php7 加密模式AES AES-128-CBC 填充PKCS7Padding 加密hex 字符集utf8

原創 qq_27229113 2019-08-02 08:21

AES,高級加密標準（英語：Advanced Encryption Standard，縮寫：AES），在密碼學中又稱Rijndael加密法，是美國聯邦政府採用的一種區塊加密標準。這個標準用來替代原先的DES，已經被多方分析且廣爲全世界所使用。嚴格地說，AES和Rijndael加密法並不完全一樣（雖然在實際應用中二者可以互換），因爲Rijndael加密法可以支持更大範圍的區塊和密鑰長度：AES的區塊長度固定爲128 比特，密鑰長度則可以是128，192或256比特；而Rijndael使用的密鑰和區塊長度可以是32位的整數倍，以128位爲下限，256比特爲上限。包括AES-ECB,AES-CBC,AES-CTR,AES-OFB,AES-CFB

注:在搞這個高級加密的時候發現很多問題,一羣複製粘貼黨浪費我這麼多時間,多看文檔

參考手冊 http://www.php.net/manual/en/function.openssl-decrypt.php

```
Parameters may seem obvius to some but not for everyone so:

- $data can be as the description says raw or base64. If no $option is set (this is, if value of 0 is passed in this parameter), data will be assumed to be base64 encoded. If parameter OPENSSL_RAW_DATA is set, it will be understood as row data.

- $password (key) is a String of [pseudo] bytes as those generated by the function openssl_random_pseudo_bytes().

- $options as (as for 2016) two possible values OPENSSL_RAW_DATA and OPENSSL_ZERO_PADDING. Setting both can be done by OPENSSL_RAW_DATA|OPENSSL_ZERO_PADDING. If no OPENSSL_ZERO_PADDING is specify, default pading of PKCS#7 will be done as it's been observe by [openssl at mailismagic dot com]'s coment in openssl_encrypt()

- $iv is as in the case of $password, a String of bytes. Its length depends on the algorithm used. May be the best way to generate an $iv is by:
```

我也看不懂翻譯一下:

有些人可能覺得參數很明顯，但並非每個人都如此:

-$data可以如描述中所說的raw或base64。如果沒有設置$option（如果此參數中傳遞的值爲0），則假定數據是base64編碼的。如果設置參數openssl_raw_data，它將被理解爲行數據。

-$password（key）是由函數openssl_random_pseudo_bytes（）生成的[pseudo]字節字符串。

-$options as（截至2016年）兩個可能的值openssl_raw_data和openssl_zero_padding。兩種設置都可以通過openssl_raw_data_openssl_zero_padding完成。如果沒有指定openssl_zero_padding，pkcs 7的默認padding將按照openssl_encrypt（）中[openssl at mailismagic dot com]的coment所觀察的方式進行。

-$IV和$password一樣，是一個字節字符串。它的長度取決於使用的算法。產生IV美元的最好方法是:

再注一下 : 參數 options 打開源碼這裏定義了一下,所以直接填1即可

```
define('OPENSSL_RAW_DATA', 1);
```

還一個標註一下:iv默認就是16位,相信大家會遇到如下報錯,openssl_encrypt 加密會把iv默認截成16位,所有就是你的iv如果是17位.你的iv會在末尾減一位,好了廢話有點多,相信能幫助到大家,

```
Warning: openssl_encrypt(): IV passed is 17 bytes long which is longer than the 16 expected by selected cipher, truncating in
```

如果幫到大家請掃下面微信收款碼,哈哈哈哈哈!!!!!!!!!!

```php
<?php

class AES
{
    /**
     * var string $method 加解密方法，可通過openssl_get_cipher_methods()獲得
     */
    protected $method;

    /**
     * var string $secret_key 加解密的密鑰
     */
    protected $secret_key;

    /**
     * var string $iv 加解密的向量，有些方法需要設置比如CBC
     */
    protected $iv;

    /**
     * var string $options （不知道怎麼解釋，目前設置爲0沒什麼問題）
     */
    protected $options;

    /**
     * 構造函數
     *
     * @param string $key 密鑰
     * @param string $method 加密方式
     * @param string $iv iv向量
     * @param mixed $options 還不是很清楚
     *
     */
    public function __construct($key, $method = 'AES-128-CBC', $iv = '', $options = 0)
    {
        // key是必須要設置的
        $this->secret_key = isset($key) ? $key : exit('key爲必須項');

        $this->method = $method;

        $this->iv = $iv;

        $this->options = $options;
    }

    /**
     * 加密方法，對數據進行加密，返回加密後的數據
     *
     * @param string $data 要加密的數據
     *
     * @return string
     *
     */
    public function encrypt($data)
    {
        $en = openssl_encrypt($data, $this->method, $this->secret_key, $this->options, $this->iv);
        $en = $this->String2Hex($en);
        return $en;
    }

    /**
     * 解密方法，對數據進行解密，返回解密後的數據
     *
     * @param string $data 要解密的數據
     *
     * @return string
     *
     */
```

```
    }


    public function String2Hex($string){


        $hex='';
//        for ($i=0; $i < strlen($string); $i++){
//            $hex .= dechex(ord($string[$i]));
//        }
        $hex = bin2hex($string);
        return $hex;
    }

    public function Hex2String($hex){
        $string='';
        for ($i=0; $i < strlen($hex)-1; $i+=2){
            $string .= chr(hexdec($hex[$i].$hex[$i+1]));
        }
        return $string;
    }
}


$data =
'{"messageid":15645624658187,"timestamp":1564562465,"deviceid":"AD13L1907310001","cmd":"CMD-
01","desired":{"allget":1}}';
$key = 'FW2VN#N8DAL147L*';
//$aes = new Aes($key, 'AES-128-CBC', '2398DHY433UGFKL1X',  1);
$aes = new Aes($key, 'AES-128-CBC', '2398DHY433UGFKL1X',  1);
$encode = $aes->encrypt($data);
echo "#####encode#####" . $encode . PHP_EOL;
$decode = $aes->decrypt($encode);
echo "#####decode#####" . $decode . PHP_EOL;
```


發表評論

登錄以後才評論...

所有評論

還沒有人評論，想成為第一個評論的人麼? 請在上方評論欄輸入並且點擊發布.

相關文章

PHP 代碼行數統計

<?php // 行數 $line = 0; // 需要統計的文件類型 $arr = array("php", "html", "css", "js"); // 過濾的文件夾 $filtering = array("ui", "dist

avenjan 2020-07-08 12:38:08

慎用PHP $_REQUEST數組

我平時總是喜歡用$_REQUEST這個數組，不是因爲別的，簡單，而且想用GET時候就用GET直接測試即可。還可以把URL打出來，很是方便。從而很少用$_GET和$_POST超全局變量。 不過，從今以後我會盡量不再使用$_REQUEST

二两天涯 2020-07-08 12:16:43

php函數名前面加@是何意

一、、、、@ 運算符只對表達式有效。對新手來說一個簡單的規則就是：如果能從某處得到值，就能在它前面加上 @ 運算符。例如，可以把它放在變量，函數和 include() 調用，常量，等等之前。不能把它放在函數或類的定義之前，也不能用於條件

二两天涯 2020-07-08 12:16:42

PHP和Javascript的JSON交互（處理一個二維數組）(轉)

xmphoenix 2020-07-08 12:00:47

php,checkbox多選框上傳失敗

用慣java和其他語言的時候，表單上傳只需要checkbox的name相同的時候就可以上傳了 <input type="checkbox" name="checkbox" value="1"> 選項1 <input type="c

阿冰介 2020-07-08 11:48:15

php中的&&運算符

今天看discuz源碼，在一個函數裏發現這麼個語句: http:// $output && print($ret); 其中$output是這個函數的一個參數，值爲true或false;$ret是一個字符串. 測試了一下，如果$output

yangmingysc 2020-07-08 11:45:39

php+mysql存儲html文件

$fileContent = trim($fileContent); $fileContent=$queueList->characet($fileContent);

moliyiran 2020-07-08 11:15:53

php+go實現grpc

1.先安裝編譯器:https://github.com/google/protobuf/releases把bin下的exe放到環境PATH目錄。做成環境變量. 2.獲取go支持庫的插件: // gRPC運行時接口編解碼支持庫 g

moliyiran 2020-07-08 11:15:42

Linux中PHP鏈接擴展.so動態庫

前幾天的一個實驗中涉及到使用PHP將本地文件部署到雲端，但是具體的實現卻還是需要費一番手腳，在網上找到的

PHP之TRUE與FALSE總結

以下代碼主要用於測試PHP中進行條件判斷時各種情況。 <?php /** * the file use to test all kinds of true and false. */ class Sample { public f

taotaoyouarebaby 2020-07-08 11:05:39

PHP配置使PHP在頁面中支持輸出內容

解決辦法： 找到系統中php.ini文件編輯，查找short_open_tag關鍵字，並將其設置爲：short_open_tag = On 注：需要找到short_open_tag = xx片段，可能會找到描述片段，修改並不起

念旧丶 2020-07-08 11:00:42

php操作xml最快的速度學習

做分享做總結 不多嗶嗶，直接上代碼：掌握php如何通過dom對象創建xml文件，php如何讀取xml及如何讀取xml文件，獲取到讀取的xml對象就可以直接操作了 <?php /** * Created by PhpStorm. *

jacklin_001 2020-07-08 10:52:26

wordpress數據字典

1.wordpress數據字典： 1.wp_categories: 用於保存分類相關信息的表。包括了5個字段，分別是: cat_ID – 每個分類唯一的ID號，爲一個bigint(20)值，且帶有附加屬性au

incloud_anke 2020-07-08 10:22:11

linux下面安裝php xdebug擴展

1.在框架裏經常會遇到debug模式！開啓選項就可以通過日誌文件快速的定位到問題 在win下面通過集成的開發包比如phpstudy就可以很容易的安裝xdebug的擴展 2.在linux下面就要通過編譯安裝來實現xde

incloud_anke 2020-07-08 10:22:10

wordpress rest api插件使用

1.wordpress rest api 插件下載： https://wordpress.org/plugins/rest-api/ 2.將下載的包解壓到wp-content/plugins目錄下 3.刷新後

incloud_anke 2020-07-08 10:22:10