

# md5

- description : md5
- author :
- email : shlim@repia.com
- lastupdate : 2022-04-18 Mon

# md5

(block length):

( ) , , 가 .

### (Hash)

- (block length) . ( : IT
- ) 가 .
- 가 . ( : IT - ) 가 ( : )

## Class MessageDigest

MessageDigest SHA-1 SHA-256 Message Digest

**Message Digest** 가 가

(Message digests are secure one-way hash functions that take arbitrary-sized data and output a fixed-length hash value.)

Java MessageDigest .

- MD5
- SHA-1
- SHA-256

## Class DigestUtils

MessageDigest	가	MessageDigest
MessageDigestAlgorithms	getDigest(String) digest	Digest

## md5Hex

```
public static String md5Hex(String data)
```

Calculates the MD5 digest and returns the value as a 32 character hex string.  
 MD% digest      , 32      16

```
package com.ocean.crypto.md5;

import org.apache.commons.codec.digest.DigestUtils;

public class MD5HashDemo {

    public static void main(String[] args) {
        // Calculates the MD5 digest for the password text and returns
        // the value as a 32 character hex string
        String password = "s3cretw0rd**";
        String digest = DigestUtils.md5Hex(password);

        // Prints the plain text password, the digest and the Length of the
        // digest
        System.out.println("Password            = " + password);            //
        Password            = s3cretw0rd**
        System.out.println("Password Digest = " + digest);            //
        Password Digest = 203c603a7330ab3ea032f4b9f140cf95
        System.out.println("Length            = " + digest.length());    //
        Length            = 32

        // Calculates the MD5 digest for the Long texts.
        String md5 = ""
            + "The MD5 message-digest algorithm is a formerly \
            + "widely used cryptographic hash function that produces \
            + "a 128 bit long message digest."
    }
}
```

a 128-bit (16-byte) hash value. Specified in RFC 1321, MD5 has been utilized in a wide variety of security applications, and is also commonly used to check data integrity. MD5 was designed by Ron Rivest in 1991 to replace an earlier hash function, MD4. An MD5 hash value is typically expressed as a hexadecimal number, 32 digits long.

```
""";
```

```
String fingerprint = DigestUtils.md2Hex(md5);
```

```
// Prints the text, the fingerprint and the Length of the digest /
fingerprint
```

```
System.out.println("Text          = " + md5);
```

```
// Text          = The MD5 message-digest algorithm is a formerly
widely used cryptographic hash function that produces a 128-bit (16-byte)
hash value.
```

```
// Specified in RFC 1321, MD5 has been utilized in a wide variety of
security applications, and is also commonly used to check data integrity.
```

```
// MD5 was designed by Ron Rivest in 1991 to replace an earlier hash
function, MD4. An MD5 hash value is typically expressed as a hexadecimal
number, 32 digits long.
```

```
System.out.println("Fingerprint = " + fingerprint); //
```

```
Fingerprint = 09ad24fef35b06e6add520b5c6fff1d6
```

```
System.out.println("Length      = " + fingerprint.length()); //
```

```
Length      = 32
```

```
}
```

```
}
```

SHA	Secure Hash Algorithm,	
SHA-256	128	256
SHA-384	SHA512	.
SHA-512	256	512

## Ref Site

[Message Digest, FingerPrint -](#)

[Class DigestUtils](#)

[Class MessageDigest](#)

[How do I calculate the MD5 digest of a string?](#)

- Hash( ) Salt( )

RFC1321 - The MD5 Message\_Digest Algorithm

Class Hashtable<K,V>

MD5 Hashing in Java

Guide to hashCode() in Java

Java equals() hashCode()

Guideto GetHashCode() in Java

Hashing Algorithm in Java

[ ]Hash

[ / ] (Hash) ?

[java]Hash 가?

Message Digest

MD5

MessageDigest Algorithms

., md5

From: http://rwiki.repia.com/ - . - 2023.12

Permanent link: <http://rwiki.repia.com/doku.php?id=wiki:miscellaneous:md5&rev=1650342779>



Last update: 2022/04/19 13:32