Core Java,J2EE,Spring,Hibernate,JAX-RS,EJB Tutorials

| Home | Core Java | Spring | Hibernate | JAX-RS | Servlets | EJB | Maven | JAX-WS | Log4j | RMI | J2EE | About Author | Contac

Tuesday, September 03, 2013

Data Encryption Decryption using DES Algorithm in Java

G+1 +23 Recommend this on Google Posted by Anuj Patel at 9/03/2013

Encryption is process of converting plan text to cypher text using encryption algorithm and encryption Key.
Decryption is reverse process of encryption which recover original data from encrypted data using decryption key.

Here, One should understood **Cryptography** concept before moving into encryption and description world. It's basically making communication private - Protect Sensitive Information. Refer to wiki for more details.

Types of Cryptography :

1. **Symmetric**
2. **ASymmetric**

Symmetric Cryptography:

- Here, Encryption and decryption parties uses same secret key as private key
- Using this private Key, they will encrypt or decrypt data.
- common symmetric algorithm are **DES(Data Encryption Standard),3DES,AES(Advance Encryption Standard)**
- **DES** accepts 64 bits.
- **3DES -** it works using cascading three instance of DES**.**
- **AES** is advance one. it accepts 128,192,256 bits. **- Recommended one**

ASymmetric Cryptography:

- It uses concept of public key and private key
- We can distribute public key to anyone and using this public key they can encrypt data
- Encrypted Data only can be decrypted by one who has associated private key
- Here, Encryption Key and Decryption Key should be different.

Ex. RSA algorithm named after Rivest,Shamir and Adleman.

Please refer to Cipher API Documentation before using.

Java Program for Data Encryption Decryption using DES Algorithm :

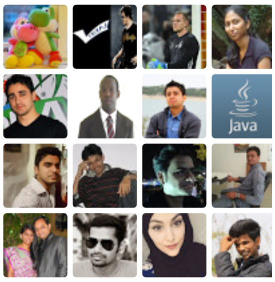
view plain print ?

```java
package com.anuj.security.encryption;

import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;

import javax.crypto.BadPaddingException;
import javax.crypto.Cipher;
import javax.crypto.IllegalBlockSizeException;
import javax.crypto.KeyGenerator;
import javax.crypto.NoSuchPaddingException;
import javax.crypto.SecretKey;

/**
 *
 * @author Anuj
 *
 */
public class DESEncryptionDecryption {

 private static Cipher encryptCipher;
 private static Cipher decryptCipher;

 public static void main(String[] args) {
  try {
   KeyGenerator keygenerator = KeyGenerator.getInstance("DES");
   SecretKey secretKey = keygenerator.generateKey();

   encryptCipher = Cipher.getInstance("DES/ECB/PKCS5Padding");
   encryptCipher.init(Cipher.ENCRYPT_MODE, secretKey);
   byte[] encryptedData = encryptData("Classified Information!");

   decryptCipher = Cipher.getInstance("DES/ECB/PKCS5Padding");
   decryptCipher.init(Cipher.DECRYPT_MODE, secretKey);
   decryptData(encryptedData);

  } catch (NoSuchAlgorithmException e) {
   e.printStackTrace();
  } catch (NoSuchPaddingException e) {
   e.printStackTrace();
  } catch (InvalidKeyException e) {
   e.printStackTrace();
  } catch (IllegalBlockSizeException e) {
   e.printStackTrace();
  } catch (BadPaddingException e) {
   e.printStackTrace();
  }

```

G+ Followers

Goldenpackagebyanuj

Follow



39 have us in circles

Subscribe Feeds

29 readers BY FEEDBURNER

Clouds

Android (3) Core Java (9 EncryptionDecryption (3) Hibernet (2) J2ME (2) Java Algorithms (13) Java N java8 (2) JAX-RS (5) JAX-WS (1) JMS Maven (5) mysql (2) Python (1) RMI (1 Spring (20) Weblogic (3)

About Me

Anuj Patel

G+ Follow

Sr. J2EE Software

View my complete

Follow @AnujPatel01

My Work

GitHub Repositories

Total Pageviews

187452

Get Latest Posts

Email address...

Translate

Select Language ▼

```
}

/**
 * Encrypt Data
 * @param data
 * @return
 * @throws IllegalBlockSizeException
 * @throws BadPaddingException
 */
private static byte[] encryptData(String data)
  throws IllegalBlockSizeException, BadPaddingException {
 System.out.println("Data Before Encryption :" + data);
 byte[] dataToEncrypt = data.getBytes();
 byte[] encryptedData = encryptCipher.doFinal(dataToEncrypt);
 System.out.println("Encryted Data: " + encryptedData);

 return encryptedData;
}

/**
 * Decrypt Data
 * @param data
 * @throws IllegalBlockSizeException
 * @throws BadPaddingException
 */
private static void decryptData(byte[] data)
  throws IllegalBlockSizeException, BadPaddingException {
 byte[] textDecrypted = decryptCipher.doFinal(data);
 System.out.println("Decryted Data: " + new String(textDecrypted));
}
}
```

Here,
DES = Data Encryption Standard.
ECB = Electronic Codebook mode.
PKCS5Padding = PKCS #5-style padding

While initializing Cipher, we can pass Key,Certificate and AlgorithParameters as well.

Output :

```
Data Before Encryption :Classified Information!
Encryted Data: [B@bc6007
Decryted Data: Classified Information!
```

Author : Anuj Patel
Blog : http://goldenpackagebyanuj.blogspot.in/

Labels: Core Java, EncryptionDecryption, Java Algorithms

Anuj Patel
Sr. J2EE Software Developer

16 comments

Add a comment as VISHWARUP SINGH BAGHEL

Top comments

Anuj Patel shared this 2 years ago - Java (Java)

+7 1

Prakash Tekam 2 years ago
good

Caleb Wilson 2 years ago +1
Have you ever made your own encryption algorithm?

Anshu Kumar 2 years ago - Shared publicly
good

1 · Reply

Anuj Patel 2 years ago (edited) - Shared publicly
+**Joseph Greenawalt** - for Asymmetric Algorithm example using public and Private key concept - refer to http://goldenpackagebyanuj.blogspot.in/2013/10/RSA-Encryption-Decryption-algorithm-in-java.html

+1 1

dibyendu tiwary 2 years ago
you can get a domain name for 500/- per year .. that way people who have blogs blocked can access your

Live Traffic Feed

A visitor from Mumbai, Mahara viewed "Core Java,J2EE,Spring,Hibernate,JA RS,EJB Tutorials: RSA Public Encryption and Private Key Decryption using Java" 19 mins

A visitor from Nagpur, Maharas viewed "Core Java,J2EE,Spring,Hibernate,JA RS,EJB Tutorials: RSA Public Encryption and Private Key Decryption using Java" 1 hr 22 ago

A visitor from Hyderabad, And "Core Java,J2EE,Spring,Hibern Tutorials: java.lang.ClassNotFo org.springframework.web.servl 1 hr 27 mins ago

A visitor from India viewed "C Java,J2EE,Spring,Hibernate,JA RS,EJB Tutorials: How to write Custom JSR 303 Validation usi ConstraintValidator" 1 hr 54 mi

A visitor from Hyderabad, And Pradesh viewed "Core Java,J2EE,Spring,Hibernate,JA RS,EJB Tutorials: Common Aw Interfaces used in Spring" 2 hrs

A visitor from Cairo, Al Qahira viewed "Core Java,J2EE,Spring,Hibernate,JA RS,EJB Tutorials: Hibernate - S and Retrieve Data using XML" 3 hrs

A visitor from Rutherford, New viewed "Core Java,J2EE,Spring,Hibernate,JA RS,EJB Tutorials: RSA Public Encryption and Private Key Decryption using Java" 3 hrs 26 mins ago

A visitor from India viewed "C Java,J2EE,Spring,Hibernate,JA RS,EJB Tutorials: Spring - java.lang.ClassNotFoundExcep org.aopalliance.aop.Advice" 3 h mins ago

A visitor from Malaysia viewed Java,J2EE,Spring,Hibernate,JA RS,EJB Tutorials: RSA Public Encryption and Private Key Decryption using Java" 4 hrs 7 ago

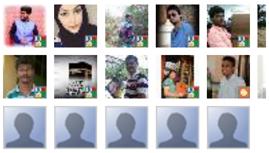
A visitor from Jacksonville, Flo viewed "Core Java,J2EE,Spring,Hibernate,JA RS,EJB Tutorials: Listener

Real-time view · Get Feedjit

Followers

Join this site
with Google Friend Connect

Members (17)



Already a member? Sign in

Labels

Core Java	(93)
j2EE	(50)
Spring	(20)
Java Algorithms	(13)
JAX-RS	(5)
Java Networking	(5)
Maven	(5)
Servlets	(4)
Android	(3)
EJB	(3)
EncryptionDecryption	(3)
Weblogic	(3)
Hibernet	(2)
J2ME	(2)

site

Gangapatnam Anil 2 weeks ago - Shared publicly

Hi Anuj patel,Please Tell me Your Mail id,i have some doubts in This Topic

1 · Reply

Muhammet Öztürk 2 years ago - Shared publicly

thank you

1 · Reply

Asma Mubarak 4 months ago - Shared publicly

What if I didn't want the key to be generated,

I mean if I wanted to assign it by my self

+1 1 · Reply

Prakash Tekam 2 years ago - Shared publicly

very nice

+2 1 · Reply

Muhammet Öztürk 2 years ago - Shared publicly

very nice

1 · Reply

shravan kumar 1 year ago - Shared publicly

With out using built in libraries .Can i have the code for DES which encrypt and decrypt the String message!! Can i have the code for this ???

1

Anuj Patel shared this 1 year ago - Java (Java)

+1 1

Anuj Patel 1 year ago - Shared publicly

Thanks All for Stopping by this blog post !

1

Goldenpackagebyanuj shared this via Google+ 1 year ago (edited) - Shared publicly

1 · Reply

Abhi Singh 1 year ago - Shared publicly

package com.anuj.security.encryption; m anuj is self make package ;

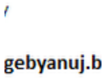
1 · Reply

JMS (2)
java8 (2)
mysql (2)
JAX-WS (1)
Log4j (1)
Python (1)
RMI (1)

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

Popular Posts



RSA Public Key Encryption and Private Key Decryption using Java
In Previous Post, I have discussed about What is Cryptography, What are Types of it and How we can encrypt and decrypt data using DES Algor...

Data Encryption Decryption using DES Algorithm in Java
Encryption is process of converting plan text to cypher text using encryption algorithm and encryption Key. Decryption is reverse proces...

How to write Custom JSR 303 Validation using ConstraintValidator

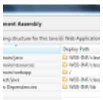
Subscribe To

Posts

Comments

G+1 3

What is JSR 303? JSR 303 is Java Bean Validation framework which comes as part of J2EE 6. So in order to use classes specified by them, f...

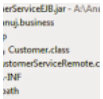


java.lang.ClassNotFoundException: org.springframework.web.servlet.DispatcherServlet

While developing SpringMVC application in Eclipse, All require dependencies has been added to maven dependencies in pom.xml. Yet running ap...

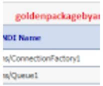
javax.validation.ValidationException: Unable to create a Configuration, because no Bean Validation provider could be found

I was working on writing JSR 303 Custom Validation to validate Email Address and encountered with following exception. javax.validation....



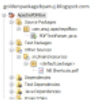
EJB 3.1 SessionBean Example with Remote Interface using WebLogic 12.1.1

EJB stands for Enterprise Java Bean. If you are not similar with EJB, Please read below in order to move ahead with "Creating EJB 3....



Reading Messages from JMS Queue in Weblogic 12.1.1 using Java

Suppose I have Queue configured in Weblogic and I want to write application in which Program A will put messages to this queue and Progra...



Apache PDFBox - Parse PDF to text using java

Apache PDFBox is library which allows you to create PDF documents, manipulate of Existing documents and even extract content from existing...

Common Aware Interfaces used in Spring

If You are developing application using Spring then sometime it's important that your beans aware about Spring IOC container resources....

Spring JdbcTemplate and Spring SimpleJdbcTemplate difference with Example

To use the SimpleJdbcTemplate you need to use JDK 1.5 or higher. SimpleJdbcTemplate takes advantage of the Java 5 language features like ...

Goldenpackagebyanuj. Powered by Blogger.