| | [**Overview**](http://docs.google.com/overview-summary.html) | [**Package**](http://docs.google.com/package-summary.html) | **Class** | [**Use**](http://docs.google.com/class-use/MessageDigest.html) | [**Tree**](http://docs.google.com/package-tree.html) | [**Deprecated**](http://docs.google.com/deprecated-list.html) | [**Index**](http://docs.google.com/index-files/index-1.html) | [**Help**](http://docs.google.com/help-doc.html) | | --- | --- | --- | --- | --- | --- | --- | --- | | | ***Java™ Platform***  ***Standard Ed. 6*** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [**PREV CLASS**](http://docs.google.com/java/security/KeyStoreSpi.html)   [**NEXT CLASS**](http://docs.google.com/java/security/MessageDigestSpi.html) | [**FRAMES**](http://docs.google.com/index.html?java/security/MessageDigest.html)    [**NO FRAMES**](http://docs.google.com/MessageDigest.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |
| SUMMARY: NESTED | FIELD | [CONSTR](#3znysh7) | [METHOD](#2et92p0) | DETAIL: FIELD | [CONSTR](#1t3h5sf) | [METHOD](#2s8eyo1) |

## **java.security**

Class MessageDigest

[java.lang.Object](http://docs.google.com/java/lang/Object.html)  
 [java.security.MessageDigestSpi](http://docs.google.com/java/security/MessageDigestSpi.html)  
 **java.security.MessageDigest**

public abstract class **MessageDigest**extends [MessageDigestSpi](http://docs.google.com/java/security/MessageDigestSpi.html)

This MessageDigest class provides applications the functionality of a message digest algorithm, such as MD5 or SHA. Message digests are secure one-way hash functions that take arbitrary-sized data and output a fixed-length hash value.

A MessageDigest object starts out initialized. The data is processed through it using the [update](http://docs.google.com/java/security/MessageDigest.html#update(byte)) methods. At any point [reset](http://docs.google.com/java/security/MessageDigest.html#reset()) can be called to reset the digest. Once all the data to be updated has been updated, one of the [digest](http://docs.google.com/java/security/MessageDigest.html#digest()) methods should be called to complete the hash computation.

The digest method can be called once for a given number of updates. After digest has been called, the MessageDigest object is reset to its initialized state.

Implementations are free to implement the Cloneable interface. Client applications can test cloneability by attempting cloning and catching the CloneNotSupportedException:

MessageDigest md = MessageDigest.getInstance("SHA");  
  
 try {  
 md.update(toChapter1);  
 MessageDigest tc1 = md.clone();  
 byte[] toChapter1Digest = tc1.digest();  
 md.update(toChapter2);  
 ...etc.  
 } catch (CloneNotSupportedException cnse) {  
 throw new DigestException("couldn't make digest of partial content");  
 }

Note that if a given implementation is not cloneable, it is still possible to compute intermediate digests by instantiating several instances, if the number of digests is known in advance.

Note that this class is abstract and extends from MessageDigestSpi for historical reasons. Application developers should only take notice of the methods defined in this MessageDigest class; all the methods in the superclass are intended for cryptographic service providers who wish to supply their own implementations of message digest algorithms.

**See Also:**[DigestInputStream](http://docs.google.com/java/security/DigestInputStream.html), [DigestOutputStream](http://docs.google.com/java/security/DigestOutputStream.html)

| **Constructor Summary** | |
| --- | --- |
| protected | [**MessageDigest**](http://docs.google.com/java/security/MessageDigest.html#MessageDigest(java.lang.String))([String](http://docs.google.com/java/lang/String.html) algorithm)            Creates a message digest with the specified algorithm name. |

| **Method Summary** | |
| --- | --- |
| [Object](http://docs.google.com/java/lang/Object.html) | [**clone**](http://docs.google.com/java/security/MessageDigest.html#clone())()            Returns a clone if the implementation is cloneable. |
| byte[] | [**digest**](http://docs.google.com/java/security/MessageDigest.html#digest())()            Completes the hash computation by performing final operations such as padding. |
| byte[] | [**digest**](http://docs.google.com/java/security/MessageDigest.html#digest(byte%5B%5D))(byte[] input)            Performs a final update on the digest using the specified array of bytes, then completes the digest computation. |
| int | [**digest**](http://docs.google.com/java/security/MessageDigest.html#digest(byte%5B%5D,%20int,%20int))(byte[] buf, int offset, int len)            Completes the hash computation by performing final operations such as padding. |
| [String](http://docs.google.com/java/lang/String.html) | [**getAlgorithm**](http://docs.google.com/java/security/MessageDigest.html#getAlgorithm())()            Returns a string that identifies the algorithm, independent of implementation details. |
| int | [**getDigestLength**](http://docs.google.com/java/security/MessageDigest.html#getDigestLength())()            Returns the length of the digest in bytes, or 0 if this operation is not supported by the provider and the implementation is not cloneable. |
| static [MessageDigest](http://docs.google.com/java/security/MessageDigest.html) | [**getInstance**](http://docs.google.com/java/security/MessageDigest.html#getInstance(java.lang.String))([String](http://docs.google.com/java/lang/String.html) algorithm)            Returns a MessageDigest object that implements the specified digest algorithm. |
| static [MessageDigest](http://docs.google.com/java/security/MessageDigest.html) | [**getInstance**](http://docs.google.com/java/security/MessageDigest.html#getInstance(java.lang.String,%20java.security.Provider))([String](http://docs.google.com/java/lang/String.html) algorithm, [Provider](http://docs.google.com/java/security/Provider.html) provider)            Returns a MessageDigest object that implements the specified digest algorithm. |
| static [MessageDigest](http://docs.google.com/java/security/MessageDigest.html) | [**getInstance**](http://docs.google.com/java/security/MessageDigest.html#getInstance(java.lang.String,%20java.lang.String))([String](http://docs.google.com/java/lang/String.html) algorithm, [String](http://docs.google.com/java/lang/String.html) provider)            Returns a MessageDigest object that implements the specified digest algorithm. |
| [Provider](http://docs.google.com/java/security/Provider.html) | [**getProvider**](http://docs.google.com/java/security/MessageDigest.html#getProvider())()            Returns the provider of this message digest object. |
| static boolean | [**isEqual**](http://docs.google.com/java/security/MessageDigest.html#isEqual(byte%5B%5D,%20byte%5B%5D))(byte[] digesta, byte[] digestb)            Compares two digests for equality. |
| void | [**reset**](http://docs.google.com/java/security/MessageDigest.html#reset())()            Resets the digest for further use. |
| [String](http://docs.google.com/java/lang/String.html) | [**toString**](http://docs.google.com/java/security/MessageDigest.html#toString())()            Returns a string representation of this message digest object. |
| void | [**update**](http://docs.google.com/java/security/MessageDigest.html#update(byte))(byte input)            Updates the digest using the specified byte. |
| void | [**update**](http://docs.google.com/java/security/MessageDigest.html#update(byte%5B%5D))(byte[] input)            Updates the digest using the specified array of bytes. |
| void | [**update**](http://docs.google.com/java/security/MessageDigest.html#update(byte%5B%5D,%20int,%20int))(byte[] input, int offset, int len)            Updates the digest using the specified array of bytes, starting at the specified offset. |
| void | [**update**](http://docs.google.com/java/security/MessageDigest.html#update(java.nio.ByteBuffer))([ByteBuffer](http://docs.google.com/java/nio/ByteBuffer.html) input)            Update the digest using the specified ByteBuffer. |

| **Methods inherited from class java.security.**[**MessageDigestSpi**](http://docs.google.com/java/security/MessageDigestSpi.html) |
| --- |
| [engineDigest](http://docs.google.com/java/security/MessageDigestSpi.html#engineDigest()), [engineDigest](http://docs.google.com/java/security/MessageDigestSpi.html#engineDigest(byte%5B%5D,%20int,%20int)), [engineGetDigestLength](http://docs.google.com/java/security/MessageDigestSpi.html#engineGetDigestLength()), [engineReset](http://docs.google.com/java/security/MessageDigestSpi.html#engineReset()), [engineUpdate](http://docs.google.com/java/security/MessageDigestSpi.html#engineUpdate(byte)), [engineUpdate](http://docs.google.com/java/security/MessageDigestSpi.html#engineUpdate(byte%5B%5D,%20int,%20int)), [engineUpdate](http://docs.google.com/java/security/MessageDigestSpi.html#engineUpdate(java.nio.ByteBuffer)) |

| **Methods inherited from class java.lang.**[**Object**](http://docs.google.com/java/lang/Object.html) |
| --- |
| [equals](http://docs.google.com/java/lang/Object.html#equals(java.lang.Object)), [finalize](http://docs.google.com/java/lang/Object.html#finalize()), [getClass](http://docs.google.com/java/lang/Object.html#getClass()), [hashCode](http://docs.google.com/java/lang/Object.html#hashCode()), [notify](http://docs.google.com/java/lang/Object.html#notify()), [notifyAll](http://docs.google.com/java/lang/Object.html#notifyAll()), [wait](http://docs.google.com/java/lang/Object.html#wait()), [wait](http://docs.google.com/java/lang/Object.html#wait(long)), [wait](http://docs.google.com/java/lang/Object.html#wait(long,%20int)) |

| **Constructor Detail** |
| --- |

### MessageDigest

protected **MessageDigest**([String](http://docs.google.com/java/lang/String.html) algorithm)

Creates a message digest with the specified algorithm name.

**Parameters:**algorithm - the standard name of the digest algorithm. See Appendix A in the  [Java Cryptography Architecture API Specification & Reference](http://docs.google.com/technotes/guides/security/crypto/CryptoSpec.html#AppA)  for information about standard algorithm names.

| **Method Detail** |
| --- |

### getInstance

public static [MessageDigest](http://docs.google.com/java/security/MessageDigest.html) **getInstance**([String](http://docs.google.com/java/lang/String.html) algorithm)  
 throws [NoSuchAlgorithmException](http://docs.google.com/java/security/NoSuchAlgorithmException.html)

Returns a MessageDigest object that implements the specified digest algorithm.

This method traverses the list of registered security Providers, starting with the most preferred Provider. A new MessageDigest object encapsulating the MessageDigestSpi implementation from the first Provider that supports the specified algorithm is returned.

Note that the list of registered providers may be retrieved via the [Security.getProviders()](http://docs.google.com/java/security/Security.html#getProviders()) method.

**Parameters:**algorithm - the name of the algorithm requested. See Appendix A in the  [Java Cryptography Architecture API Specification & Reference](http://docs.google.com/technotes/guides/security/crypto/CryptoSpec.html#AppA)  for information about standard algorithm names. **Returns:**a Message Digest object that implements the specified algorithm. **Throws:** [NoSuchAlgorithmException](http://docs.google.com/java/security/NoSuchAlgorithmException.html) - if no Provider supports a MessageDigestSpi implementation for the specified algorithm.**See Also:**[Provider](http://docs.google.com/java/security/Provider.html)

### getInstance

public static [MessageDigest](http://docs.google.com/java/security/MessageDigest.html) **getInstance**([String](http://docs.google.com/java/lang/String.html) algorithm,  
 [String](http://docs.google.com/java/lang/String.html) provider)  
 throws [NoSuchAlgorithmException](http://docs.google.com/java/security/NoSuchAlgorithmException.html),  
 [NoSuchProviderException](http://docs.google.com/java/security/NoSuchProviderException.html)

Returns a MessageDigest object that implements the specified digest algorithm.

A new MessageDigest object encapsulating the MessageDigestSpi implementation from the specified provider is returned. The specified provider must be registered in the security provider list.

Note that the list of registered providers may be retrieved via the [Security.getProviders()](http://docs.google.com/java/security/Security.html#getProviders()) method.

**Parameters:**algorithm - the name of the algorithm requested. See Appendix A in the  [Java Cryptography Architecture API Specification & Reference](http://docs.google.com/technotes/guides/security/crypto/CryptoSpec.html#AppA)  for information about standard algorithm names.provider - the name of the provider. **Returns:**a MessageDigest object that implements the specified algorithm. **Throws:** [NoSuchAlgorithmException](http://docs.google.com/java/security/NoSuchAlgorithmException.html) - if a MessageDigestSpi implementation for the specified algorithm is not available from the specified provider. [NoSuchProviderException](http://docs.google.com/java/security/NoSuchProviderException.html) - if the specified provider is not registered in the security provider list. [IllegalArgumentException](http://docs.google.com/java/lang/IllegalArgumentException.html) - if the provider name is null or empty.**See Also:**[Provider](http://docs.google.com/java/security/Provider.html)

### getInstance

public static [MessageDigest](http://docs.google.com/java/security/MessageDigest.html) **getInstance**([String](http://docs.google.com/java/lang/String.html) algorithm,  
 [Provider](http://docs.google.com/java/security/Provider.html) provider)  
 throws [NoSuchAlgorithmException](http://docs.google.com/java/security/NoSuchAlgorithmException.html)

Returns a MessageDigest object that implements the specified digest algorithm.

A new MessageDigest object encapsulating the MessageDigestSpi implementation from the specified Provider object is returned. Note that the specified Provider object does not have to be registered in the provider list.

**Parameters:**algorithm - the name of the algorithm requested. See Appendix A in the  [Java Cryptography Architecture API Specification & Reference](http://docs.google.com/technotes/guides/security/crypto/CryptoSpec.html#AppA)  for information about standard algorithm names.provider - the provider. **Returns:**a MessageDigest object that implements the specified algorithm. **Throws:** [NoSuchAlgorithmException](http://docs.google.com/java/security/NoSuchAlgorithmException.html) - if a MessageDigestSpi implementation for the specified algorithm is not available from the specified Provider object. [IllegalArgumentException](http://docs.google.com/java/lang/IllegalArgumentException.html) - if the specified provider is null.**Since:** 1.4 **See Also:**[Provider](http://docs.google.com/java/security/Provider.html)

### getProvider

public final [Provider](http://docs.google.com/java/security/Provider.html) **getProvider**()

Returns the provider of this message digest object.

**Returns:**the provider of this message digest object

### update

public void **update**(byte input)

Updates the digest using the specified byte.

**Parameters:**input - the byte with which to update the digest.

### update

public void **update**(byte[] input,  
 int offset,  
 int len)

Updates the digest using the specified array of bytes, starting at the specified offset.

**Parameters:**input - the array of bytes.offset - the offset to start from in the array of bytes.len - the number of bytes to use, starting at offset.

### update

public void **update**(byte[] input)

Updates the digest using the specified array of bytes.

**Parameters:**input - the array of bytes.

### update

public final void **update**([ByteBuffer](http://docs.google.com/java/nio/ByteBuffer.html) input)

Update the digest using the specified ByteBuffer. The digest is updated using the input.remaining() bytes starting at input.position(). Upon return, the buffer's position will be equal to its limit; its limit will not have changed.

**Parameters:**input - the ByteBuffer**Since:** 1.5

### digest

public byte[] **digest**()

Completes the hash computation by performing final operations such as padding. The digest is reset after this call is made.

**Returns:**the array of bytes for the resulting hash value.

### digest

public int **digest**(byte[] buf,  
 int offset,  
 int len)  
 throws [DigestException](http://docs.google.com/java/security/DigestException.html)

Completes the hash computation by performing final operations such as padding. The digest is reset after this call is made.

**Parameters:**buf - output buffer for the computed digestoffset - offset into the output buffer to begin storing the digestlen - number of bytes within buf allotted for the digest **Returns:**the number of bytes placed into buf **Throws:** [DigestException](http://docs.google.com/java/security/DigestException.html) - if an error occurs.

### digest

public byte[] **digest**(byte[] input)

Performs a final update on the digest using the specified array of bytes, then completes the digest computation. That is, this method first calls [update(input)](http://docs.google.com/java/security/MessageDigest.html#update(byte%5B%5D)), passing the *input* array to the update method, then calls [digest()](http://docs.google.com/java/security/MessageDigest.html#digest()).

**Parameters:**input - the input to be updated before the digest is completed. **Returns:**the array of bytes for the resulting hash value.

### toString

public [String](http://docs.google.com/java/lang/String.html) **toString**()

Returns a string representation of this message digest object.

**Overrides:**[toString](http://docs.google.com/java/lang/Object.html#toString()) in class [Object](http://docs.google.com/java/lang/Object.html) **Returns:**a string representation of the object.

### isEqual

public static boolean **isEqual**(byte[] digesta,  
 byte[] digestb)

Compares two digests for equality. Does a simple byte compare.

**Parameters:**digesta - one of the digests to compare.digestb - the other digest to compare. **Returns:**true if the digests are equal, false otherwise.

### reset

public void **reset**()

Resets the digest for further use.

### getAlgorithm

public final [String](http://docs.google.com/java/lang/String.html) **getAlgorithm**()

Returns a string that identifies the algorithm, independent of implementation details. The name should be a standard Java Security name (such as "SHA", "MD5", and so on). See Appendix A in the  [Java Cryptography Architecture API Specification & Reference](http://docs.google.com/technotes/guides/security/crypto/CryptoSpec.html#AppA)  for information about standard algorithm names.

**Returns:**the name of the algorithm

### getDigestLength

public final int **getDigestLength**()

Returns the length of the digest in bytes, or 0 if this operation is not supported by the provider and the implementation is not cloneable.

**Returns:**the digest length in bytes, or 0 if this operation is not supported by the provider and the implementation is not cloneable.**Since:** 1.2

### clone

public [Object](http://docs.google.com/java/lang/Object.html) **clone**()  
 throws [CloneNotSupportedException](http://docs.google.com/java/lang/CloneNotSupportedException.html)

Returns a clone if the implementation is cloneable.

**Overrides:**[clone](http://docs.google.com/java/security/MessageDigestSpi.html#clone()) in class [MessageDigestSpi](http://docs.google.com/java/security/MessageDigestSpi.html) **Returns:**a clone if the implementation is cloneable. **Throws:** [CloneNotSupportedException](http://docs.google.com/java/lang/CloneNotSupportedException.html) - if this is called on an implementation that does not support Cloneable.**See Also:**[Cloneable](http://docs.google.com/java/lang/Cloneable.html)

| | [**Overview**](http://docs.google.com/overview-summary.html) | [**Package**](http://docs.google.com/package-summary.html) | **Class** | [**Use**](http://docs.google.com/class-use/MessageDigest.html) | [**Tree**](http://docs.google.com/package-tree.html) | [**Deprecated**](http://docs.google.com/deprecated-list.html) | [**Index**](http://docs.google.com/index-files/index-1.html) | [**Help**](http://docs.google.com/help-doc.html) | | --- | --- | --- | --- | --- | --- | --- | --- | | | ***Java™ Platform***  ***Standard Ed. 6*** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| [**PREV CLASS**](http://docs.google.com/java/security/KeyStoreSpi.html)   [**NEXT CLASS**](http://docs.google.com/java/security/MessageDigestSpi.html) | [**FRAMES**](http://docs.google.com/index.html?java/security/MessageDigest.html)    [**NO FRAMES**](http://docs.google.com/MessageDigest.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |
| SUMMARY: NESTED | FIELD | [CONSTR](#3znysh7) | [METHOD](#2et92p0) | DETAIL: FIELD | [CONSTR](#1t3h5sf) | [METHOD](#2s8eyo1) |

[Submit a bug or feature](http://bugs.sun.com/services/bugreport/index.jsp)

For further API reference and developer documentation, see [Java SE Developer Documentation](http://docs.google.com/webnotes/devdocs-vs-specs.html). That documentation contains more detailed, developer-targeted descriptions, with conceptual overviews, definitions of terms, workarounds, and working code examples.

Copyright 2006 Sun Microsystems, Inc. All rights reserved. Use is subject to [license terms](http://docs.google.com/legal/license.html). Also see the [documentation redistribution policy](http://java.sun.com/docs/redist.html).