

SHA1 C-Library with Test Class

Generated by Doxygen 1.8.11

Contents

1	Hierarchical Index	1
1.1	Class Hierarchy	1
2	Class Index	3
2.1	Class List	3
3	File Index	5
3.1	File List	5
4	Class Documentation	7
4.1	Test_SHA1 Class Reference	7
4.1.1	Member Function Documentation	8
4.1.1.1	HMAC_SHA1_test1()	8
4.1.1.2	HMAC_SHA1_test2()	8
4.1.1.3	HMAC_SHA1_test3()	8
4.1.1.4	SHA1_Concat_test1()	8
4.1.1.5	SHA1_Concat_test2()	8
4.1.1.6	SHA1_Concat_test3()	9
4.1.1.7	SHA1_File_test1()	9
4.1.1.8	SHA1_test1()	9
4.1.1.9	SHA1_test2()	9
5	File Documentation	11
5.1	sha1.h File Reference	11
5.1.1	Detailed Description	11
5.1.2	Function Documentation	11
5.1.2.1	HMAC_SHA1(char *key, unsigned int key_size, char *text, uint64_t text_size, uint32_t *digest)	11
5.1.2.2	SHA1(char *text, uint64_t text_byte_size, uint32_t *hash)	12
5.1.2.3	SHA1_Concat(char **strings, uint64_t nr_of_strings, uint64_t *strings_byte_len, uint32_t *hash)	12
5.1.2.4	SHA1_File(char *filename, uint32_t *hash)	12
	Index	15

Chapter 1

Hierarchical Index

1.1 Class Hierarchy

This inheritance list is sorted roughly, but not completely, alphabetically:

TestCase	
Test_SHA1	7

Chapter 2

Class Index

2.1 Class List

Here are the classes, structs, unions and interfaces with brief descriptions:

Test_SHA1	7
-------------------------------------	-------------------

Chapter 3

File Index

3.1 File List

Here is a list of all documented files with brief descriptions:

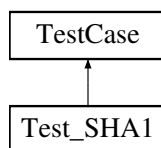
sha1.h	Function prototypes for the SHA1 library	11
test_sha1.h	??

Chapter 4

Class Documentation

4.1 Test_SHA1 Class Reference

Inheritance diagram for Test_SHA1:



Public Member Functions

- **CPPUNIT_TEST_SUITE** ([Test_SHA1](#))
- **CPPUNIT_TEST** ([SHA1_Concat_test1](#))
- **CPPUNIT_TEST** ([SHA1_Concat_test2](#))
- **CPPUNIT_TEST** ([SHA1_Concat_test3](#))
- **CPPUNIT_TEST** ([SHA1_test1](#))
- **CPPUNIT_TEST** ([SHA1_test2](#))
- **CPPUNIT_TEST** ([SHA1_File_test1](#))
- **CPPUNIT_TEST** ([HMAC_SHA1_test1](#))
- **CPPUNIT_TEST** ([HMAC_SHA1_test2](#))
- **CPPUNIT_TEST** ([HMAC_SHA1_test3](#))
- **CPPUNIT_TEST_SUITE_END** ()
- void [SHA1_Concat_test1](#) ()
- void [SHA1_Concat_test2](#) ()
- void [SHA1_Concat_test3](#) ()
- void [SHA1_test1](#) ()
- void [SHA1_test2](#) ()
- void [SHA1_File_test1](#) ()
- void [HMAC_SHA1_test1](#) ()
- void [HMAC_SHA1_test2](#) ()
- void [HMAC_SHA1_test3](#) ()

4.1.1 Member Function Documentation

4.1.1.1 void Test_SHA1::HMAC_SHA1_test1 ()

Test of HMAC_SHA1 with both text and key shorter than the block-size of 64 bytes

text: "what do ya want for nothing?"

key: "Jefe"

digest: 0xeffcdf6a, 0xe5eb2fa2, 0xd27416d5, 0xf184df9c, 0x259a7c79

4.1.1.2 void Test_SHA1::HMAC_SHA1_test2 ()

Test of HMAC_SHA1 with both text and key longer than the block size of 64 bytes

text: "Test Using Larger Than Block-Size Key and Larger Than One Block-Size Data"

key: 0xaa repeated 80 times

digest: 0xe8e99d0f, 0x45237d78, 0x6d6bbaa7, 0x965c7808, 0xbbff1a91

4.1.1.3 void Test_SHA1::HMAC_SHA1_test3 ()

Test of HMAC_SHA1 with both text and key defined by number sequences

text: 0xcd repeated 50 times

key: 0x 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19

digest: 0x4c9007f4, 0x026250c6, 0xbc8414f9, 0xbf50c86c, 0x2d7235da

4.1.1.4 void Test_SHA1::SHA1_Concat_test1 ()

Test of SHA1_Concat with short text

text: "abc"

digest: 0xa9993e36, 0x4706816a, 0xba3e2571, 0x7850c26c, 0x9cd0d89d

4.1.1.5 void Test_SHA1::SHA1_Concat_test2 ()

Test of SHA1_Concat with total text size shorter than the block-size of 64 bytes

text: "abcdcbcdcedefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq"

digest: 0x84983e44, 0x1c3bd26e, 0xbaae4aa1, 0xf95129e5, 0xe54670f1

4.1.1.6 void Test_SHA1::SHA1_Concat_test3 ()

Test of SHA1_Concat with total text size larger than the block-size of 64 bytes

```
text: "abcdefghbcdefghicdefghijdefghijkefghijklfghijklmghijklmnhijklmnoijklmnopjklmnopqklmnopqrlmnopqrsmnopqrstnopqrstu"
```

digest: 0xa49b2446, 0xa02c645b, 0xf419f995, 0xb6709125, 0x3a04a259

4.1.1.7 void Test_SHA1::SHA1_File_test1 ()

Test of SHA1_File with file "testfile.txt" containing the opening monologue of Richard III

digest: 0xc52c440c, 0xe2bbb52d, 0x6f0284a5, 0xe33c02eb, 0x68fdbf6c

4.1.1.8 void Test_SHA1::SHA1_test1 ()

Test of SHA1 with total text size larger than the block-size of 64 bytes

```
text: "abcdefghijklmnopqrstuvwxyz"
```

digest: 0xa49b2446, 0xa02c645b, 0xf419f995, 0xb6709125, 0x3a04a259

4.1.1.9 void Test_SHA1::SHA1_test2 ()

Test of SHA1 with long text

```
text: The letter 'a' repeated 1'000'000 times
```

digest: 0x34aa973c, 0xd4c4daa4, 0xf61eeb2b, 0xdbad2731, 0x6534016f

The documentation for this class was generated from the following files:

- test_sha1.h
- test_sha1.cpp

Chapter 5

File Documentation

5.1 sha1.h File Reference

Function prototypes for the SHA1 library.

Functions

- void [SHA1_Concat](#) (char **strings, uint64_t nr_of_strings, uint64_t *strings_byte_len, uint32_t *hash)
Takes as an argument a collection of char arrays, performs a virtual concatenation of these arrays in their given order, implements the SHA1 algorithm on the concatenated array and stores the resulting hash.
- void [SHA1](#) (char *text, uint64_t text_byte_size, uint32_t *hash)
Takes as an argument a char array, implements the SHA1 algorithm on the array and stores the resulting hash.
- int [SHA1_File](#) (char *filename, uint32_t *hash)
Takes as an argument a file name, implements the SHA1 algorithm on the file and stores the resulting hash.
- void [HMAC_SHA1](#) (char *key, unsigned int key_size, char *text, uint64_t text_size, uint32_t *digest)
Takes as an argument a string and a key, implements the HMAC-SHA1 algorithm and stores the resulting digest.

5.1.1 Detailed Description

Function prototypes for the SHA1 library.

Author

Anders Nordenfelt

5.1.2 Function Documentation

5.1.2.1 void HMAC_SHA1 (char * key, unsigned int key_size, char * text, uint64_t text_size, uint32_t * digest)

Takes as an argument a string and a key, implements the HMAC-SHA1 algorithm and stores the resulting digest.

Parameters

<i>key</i>	pointer to the char array containing the key
<i>key_size</i>	the key size in bytes
<i>text</i>	pointer to the char array containing the text
<i>text_size</i>	the text size in bytes
<i>hash</i>	pointer to the uint32_t array where the resulting hash is to be stored

Returns

void

5.1.2.2 void SHA1 (char * *text*, uint64_t *text_byte_size*, uint32_t * *hash*)

Takes as an argument a char array, implements the SHA1 algorithm on the array and stores the resulting hash.

Parameters

<i>text</i>	the pointer to the char array containing the text to be hashed
<i>text_byte_size</i>	the text size in bytes
<i>hash</i>	pointer to the uint32_t array where the resulting hash is to be stored

Returns

void

5.1.2.3 void SHA1_Concat (char ** *strings*, uint64_t *nr_of_strings*, uint64_t * *strings_byte_len*, uint32_t * *hash*)

Takes as an argument a collection of char arrays, performs a virtual concatenation of these arrays in their given order, implements the SHA1 algorithm on the concatenated array and stores the resulting hash.

Parameters

<i>strings</i>	the pointer to the char* array containing the pointers to the char arrays in the concatenation
<i>nr_of_strings</i>	the number of char arrays in the concatenation
<i>strings_byte_size</i>	pointer to the uint64_t array containing the size in bytes of each char array in the order they appear
<i>hash</i>	pointer to the uint32_t array where the resulting hash is to be stored

Returns

void

5.1.2.4 int SHA1_File (char * *filename*, uint32_t * *hash*)

Takes as an argument a file name, implements the SHA1 algorithm on the file and stores the resulting hash.

Parameters

<i>filename</i>	the pointer to the char array containing the file name
<i>hash</i>	pointer to the uint32_t array where the resulting hash is to be stored

Returns

int

Index

HMAC_SHA1

sha1.h, [11](#)

HMAC_SHA1_test1

Test_SHA1, [8](#)

HMAC_SHA1_test2

Test_SHA1, [8](#)

HMAC_SHA1_test3

Test_SHA1, [8](#)

SHA1

sha1.h, [12](#)

SHA1_Concat

sha1.h, [12](#)

SHA1_Concat_test1

Test_SHA1, [8](#)

SHA1_Concat_test2

Test_SHA1, [8](#)

SHA1_Concat_test3

Test_SHA1, [8](#)

SHA1_File

sha1.h, [12](#)

SHA1_File_test1

Test_SHA1, [9](#)

SHA1_test1

Test_SHA1, [9](#)

SHA1_test2

Test_SHA1, [9](#)

sha1.h, [11](#)

HMAC_SHA1, [11](#)

SHA1, [12](#)

SHA1_Concat, [12](#)

SHA1_File, [12](#)

Test_SHA1, [7](#)

HMAC_SHA1_test1, [8](#)

HMAC_SHA1_test2, [8](#)

HMAC_SHA1_test3, [8](#)

SHA1_Concat_test1, [8](#)

SHA1_Concat_test2, [8](#)

SHA1_Concat_test3, [8](#)

SHA1_File_test1, [9](#)

SHA1_test1, [9](#)

SHA1_test2, [9](#)