libmd5 Overview

PlayStation®Vita Programmer Tool Runtime Library Release 3.50

Table of Contents

1 Library Overview

Overview

libmd5 is a library that is used to generate a digest value using the MD5 Message-Digest Algorithm format as defined by RFC1321. It can be used to detect data corruption and prevent data tampering through the use of Keyed-Hashing for Message Authentication (HMAC).

Files

The following files are required to use libmd5.

Filename	Description
libmd5.h	Header file
libSceMd5.a	Static link library file
libSceMd5_stub.a	Stub library file
libSceMd5_stub_weak.a	weak import stub library file
libmd5.suprx	PRX module file

2 Usage Procedure

Basic Usage Procedure

(1) MD5 digest value computation (comprehensive method)

No specific initialization is required to use libmd5.

```
SceUChar8 digest[SCE_MD5_DIGEST_SIZE];

sceMd5Digest(plaintext, length, digest);
```

You can compute the digest value simply by calling the `sceMd5Digest()` function, as shown above.

(2) MD5 digest computation (divided method)

You can compute the digest value for a large amount of data by breaking up the calculation of the hash value as shown below.

```
SceMd5Context ctx;
SceUChar8 digest[SCE_MD5_DIGEST_SIZE];

sceMd5BlockInit(&ctx);
sceMd5BlockUpdate(&ctx, plain1, len1);
sceMd5BlockUpdate(&ctx, plain2, len2);
sceMd5BlockUpdate(&ctx, plain3, len3);
        :           Repeat an arbitrary number of times
sceMd5BlockResult(&ctx, digest);
```

To use this method, first call the `sceMd5BlockInit()` function to initialize the `SceMd5Context` structure. Then, call the `sceMd5BlockUpdate()` function an arbitrary number of times. Finally, call the `sceMd5BlockResult()` function to compute the digest value.