

[Home](#) [Java Core](#) [Java Swing](#) [Web Services](#) [Oracle](#) [Unit Testing](#) [Web Server](#) [Other](#)

Java MD5 example



Posted by: [admin](#) On September 18, 2010 Filed under: [Core Java](#)
Version 1.0 Copyright © 2007 - 2013 Asjava.com

Java MD5 Overview

MD5 (Message-Digest algorithm 5) is a widely used cryptographic hash function with a 128-bit hash value, specified in RFC 1321, MD5 is one in a series of message digest algorithms designed by Professor Ronald Rivest of MIT (Rivest, 1994). MD5 has been employed in a wide variety of security applications, and is also worldwide used to check the integrity of files.

MD5 is a perfect solution for security thinking. The Java developers usually may take over or code MD5 encryption, the MD5 encryption is complicated, for self-coding it's hard to implement. Java standard edition has MD5 support built in. in package `java.security`, class `MessageDigest` supports functionality of a message digest algorithm, such as MD5 or SHA.

1. Example to Hash a String with MD5 algorithm

This is a Java MD5 example, it passes into a string and returns the MD5 encryption value, we used the method `getBytes()` that converts a plain text to byte array, the digest is then updated from the bytes from the byte array and a hash computation is conducted upon them(using `MessageDigest`).

MD5.java

```
1 import java.io.FileInputStream;
2 import java.io.UnsupportedEncodingException;
3 import java.math.BigInteger;
4 import java.security.MessageDigest;
5 import java.security.NoSuchAlgorithmException;
6
7 public class MD5 {
8     public static String getMD5(String input) {
9         try {
10             MessageDigest md = MessageDigest.getInstance("MD5");
11             byte[] messageDigest = md.digest(input.getBytes());
12             BigInteger number = new BigInteger(1, messageDigest);
13             String hashtext = number.toString(16);
14             // Now we need to zero pad it if you actually want the full 32 chars
15             while (hashtext.length() < 32) {
16                 hashtext = "0" + hashtext;
17             }
18             return hashtext;
19         }
20         catch (NoSuchAlgorithmException e) {
21             throw new RuntimeException(e);
22         }
23     }
24
25     public static void main(String[] args) throws NoSuchAlgorithmException {
26         System.out.println(getMD5("Javarmi.com"));
27     }
28 }
```

Java MD5 example Output:

```
0127f712fc008f857e77a2f3f179c710
```

2. Another way Hashing String with MD5 algorithm

This is another Java MD5 encryption example, it accepts string and returns MD5 encryption value.

```
1 import java.io.FileInputStream;
2 import java.io.UnsupportedEncodingException;
3 import java.math.BigInteger;
4 import java.security.MessageDigest;
```

Recent Articles

[Capture HTTP/HTTPS traffic from Java programs with Fiddler](#)
[Java 7 Applet is Blocked and Warning on Security Permissions](#)
[How to write to a file in Ant](#)
[Ant - How to print classpath in Ant script](#)
[How to enable ANT verbose?](#)
[Thread-safe Hash Map in Java and their performance benchmark](#)
[TCPMon Tutorial - Web Service Debugging Tool](#)
[Write For Us](#)
[Ant - how to get current directory in Ant](#)
[How to convert milliseconds to date string in Oracle SQL](#)

[Subscribe to the RSS feed](#)

All Available Tutorials

- [Java Core Technologies](#)
- [Database related](#)
- [Web Service](#)
- [Open source and Tools](#)
- [Others](#)

Favorites Documents

- [Java API - Oracle Documentation](#)
- [Struts 2 documentation](#)

Friends & Links

- [Java & Co. Tutorials](#)
- [Javatips](#)

```

5  import java.security.NoSuchAlgorithmException;
6
7  public class MD5 {
8      public static String getMD5(String input) {
9          byte[] source;
10         try {
11             //Get byte according by specified coding.
12             source = input.getBytes("UTF-8");
13         } catch (UnsupportedEncodingException e) {
14             source = input.getBytes();
15         }
16         String result = null;
17         char hexDigits[] = {'0', '1', '2', '3', '4', '5', '6', '7',
18             '8', '9', 'a', 'b', 'c', 'd', 'e', 'f'};
19         try {
20             MessageDigest md = MessageDigest.getInstance("MD5");
21             md.update(source);
22             //The result should be one 128 integer
23             byte temp[] = md.digest();
24             char str[] = new char[16 * 2];
25             int k = 0;
26             for (int i = 0; i < 16; i++) {
27                 byte byte0 = temp[i];
28                 str[k++] = hexDigits[byte0 >>> 4 & 0xf];
29                 str[k++] = hexDigits[byte0 & 0xf];
30             }
31             result = new String(str);
32         } catch (Exception e) {
33             e.printStackTrace();
34         }
35         return result;
36     }
37
38     public static void main(String[] args) throws NoSuchAlgorithmException {
39         System.out.println(getMD5("Javarmi.com"));
40     }
41 }

```

Java MD5 example Output

```
0127f712fc008f857e77a2f3f179c710
```

3. File checksum using Java MD5

MD5 algorithm is also widely used for file checksum to ensure that files were not modified by attacker, an example is below that uses Java MD5 hashing algorithm to generate a checksum for file "c:\apache\cxj.jar". you can check whether the printed value matches the original MD5 value which was released by Jar Publisher.

```

1  public static void main(String[] args) throws Exception {
2      MessageDigest md = MessageDigest.getInstance("MD5");
3      FileInputStream fis = new FileInputStream("c:\\apache\\cxj.jar");
4
5      byte[] dataBytes = new byte[1024];
6
7      int nread = 0;
8      while ((nread = fis.read(dataBytes)) != -1) {
9          md.update(dataBytes, 0, nread);
10     };
11     byte[] mdbytes = md.digest();
12     StringBuffer sb = new StringBuffer();
13     for (int i = 0; i < mdbytes.length; i++) {
14         sb.append(Integer.toString((mdbytes[i] & 0xff) + 0x100, 16).substring(1)
15     );
16     System.out.println("Digest(in hex format):: " + sb.toString());
17 }

```

Reference

<http://download.oracle.com/javase/1.4.2/docs/api/java/security/MessageDigest.html>

Tags: **Java**

You can follow any responses to this entry through the [RSS 2.0 feed](#). You can [leave a response](#), or [trackback](#) from your own site.

8 THOUGHTS ON "JAVA MD5 EXAMPLE"



MD5 Example on September 26, 2010 at 8:35 am said:

Thanks your Java MD5 checksum. I am happy Java support MessageDigest to help to implement MD5 checksum.

Reply ↓



Viraf Karai on January 1, 2013 at 9:25 pm said:

I feel that instead of writing all this code, it is preferable to use Apache Commons Codec and write very little code such as:

~~~~~

```
final String stringForMD5 = "Mary had a little lamb, its fleece was white as snow";
```

```
final String md5Hex = DigestUtils.md5Hex (stringForMD5);
```

```
final String result = String.format("MD5 for %s is %s %n", stringForMD5, md5Hex);
```

```
System.out.println (result);
```

Reply ↓



**admin**

on January 2, 2013 at 12:42 pm said:

You are right, Apache Codec is an alternative approach to implement MD5, but we have to import the 3th library to have this feature included, In Java, we actually don't need write much code as well, just a little code lines...

Reply ↓

[BACK TO TOP](#)



**Ankur parihar** on March 12, 2013 at 5:58 am said:

plz md5 to plaintext in PHP..

Reply ↓



**admin**

on October 5, 2013 at 2:11 pm said:

Sorry, I don't know much about PHP.

Reply ↓



**Muhammad Tahir Qaiser**

on January 21, 2015 at 5:05 pm said:

```
In php , it's simple
$password="password";
$hash=md5($password);
echo $hash;
```

And Thanks to admin for Java md5 code 😊

Reply ↓



**vishal**

on August 31, 2015 at 8:05 am said:

Description :-

```
string md5 ( string $str [, bool $raw_output = false ] )
Calculates the MD5 hash of str using the » RSA Data Security, Inc. MD5 Message-Digest
Algorithm, and returns that hash.
```

Parameters:-

str:The string.

**raw\_output:** If the optional `raw_output` is set to `TRUE`, then the md5 digest is instead returned in raw binary format with a length of 16.

**Return Values:** Returns the hash as a 32-character hexadecimal number.

**Examples :**

Reply ↓



**vishal**

on August 31, 2015 at 8:08 am said:

Sometimes it's useful to get the actual, binary, md5 digest.  
You can use this function for it:

<?php

```
function md5bin( $target ) {  
    $md5 = md5( $target );  
    $ret = '';
```

```
    for ( $i = 0; $i
```

Reply ↓

## Leave a Reply

Your email address will not be published. Required fields are marked \*

Name \*

Email \*

Website

Comment

You may use these HTML tags and attributes: `<a href="" title="">` `<abbr title="">` `<acronym title="">` `<b>` `<blockquote cite="">` `<cite>` `<code>` `<del datetime="">` `<em>` `<i>` `<q cite="">` `<strike>` `<strong>`

Post Comment

## About Us

Asjava.com regularly discuss a wide array of java-related topics, and share Java, JDBC, Webservice, Swing, Tomcat, Spring, Struts, Hibernate tutorials in a straightforward, no-nonsense manner.

[Log in](#) - [Contact us](#) - Copyright. 2009-2011 Java development tutorials and examples All rights reserved