| | [**Overview**](http://docs.google.com/overview-summary.html) | [**Package**](http://docs.google.com/package-summary.html) | **Class** | [**Use**](http://docs.google.com/class-use/DHParameterSpec.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/javax/crypto/spec/DHGenParameterSpec.html)   [**NEXT CLASS**](http://docs.google.com/javax/crypto/spec/DHPrivateKeySpec.html) | [**FRAMES**](http://docs.google.com/index.html?javax/crypto/spec/DHParameterSpec.html)    [**NO FRAMES**](http://docs.google.com/DHParameterSpec.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |
| SUMMARY: NESTED | FIELD | [CONSTR](#3znysh7) | [METHOD](#2et92p0) | DETAIL: FIELD | [CONSTR](#3dy6vkm) | [METHOD](#2s8eyo1) |

## **javax.crypto.spec**

Class DHParameterSpec

[java.lang.Object](http://docs.google.com/java/lang/Object.html)  
 **javax.crypto.spec.DHParameterSpec**

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

public class **DHParameterSpec**extends [Object](http://docs.google.com/java/lang/Object.html)implements [AlgorithmParameterSpec](http://docs.google.com/java/security/spec/AlgorithmParameterSpec.html)

This class specifies the set of parameters used with the Diffie-Hellman algorithm, as specified in PKCS #3: *Diffie-Hellman Key-Agreement Standard*.

A central authority generates parameters and gives them to the two entities seeking to generate a secret key. The parameters are a prime p, a base g, and optionally the length in bits of the private value, l.

It is possible that more than one instance of parameters may be generated by a given central authority, and that there may be more than one central authority. Indeed, each individual may be its own central authority, with different entities having different parameters.

Note that this class does not perform any validation on specified parameters. Thus, the specified values are returned directly even if they are null.

**Since:** 1.4 **See Also:**[KeyAgreement](http://docs.google.com/javax/crypto/KeyAgreement.html)

| **Constructor Summary** | |
| --- | --- |
| [**DHParameterSpec**](http://docs.google.com/javax/crypto/spec/DHParameterSpec.html#DHParameterSpec(java.math.BigInteger,%20java.math.BigInteger))([BigInteger](http://docs.google.com/java/math/BigInteger.html) p, [BigInteger](http://docs.google.com/java/math/BigInteger.html) g)            Constructs a parameter set for Diffie-Hellman, using a prime modulus p and a base generator g. |
| [**DHParameterSpec**](http://docs.google.com/javax/crypto/spec/DHParameterSpec.html#DHParameterSpec(java.math.BigInteger,%20java.math.BigInteger,%20int))([BigInteger](http://docs.google.com/java/math/BigInteger.html) p, [BigInteger](http://docs.google.com/java/math/BigInteger.html) g, int l)            Constructs a parameter set for Diffie-Hellman, using a prime modulus p, a base generator g, and the size in bits, l, of the random exponent (private value). |

| **Method Summary** | |
| --- | --- |
| [BigInteger](http://docs.google.com/java/math/BigInteger.html) | [**getG**](http://docs.google.com/javax/crypto/spec/DHParameterSpec.html#getG())()            Returns the base generator g. |
| int | [**getL**](http://docs.google.com/javax/crypto/spec/DHParameterSpec.html#getL())()            Returns the size in bits, l, of the random exponent (private value). |
| [BigInteger](http://docs.google.com/java/math/BigInteger.html) | [**getP**](http://docs.google.com/javax/crypto/spec/DHParameterSpec.html#getP())()            Returns the prime modulus p. |

| **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** |
| --- |

### DHParameterSpec

public **DHParameterSpec**([BigInteger](http://docs.google.com/java/math/BigInteger.html) p,  
 [BigInteger](http://docs.google.com/java/math/BigInteger.html) g)

Constructs a parameter set for Diffie-Hellman, using a prime modulus p and a base generator g.

**Parameters:**p - the prime modulusg - the base generator

### DHParameterSpec

public **DHParameterSpec**([BigInteger](http://docs.google.com/java/math/BigInteger.html) p,  
 [BigInteger](http://docs.google.com/java/math/BigInteger.html) g,  
 int l)

Constructs a parameter set for Diffie-Hellman, using a prime modulus p, a base generator g, and the size in bits, l, of the random exponent (private value).

**Parameters:**p - the prime modulusg - the base generatorl - the size in bits of the random exponent (private value)

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

### getP

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

Returns the prime modulus p.

**Returns:**the prime modulus p

### getG

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

Returns the base generator g.

**Returns:**the base generator g

### getL

public int **getL**()

Returns the size in bits, l, of the random exponent (private value).

**Returns:**the size in bits, l, of the random exponent (private value), or 0 if this size has not been set

| | [**Overview**](http://docs.google.com/overview-summary.html) | [**Package**](http://docs.google.com/package-summary.html) | **Class** | [**Use**](http://docs.google.com/class-use/DHParameterSpec.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/javax/crypto/spec/DHGenParameterSpec.html)   [**NEXT CLASS**](http://docs.google.com/javax/crypto/spec/DHPrivateKeySpec.html) | [**FRAMES**](http://docs.google.com/index.html?javax/crypto/spec/DHParameterSpec.html)    [**NO FRAMES**](http://docs.google.com/DHParameterSpec.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |
| SUMMARY: NESTED | FIELD | [CONSTR](#3znysh7) | [METHOD](#2et92p0) | DETAIL: FIELD | [CONSTR](#3dy6vkm) | [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).