LOGIC & CODE

ACTIVITY ANDROID CORE JAVA COUCHBASE JSF JSP KOTLIN MEMBERS RESTFUL

SPRING BOOT STRUTS UNIT TESTING

String Encryption and Decryption in java using Cipher class

18th June 2015 Nirmal Dhara CoreJava, Java Security 4

SEARCH …

60

Nirmal Dhara
1,131
● 9 ● 22

EXAMPLES

- Android
- Apache POI
- CoreJava
- Couchbase
- Java Security
- Jquery
- Jsp
- Junit

There are many ways to encrypt and decrypt String in java. I will discuss how to encrypt or decrypt data using Cipher class. Cipher class is the part of Java Cryptographic Extension (JCE) framework.

The Cipher class is part of javax.crypto package.

How it works?

Encryption = cleartext + secret key +AES algorithm = ciphertext(encrypted text)

Decryption = ciphertext + secret key +AES algorithm = cleartext

Types of encryption

1. **Symmetric**

   Same secret key for encryption and decryption.

2. **Asymmetric**

   Public/private key pair for encryption and decryption, encryption with public key and decryption with same pare private key example – RSA

Quartz Scheduler

RestFul

Struts

Uncategorised

Name

Email *

Subscribe

POPULAR POSTS

viewpager with circle indicator in android
32,190 views | under Android

How to use properties file in Android ?
5,202 views | under Uncategorised

String Encryption and Decryption in java using Cipher class
4,427 views | under Java Security

Read properties file in Jsp
3,904 views | under Jsp

Dynamic autocomplete using Jquery, Struts2 and oracle
3,479 views | under Struts

Consume a restful webservice in android
3,132 views | under RestFul

How to make .apk file in android studio
2,666 views | under Android

Encrypt Decrypt File in Java Using Cipher class and RSA algorithm
2,425 views | under Java Security

Typers of ciphers

1. **Block Cipher**

   Process entire block at a time.

2. **Stream Cipher**

   Process incoming data unit by unit, unit size can be 1 byte or a bit.

Standard Cipher implementations.

Cipher object can be created from the below implementations.

Algorithm/mode/padding (key size)

AES/CBC/NoPadding (128)
AES/CBC/PKCS5Padding (128)
AES/ECB/NoPadding (128)
AES/ECB/PKCS5Padding (128)
DES/CBC/NoPadding (56)
DES/CBC/PKCS5Padding (56)
DES/ECB/NoPadding (56)
DES/ECB/PKCS5Padding (56)
DESede/CBC/NoPadding (168)
DESede/CBC/PKCS5Padding (168)
DESede/ECB/NoPadding (168)
DESede/ECB/PKCS5Padding (168)
RSA/ECB/PKCS1Padding (1024, 2048)
RSA/ECB/OAEPWithSHA-1AndMGF1Padding (1024, 2048)
RSA/ECB/OAEPWithSHA-256AndMGF1Padding (1024, 2048)

Load data while scrolling down using STRUTS 2 and jquery
2,207 views | under Struts

Spring Boot
2,122 views

ARCHIVES

May 2016
April 2016
March 2016
November 2015
October 2015
September 2015
August 2015
July 2015
June 2015
February 2015
January 2015
December 2014
November 2014
October 2014

AES– Advanced Encryption Standard
DES – Data Encryption Standard
DESede – (3DES) Triple DES
RSA – Rivest-Shamir-Adleman
CBC– cipher block chaining
ECB – electronic code book

How to create cipher Object?

Cipher cipherObject = Cipher.getInstance(“DES/CBC/PKCS5Padding”);

Modes of cipher object

1. **ENCRYPT_MODE** – data encryption
2. **DECRYPT_MODE** – decrypt the encrypted data.
3. **WRAP_MODE** – wrap the key into byte to transport securely.
4. **UNWRAP_MODE** – Unwrap the wrap key into java object.

Sample Code

EncryptionDecryption .java

```java
package com.javaant;

public class EncryptionDecryption {

public static void main(String args[]) {

    System.out.println("string after encription of (Nirmal Dhara)  :: "+CipherUtils.getEncryptedString("Nirmal Dhara"));
    System.out.println("String after decription of (8TymgE7S7Px6uZXScZlrRQ==) :: "+CipherUtils.getDecriyptedString("8TymgE7S7Px6uZXScZlrRQ=="));

```

```
  }

}
```

CipherUtils .java

```
package com.javaant;

import javax.crypto.Cipher;
import javax.crypto.spec.SecretKeySpec;

import org.apache.commons.codec.binary.Base64;

public class CipherUtils {

  private static byte[] key = { 0x24, 0x68, 0x78, 0x71, 0x49, 0x73, 0x41,
    0x24, 0x28, 0x78, 0x41, 0x49, 0x63, 0x41,0x73, 0x9};// "this Is A SecretKey you can change it, size is 16";

  public static String encrypt(String strToEncrypt) {
    try {
      Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5PADDING");
      final SecretKeySpec secretKey = new SecretKeySpec(key, "AES");
      cipher.init(Cipher.ENCRYPT_MODE, secretKey);
      final String encryptedString = Base64.encodeBase64String(cipher
          .doFinal(strToEncrypt.getBytes()));
      return encryptedString;
    } catch (Exception e) {
      e.printStackTrace();
    }
    return null;

  }

  public static String decrypt(String strToDecrypt) {
    try {
      Cipher cipher = Cipher.getInstance("AES/ECB/PKCS5PADDING");
      final SecretKeySpec secretKey = new SecretKeySpec(key, "AES");
      cipher.init(Cipher.DECRYPT_MODE, secretKey);
      final String decryptedString = new String(cipher.doFinal(Base64.decodeBase64(strToDecrypt)));
      return decryptedString;
    } catch (Exception e) {
      e.printStackTrace();

    }
    return null;
  }

  public static String getEncryptedString(String str) {
    final String strToEncrypt = str;
    final String encryptedStr = CipherUtils.encrypt(strToEncrypt.trim());

    return encryptedStr;
  }

  public static String getDecriyptedString(String str) {
    final String strToDecrypt = str;
    final String decryptedStr = CipherUtils.decrypt(strToDecrypt.trim());

    return decryptedStr;
  }


}
```

60

CIPHER DECRYPTION ENCRYPTION JAVA ENCRYPTION JAVA STRING ENCRYPTION JCE RSA ENCRYPTION

About Nirmal Dhara › 26 Articles

Java Developer

PREVIOUS ARTICLE

NEXT ARTICLE

4 COMMENTS ON STRING ENCRYPTION AND DECRYPTION IN JAVA USING CIPHER CLASS

Palanikumar 22ND MARCH 2016 AT 3:23 PM

Dear Nirmal,

I read very useful message from this site . truly i appreciate am very proud of you. better to add some mini project that's good thinking

REPLY

Nirmal Dhara 22ND MARCH 2016 AT 3:31 PM

Thanks to you and i am very glad to know that you like this site. Sure, I have that plan also.very soon i will post some projects.

REPLY

ramireddy vakamalla 24TH MARCH 2016 AT 5:00 PM

Hi Nirmal Dhara,
How to encypt and decrypt java bean object using cipher , sealedobject using RSA algorithm , i don't want to string .
Thanks,
RamiReddy.

REPLY

Nirmal Dhara 24TH MARCH 2016 AT 7:16 PM

Hi Thanks for the comments, I will post that very soon. If you want now please follow the below steps and Encrypt and Decrypt the object.

1. The class you want to Encrypt make Serializable.
2. Make Cipher Object for Encryption and Decryption.
3. Make a SealedObject object using The class you want to Encrypt and Cipher class object

Above 3 steps for Encrypt an object.

For Decryption
1. use SealedObject and Cipher object.
2. Get object and typecast to your class type.
2. use the methods or user class.

Example

```
Cipher encryptionObject;// Check my previous post how to create
Cipher DecryptionObject.
EncriptThisClass so = new EncriptThisClass();

SealedObject sealedObject = new SealedObject(so, encryptionObject);
EncriptThisClass o = (EncriptThisClass)
sealedObject.getObject(DecryptionObject);

o.Test();
```

```
/// this class object your are going to encrypt

public static class EncriptThisClass implements Serializable {

private static final long serialVersionUID = 1L;

public void Test() {
System.out.println("Object encription example");
}

}
```

Hope it will help you.

REPLY

Leave a Reply

Your email address will not be published.

Comment

Name*

Email*

Website

POST COMMENT

POPULAR POST

viewpager with circle indicator in android In many android apps we have seen sliding i...
0 comments | 37 views

How to use properties file in Android ? What is properties file? Properties files ...
0 comments | 24 views

String Encryption and Decryption in java using Cipher class There are many ways to encrypt and decrypt ...
0 comments | 19 views

Read properties file in Jsp Reading a properties file in java is common, same way w...
0 comments | 14 views

Encrypt Decrypt File in Java Using Cipher class and RSA algorithm How to Encrypt Decrypt File in Java ? Us...
0 comments | 9 views

Hello World using Android Studio 1.0 Hope you have installed the Android studio ...
0 comments | 6 views

Dynamic autocomplete using Jquery, Struts2 and oracle Hi Friends hope everyone knows autocomplete in jquery. ...

0 comments | 4 views

How to make .apk file in android studio Follow the below steps to generate .apk fil...

0 comments | 3 views

Consuming RESTful webservices with basic authentication. We can consume Restful webservices many way...

0 comments | 3 views

Dynamic Accordion Menu Using oracle java/j2ee and jquery Sometimes we need ‘Accordion Menu ‘ in our project. I f...

0 comments | 3 views