus ba1a8a1b = 1f1419c2$$
$$Y_7 = befa4fa4 \boxplus 3e1ca2f1 = fd16f295$$

The following are (hexadecimal representations of) the successive values of the variables Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6, Y_7 in the second block process.

```
 init: 8250e65d bcf62f84 66659c33 33e5e91a 10c8b7b0 95392769 1f1419c2 fd16f295
     0 692e407d 8250e65d bcf62f84 66659c33 e4be1e69 10c8b7b0 95392769 1f1419c2
     1 608d83e1 692e407d 8250e65d bcf62f84 3ddb8cee e4be1e69 10c8b7b0 95392769
     2 09bfa89f 608d83e1 692e407d 8250e65d f5813490 3ddb8cee e4be1e69 10c8b7b0
     3 2375fbc5 09bfa89f 608d83e1 692e407d c3e18529 f5813490 3ddb8cee e4be1e69
     4 717e79e7 2375fbc5 09bfa89f 608d83e1 77d39ccc c3e18529 f5813490 3ddb8cee
     5 a9319748 717e79e7 2375fbc5 09bfa89f fdbb9913 77d39ccc c3e18529 f5813490
     6 27a42f04 a9319748 717e79e7 2375fbc5 b999cce4 fdbb9913 77d39ccc c3e18529
     7 3419081e 27a42f04 a9319748 717e79e7 54e69e21 b999cce4 fdbb9913 77d39ccc
     8 0ab393c2 3419081e 27a42f04 a9319748 ad29647e 54e69e21 b999cce4 fdbb9913
     9 006784eb 0ab393c2 3419081e 27a42f04 aff457e7 ad29647e 54e69e21 b999cce4
    10 ecd5c9db 006784eb 0ab393c2 3419081e 9af42a0e aff457e7 ad29647e 54e69e21
    11 4762e8f0 ecd5c9db 006784eb 0ab393c2 8fb6f3d8 9af42a0e aff457e7 ad29647e
    12 af93b2a8 4762e8f0 ecd5c9db 006784eb 97e63d39 8fb6f3d8 9af42a0e aff457e7
    13 533c517c af93b2a8 4762e8f0 ecd5c9db 7364bae6 97e63d39 8fb6f3d8 9af42a0e
    14 03c0a51b 533c517c af93b2a8 4762e8f0 3afb010d 7364bae6 97e63d39 8fb6f3d8
    15 5fd065bd 03c0a51b 533c517c af93b2a8 b8e64229 3afb010d 7364bae6 97e63d39
    16 18b268b5 5fd065bd 03c0a51b 533c517c 38eda38d b8e64229 3afb010d 7364bae6
    17 b87d63b4 18b268b5 5fd065bd 03c0a51b 25c2c397 38eda38d b8e64229 3afb010d
    18 b1d846e0 b87d63b4 18b268b5 5fd065bd d674405f 25c2c397 38eda38d b8e64229
    19 8ba0aed6 b1d846e0 b87d63b4 18b268b5 b8109422 d674405f 25c2c397 38eda38d
    20 1485f843 8ba0aed6 b1d846e0 b87d63b4 1c58cd66 b8109422 d674405f 25c2c397
    21 238f4cda 1485f843 8ba0aed6 b1d846e0 39b2eb5f 1c58cd66 b8109422 d674405f
    22 7031b061 238f4cda 1485f843 8ba0aed6 4b8262ad 39b2eb5f 1c58cd66 b8109422
    23 d4e7ec62 7031b061 238f4cda 1485f843 163c3aa0 4b8262ad 39b2eb5f 1c58cd66
    24 66582df3 d4e7ec62 7031b061 238f4cda c0976260 163c3aa0 4b8262ad 39b2eb5f
    25 dedb8199 66582df3 d4e7ec62 7031b061 b73e2dec c0976260 163c3aa0 4b8262ad
    26 f8536917 dedb8199 66582df3 d4e7ec62 7c2af9c4 b73e2dec c0976260 163c3aa0
    27 d7333b8a f8536917 dedb8199 66582df3 b2b0b71a 7c2af9c4 b73e2dec c0976260
    28 760847c1 d7333b8a f8536917 dedb8199 5898eff2 b2b0b71a 7c2af9c4 b73e2dec
    29 7eabc6d7 760847c1 d7333b8a f8536917 24dd3883 5898eff2 b2b0b71a 7c2af9c4
    30 90c49624 7eabc6d7 760847c1 d7333b8a cce25e67 24dd3883 5898eff2 b2b0b71a
    31 0b876264 90c49624 7eabc6d7 760847c1 e4e4a53b cce25e67 24dd3883 5898eff2
    32 04cb36c0 0b876264 90c49624 7eabc6d7 5403a391 e4e4a53b cce25e67 24dd3883
    33 d58cc34a 04cb36c0 0b876264 90c49624 b78767c3 5403a391 e4e4a53b cce25e67
    34 0ed14dd7 d58cc34a 04cb36c0 0b876264 fdcdc9d9 b78767c3 5403a391 e4e4a53b
    35 5a89a942 0ed14dd7 d58cc34a 04cb36c0 790c4a20 fdcdc9d9 b78767c3 5403a391
    36 4d30424c 5a89a942 0ed14dd7 d58cc34a f95bf853 790c4a20 fdcdc9d9 b78767c3
    37 47f58c5c 4d30424c 5a89a942 0ed14dd7 0ec9be3b f95bf853 790c4a20 fdcdc9d9
    38 b5ad85d7 47f58c5c 4d30424c 5a89a942 cf9f1dbe 0ec9be3b f95bf853 790c4a20
    39 762fecbc b5ad85d7 47f58c5c 4d30424c 15427ed3 cf9f1dbe 0ec9be3b f95bf853
```

© ISO/IEC 2006 – 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

```
40 32abe746 762fecbc b5ad85d7 47f58c5c 4053e12e 15427ed3 cf9f1dbe 0ec9be3b
41 84adb2a0 32abe746 762fecbc b5ad85d7 7cece4e2 4053e12e 15427ed3 cf9f1dbe
42 c6e1c5af 84adb2a0 32abe746 762fecbc 42f9990b 7cece4e2 4053e12e 15427ed3
43 35e14bfa c6e1c5af 84adb2a0 32abe746 c9965792 42f9990b 7cece4e2 4053e12e
44 7410bfd8 35e14bfa c6e1c5af 84adb2a0 ca54ce51 c9965792 42f9990b 7cece4e2
45 3fe9e763 7410bfd8 35e14bfa c6e1c5af ae7cdb66 ca54ce51 c9965792 42f9990b
46 853c3a00 3fe9e763 7410bfd8 35e14bfa c2be054d ae7cdb66 ca54ce51 c9965792
47 f7d035e7 853c3a00 3fe9e763 7410bfd8 f6d59d2c c2be054d ae7cdb66 ca54ce51
48 20bae2b8 f7d035e7 853c3a00 3fe9e763 cab73f06 f6d59d2c c2be054d ae7cdb66
49 ae6bf667 20bae2b8 f7d035e7 853c3a00 52384d2f cab73f06 f6d59d2c c2be054d
50 12e504e5 ae6bf667 20bae2b8 f7d035e7 f9a8377f 52384d2f cab73f06 f6d59d2c
51 f3497054 12e504e5 ae6bf667 20bae2b8 d0ab7cfc f9a8377f 52384d2f cab73f06
52 9f166cdb f3497054 12e504e5 ae6bf667 71b3459b d0ab7cfc f9a8377f 52384d2f
53 ccd8fa44 9f166cdb f3497054 12e504e5 0f557ddd 71b3459b d0ab7cfc f9a8377f
54 f5e664bd ccd8fa44 9f166cdb f3497054 a679a5e9 0f557ddd 71b3459b d0ab7cfc
55 d4ea8c7e f5e664bd ccd8fa44 9f166cdb 2958ce2a a679a5e9 0f557ddd 71b3459b
56 e8c8fec7 d4ea8c7e f5e664bd ccd8fa44 35f6800e 2958ce2a a679a5e9 0f557ddd
57 882ed69e e8c8fec7 d4ea8c7e f5e664bd 30267d8e 35f6800e 2958ce2a a679a5e9
58 4ec725f6 882ed69e e8c8fec7 d4ea8c7e ce1d1ce4 30267d8e 35f6800e 2958ce2a
59 5c9cfc69 4ec725f6 882ed69e e8c8fec7 c8242b92 ce1d1ce4 30267d8e 35f6800e
60 c9a31836 5c9cfc69 4ec725f6 882ed69e 9e40a370 c8242b92 ce1d1ce4 30267d8e
61 f754c16e c9a31836 5c9cfc69 4ec725f6 333e0b63 9e40a370 c8242b92 ce1d1ce4
62 94314748 f754c16e c9a31836 5c9cfc69 1fbc63b0 333e0b63 9e40a370 c8242b92
63 f2e7a4b9 94314748 f754c16e c9a31836 9ffd8dac 1fbc63b0 333e0b63 9e40a370
```

The following eight words Y_0, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6, Y_7 represent the output of the final iteration of the round-function.

$$Y_0 = 8250e65d \boxplus f2e7a4b9 = 75388b16$$
$$Y_1 = bcf62f84 \boxplus 94314748 = 512776cc$$
$$Y_2 = 66659c33 \boxplus f754c16e = 5dba5da1$$
$$Y_3 = 33e5e91a \boxplus c9a31836 = fd890150$$
$$Y_4 = 10c8b7b0 \boxplus 9ffd8dac = b0c6455c$$
$$Y_5 = 95392769 \boxplus 1fbc63b0 = b4f58b19$$
$$Y_6 = 1f1419c2 \boxplus 333e0b63 = 52522525$$
$$Y_7 = fd16f295 \boxplus 9e40a370 = 635651e5$$

The hash value is the following 224-bit string.

```
75388b16 512776cc 5dba5da1 fd890150 b0c6455c b4f58b19 52522525
```

A.8.8 Example 8

In this example the data-string is the 1,000,000-byte string consisting of the ASCII-coded version of ‘a’ repeated 10^6 times.

The hash-code is the following 224-bit string.

```
20794655 980c91d8 bbb4c1ea 97618a4b f03f4258 1948b2ee 4ee7ad67
```

--`,,```,,,,````-`-`,,`,,`,`,,`---
8
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
© ISO/IEC 2006 – All rights reserved
Not for Resale

A.8.9 Example 9

In this example the data-string consists of a single bit, namely `0`.

The hash-code is the following 224-bit string.

```
d3fe57cb 76cdd24e 9eb23e7e 15684e03 9c75459b eaae100f 89712e9d
```

A.8.10 Example 10

In this example the data-string consists of a single bit, namely `1`.

The hash-code is the following 224-bit string.

```
0d05096b ca2a4a77 a2b47a05 a59618d0 1174b378 92376135 c1b6e957
```

A.8.11 Example 11

In this example the data-string consists of 101 bits, namely `1010101…01`.

The hash-code is the following 224-bit string.

```
2b1d4a34 155c04d7 a51065d6 a4476203 9a38dffd 73e76b17 b043555c
```

A.8.12 Example 12

In this example the data-string consists of 256 octets, namely `00 01 02 03 … FE FF`.

The hash-code is the following 224-bit string.

```
88702e63 237824c4 eb0d0fcf e41469a4 62493e8b eb2a75bb e5981734
```

A.8.13 Example 13

In this example the data-string is the H_0 consists of 224 0 bits. For i = 1 to 100 let H_i be the hash-code of H_{i-1}.

The hash-code H_{100} is the following 224-bit string.

```
a0884cc1 a335042b fe452bf4 6777ed20 217a3472 81dc389e 7b1fbfee
```

A.9 Complete test vectors for Dedicated Hash-Functions 4, 5, 6 and 8

As a part of ISO/IEC 10118-3, the dedicated hash-functions SHA-256, SHA-384, SHA-512 and SHA-224 are described. Annex A.4, A.5, A.6 and A.8 respectively provide example test vectors for these four hash functions. An important shortcoming of these examples is that all of the input values are composed solely of ASCII-encoded alphanumeric characters. This addendum contains a more complete set of test vectors for these hash functions.

The choice of test vectors is based on the following considerations:

1. Inputs of length 1 up to 512 (for SHA-224 and SHA-256) or 1024 (for SHA-384 and SHA-512) have been defined in order to test the padding scheme. (The examples in Annex A.4 – A.6 and A.8 contain only messages with lengths that are a multiple of 8.) A small number of test vectors with greater length have been included.

© ISO/IEC 2006 – 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

2. It has been ensured that all 32-bit words (SHA-224 and SHA-256) or all 64-bit words (SHA-384 and SHA-512) with Hamming weight 1 occur at least once as part of the input. This has been done in order to test the message expansion functions.

3. The treatment of carry overflow from one byte to another is tested by ensuring that the following additions occur at least once:

a. For SHA-224 and SHA-256

i. 0xFFFFFFFF + 0x00000001
ii. 0xFFFF0000 + 0x00010000
iii. 0x0000FFFF + 0x00000001
iv. 0xFF00FF00 + 0x01000100
v. 0x00FF00FF + 0x00010001

b. For SHA-384 and SHA-512

i. 0xFFFFFFFFFFFFFFFF + 0x0000000000000001
ii. 0xFFFFFFFF00000000 + 0x0000000100000000
iii. 0x00000000FFFFFFFF + 0x0000000000000001
iv. 0xFFFF0000FFFF0000 + 0x0001000000010000
v. 0x0000FFFF0000FFFF + 0x0000000100000001
vi. 0xFF00FF00FF00FF00 + 0x0100010001000100
vii. 0x00FF00FF00FF00FF + 0x0001000100010001

The complete list of test vectors can be found at the following URL:

http://www.iaik.tu-graz.ac.at/research/sha2_testvectors.zip.

NOTE Complete test vectors for the remaining hash functions contained in this part of ISO/IEC 10118 are not available at the above referenced URL. Analysis is currently ongoing to determine whether additional test vectors will be required for the remaining hash functions, and if so, what the required considerations will be. If additional test vectors are necessary, a second amendment to this part of ISO/IEC 10118 may be considered.

© ISO/IEC 2006 – 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

ICS 35.040

Price based on 10 pages

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

© ISO/IEC 2006 – 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