|  |
| --- |
|  |
| AES256 사용방법 |
|  |
|  |

**AON REAR ESTATE LLC.**

2016 March 16

저자: 김형진

AES256 사용방법

1. JCE Policy 라이브러리적용..

오라클 사이트인 <http://www.oracle.com>에서 Java 버전에 맞는 JCE Policy파일을 다운로드 하여 압축을 푼 후, jre설치경로\bin\security에 local\_policy.jar, US\_export\_policy.jar를 덮어 쓰기를 합니다.

2. AES256 암호화.

다음과 같이 String값을 AES256으로 암호화 합니다.

AES256Cipher.encodeByAES(email)

3. AES256 복호화.

다음과 같이 암호화된 String값을 AES256로 복호화 합니다.

AES256Cipher.decodeByAES(email)

**[AES256Chipher.java]**

package com.aonre.buyinfo.security;

import java.io.UnsupportedEncodingException;

import java.security.InvalidAlgorithmParameterException;

import java.security.InvalidKeyException;

import java.security.NoSuchAlgorithmException;

import javax.crypto.BadPaddingException;

import javax.crypto.Cipher;

import javax.crypto.IllegalBlockSizeException;

import javax.crypto.NoSuchPaddingException;

import javax.crypto.SecretKey;

import javax.crypto.spec.IvParameterSpec;

import javax.crypto.spec.SecretKeySpec;

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

public class AES256Cipher {

private static volatile AES256Cipher INSTANCE;

final static String secretKey = "12345678901234567890123456789012"; // 32bit

static String IV = "1234567890123456"; // 16bit

public static AES256Cipher getInstance() {

if (INSTANCE == null) {

synchronized (AES256Cipher.class) {

if (INSTANCE == null)

INSTANCE = new AES256Cipher();

}

}

return INSTANCE;

}

private AES256Cipher() {

}

// 암호화

public static String encodeByAES(String str)

throws UnsupportedEncodingException, NoSuchAlgorithmException, NoSuchPaddingException, InvalidKeyException,

InvalidAlgorithmParameterException, IllegalBlockSizeException, BadPaddingException {

byte[] keyData = secretKey.getBytes();

SecretKey secureKey = new SecretKeySpec(keyData, "AES");

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

c.init(Cipher.ENCRYPT\_MODE, secureKey, new IvParameterSpec(IV.getBytes()));

byte[] encrypted = c.doFinal(str.getBytes("UTF-8"));

String enStr = new String(Base64.encodeBase64(encrypted));

return enStr;

}

// 복호화

public static String decodeByAES(String str)

throws UnsupportedEncodingException, NoSuchAlgorithmException, NoSuchPaddingException, InvalidKeyException,

InvalidAlgorithmParameterException, IllegalBlockSizeException, BadPaddingException {

byte[] keyData = secretKey.getBytes();

SecretKey secureKey = new SecretKeySpec(keyData, "AES");

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

c.init(Cipher.DECRYPT\_MODE, secureKey, new IvParameterSpec(IV.getBytes("UTF-8")));

byte[] byteStr = Base64.decodeBase64(str.getBytes());

return new String(c.doFinal(byteStr), "UTF-8");

}

}