[**JAVA加密算法系列-AesCBC**](http://www.cnblogs.com/dava/p/6416638.html)

<https://www.cnblogs.com/dava/p/6416638.html>

[**JAVA加密算法系列-AesCBC**](http://www.cnblogs.com/dava/p/6416638.html)

[复制代码](javascript:void(0);)

package \*\*\*;

import javax.crypto.Cipher;

import javax.crypto.spec.IvParameterSpec;

import javax.crypto.spec.SecretKeySpec;

import sun.misc.BASE64Decoder;

import sun.misc.BASE64Encoder;

/\*\*

\* AES 是一种可逆加密算法，对用户的敏感信息加密处理

\* 对原始数据进行AES加密后，在进行Base64编码转化；

\* 正确

\*/

public class AesCBC {

/\*已确认

\* 加密用的Key 可以用26个字母和数字组成

\* 此处使用AES-128-CBC加密模式，key需要为16位。

\*/

private static String sKey="1234567890123456";

private static String ivParameter="1234567890123456";

private static AesCBC instance=null;

//private static

private AesCBC(){

}

public static AesCBC getInstance(){

if (instance==null)

instance= new AesCBC();

return instance;

}

// 加密

public String encrypt(String sSrc, String encodingFormat, String sKey, String ivParameter) throws Exception {

Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");

byte[] raw = sKey.getBytes();

SecretKeySpec skeySpec = new SecretKeySpec(raw, "AES");

IvParameterSpec iv = new IvParameterSpec(ivParameter.getBytes());//使用CBC模式，需要一个向量iv，可增加加密算法的强度

cipher.init(Cipher.ENCRYPT\_MODE, skeySpec, iv);

byte[] encrypted = cipher.doFinal(sSrc.getBytes(encodingFormat));

return new BASE64Encoder().encode(encrypted);//此处使用BASE64做转码。

}

// 解密

public String decrypt(String sSrc, String encodingFormat, String sKey, String ivParameter) throws Exception {

try {

byte[] raw = sKey.getBytes("ASCII");

SecretKeySpec skeySpec = new SecretKeySpec(raw, "AES");

Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");

IvParameterSpec iv = new IvParameterSpec(ivParameter.getBytes());

cipher.init(Cipher.DECRYPT\_MODE, skeySpec, iv);

byte[] encrypted1 = new BASE64Decoder().decodeBuffer(sSrc);//先用base64解密

byte[] original = cipher.doFinal(encrypted1);

String originalString = new String(original,encodingFormat);

return originalString;

} catch (Exception ex) {

return null;

}

}

public static void main(String[] args) throws Exception {

// 需要加密的字串

String cSrc = "123456";

System.out.println("加密前的字串是："+cSrc);

// 加密

String enString = AesCBC.getInstance().encrypt(cSrc,"utf-8",sKey,ivParameter);

System.out.println("加密后的字串是："+ enString);

System.out.println("1jdzWuniG6UMtoa3T6uNLA==".equals(enString));

// 解密

String DeString = AesCBC.getInstance().decrypt(enString,"utf-8",sKey,ivParameter);

System.out.println("解密后的字串是：" + DeString);

}

}

[复制代码](javascript:void(0);)

一步一步行走，做好每一件事情。