Mcrypt

mcrypt是php里面重要的加密支持扩展库，linux环境下默认情况下不开启，windows环境下php>5.3默认开启mcrypt扩展。

该扩展提供了类型，算法繁多的加密和解密功能。

**简介**

This is an interface to the mcrypt library, which supports a wide variety of block algorithms（块算法） such as DES, TripleDES, Blowfish (default), 3-WAY, SAFER-SK64, SAFER-SK128, TWOFISH, TEA, RC2 and GOST in CBC, OFB, CFB and ECB cipher modes. Additionally, it supports RC6 and IDEA which are considered "non-free". CFB/OFB are 8bit by default.

安装/配置

需求

These functions work using [» mcrypt](http://mcrypt.sourceforge.net/). To use it, download libmcrypt-x.x.tar.gz from [» http://mcrypt.sourceforge.net/](http://mcrypt.sourceforge.net/) and follow the included installation instructions.

As of PHP 5.0.0 you will need libmcrypt Version 2.5.6 or greater.

Windows users will find the library is the PHP 5.2 Windows binaries release（5.2版的为二进制发行版）. PHP 5.3 Windows binaries uses the static version of the MCrypt library（5.3版的为静态库，不在需要dll库了）, no DLL are needed.

If you linked against libmcrypt 2.4.x or higher, the following additional block algorithms are supported: CAST, LOKI97, RIJNDAEL, SAFERPLUS, SERPENT and the following stream ciphers（流密码）: ENIGMA (crypt), PANAMA, RC4 and WAKE. With libmcrypt 2.4.x or higher another cipher mode is also available; nOFB

安装

You need to compile PHP with the **--with-mcrypt[=DIR]** parameter to enable this extension（使参数编译时指定扩展的目录）. DIR is the mcrypt install directory. Make sure you compile libmcrypt with the option **--disable-posix-threads（确保编译了libmcrypt）** .

## 运行时配置

这些函数的行为受 php.ini 中的设置影响。

| **Mcrypt configuration options** | | | |
| --- | --- | --- | --- |
| **名字** | **默认** | **可修改范围** | **更新日志** |
| [mcrypt.algorithms\_dir](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/mcrypt.configuration.html#ini.mcrypt.algorithms-dir) | **NULL** | PHP\_INI\_ALL |  |
| [mcrypt.modes\_dir](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/mcrypt.configuration.html#ini.mcrypt.modes-dir) | **NULL** | PHP\_INI\_ALL |  |

有关 PHP\_INI\_\* 样式的更多详情与定义，见 [配置可被设定范围](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/configuration.changes.modes.html)。

这是配置指令的简短说明。

*mcrypt.algorithms\_dir* [string](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/language.types.string.html)

The directory that contains the algorithms(算法). Defaults to the directories compiled within libmcrypt（默认的目录为编译libmcrypt的目录）, which is typically /usr/local/lib/libmcrypt. See [mcrypt\_list\_algorithms()](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-list-algorithms.html) for additional details.

*mcrypt.modes\_dir* [string](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/language.types.string.html)

The directory that contains the modes（模式）. Defaults to the directories compiled within libmcrypt（默认的目录也为libmcrypt的目录）, which is typically /usr/local/lib/libmcrypt. See [mcrypt\_list\_modes()](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-list-modes.html) for additional details.

资源类型

[mcrypt\_module\_open()](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-module-open.html) returns an encryption descriptor（加密描述器）.

预定义常量

下列常量由此扩展定义，且仅在此扩展编译入 PHP 或在运行时动态载入时可用。

Mcrypt can operate in four block cipher modes（在四中块加密模式下工作） (*CBC*, *OFB*, *CFB*, and *ECB*). If linked against libmcrypt-2.4.x or higher the functions can also operate in the block cipher mode *nOFB* and in *STREAM* mode（流模式）. Below you find a list with all supported encryption modes together with the constants（常量） that are defines for the encryption mode. For a more complete reference and discussion see Applied Cryptography by Schneier (ISBN 0-471-11709-9).

* **MCRYPT\_MODE\_ECB** (*electronic codebook*) is suitable for random data, such as encrypting other keys. Since data there is short and random, the disadvantages of ECB have a favorable negative effect.
* **MCRYPT\_MODE\_CBC** (*cipher block chaining*) is especially suitable for encrypting files where the security is increased over *ECB* significantly.
* **MCRYPT\_MODE\_CFB** (*cipher feedback*) is the best mode for encrypting byte streams where single bytes must be encrypted.
* **MCRYPT\_MODE\_OFB** (*output feedback, in 8bit*) is comparable to *CFB*, but can be used in applications where error propagation cannot be tolerated. It's insecure (because it operates in 8bit mode) so it is not recommended to use it.
* **MCRYPT\_MODE\_NOFB** (*output feedback, in nbit*) is comparable to OFB, but more secure because it operates on the block size of the algorithm.
* **MCRYPT\_MODE\_STREAM** is an extra mode to include some stream algorithms like *"WAKE"* or *"RC4"*.

Some other mode and random device constants:

**MCRYPT\_ENCRYPT** ( [integer](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/language.types.integer.html) )

**MCRYPT\_DECRYPT** ( [integer](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/language.types.integer.html) )

**MCRYPT\_DEV\_RANDOM** ( [integer](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/language.types.integer.html) )

**MCRYPT\_DEV\_URANDOM** ( [integer](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/language.types.integer.html) )

**MCRYPT\_RAND** ( [integer](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/language.types.integer.html) )

**Mcrypt ciphers（加密）**

Here is a list of ciphers which are currently supported by the mcrypt extension. For a complete list of supported ciphers, see the defines at the end of *mcrypt.h*. The general rule（通常的规则是） with the mcrypt-2.2.x API is that you can access the cipher from PHP with MCRYPT\_ciphername（直接使用名字就可以连接加密器）. With the libmcrypt-2.4.x and libmcrypt-2.5.x API these constants also work, but it is possible to specify the name of the cipher as a string with a call to [mcrypt\_module\_open()](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-module-open.html)（最好使用这个模式打开的方法来更安全） .

* MCRYPT\_3DES
* MCRYPT\_ARCFOUR\_IV (libmcrypt > 2.4.x only)
* MCRYPT\_ARCFOUR (libmcrypt > 2.4.x only)
* MCRYPT\_BLOWFISH
* MCRYPT\_CAST\_128
* MCRYPT\_CAST\_256
* MCRYPT\_CRYPT
* MCRYPT\_DES
* MCRYPT\_DES\_COMPAT (libmcrypt 2.2.x only)
* MCRYPT\_ENIGMA (libmcrypt > 2.4.x only, alias for MCRYPT\_CRYPT)
* MCRYPT\_GOST
* MCRYPT\_IDEA (non-free)
* MCRYPT\_LOKI97 (libmcrypt > 2.4.x only)
* MCRYPT\_MARS (libmcrypt > 2.4.x only, non-free)
* MCRYPT\_PANAMA (libmcrypt > 2.4.x only)
* MCRYPT\_RIJNDAEL\_128 (libmcrypt > 2.4.x only)
* MCRYPT\_RIJNDAEL\_192 (libmcrypt > 2.4.x only)
* MCRYPT\_RIJNDAEL\_256 (libmcrypt > 2.4.x only)
* MCRYPT\_RC2
* MCRYPT\_RC4 (libmcrypt 2.2.x only)
* MCRYPT\_RC6 (libmcrypt > 2.4.x only)
* MCRYPT\_RC6\_128 (libmcrypt 2.2.x only)
* MCRYPT\_RC6\_192 (libmcrypt 2.2.x only)
* MCRYPT\_RC6\_256 (libmcrypt 2.2.x only)
* MCRYPT\_SAFER64
* MCRYPT\_SAFER128
* MCRYPT\_SAFERPLUS (libmcrypt > 2.4.x only)
* MCRYPT\_SERPENT(libmcrypt > 2.4.x only)
* MCRYPT\_SERPENT\_128 (libmcrypt 2.2.x only)
* MCRYPT\_SERPENT\_192 (libmcrypt 2.2.x only)
* MCRYPT\_SERPENT\_256 (libmcrypt 2.2.x only)
* MCRYPT\_SKIPJACK (libmcrypt > 2.4.x only)
* MCRYPT\_TEAN (libmcrypt 2.2.x only)
* MCRYPT\_THREEWAY
* MCRYPT\_TRIPLEDES (libmcrypt > 2.4.x only)
* MCRYPT\_TWOFISH (for older mcrypt 2.x versions, or mcrypt > 2.4.x )
* MCRYPT\_TWOFISH128 (TWOFISHxxx are available in newer 2.x versions, but not in the 2.4.x versions)
* MCRYPT\_TWOFISH192
* MCRYPT\_TWOFISH256
* MCRYPT\_WAKE (libmcrypt > 2.4.x only)
* MCRYPT\_XTEA (libmcrypt > 2.4.x only)

You must (in **CFB** and **OFB** mode) or can (in **CBC** mode) supply an initialization vector (IV)（提供一个初始化的量） to the respective cipher function（各自的加密函数）. The IV must be unique（唯一） and must be the same when decrypting/encrypting. With data which is stored encrypted, you can take the output of a function（方程的输出） of the index under which the data is stored (e.g. the MD5 key of the filename). Alternatively, you can transmit（传送） the IV together with the encrypted data (see chapter 9.3 of Applied Cryptography by Schneier (ISBN 0-471-11709-9) for a discussion of this topic).

# 范例

Mcrypt can be used to encrypt and decrypt using the above mentioned ciphers（加密器）. If you linked against libmcrypt-2.2.x, the four important mcrypt commands ( [mcrypt\_cfb()](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-cfb.html) , [mcrypt\_cbc()](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-cbc.html) , [mcrypt\_ecb()](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-ecb.html) , and [mcrypt\_ofb()](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-ofb.html) ) can operate in both modes which are named **MCRYPT\_ENCRYPT** and **MCRYPT\_DECRYPT** , respectively.

If you linked against libmcrypt 2.4.x or 2.5.x, these functions are still available, but it is recommended that you use the advanced functions.

**Example #1 Encrypt an input value with TripleDES under 2.4.x and higher in ECB mode**

<?php  
    $key  =  "this is a secret key" ;  
     $input  =  "Let us meet at 9 o'clock at the secret place." ;  
  
     $td  =  mcrypt\_module\_open ( 'tripledes' ,  '' ,  'ecb' ,  '' );  
     $iv  =  mcrypt\_create\_iv ( mcrypt\_enc\_get\_iv\_size ( $td ),  MCRYPT\_RAND );  
     mcrypt\_generic\_init ( $td ,  $key ,  $iv );  
     $encrypted\_data  =  mcrypt\_generic ( $td ,  $input );  
     mcrypt\_generic\_deinit ( $td );  
     mcrypt\_module\_close ( $td );  
?>

This example will give you the encrypted data as a string in $encrypted\_data. For a full example see [mcrypt\_module\_open()](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-module-open.html) .

# Mcrypt 函数

## Table of Contents

* [mcrypt\_cbc](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-cbc.html) — Encrypts/decrypts data in CBC mode 以cbc模式加密和解密。php>=5.5废弃
* [mcrypt\_cfb](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-cfb.html) — Encrypts/decrypts data in CFB mode 以cfb模式，php>=5.5废弃
* [mcrypt\_create\_iv](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-create-iv.html) — Creates an initialization vector (IV) from a random source 从随机资源创建一个初始化量

$size = mcrypt\_get\_iv\_size ( MCRYPT\_CAST\_256 , MCRYPT\_MODE\_CFB );

$iv = mcrypt\_create\_iv ( $size , MCRYPT\_DEV\_RANDOM );

var\_dump($size);

var\_dump($iv);

* [mcrypt\_decrypt](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-decrypt.html) — Decrypts crypttext with given parameters 以给定参数解密crpy文本

语法：string **mcrypt\_decrypt** ( string $cipher , string $key , string $data , string $mode [, string $iv ] )

Decrypts the *data* and returns the unencrypted data.

需要在转换为字符串的时候移除填充的0

To Remove PKCS7 padding:

$decrypted = mdecrypt\_generic($td, base64\_decode($enc\_auth\_token));   
    $dec\_s = strlen($decrypted);   
    $padding = ord($decrypted[$dec\_s-1]);   
    $decrypted = substr($decrypted, 0, -$padding);

* [mcrypt\_ecb](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-ecb.html) — Deprecated: Encrypts/decrypts data in ECB mode php>=5.5被放弃的函数
* [mcrypt\_enc\_get\_algorithms\_name](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-enc-get-algorithms-name.html) — Returns the name of the opened algorithm 返回被打开的算法名字

string **mcrypt\_enc\_get\_algorithms\_name** ( resource $td )

参数为加密描述器

$td  =  mcrypt\_module\_open ( MCRYPT\_CAST\_256 ,  '' ,  MCRYPT\_MODE\_CFB ,  '' );  
echo  mcrypt\_enc\_get\_algorithms\_name ( $td ).  "\n" ;  
  
$td  =  mcrypt\_module\_open ( 'cast-256' ,  '' ,  MCRYPT\_MODE\_CFB ,  '' );  
echo  mcrypt\_enc\_get\_algorithms\_name ( $td ).  "\n" ;

* [mcrypt\_enc\_get\_block\_size](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-enc-get-block-size.html) — Returns the blocksize of the opened algorithm 返回被打开的算法的块的字节大小

语法：int **mcrypt\_enc\_get\_block\_size** ( resource $td )

参数为加密描述器

* [mcrypt\_enc\_get\_iv\_size](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-enc-get-iv-size.html) — Returns the size of the IV of the opened algorithm 返回打开的算法的iv的大小

语法：int **mcrypt\_enc\_get\_iv\_size** ( resource $td )

var\_dump(mcrypt\_enc\_get\_iv\_size($td));

* [mcrypt\_enc\_get\_key\_size](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-enc-get-key-size.html) — Returns the maximum supported keysize of the opened mode 返回打开的模式的最大可支持的key的长度

语法：int **mcrypt\_enc\_get\_key\_size** ( resource $td )

var\_dump(mcrypt\_enc\_get\_key\_size($td));

* [mcrypt\_enc\_get\_modes\_name](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-enc-get-modes-name.html) — Returns the name of the opened mode 返回打开模式的名字

echo mcrypt\_enc\_get\_modes\_name($td)

* [mcrypt\_enc\_get\_supported\_key\_sizes](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-enc-get-supported-key-sizes.html) — Returns an array with the supported keysizes of the opened algorithm 返回打开的算法支持的key的大小的数组

语法：array **mcrypt\_enc\_get\_supported\_key\_sizes** ( resource $td )

var\_dump(mcrypt\_get\_key\_size(MCRYPT\_CAST\_256, MCRYPT\_MODE\_CFB));

MCRYPT\_CAST\_256, MCRYPT\_MODE\_CFB定义了一个加密器

* [mcrypt\_enc\_is\_block\_algorithm\_mode](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-enc-is-block-algorithm-mode.html) — Checks whether the encryption of the opened mode works on blocks 检查打开模式的加密器是否在块上工作

var\_dump(mcrypt\_enc\_is\_block\_algorithm($td));

* [mcrypt\_enc\_is\_block\_algorithm](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-enc-is-block-algorithm.html) — Checks whether the algorithm of the opened mode is a block algorithm 检查打开的模式的算法是否是一个块算法
* [mcrypt\_enc\_is\_block\_mode](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-enc-is-block-mode.html) — Checks whether the opened mode outputs blocks 检查打开的模式输出是否为块模式

如果是则返回true，表明输出的为块的bytes（blocks of bytes）

否则输出false，表明输出的仅仅为bytes

输出的为块模式可能涉及取掉填充的空格或者0；它只以一定大小的块来输出，而不像bytes可以输出任意大小。

* [mcrypt\_enc\_self\_test](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-enc-self-test.html) — Runs a self test on the opened module 运行一个自检查在打开的模式上

成功返回false，失败返回true

* [mcrypt\_encrypt](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-encrypt.html) — Encrypts plaintext with given parameters 以给定的参数加密纯文本

语法：string **mcrypt\_encrypt** ( string $cipher , string $key , string $data , string $mode [, string $iv ] )

* [mcrypt\_generic\_deinit](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-generic-deinit.html) — This function deinitializes an encryption module 释放一个加密模式

它终止一个被传入的参数指定的加密器，清空所有的缓存，但是不会关闭模式；如果关闭模式需要调用mcrypt\_module\_close函数

成功返回true，失败返回false

* [mcrypt\_generic\_end](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-generic-end.html) — This function terminates encryption 终止一个加密，被放弃的函数，使用mcrypt\_generic\_deinit()来替代
* [mcrypt\_generic\_init](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-generic-init.html) — This function initializes all buffers needed for encryption 初始化加密所需要的缓冲

语法：int **mcrypt\_generic\_init** ( resource $td , string $key , string $iv )

在调用mcrypt\_generic或者mdecrypt\_generic之前调用这个函数

* [mcrypt\_generic](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-generic.html) — This function encrypts data 加密数据

语法：string **mcrypt\_generic** ( resource $td , string $data )

为了长度是blocksize的整数倍会填充0；

* [mcrypt\_get\_block\_size](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-get-block-size.html) — Gets the block size of the specified cipher 获得指定加密器的块大小
* int **mcrypt\_get\_block\_size** ( int $cipher ) libcrypt 为2.2.x
* int **mcrypt\_get\_block\_size** ( string $cipher , string $mode ) libcrype 2.4.x或者2.5.x

* [mcrypt\_get\_cipher\_name](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-get-cipher-name.html) — Gets the name of the specified cipher 获取指定加密器的名字

语法

* string **mcrypt\_get\_cipher\_name** ( int $cipher )
* string **mcrypt\_get\_cipher\_name** ( string $cipher )

参数cipher为**MCRYPT\_ciphername** 常量中的一个，或者是字符串值的算法名称

* [mcrypt\_get\_iv\_size](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-get-iv-size.html) — Returns the size of the IV belonging to a specific cipher/mode combination

int **mcrypt\_get\_iv\_size** ( string $cipher , string $mode )

使用**mcrypt\_enc\_get\_iv\_size**更好

* [mcrypt\_get\_key\_size](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-get-key-size.html) — Gets the key size of the specified cipher

语法：

* int **mcrypt\_get\_key\_size** ( int $cipher )
* int **mcrypt\_get\_key\_size** ( string $cipher , string $mode )

使用mcrypt\_enc\_get\_key\_size更好

* [mcrypt\_list\_algorithms](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-list-algorithms.html) — Gets an array of all supported ciphers 获取所有支持的加密器的数组

print\_r(mcrpt\_list\_algorithms());

Array

(

[0] => cast-128

[1] => gost

[2] => rijndael-128

[3] => twofish

[4] => cast-256

[5] => loki97

[6] => rijndael-192

[7] => saferplus

[8] => wake

[9] => blowfish-compat

[10] => des

[11] => rijndael-256

[12] => serpent

[13] => xtea

[14] => blowfish

[15] => enigma

[16] => rc2

[17] => tripledes

[18] => arcfour

)

* [mcrypt\_list\_modes](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-list-modes.html) — Gets an array of all supported modes 获取所有支持的模式的数组

print\_r(mcrypt\_list\_modes());

Array

(

[0] => cbc

[1] => cfb

[2] => ctr

[3] => ecb

[4] => ncfb

[5] => nofb

[6] => ofb

[7] => stream

)

* [mcrypt\_module\_close](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-module-close.html) — Closes the mcrypt module 关闭mcrypt模型
* [mcrypt\_module\_get\_algo\_block\_size](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-module-get-algo-block-size.html) — Returns the blocksize of the specified algorithm 获取指定算法的块大小

语法：bool **mcrypt\_module\_close** ( resource $td )

参数为[mcrypt\_module\_open()](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-module-open.html)的返回值

* [mcrypt\_module\_get\_algo\_key\_size](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-module-get-algo-key-size.html) — Returns the maximum supported keysize of the opened mode 获取打开的算法能够支持的最大key的大小

语法：array **mcrypt\_module\_get\_supported\_key\_sizes** ( string $algorithm [, string $lib\_dir ] )

var\_dump(mcrypt\_module\_get\_algo\_key\_size('gost'));

* [mcrypt\_module\_get\_supported\_key\_sizes](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-module-get-supported-key-sizes.html) — Returns an array with the supported keysizes of the opened algorithm 返回打开的算法支持的key大小的数组

var\_dump(mcrypt\_module\_get\_supported\_key\_sizes('wake'));

* [mcrypt\_module\_is\_block\_algorithm\_mode](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-module-is-block-algorithm-mode.html) — Returns if the specified module is a block algorithm or not 返回指定的module是否是一个块算法

语法：bool **mcrypt\_module\_is\_block\_algorithm\_mode** ( string $mode [, string $lib\_dir ] )

var\_dump(mcrypt\_module\_is\_block\_algorithm\_mode('cbc'));

* [mcrypt\_module\_is\_block\_algorithm](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-module-is-block-algorithm.html) — This function checks whether the specified algorithm is a block algorithm 检查指定的算法是否是一个块算法

语法：bool **mcrypt\_module\_is\_block\_algorithm** ( string $algorithm [, string $lib\_dir ] )

是返回true，否则返回false，表明是一个流（stream)算法

var\_dump(mcrypt\_module\_is\_block\_algorithm('rc2'));

* [mcrypt\_module\_is\_block\_mode](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-module-is-block-mode.html) — Returns if the specified mode outputs blocks or not返回指定的模式是否输出块
* [mcrypt\_module\_open](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-module-open.html) — Opens the module of the algorithm and the mode to be used 打开算法module和使用的模式

This function opens the module of the algorithm and the mode to be used. The name of the algorithm is specified in algorithm, e.g. "twofish" or is one of the **MCRYPT\_ciphername** constants. The module is closed by calling [mcrypt\_module\_close()](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-module-close.html)

语法：resource **mcrypt\_module\_open** ( string $algorithm , string $algorithm\_directory , string $mode , string $mode\_directory )

* [mcrypt\_module\_self\_test](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-module-self-test.html) — This function runs a self test on the specified module 运行一个自检查在指定的module上

语法：bool **mcrypt\_module\_self\_test** ( string $algorithm [, string $lib\_dir ] )

成功返回true，失败返回false

* [mcrypt\_ofb](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mcrypt-ofb.html) — Encrypts/decrypts data in OFB mode 以ofb模式加密和解密，php>=5.5被放弃
* [mdecrypt\_generic](mk:@MSITStore:E:\deleting\enhancingProgram\PHP\php_manual_zh_review.chm::/res/function.mdecrypt-generic.html) — Decrypts data 解密数据

语法：string **mcrypt\_generic** ( resource $td , string $data )

返回加密的数据