| | [**Overview**](http://docs.google.com/overview-summary.html) | [**Package**](http://docs.google.com/package-summary.html) | **Class** | [**Use**](http://docs.google.com/class-use/RSAMultiPrimePrivateCrtKeySpec.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/spec/RSAKeyGenParameterSpec.html)   [**NEXT CLASS**](http://docs.google.com/java/security/spec/RSAOtherPrimeInfo.html) | [**FRAMES**](http://docs.google.com/index.html?java/security/spec/RSAMultiPrimePrivateCrtKeySpec.html)    [**NO FRAMES**](http://docs.google.com/RSAMultiPrimePrivateCrtKeySpec.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.spec**

Class RSAMultiPrimePrivateCrtKeySpec

[java.lang.Object](http://docs.google.com/java/lang/Object.html)  
 [java.security.spec.RSAPrivateKeySpec](http://docs.google.com/java/security/spec/RSAPrivateKeySpec.html)  
 **java.security.spec.RSAMultiPrimePrivateCrtKeySpec**

**All Implemented Interfaces:** [KeySpec](http://docs.google.com/java/security/spec/KeySpec.html)

public class **RSAMultiPrimePrivateCrtKeySpec**extends [RSAPrivateKeySpec](http://docs.google.com/java/security/spec/RSAPrivateKeySpec.html)

This class specifies an RSA multi-prime private key, as defined in the PKCS#1 v2.1, using the Chinese Remainder Theorem (CRT) information values for efficiency.

**Since:** 1.4 **See Also:**[Key](http://docs.google.com/java/security/Key.html), [KeyFactory](http://docs.google.com/java/security/KeyFactory.html), [KeySpec](http://docs.google.com/java/security/spec/KeySpec.html), [PKCS8EncodedKeySpec](http://docs.google.com/java/security/spec/PKCS8EncodedKeySpec.html), [RSAPrivateKeySpec](http://docs.google.com/java/security/spec/RSAPrivateKeySpec.html), [RSAPublicKeySpec](http://docs.google.com/java/security/spec/RSAPublicKeySpec.html), [RSAOtherPrimeInfo](http://docs.google.com/java/security/spec/RSAOtherPrimeInfo.html)

| **Constructor Summary** | |
| --- | --- |
| [**RSAMultiPrimePrivateCrtKeySpec**](http://docs.google.com/java/security/spec/RSAMultiPrimePrivateCrtKeySpec.html#RSAMultiPrimePrivateCrtKeySpec(java.math.BigInteger,%20java.math.BigInteger,%20java.math.BigInteger,%20java.math.BigInteger,%20java.math.BigInteger,%20java.math.BigInteger,%20java.math.BigInteger,%20java.math.BigInteger,%20java.security.spec.RSAOtherPrimeInfo%5B%5D))([BigInteger](http://docs.google.com/java/math/BigInteger.html) modulus, [BigInteger](http://docs.google.com/java/math/BigInteger.html) publicExponent, [BigInteger](http://docs.google.com/java/math/BigInteger.html) privateExponent, [BigInteger](http://docs.google.com/java/math/BigInteger.html) primeP, [BigInteger](http://docs.google.com/java/math/BigInteger.html) primeQ, [BigInteger](http://docs.google.com/java/math/BigInteger.html) primeExponentP, [BigInteger](http://docs.google.com/java/math/BigInteger.html) primeExponentQ, [BigInteger](http://docs.google.com/java/math/BigInteger.html) crtCoefficient, [RSAOtherPrimeInfo](http://docs.google.com/java/security/spec/RSAOtherPrimeInfo.html)[] otherPrimeInfo)            Creates a new RSAMultiPrimePrivateCrtKeySpec given the modulus, publicExponent, privateExponent, primeP, primeQ, primeExponentP, primeExponentQ, crtCoefficient, and otherPrimeInfo as defined in PKCS#1 v2.1. |

| **Method Summary** | |
| --- | --- |
| [BigInteger](http://docs.google.com/java/math/BigInteger.html) | [**getCrtCoefficient**](http://docs.google.com/java/security/spec/RSAMultiPrimePrivateCrtKeySpec.html#getCrtCoefficient())()            Returns the crtCoefficient. |
| [RSAOtherPrimeInfo](http://docs.google.com/java/security/spec/RSAOtherPrimeInfo.html)[] | [**getOtherPrimeInfo**](http://docs.google.com/java/security/spec/RSAMultiPrimePrivateCrtKeySpec.html#getOtherPrimeInfo())()            Returns a copy of the otherPrimeInfo or null if there are only two prime factors (p and q). |
| [BigInteger](http://docs.google.com/java/math/BigInteger.html) | [**getPrimeExponentP**](http://docs.google.com/java/security/spec/RSAMultiPrimePrivateCrtKeySpec.html#getPrimeExponentP())()            Returns the primeExponentP. |
| [BigInteger](http://docs.google.com/java/math/BigInteger.html) | [**getPrimeExponentQ**](http://docs.google.com/java/security/spec/RSAMultiPrimePrivateCrtKeySpec.html#getPrimeExponentQ())()            Returns the primeExponentQ. |
| [BigInteger](http://docs.google.com/java/math/BigInteger.html) | [**getPrimeP**](http://docs.google.com/java/security/spec/RSAMultiPrimePrivateCrtKeySpec.html#getPrimeP())()            Returns the primeP. |
| [BigInteger](http://docs.google.com/java/math/BigInteger.html) | [**getPrimeQ**](http://docs.google.com/java/security/spec/RSAMultiPrimePrivateCrtKeySpec.html#getPrimeQ())()            Returns the primeQ. |
| [BigInteger](http://docs.google.com/java/math/BigInteger.html) | [**getPublicExponent**](http://docs.google.com/java/security/spec/RSAMultiPrimePrivateCrtKeySpec.html#getPublicExponent())()            Returns the public exponent. |

| **Methods inherited from class java.security.spec.**[**RSAPrivateKeySpec**](http://docs.google.com/java/security/spec/RSAPrivateKeySpec.html) |
| --- |
| [getModulus](http://docs.google.com/java/security/spec/RSAPrivateKeySpec.html#getModulus()), [getPrivateExponent](http://docs.google.com/java/security/spec/RSAPrivateKeySpec.html#getPrivateExponent()) |

| **Methods inherited from class java.lang.**[**Object**](http://docs.google.com/java/lang/Object.html) |
| --- |
| [clone](http://docs.google.com/java/lang/Object.html#clone()), [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()), [toString](http://docs.google.com/java/lang/Object.html#toString()), [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** |
| --- |

### RSAMultiPrimePrivateCrtKeySpec

public **RSAMultiPrimePrivateCrtKeySpec**([BigInteger](http://docs.google.com/java/math/BigInteger.html) modulus,  
 [BigInteger](http://docs.google.com/java/math/BigInteger.html) publicExponent,  
 [BigInteger](http://docs.google.com/java/math/BigInteger.html) privateExponent,  
 [BigInteger](http://docs.google.com/java/math/BigInteger.html) primeP,  
 [BigInteger](http://docs.google.com/java/math/BigInteger.html) primeQ,  
 [BigInteger](http://docs.google.com/java/math/BigInteger.html) primeExponentP,  
 [BigInteger](http://docs.google.com/java/math/BigInteger.html) primeExponentQ,  
 [BigInteger](http://docs.google.com/java/math/BigInteger.html) crtCoefficient,  
 [RSAOtherPrimeInfo](http://docs.google.com/java/security/spec/RSAOtherPrimeInfo.html)[] otherPrimeInfo)

Creates a new RSAMultiPrimePrivateCrtKeySpec given the modulus, publicExponent, privateExponent, primeP, primeQ, primeExponentP, primeExponentQ, crtCoefficient, and otherPrimeInfo as defined in PKCS#1 v2.1.

Note that the contents of otherPrimeInfo are copied to protect against subsequent modification when constructing this object.

**Parameters:**modulus - the modulus n.publicExponent - the public exponent e.privateExponent - the private exponent d.primeP - the prime factor p of n.primeQ - the prime factor q of n.primeExponentP - this is d mod (p-1).primeExponentQ - this is d mod (q-1).crtCoefficient - the Chinese Remainder Theorem coefficient q-1 mod p.otherPrimeInfo - triplets of the rest of primes, null can be specified if there are only two prime factors (p and q). **Throws:** [NullPointerException](http://docs.google.com/java/lang/NullPointerException.html) - if any of the parameters, i.e. modulus, publicExponent, privateExponent, primeP, primeQ, primeExponentP, primeExponentQ, crtCoefficient, is null. [IllegalArgumentException](http://docs.google.com/java/lang/IllegalArgumentException.html) - if an empty, i.e. 0-length, otherPrimeInfo is specified.

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

### getPublicExponent

public [BigInteger](http://docs.google.com/java/math/BigInteger.html) **getPublicExponent**()

Returns the public exponent.

**Returns:**the public exponent.

### getPrimeP

public [BigInteger](http://docs.google.com/java/math/BigInteger.html) **getPrimeP**()

Returns the primeP.

**Returns:**the primeP.

### getPrimeQ

public [BigInteger](http://docs.google.com/java/math/BigInteger.html) **getPrimeQ**()

Returns the primeQ.

**Returns:**the primeQ.

### getPrimeExponentP

public [BigInteger](http://docs.google.com/java/math/BigInteger.html) **getPrimeExponentP**()

Returns the primeExponentP.

**Returns:**the primeExponentP.

### getPrimeExponentQ

public [BigInteger](http://docs.google.com/java/math/BigInteger.html) **getPrimeExponentQ**()

Returns the primeExponentQ.

**Returns:**the primeExponentQ.

### getCrtCoefficient

public [BigInteger](http://docs.google.com/java/math/BigInteger.html) **getCrtCoefficient**()

Returns the crtCoefficient.

**Returns:**the crtCoefficient.

### getOtherPrimeInfo

public [RSAOtherPrimeInfo](http://docs.google.com/java/security/spec/RSAOtherPrimeInfo.html)[] **getOtherPrimeInfo**()

Returns a copy of the otherPrimeInfo or null if there are only two prime factors (p and q).

**Returns:**the otherPrimeInfo. Returns a new array each time this method is called.

| | [**Overview**](http://docs.google.com/overview-summary.html) | [**Package**](http://docs.google.com/package-summary.html) | **Class** | [**Use**](http://docs.google.com/class-use/RSAMultiPrimePrivateCrtKeySpec.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/spec/RSAKeyGenParameterSpec.html)   [**NEXT CLASS**](http://docs.google.com/java/security/spec/RSAOtherPrimeInfo.html) | [**FRAMES**](http://docs.google.com/index.html?java/security/spec/RSAMultiPrimePrivateCrtKeySpec.html)    [**NO FRAMES**](http://docs.google.com/RSAMultiPrimePrivateCrtKeySpec.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).