| | [**Overview**](http://docs.google.com/overview-summary.html) | **Package** | Class | [**Use**](http://docs.google.com/package-use.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 PACKAGE**](http://docs.google.com/javax/crypto/interfaces/package-summary.html)   [**NEXT PACKAGE**](http://docs.google.com/javax/imageio/package-summary.html) | [**FRAMES**](http://docs.google.com/index.html?javax/crypto/spec/package-summary.html)    [**NO FRAMES**](http://docs.google.com/package-summary.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |

## Package javax.crypto.spec

Provides classes and interfaces for key specifications and algorithm parameter specifications.

**See:**

[**Description**](#3znysh7)

| **Class Summary** | |
| --- | --- |
| [**DESedeKeySpec**](http://docs.google.com/javax/crypto/spec/DESedeKeySpec.html) | This class specifies a DES-EDE ("triple-DES") key. |
| [**DESKeySpec**](http://docs.google.com/javax/crypto/spec/DESKeySpec.html) | This class specifies a DES key. |
| [**DHGenParameterSpec**](http://docs.google.com/javax/crypto/spec/DHGenParameterSpec.html) | This class specifies the set of parameters used for generating Diffie-Hellman (system) parameters for use in Diffie-Hellman key agreement. |
| [**DHParameterSpec**](http://docs.google.com/javax/crypto/spec/DHParameterSpec.html) | This class specifies the set of parameters used with the Diffie-Hellman algorithm, as specified in PKCS #3: *Diffie-Hellman Key-Agreement Standard*. |
| [**DHPrivateKeySpec**](http://docs.google.com/javax/crypto/spec/DHPrivateKeySpec.html) | This class specifies a Diffie-Hellman private key with its associated parameters. |
| [**DHPublicKeySpec**](http://docs.google.com/javax/crypto/spec/DHPublicKeySpec.html) | This class specifies a Diffie-Hellman public key with its associated parameters. |
| [**IvParameterSpec**](http://docs.google.com/javax/crypto/spec/IvParameterSpec.html) | This class specifies an *initialization vector* (IV). |
| [**OAEPParameterSpec**](http://docs.google.com/javax/crypto/spec/OAEPParameterSpec.html) | This class specifies the set of parameters used with OAEP Padding, as defined in the [PKCS #1](http://www.ietf.org/rfc/rfc3447.txt) standard. |
| [**PBEKeySpec**](http://docs.google.com/javax/crypto/spec/PBEKeySpec.html) | A user-chosen password that can be used with password-based encryption (*PBE*). |
| [**PBEParameterSpec**](http://docs.google.com/javax/crypto/spec/PBEParameterSpec.html) | This class specifies the set of parameters used with password-based encryption (PBE), as defined in the [PKCS #5](http://www.ietf.org/rfc/rfc2898.txt) standard. |
| [**PSource**](http://docs.google.com/javax/crypto/spec/PSource.html) | This class specifies the source for encoding input P in OAEP Padding, as defined in the [PKCS #1](http://www.ietf.org/rfc/rfc3447.txt) standard. |
| [**PSource.PSpecified**](http://docs.google.com/javax/crypto/spec/PSource.PSpecified.html) | This class is used to explicitly specify the value for encoding input P in OAEP Padding. |
| [**RC2ParameterSpec**](http://docs.google.com/javax/crypto/spec/RC2ParameterSpec.html) | This class specifies the parameters used with the [*RC2*](http://www.ietf.org/rfc/rfc2268.txt) algorithm. |
| [**RC5ParameterSpec**](http://docs.google.com/javax/crypto/spec/RC5ParameterSpec.html) | This class specifies the parameters used with the [*RC5*](http://www.ietf.org/rfc/rfc2040.txt) algorithm. |
| [**SecretKeySpec**](http://docs.google.com/javax/crypto/spec/SecretKeySpec.html) | This class specifies a secret key in a provider-independent fashion. |

## Package javax.crypto.spec Description

Provides classes and interfaces for key specifications and algorithm parameter specifications.

A key specification is a transparent representation of the key material that constitutes a key. A key may be specified in an algorithm-specific way, or in an algorithm-independent encoding format (such as ASN.1). This package contains key specifications for Diffie-Hellman public and private keys, as well as key specifications for DES, Triple DES, and PBE secret keys.

An algorithm parameter specification is a transparent representation of the sets of parameters used with an algorithm. This package contains algorithm parameter specifications for parameters used with the Diffie-Hellman, DES, Triple DES, PBE, RC2 and RC5 algorithms.

## Package Specification

* PKCS #3: Diffie-Hellman Key-Agreement Standard, Version 1.4, November 1993.
* PKCS #5: Password-Based Encryption Standard, Version 1.5, November 1993
* Federal Information Processing Standards Publication (FIPS PUB) 46-2: Data Encryption Standard (DES)

## Related Documentation

For documentation that includes information about algorithm parameter and key specifications, please see:

* [**JavaTM Cryptography Architecture API Specification and Reference**](http://docs.google.com/technotes/guides/security/crypto/CryptoSpec.html)
* [**How to Implement a Provider for the JavaTM Cryptography Architecture**](http://docs.google.com/technotes/guides/security/crypto/HowToImplAProvider.html)

**Since:** JCE1.2

| | [**Overview**](http://docs.google.com/overview-summary.html) | **Package** | Class | [**Use**](http://docs.google.com/package-use.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 PACKAGE**](http://docs.google.com/javax/crypto/interfaces/package-summary.html)   [**NEXT PACKAGE**](http://docs.google.com/javax/imageio/package-summary.html) | [**FRAMES**](http://docs.google.com/index.html?javax/crypto/spec/package-summary.html)    [**NO FRAMES**](http://docs.google.com/package-summary.html)     [**All Classes**](http://docs.google.com/allclasses-noframe.html) |

[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).