



# Java : Encryption and Decryption of Data using AES algorithm with example code

There are many problems when you try encrypting a string such password, credit card nos, phone no. etc ie

1. which algorithm to use.
2. how to store the generated Key in the database.
3. should i use MD5, AES etc.

Here is the question to all your answers.  
After spending sometime on this i finally got the best algorithm that a person can use to encrypt and decrypt data while he/she also wants to store those encrypted strings and later on want to decrypt it while retrieving the data.

Many people face problem while decrypting the encrypted data as the KEY used for encryption if stored as String in database then it becomes very tough to use that string as the KEY. So below is the code where you only need to store the encrypted code and not the key. The decryption will take place as an when wanted.

For encryption we must use a secret key along with an algorithm. In the following example we use an algorithm called **AES 128** and the bytes of the word

## Translate

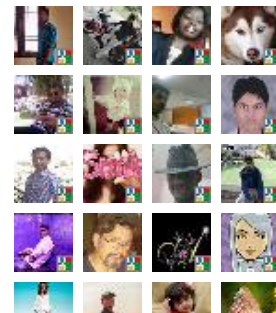
Select Language ▼

## Followers

Join this site  
with Google Friend Connect



Members (155) [More »](#)



## Popular Posts

[Java : Encryption and Decryption of Data using AES algorithm with example code](#)

There are many problems when you try encrypting a string such password, credit card nos, phone no. etc ie 1. which algorithm to use. 2. ...

[QuickSort Algorithm Tutorial](#)

We have already done tutorial on Merge Sort and a tutorial on Heap Sort

(Array Based) with both having a time complexity of  $O(n \log n)$ . ...

"TheBestSecretKey" as the secret key (the best secret key we found in this world). AES algorithm can use a key of 128 bits (16 bytes \* 8); so we selected that key.

```
package nomad;
```

```
import java.security.*;
```

```
import java.security.spec.InvalidKeySpecException;
```

```
import javax.crypto.*;
```

```
import sun.misc.*;
```

```
public class AESencrp {
```

```
    private static final String ALGO = "AES";
```

```
    private static final byte[] keyValue =
```

```
        new byte[] { 'T', 'h', 'e', 'B', 'e', 's', 't',
```

```
        'S', 'e', 'c', 'r', 'e', 't', 'K', 'e', 'y' };
```

```
public static String encrypt(String Data) throw:
```

```
    Key key = generateKey();
```

```
    Cipher c = Cipher.getInstance(ALGO);
```

```
    c.init(Cipher.ENCRYPT_MODE, key);
```

```
    byte[] encVal = c.doFinal(Data.getBytes());
```

```
    String encryptedValue = new BASE64Encoder().
```

```
        return encryptedValue;
```

## HeapSort ( array Based) implementation in Java

There are two types of heaps. First one is Max heap and second one is Min heap. Heap (Max/Min) is a special type of binary tree. The roots o...



Image



Processing :

Edge Detection

## of Image Using MATLAB

There are many operators in MATLAB for finding images

1. Sobels Operator
2. Roberts Operator
3. Prewitts Operator
4. Laplacian of Gauss...

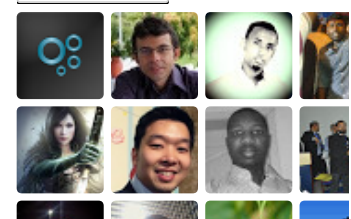
## Counting Sort Algorithm with Example

After a long interval of time I am writing a post on ALGORITHMS . After writing posts on Heap Sort , Merge Sort and Insertion Sort , I de...

Code2Learn on Google+

Code 2 Learn

Follow



}

```

public static String decrypt(String encryptedI
    Key key = generateKey();
    Cipher c = Cipher.getInstance(ALGO);
    c.init(Cipher.DECRYPT_MODE, key);
    byte[] decordedValue = new BASE64Decode
    byte[] decValue = c.doFinal(decordedValue);
    String decryptedValue = new String(decVal
    return decryptedValue;
}

private static Key generateKey() throws Exce
    Key key = new SecretKeySpec(keyValue, AL
    return key;
}

}

```



We use "generateKey()" method to generate a secret key for AES algorithm with a given key.

Below is the code how you can use the above encryption algorithm.

```

package nomad;

```

```

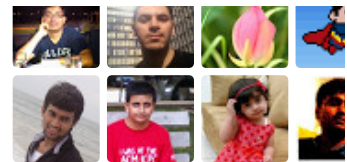
public class Checker {

```

```

    public static void main(String[] args) throws

```



325 have us in circles

## Tutorials

[algorithms](#)  
[CodeIgniter](#)  
[data mining](#)  
[Data Warehouse](#)  
[excel tutorial](#)  
[image processing tutorial](#)  
[java tutorial](#)  
[javascript tutorial](#)  
[jdbc tutorial](#)  
[php tutorial](#)  
[problems](#)  
[python tutorial](#)  
[sql tutorial](#)  
[Teradata](#)  
[Unix program](#)  
[visual basic tutorial](#)

## Blog Archive

- 2015 (5)
- 2013 (6)
- 2012 (44)
- ▼ 2011 (67)
  - December (5)
  - November (18)
  - October (6)
  - September (6)
  - August (2)
  - July (4)
  - ▼ June (4)

[Java : Encryption and  
Decryption of Data  
using AES...](#)

[Microsoft SQL Server  
2008 installation](#)

```

String password = "mypassword";
String passwordEnc = AESencrp.encrypt(pas
String passwordDec = AESencrp.decrypt(pas

System.out.println("Plain Text : " + passwor
System.out.println("Encrypted Text : " + pas
System.out.println("Decrypted Text : " + pas
    }
}

```

[tutorial](#)[Java Servlet Basics](#)[Image Processing :](#)[Morphology based](#)[Segmentation u...](#)[► May \(4\)](#)[► April \(4\)](#)[► March \(2\)](#)[► February \(4\)](#)[► January \(8\)](#)[► 2010 \(9\)](#)

Code 2 Learn. Powered by

[Blogger.](#)

## NOTE :

I have got emails from user saying that the above code gives error when using in ECLIPSE. Error like :

Access restriction: The type BASE64Decoder is not accessible due

to restriction on required library C:\Program

Files\Java\jre6\lib\rt.jar

So to avoid this do the following :

\* GO to **Window-->Preferences--**

**>Java-->Compiler--**

**>Error/Warnings.**

\* Select **Deprecated and Restricted API**. Change it to warning.

\* Change **forbidden and Discouraged Reference** and change it to warning. (or as your need.)

Note: 12-12-2013

One of our readers (Saurabh Mehta) has

One of our readers (Saurabh Mogner), has given a solution about some issue:

Issue: Issue Of Access Restriction

Solution: Removing JRE system Library then adding it back from Build Path settings in the project properties.

🕒 6/28/2011 👤 FARHAN KHWAJA 🏷️ AES, DECRYPTION JAVA, ENCRYPTION JAVA, JAVA AES, JAVA TUTORIAL 💬 31 COMMENTS

### SHARE THIS POST:

Tweet

7

G+1

6

Share



### Related Posts:



#### Java : Encryption and Decryption of Data using AES algorithm with example code

There are many problems when you try encrypting a string such password, credit card nos, phone no. etc ie 1. which algorithm to use. 2. how to store the generated Key in the database. 3. should i use MD5, AES etc. Here is ... [Read More](#)

← Newer Post

Home

Older Post →

31 comments:

**auto cars** July 31, 2011 at 8:37 AM

what a great post

thanks

**Donky**

reply

**vivek** October 19, 2011 at 9:39 AM

awesome...thanks dude

Reply

**Anonymous** November 22, 2011 at 1:26 AM

good one.....quite helpful

Reply



**Farhan Khwaja** November 22, 2011 at 6:52 AM

@Anonymous thank you dear..

Reply



**Jason** November 28, 2011 at 4:22 PM

The above code is still really basic its not the best we can do with AES.

```
byte[] key = null; // TODO
```

```
byte[] input = null; // TODO
```

```
byte[] output = null;
```

```
SecretKeySpec keySpec = null;
```

```
keySpec = new SecretKeySpec(key, "AES");
```

```
Cipher cipher =
```

```
Cipher.getInstance("AES/CBC/PKCS7Padding");
```

```
cipher.init(Cipher.ENCRYPT_MODE, keySpec);
```

```
output = cipher.doFinal(input)
```

an you can pad the password to 256 and not 128

Reply



**farhan khwaja** November 28, 2011 at 8:08 PM

@Jason Yes its a basic code. I never said its the best Code using AES. I just posted the Basic structure of how to use AES in java

Reply

**Javin @ ArrayList vs Vector in java** November 29, 2011 at 5:28 AM

Nice post farhan, spring security also provides way to encrypt password outofbox using MD5 and other encryption algorithm. Though this can be used a nice utility.

Thanks

Javin

**Ldap authentication using Spring with Example**

Reply



**Student** December 17, 2011 at 12:31 AM

Hello

i have an error with this code.. could you help me ?  
the error is class, interface, or enum expected;

Reply



**farhan khwaja** December 17, 2011 at 3:07 AM

@Student Make sure the class name and the file name both are the exact same..

I made this program in ECLIPSE IDE.. in that i make a project and then in that i made a package named 'nomad' and inside it i had these two classes.

Here is the link on **Java programming with eclipse : Basic**

Reply



**Unknown** April 1, 2012 at 2:05 AM

Thanks!

Small improvement to the code is to change the usage of sun.misc.BASE64 to Apache Commons Codec which provides Base64  
<http://commons.apache.org/codec/api-release/org/apache/commons/codec/binary/Base64>.

html

You should be using `java.sun.misc.base64` even in Java 6, because it's not part of the API of java.

For more info:

<http://java.sun.com/products/jdk/faq/faq-sun-packages.html>

Reply



**farhan khwaja** April 1, 2012 at 2:13 AM

@Unknown Thank you for the information..

Reply

**fares Berramdane** January 2, 2015 at 3:53 PM



Split Sort Java Code SVP?

Reply



**Kanika Pathak** February 13, 2015 at 10:16 AM

is there any method for steganography like this??????????

Reply

Replies



**Admin** February 14, 2015 at 1:50 PM

Well I don't have any experience on Steganography. But yeah there are blog posts available.

**Anonymous** March 8, 2015 at 12:22 AM

hey there could you please help me out i have an error with this code posted above and it says "Base64.decode cannot be resolved to a type"

Reply



**Anonymous** March 8, 2015 at 12:28 AM

hey there could you please help me out i've an error that says "Base64.decode cannot be resolved to a type"

[Reply](#)



**mikky** March 19, 2015 at 11:46 PM

*This comment has been removed by a blog administrator.*

[Reply](#)



**Rishabh Upadhyay** March 30, 2015 at 4:46 AM

how to make it with with password i.e

we pass the data and the password to encrypt with...

??

i tried creating a function which takes the password ,converts it to byte and then store it in keyValue

but it gives a error of "Invalid AES key length: 10 bytes"

plz reply ..i need it for my project

[Reply](#)



**Pedro Cortez** May 26, 2015 at 1:07 PM

What is the correct way to save the keyValue? (java keystore?)

[Reply](#)

**David** May 28, 2015 at 11:44 PM

Thanks, that was exactly wath I was looking for. But since Base64 is now in Java8, it's better to use Base64.getEncoder() (import java.util.Base64;) rather than new BASE64Encoder().encode()

[Reply](#)

**Anonymous** June 26, 2015 at 4:03 AM

very good.. works with eclipse

[Reply](#)



**Ankita** June 30, 2015 at 3:18 AM

hello...can u give me MATLAB code of AES for images

[Reply](#)



**Shweta Garg** July 31, 2015 at 6:48 AM

Thank you for writing this. It was very useful for me.

[Reply](#)



**Thoha** August 13, 2015 at 5:58 PM

useful for me, many thanks!

[Reply](#)



**Ityav Nobles** August 28, 2015 at 9:47 PM

You have really save me from a very big challenge that gave me sleepless nite.

I was just looking for something like this to know my way forward and all i could get from Stackoverflow was the first class AESencrp but how to checkout was another brain dump.

[Reply](#)

[Replies](#)



**Unknown** October 27, 2015 at 5:25 AM

I believe you have got this code working.

I'm getting this error when i run the file!

AESencrp.java:21: warning:

BASE64Encoder is internal proprietary API and may be removed in a future

release

```
release
```

```
String    encryptedValue    =    new
BASE64Encoder().encode(encVal);
```

```
^
```

```
AESEncrp.java:29:          warning:
BASE64Decoder is internal proprietary
API and may be removed in a future
```

```
release
```

```
byte[]    decordedValue    =    new
BASE64Decoder().decodeBuffer(encrypte
dData);
```

```
^
```

```
AESEncrp.java:35: error: cannot find
symbol
```

```
Key key = new SecretKeySpec(keyValue,
ALGO);
```

```
^
```

```
symbol: class SecretKeySpec
```

```
location: class AESEncrp
```

```
1 error
```

```
2 warnings
```

## Reply

**Karthi M** August 31, 2015 at 8:08 PM

Very Useful .. Thanks a lot

Reply



**Gajendra Singh** October 7, 2015 at 3:31 AM

working

Reply



**Unknown** October 12, 2015 at 12:59 PM

Very useful. Thank you.

Reply



**Levante Tech** January 11, 2016 at 8:41 PM

Hi, Thanks a lot, it is working and very clear about it

ni, thank a lot, it is working and very clear about it.

[Reply](#)



**hossein ameri** February 21, 2016 at 2:45 PM

very useful ..... But a question. Why this program don't use many characters for its output? after encrypting, i can see only +/=0-9A-Za-z chars, its for AES algorithm or its programming

[Reply](#)

Enter your comment...

Comment as: VISHWARUP ₹ ▼

Sign out

Publish

Preview

☐ Notify me