王懿璞
三花浴山露,碧波聚海湾,白鹭清风戏暖阳,峡屿连岳笑峰颠!

< 2015年9月 >

日	一	二	三	四	五	六
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3
4	5	6	7	8	9	10

昵称: 王懿璞
园龄: 2年11个月
粉丝: 40
关注: 2
+加关注

搜索
找找看
谷歌搜索

常用链接
我的随笔
我的评论
我的参与
最新评论
我的标签

我的标签
iOS(31)
Xcode(13)
开发工具(8)
Win8(8)
掌眼(8)
Android(7)
ASP.NET(6)
虚拟机(5)
支付接口(4)
C#(4)
更多

[掌眼]iOS / Android / java / node.js 通用的 AES256 加解密算法

example.m

```
NSString *text = @"text";
NSString *key32 = @"xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx";

NSData *data = [text
dataUsingEncoding:NSUTF8StringEncoding];
NSString *encryptedData = [[data
AES256EncryptWithKey:key32]
base64EncodedStringWithOptions:0];

NSLog(@"%@",encryptedData); # => QfpLKBn20BZI1NIhigOo6g==
```

NSData+AES256.m

```
- (NSData *)AES256EncryptWithKey:(NSString *)key {
    // 'key' should be 32 bytes for AES256, will be
null-padded otherwise
    char keyPtr[kCCKeySizeAES256+1]; // room for
terminator (unused)
    bzero(keyPtr, sizeof(keyPtr)); // fill with zeroes
(for padding)

    // fetch key data
    [key getCString:keyPtr maxLength:sizeof(keyPtr)
encoding:NSUTF8StringEncoding];

    NSUInteger dataLength = [self length];

    //See the doc: For block ciphers, the output size
will always be less than or
    //equal to the input size plus the size of one block.
    //That's why we need to add the size of one block
here
    size_t bufferSize = dataLength + kCCBlockSizeAES128;
    void *buffer = malloc(bufferSize);

    size_t numBytesEncrypted = 0;
```

随笔档案

2015年4月 (2)
2015年3月 (1)
2015年2月 (3)
2014年12月 (1)
2014年9月 (1)
2014年8月 (2)
2014年7月 (5)
2014年6月 (3)
2014年5月 (15)
2014年4月 (2)
2014年3月 (7)
2013年12月 (4)
2013年9月 (1)
2013年7月 (2)
2013年6月 (2)
2013年5月 (4)
2013年4月 (3)
2013年3月 (11)
2013年2月 (6)
2013年1月 (2)
2012年12月 (1)
2012年11月 (9)

厦门软件园

厦门宇博
厦门宇博软件有限公司
掌眼官网
手机古玩平台第一门户,手机古玩店铺、手机古玩论坛、手机古玩掌上竞拍、手机古玩交易
掌眼首页
手机古玩平台第一门户,手机古玩店铺、手机古玩论坛、手机古玩掌上竞拍、手机古玩交易

最新评论

1. Re:Visual Studio使用Http代理访问NuGet官方源，可解决代理上网及超时问题
蛋疼啊，这东西也要强一下。
--xcf007
2. Re:[MAC]2015款MACBOOK使用BOOTCAMP安装WIN8.1+多分区
已经有视频教程和更为先进的安装方法百度搜索“2015款【WINDOWS 10多分区】安装教程，所有Macbook Pro Air电脑 不破坏GUID分区表”就可以


```
    CCCryptorStatus cryptStatus = CCCrypt(kCCEncrypt,
kCCAlgorithmAES128, kCCOptionPKCS7Padding,
                                          keyPtr,
kCCKeySizeAES256,
                                          NULL /*
initialization vector (optional) */,
                                          [self bytes],
dataLength, /* input */
                                          buffer,
bufferSize, /* output */

&numBytesEncrypted);
    if (cryptStatus == kCCSuccess) {
        //the returned NSData takes ownership of the
buffer and will free it on deallocation
        return [NSData dataWithBytesNoCopy:buffer
length:numBytesEncrypted];
    }

    free(buffer); //free the buffer;
    return nil;
}

- (NSData *)AES256DecryptWithKey:(NSString *)key {
    // 'key' should be 32 bytes for AES256, will be
null-padded otherwise
    char keyPtr[kCCKeySizeAES256+1]; // room for
terminator (unused)
    bzero(keyPtr, sizeof(keyPtr)); // fill with zeroes
(for padding)

    // fetch key data
    [key getCString:keyPtr maxLength:sizeof(keyPtr)
encoding:NSUTF8StringEncoding];

    NSUInteger dataLength = [self length];

    //See the doc: For block ciphers, the output size
will always be less than or
    //equal to the input size plus the size of one block.
    //That's why we need to add the size of one block
here
    size_t bufferSize = dataLength + kCCBlockSizeAES128;
    void *buffer = malloc(bufferSize);

    size_t numBytesDecrypted = 0;
    CCCryptorStatus cryptStatus = CCCrypt(kCCDecrypt,
kCCAlgorithmAES128, kCCOptionPKCS7Padding,
                                          keyPtr,
kCCKeySizeAES256,
                                          NULL /*
initialization vector (optional) */,
                                          [self bytes],
dataLength, /* input */
                                          buffer,
bufferSize, /* output */
```

找到帖子...

--格瑞

3. Re:ASP.NET：EXCEL找不到文件、权限不够之综合解决方案

非常感谢，在systemprofile中建立desktop文件夹，问题解决！

--小华2011

4. Re:[MAC]OS X Mavericks 10.9.5 / 10.10.2 VMWare vmdk 镜像，解压就能用！

@王懿璞哦，我的意思是root的密码。今天安装了ubuntu，也需要su，结果想起来了sudo passwd设置root的密码，试了一下，原来你的mac系统没有设置root密码，害得我一直试一直试，今.....

--Champ_Keh

5. Re:[MAC]2015款MACBOOK使用BOOTCAMP安装WIN8.1+多分区

兄弟太棒了！我是先装上windows，在mac下再关闭Core Storage然后分区的，导致windows无法启动。一度怀疑你这篇文章无用，真是罪过！折腾很久了，后来按照你文章的步骤来做，结果就弄好.....

--风中灵药

阅读排行榜

1. VirtualBOX 虚拟机安装 OS X 10.9 Mavericks 及 Xcode 5，本人X220亲测(37812)
2. 分享一个轻型ORM－－Dapper选用理由(19997)
3. [iOS]Win8下iTunes无法连接iPhone版本的解决方法(13500)
4. 一个苹果证书如何多次使用——导出p12文件(10124)
5. [MAC]2015款MACBOOK使用BOOTCAMP安装WIN8.1+多分区(9734)

评论排行榜

1. VirtualBOX 虚拟机安装 OS X 10.9 Mavericks 及 Xcode 5，本人X220亲测(27)
2. [MAC]OS X Mavericks

```
&numBytesDecrypted);

    if (cryptStatus == kCCSuccess) {
        //the returned NSData takes ownership of the
buffer and will free it on deallocation
        return [NSData dataWithBytesNoCopy:buffer
length:numBytesDecrypted];
    }

    free(buffer); //free the buffer;
    return nil;
}
```

AES256.java

```
/**
 * Encodes a String in AES-256 with a given key
 *
 * @param context
 * @param password
 * @param text
 * @return String Base64 and AES encoded String
 */
public static String encode(String keyString, String
stringToEncode) throws NullPointerException {
    if (keyString.length() == 0 || keyString == null) {
        throw new NullPointerException("Please give
Password");
    }

    if (stringToEncode.length() == 0 || stringToEncode
== null) {
        throw new NullPointerException("Please give
text");
    }

    try {
        SecretKeySpec skeySpec = getKey(keyString);
        byte[] clearText =
stringToEncode.getBytes("UTF8");

        // IMPORTANT TO GET SAME RESULTS ON iOS and
ANDROID
        final byte[] iv = new byte[16];
        Arrays.fill(iv, (byte) 0x00);
        IvParameterSpec ivParameterSpec = new
IvParameterSpec(iv);

        // Cipher is not thread safe
        Cipher cipher = Cipher.getInstance("AES/CBC
/PKCS7Padding");
        cipher.init(Cipher.ENCRYPT_MODE, skeySpec,
```

10.9.5 / 10.10.2 VMWare vmdk 镜像，解压就能用！(6)
3. [MAC]2015款MACBOOK使用BOOTCAMP安装WIN8.1+多分区(5)
4. Visual Studio使用Http代理访问NuGet官方源，可解决代理上网及超时问题(3)
5. AES256 = C# + Objective C(iOS) + PHP + JAVA(Android) + Perl + Javascript(2)

推荐排行榜

1. 分享一个轻型ORM－－Dapper选用理由(4)
2. AutoCAD：ObjectARX所有版本下载地址(3)
3. Xcode：Home键光标移动到行首和End键光标移动到行尾(2)
4. [MAC]OS X Mavericks 10.9.5 / 10.10.2 VMWare vmdk 镜像，解压就能用！(2)
5. [掌眼]IIS7 / IIS7.5 URL 重写 HTTP 重定向到 HTTPS(2)

```
ivParameterSpec);

        String encrypedValue =
Base64.encodeToString(cipher.doFinal(clearText),
Base64.DEFAULT);
        Log.d("jacek", "Encrypted: " + stringToEncode +
" -> " + encrypedValue);
        return encrypedValue;

    } catch (InvalidKeyException e) {
        e.printStackTrace();
    } catch (UnsupportedEncodingException e) {
        e.printStackTrace();
    } catch (NoSuchAlgorithmException e) {
        e.printStackTrace();
    } catch (BadPaddingException e) {
        e.printStackTrace();
    } catch (NoSuchPaddingException e) {
        e.printStackTrace();
    } catch (IllegalBlockSizeException e) {
        e.printStackTrace();
    } catch (InvalidAlgorithmParameterException e) {
        e.printStackTrace();
    }
    return "";
}

/**
 * Decodes a String using AES-256 and Base64
 *
 * @param context
 * @param password
 * @param text
 * @return desoded String
 */
public String decode(String password, String text)
throws NullPointerException {

    if (password.length() == 0 || password == null) {
        throw new NullPointerException("Please give
Password");
    }

    if (text.length() == 0 || text == null) {
        throw new NullPointerException("Please give
text");
    }

    try {
        SecretKey key = getKey(password);

        // IMPORTANT TO GET SAME RESULTS ON iOS and
ANDROID
        final byte[] iv = new byte[16];
        Arrays.fill(iv, (byte) 0x00);
        IvParameterSpec ivParameterSpec = new
IvParameterSpec(iv);
```

```
        byte[] encrypedPwdBytes = Base64.decode(text,
Base64.DEFAULT);
        // cipher is not thread safe
        Cipher cipher = Cipher.getInstance("AES/CBC
/PKCS7Padding");
        cipher.init(Cipher.DECRYPT_MODE, key,
ivParameterSpec);
        byte[] decrypedValueBytes =
(cipher.doFinal(encrypedPwdBytes));

        String decrypedValue = new
String(decrypedValueBytes);
        Log.d(LOG_TAG, "Decrypted: " + text + " -> " +
decrypedValue);
        return decrypedValue;

    } catch (InvalidKeyException e) {
        e.printStackTrace();
    } catch (UnsupportedEncodingException e) {
        e.printStackTrace();
    } catch (NoSuchAlgorithmException e) {
        e.printStackTrace();
    } catch (BadPaddingException e) {
        e.printStackTrace();
    } catch (NoSuchPaddingException e) {
        e.printStackTrace();
    } catch (IllegalBlockSizeException e) {
        e.printStackTrace();
    } catch (InvalidAlgorithmParameterException e) {
        e.printStackTrace();
    }
    return "";
}

/**
 * Generates a SecretKeySpec for given password
 *
 * @param password
 * @return SecretKeySpec
 * @throws UnsupportedEncodingException
 */
private static SecretKeySpec getKey(String password)
throws UnsupportedEncodingException {

    // You can change it to 128 if you wish
    int keyLength = 256;
    byte[] keyBytes = new byte[keyLength / 8];
    // explicitly fill with zeros
    Arrays.fill(keyBytes, (byte) 0x0);

    // if password is shorter then key length, it will
be zero-padded
    // to key length
    byte[] passwordBytes = password.getBytes("UTF-8");
    int length = passwordBytes.length < keyBytes.length
? passwordBytes.length : keyBytes.length;
```

```
    System.arraycopy(passwordBytes, 0, keyBytes, 0,
length);
    SecretKeySpec key = new SecretKeySpec(keyBytes,
"AES");
    return key;
}
```

node.js

```
crypto = require('crypto')
key = 'xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx'
iv = new Buffer(16)
iv.fill(0)

text = 'text'

cipher = crypto.createCipheriv('aes-256-cbc', key, iv)
output = cipher.update('text', 'utf8', 'base64')
output += cipher.final('base64')

console.log output # => QfpLKBn20BZI1NIhigOo6g==
```


« 上一篇：[掌眼]IIS7 / IIS7.5 URL 重写 HTTP 重定向到 HTTPS
» 下一篇：AES256 = C# + Objective C(iOS) + PHP + JAVA(Android) + Perl + Javascript

posted on 2014-08-12 20:56 王懿璞 阅读(3165) 评论(0) 编辑 收藏