PHP 实现 aes 加密解密、实现可解密的 uuid 加密解密

作者：ieras
原文链接：https://ld246.com/article/1612178185930
来源网站：链滴

创建加密解密类

直接上代码吧

```
<?php
/**
 * 加解密类
 *
 * @author zxq
 */

namespace App\Utils;

class Encrypt{

    protected static $instance = [];
    public $set = [];

    /*
     * 初始化加密类型
     * @param string $type
     * @param array $set
     * @return object
     */
    public static function init($type,$set){
        if (isset(self::$instance[static::class])) {
            return self::$instance[static::class];
        } else {
            return self::$instance[static::class] = new static($type,$set);
        }
    }
```

```
    /*
     * 初始化加密类型
     * @param string $type
     * @param array $set
     */
    public function __construct($type,$set){
        switch (strtolower($type)){
            case 'aes' :
                $this->set = $set;
                break;
            case 'uuid' :
                $this->set = $set;
                break;
            default :
                break;
        }
    }

    /*
     * Aes加密解密
     * (AES/CBC/PKCS5Padding或AES/CBC/PKCS7Padding)
     *
     * @param string $str 待加密/解密的恶字符串
     * @param string $type enc:加密 dec:解密
     * @return string
     */
    public function aes($str,$type = 'enc'){
        $key = $this->set['key'];
        $iv = $this->set['iv'];
        switch (strtolower($type)){
            case 'dec' ://解密
                return openssl_decrypt(base64_decode($str), 'AES-128-CBC', $key, OPENSSL_RAW_
ATA, $iv);
                break;
            default ://加密
                return base64_encode(openssl_encrypt($str, 'AES-128-CBC',$key, OPENSSL_RAW_D
TA , $iv));
                break;
        }
    }

    /*
     * 生成uuid 7f000001-0001-478c8000-4801-47242987
     *         ffffffff-dead-dba5-6edf-ee170b6a1c41
     * 解密uuid
     * Array ( [sid] => 0001 [ip] => 127.0.0.1 [unixtime] => 1200390144 [micro] => 0.28126525
78906 )
     */
    function uuid($uuid = null,$type = 'enc')
    {
        switch (strtolower($type)){
            case 'dec' ://解密
                $rez=Array();
```

```
            $u=explode("-",$uuid);
            if(is_array($u)&&count($u)==5) {
                $rez=Array(
                    'time'=>hexdec($u[0]),
                    'micro'=>(hexdec($u[1])/65536),
                    'sid'=>substr($u[4],0,4),//前4位
                    'ip'=>long2ip(hexdec(substr($u[4],4))),//4位后面的数据(8位)
                );
            }
            return $rez;
            break;
        default ://加密
            $t=explode(" ",microtime());
            $u = substr(uniqid(),-8);//13位截取后8位

            return sprintf( '%08s-%04s-%04s-%04s-%04x%08s',
                substr("00000000".dechex($t[1]),-8),   // get 8HEX of unixtime
                substr("0000".dechex(round($t[0]*65536)),-4), // get 4HEX of microtime
                substr($u,0,4),//前4位
                substr($u,-4),//后4位
                $this->set['sid'],//$serverID,
                dechex(ip2long(request()->getClientIp())));
            break;
    }
  }

}
```

使用方法

```
// Aes加密解密
$aes = Encrypt::init('aes', ['key' => '12345678','iv' => '1111111111111111',]);
$mi = $aes->aes('Hello World');
$ming = $aes->($mi,'dec')
// uuid加密解密
$uu = Encrypt::init('uuid', ['sid' => '1']);
$uuid = $uu->uuid();
$ming = $uu->($uuid,'dec')
```

结语

都是简单实现了一下哈，如果业务需求，可以扩展哦！升级更多功能～喜欢就点赞吧！