Atitit aes 加密法php实现

<?php

$data="aaaaccc";

 $secret\_key="abcdefgh";

//echo openssl\_encrypt($data, $this->method, $this->secret\_key, $this->options, $this->iv);

echo openssl\_encrypt($data, 'AES-128-ECB', $secret\_key,0, "");

echo "\r\n";

echo openssl\_decrypt("qjuIItb9e3IuYk0hi8ZN4g==", 'AES-128-ECB', $secret\_key,0, "");

* 常见的填充模式有： pkcs5、pkcs7、iso10126、ansix923、zero。
* 加密模式有：DES-ECB、DES-CBC、DES-CTR、DES-OFB、DES-CFB。

常见参数*$iv 加解密的向量，有些方法需要设置比如CBC*

*$method 加密方式*

switch($this->bit) {

case 192:$this->cipher = MCRYPT\_RIJNDAEL\_192; break;

case 256:$this->cipher = MCRYPT\_RIJNDAEL\_256; break;

default: $this->cipher = MCRYPT\_RIJNDAEL\_128;

}

switch($this->mode) {

case 'ecb':$this->mode = MCRYPT\_MODE\_ECB; break;

case 'cfb':$this->mode = MCRYPT\_MODE\_CFB; break;

case 'ofb':$this->mode = MCRYPT\_MODE\_OFB; break;

case 'nofb':$this->mode = MCRYPT\_MODE\_NOFB; break;

case 'cbc':$this->mode = MCRYPT\_MODE\_CBC; break;

default: $this->mode = MCRYPT\_MODE\_CBC;

$options 数据格式选项（可选）【选项有：】

* 0
* OPENSSL\_RAW\_DATA=1
* OPENSSL\_ZERO\_PADDING=2
* OPENSSL\_NO\_PADDING=3

##### **需要注意：如果$method为DES-ECB，则$iv无需填写**

使用案例