

PHP对接java的AES/ECB/PKCS5Padding加密方式

原创

老K8 2017-03-23 10:07:49 博主文章分类: PHP

©著作权

文章标签 java php AES 文章分类 Java 编程语言 阅读数 1.1万

因项目需要，要和一家保险公司对接调用API，我公司是PHP后台，保险公司是java后台，中间的数据传输就避免不了要加密、解密了，目前通行的加密AES比较推荐。

对接的过程中，就难免要翻山越水的了，

下面是我对接公司的加密说明：

加密说明

简要描述：

- 对于敏感的业务请求参数需要加密。
- 加密算法使用AES，密钥为secretkey经base64 decode得到的16byte(128位)。
- 如果有加密，业务原始请求参数签名是对加密后密文加密。
- 密码块工作模式和填充方法是“AES/ECB/PKCS5Padding”

参数说明：

参数名	必选	类型	说明
secretkey	是	string	合作方私钥，由和泰生成
content	是	string	业务请求参数

加密示例：

```
secretkey:eeSvvVtUDLi51TBHDjCeFw==

1. 原始请求信息：

业务请求参数：
name=testname
id=123456
userip=127.0.0.1

2. 构造业务请求参数json串：
{"name":"testname","userip":"127.0.0.1","id":123456}

3. AES加密得到byte[]，将byte[]转换成十六进制，再转大写字符
54B219CFE5287198D82E9804DA291B1088988D2C73EB5623F74C298133F6FAA8B6B32F793E8187408E65C12842DF8EC77D471C99F7E9D825BA3CCC277180D1D2

4. 构造请求：
content=54B219CFE5287198D82E9804DA291B1088988D2C73EB5623F74C298133F6FAA8B6B32F793E8187408E65C12842DF8EC77D471C99F7E9D825BA3CCC277180D1D2
```

一定要厘清楚自己的加密方式，否则一个加密模式ECB、CBC的差别，结果就千差万别的。

附上最终能使用的代码：

```
1. <?php
2. class Security {
3.     public static function encrypt($input, $key) {
4.         $size = mcrypt_get_block_size(MCRYPT_RIJNDAEL_128, MCRYPT_MODE_ECB);
5.         $input = Security::pkcs5_pad($input, $size);
6.         $td = mcrypt_module_open(MCRYPT_RIJNDAEL_128, '', MCRYPT_MODE_ECB, '');
7.         $iv = mcrypt_create_iv (mcrypt_enc_get_iv_size($td), MCRYPT_RAND);
8.         mcrypt_generic_init($td, $key, $iv);
9.         $data = mcrypt_generic($td, $input);
10.        mcrypt_generic_deinit($td);
11.        mcrypt_module_close($td);
12.        $data = base64_encode($data);
13.        return $data;
```



老K8

93

115.5万

原创

人气

4

38

翻译

转载

+ 关注

PHP分类的近期文章

- 显示 int 类型到小数点后
- array_multisort 使用碰到
- App版本升级方案
- PHP&获取两个时间日期
- 文件类型列表/docx,pptx

近期评论

- 树莓派上使用 docker 部
- 树莓派官方提供的镜像源列
- docker 启动报错--工作中
- 看网上的教程大多数碰到的
- Linux上怎么清除缓存、!
- 学习了
- Linux配置本地端口映射
- 谢谢指出，已更正！
- php 浮点数比较方法
- 棒棒棒

近期文章

- 1.显示 int 类型到小数点后
- 2.听说你的腾讯云/阿里云
- 3.array_multisort 使用碰到
- 4.fatal: unable to access
- 5.如何清理Linux服务器磁

2021年 8篇	2020
2019年 29篇	2018
2017年 29篇	2016
2015年 4篇	2014

```
18.         return $text . str_repeat(chr($pad), $pad);
19.     }
20.
21.     public static function decrypt($sStr, $sKey) {
22.         $decrypted= mcrypt_decrypt(
23.             MCRYPT_RIJNDAEL_128,
24.             $sKey,
25.             base64_decode($sStr),
26.             MCRYPT_MODE_ECB
27.         );
28.
29.         $dec_s = strlen($decrypted);
30.         $padding = ord($decrypted[$dec_s-1]);
31.         $decrypted = substr($decrypted, 0, -$padding);
32.         return $decrypted;
33.     }
34. }
35.
36.
37.
38. // $key = "1234567891234567";
39. // $data = "example";
40.
41. // $value = Security::encrypt($data , $key );
42. // echo "加密: : ".$value."<br/>";
43. // echo Security::decrypt($value, $key );
```

公共函数中调用：

```
1.  /**
2.      * request body加密
3.      * @param array $content 投保人的信息
4.      * @return string
5.      */
6.     function hetai_encrypt($content) {
7.
8.         // 方案七
9.         print_r("\r\n");
10.        vendor('encrypt.Security') or die("方案7引入失败");
11.        $sec = new \Security();
12.        $string = $content;
13.        $sec_res = $sec->encrypt($string, base64_decode("eeSvvVtUDLi5lTBHDjCeFw=="));
14.        $sec_res = strToHex($sec_res);// 结果转16进制并转成大写
15.        // 这里做了好几次的转换
16.        // 只是为了迎合出来我需要的结果而已
17.        // 根据自己的加密要求来定
18.        $encrypt_upper = strToHex(base64_decode(hexToStr($sec_res)));
19.        var_dump("\r\n方案7加密的结果\r\n" . $encrypt_upper);
20.        // 解密
21.        $sec_res_lower = strtolower($sec_res);// 转小写
22.        $sec_res_lower_tostr = hexToStr($sec_res);// 16进制转成string
23.        $sec_dec = $sec->decrypt($sec_res_lower_tostr, base64_decode("eeSvvVtUDLi5lTBHDjCeFw=="));
24.        var_dump("\r\n方案7解密的结果\r\n" . $sec_dec);
25.        return $encrypt_upper;
26.
27.    }
```

二进制字符串转16进制、16进制字符串转二进制：

```
1.  /**
2.      * 字符串转十六进制
3.      * @param string $string
4.      * @return string
5.      */
6.     function strToHex($string)
```

热评好文

- PHP对接java的AES/ECB
- Linux配置本地端口映射
- php批量导入带有图片的
- docker 启动报错--工作中
- 树莓派上使用 docker 部

七日热门

- Java入门_Java概述_Ja
- Java 解惑 (Java Puzzle
- Java 解惑 (Java Puzzle
- java心得--java类
- 【Java基础】Java拷贝
- [Java]Java分层概念
- 【java】java的Enum
- 【Java】Java反射笔记
- 【Java笔记】Java多态
- java基础--java语法

分类列表

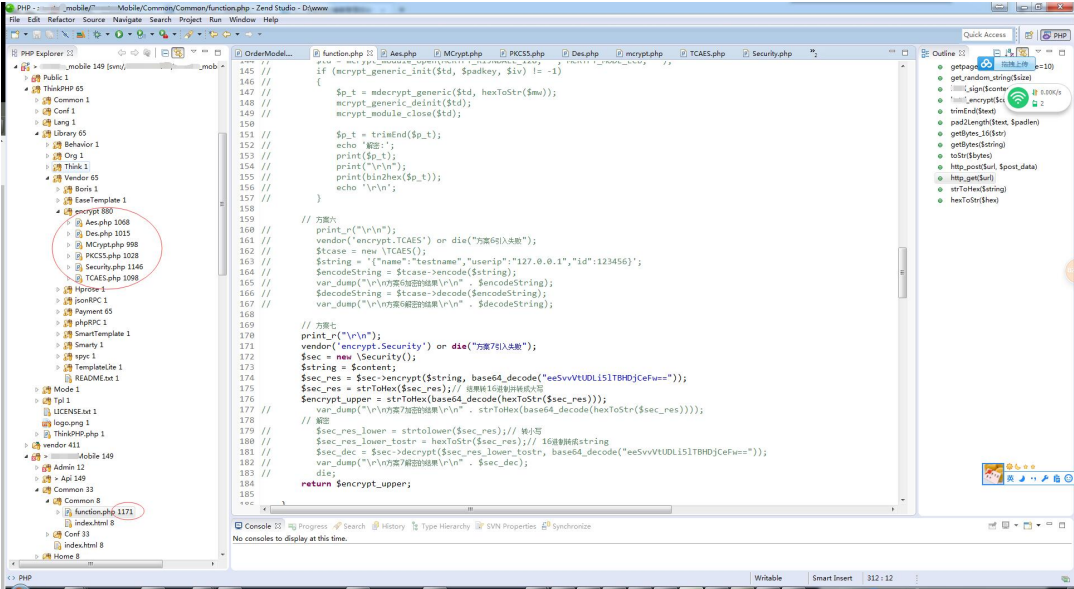
- # 升级打怪
- # Python
- # Linux
- # Nginx/Apache
- # PHP

相关标签

- aes/ecb/pkcs5padding gola
- s5padding 加密 aes/ecb/
- c++ aes/ecb/pkcs7padding
- +ecb+pkcs5padding加密
- cb java aes ecb java a
- a pkcs5padding no such
- b/pkcs5padding

```
11.         $hex=strtoupper($hex);
12.         return $hex;
13.     }
14.
15.     /**
16.      * 十六进制转字符串
17.      * 16进制的转为2进制字符串
18.      * @param 十六进制 $hex
19.      * @return string
20.      */
21.     function hexToStr($hex)
22.     {
23.         $string="";
24.         for($i=0;$i<strlen($hex)-1;$i+=2)
25.             $string.=chr(hexdec($hex[$i].$hex[$i+1]));
26.         return $string;
27.     }
```

附上折磨我三天的加密功能块，仅供自己作提醒之用，不喜勿喷~



相同问题的

赏

打赏

赞

收藏

6评论

分享

举报


上一篇：[ubuntu14php5.5安装mcrypt扩展](#)

下一篇：[原生APP内置PayPal网页支付方式](#)





提问和评论都可以，用心的回复会被更多人看到

评论

wx5a605ddf967c98 月前

java的base64和PHP的base64不一样是吗. 需要做转16进制后大写吗

 回复

 点赞

zhuangyeace2 年前

您好, 用你的方法解密没有问题, 为什么加密会比实际少几个字母


 回复

 点赞

老K8 博主 回复了 zhuangyeace2 年前

我用的版本是php5.6, 加密还是有点问题, 帮忙看一下, 谢谢了 \$string = '{"carCode":"沪A12315"}'; \$sec_res = \$sec->encrypt(\$string, base64_decode("cmVmb3JtZXJyZWZvcmlcg==")); \$sec_res = strToHex(\$sec_res);// 结果转16进制并转成大写 \$encrypt_upper = strToHex(base64_decode(hexToStr(\$sec_res))); echo"\n方案7加密的结果\n" . \$encrypt_upper."
"; //输出结果: 607CCB1B52F67DAF7C4D8C33B6503EFB0A413EED11BD9B3A35C0FD4FB22F7A //在线加密工具结果: 607CCB1B52F67DAF7C4D8C33B65003EFB0A413EED11B0D9B3A35C0FD4FB22F7A

我试了下, 没重现这个问题, 麻烦贴出来你在在线加密工具使用的方式看一看.

 回复


 点赞

zhuangyeace 回复了 老K82 年前

提醒下: mcrypt_decrypt、mcrypt_encrypt 将在 PHP7.1.0 移除废弃掉.

我用的版本是php5.6, 加密还是有点问题, 帮忙看一下, 谢谢了 \$string = '{"carCode":"沪A12315"}'; \$sec_res = \$sec->encrypt(\$string, base64_decode("cmVmb3JtZXJyZWZvcmlcg==")); \$sec_res = strToHex(\$sec_res);// 结果转16进制并转成大写 \$encrypt_upper = strToHex(base64_decode(hexToStr(\$sec_res))); echo"\n方案7加密的结果\n" . \$encrypt_upper."
"; //输出结果: 607CCB1B52F67DAF7C4D8C33B6503EFB0A413EED11BD9B3A35C0FD4FB22F7A //在线加密工具结果: 607CCB1B52F67DAF7C4D8C33B65003EFB0A413EED11B0D9B3A35C0FD4FB22F7A

 回复


 点赞

老K8 博主 回复了 zhuangyeace2 年前

提醒下: mcrypt_decrypt、mcrypt_encrypt 将在 PHP7.1.0 移除废弃掉.

 回复

 点赞

老K8 博主 回复了 zhuangyeace2 年前

1. 调试下, 自己加密、再自己解密是否正常? ? 2. \$encrypt_upper = strToHex(base64_decode(hexToStr(\$sec_res))); 留意下这里是否有问题, 有点绕.

 回复

 点赞

查看更多回复

相关文章

AES/CBC/PKCS5Padding (128)

CBC模式, 将明文分组与前一个密文分组进行XOR运算, 然后再进行加密. 每个分组的加解密都依赖于前一个分...



AES/ECB/PKCS5Padding8)

```
/** * AES/ECB/PKCS5Padding (128) * AES加密 ECB模式 PKCS5填充方式 密钥长度必须为16个字节(128位) */ pu...
```

Golang实现AES/CBC/PKCS5Padding算法

使用golang实现AES算法很简单，系统库中已自带了CBC、CFB等等许多加密模式，而且可以很方便的设置IVPara，但是前几日...

PHP进行AES/ECB/PKCS7 padding加密的例子（mcrypt）

业务需要，需要对数据进行加密（AES/ECB/PKCS7Padding），由于之前对该内容了解较少，于是去网上搜寻答案，很庆幸，...

AES对称加解密工具类（AES/GCM/PKCS5Padding）

```
import java.security.InvalidAlgorithmParameterException; import java.security.InvalidKeyException; import java.security.NoSuch...
```

PHP AES(运算模式 ECB,填充方式PKCS7) 加密解密

```
class Security{ public static function encrypt($input, $key) { if (substr(PHP_VERSION, 0, 1) == '7') { return self::opensslEncrypt(...
```

python进阶（23）用Python实现AES_ECB_PKCS5加密

前言AES加密的模式有很多种，下面来介绍ECB模式的加密解密import base64from Crypto.Cipher import AESclass AESECB: d...

OC的DES加密，使与java的Cipher类用DES/CBC/PKCS5Padding方式的加密结果同样

问题说明：近期用到DES加密，而且要与java的Cipher类加密的结果保持一致。没研究过java的Cliper，但工作中Cipher依据DE...

PHP DES-ECB加密对接Java解密

最近公司有个业务，需要对接第三方接口，但是参数是需要加密的，对方也只提供了一个java的demo，在网上到处搜索，没有找...

AES-256-ECB PKCS7Padding 解密 微信退款接口

不说别的了，直接说解密1解密方式解密步骤如下：（1）对加密串A做base64解码，得到加密串B（2）对商户key做md5，得到3...

python笔记66 - DES/CBC/pkcs5padding加解密（pyDes）

```
前言使用python代码实现 DES/CBC/pkcs5padding加解密DES加密模式加密模式：DES/CBC/pkcs5padding 加解...
```

python 实现AES CBC 与PKCS7Padding联合加密

```
from Crypto.Cipher import AESfrom binascii import b2a_hex, a2b_hexfrom cryptography.hazmat.primitives import paddingfrom ...
```

java.security.NoSuchAlgorithmException: Cannot find any provider supporting DESede/CBC/PKCS5Pa...

最近在做3DES加密，在本地window下面运行ok的程序，放到linux环境上竟然报错：Java.security.NoSuchAlgorithmException: ...

AES 加密填充 PKCS #7

使用算法AES的时候，涉及到数据填充的部分，数据的填充有很多种方案，用的比较多的有pkcs#5，pkcs#7，下面的都是从网...

What is the difference between PKCS#5 padding and PKCS#7 padding

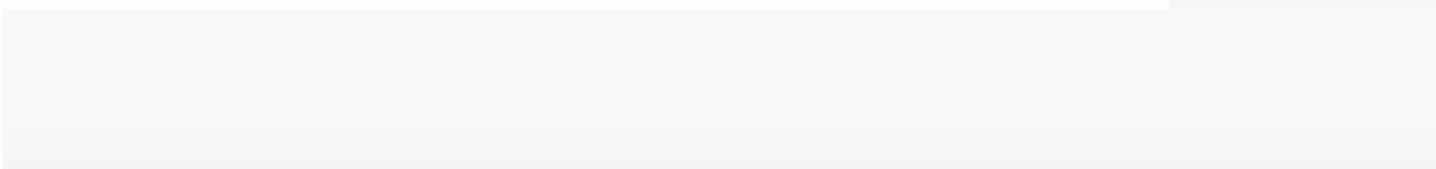
The difference between the PKCS#5 and PKCS#7 padding mechanisms is the block size; PKCS#5 padding is defined for 8-byt...

PHP AES cbc模式 pkcs7 128加密解密

今天在对接一个第三方接口的时候，对方需要AES CBC模式下的加密。这里简单写一个democlass Model_Junjingbao extends ...

java微信小程序解密AES/CBC/PKCS7Padding

摘要：微信小程序解密建议使用1.6及以上的环境使用maven下载jar包org.bouncycastlebcprov-jdk15on1.55加密类代码importor...



友情链接

51CTO鸿蒙社区

51CTO学堂

51CTO

关于我们

官方博客

意见反馈

了解我们

在线客服

网站地图

热门标签

全