PHP crypt() 函数

PHP String 函数

定义和用法

crypt() 函数返回使用 DES、Blowfish 或 MD5 算法加密的字符串。

在不同的操作系统上，该函数的行为不同，某些操作系统支持一种以上的算法类型。在安装时，PHP 会检查什么算法可用以及使用什么算法。

具体的算法依赖于 salt 参数的格式和长度。通过增加由使用特定加密方法的特定字符串所生成的字符串数量，salt 可以使加密更安全。

这里有一些和 crypt() 函数一起使用的常量。这些常量值是在安装时由 PHP 设置的。

常量：

[CRYPT_SALT_LENGTH]	默认的加密长度。使用标准的 DES 加密，长度为 2
[CRYPT_STD_DES]	基于标准 DES 算法的散列使用 "./0-9A-Za-z" 字符中的两个字符作为盐值。在盐值中使用非法的字符将导致 crypt() 失败。
[CRYPT_EXT_DES]	扩展的基于 DES 算法的散列。其盐值为 9 个字符的字符串，由 1 个下划线后面跟着 4 字节循环次数和 4 字节盐值组成。它们被编码成可打印字符，每个字符 6 位，有效位最少的优先。0 到 63 被编码为 "./0-9A-Za-z"。在盐值中使用非法的字符将导致 crypt() 失败。
[CRYPT_MD5]	MD5 散列使用一个以 1 开始的 12 字符的字符串盐值。
[CRYPT_BLOWFISH]	Blowfish 算法使用如下盐值：“$2a$”，一个两位 cost 参数，“$” 以及 64 位由 “./0-9A-Za-z” 中的字符组合而成的字符串。在盐值中使用此范围之外的字符将导致 crypt() 返回一个空字符串。两位 cost 参数是循环次数以 2 为底的对数，它的范围是 04-31，超出这个范围将导致 crypt() 失败。
CRYPT_SHA256	SHA-256 算法使用一个以 5 开头的 16 字符字符串盐值进行散列。如果盐值字符串以 “rounds=<N>$” 开头，N 的数字值将被用来指定散列循环的执行次数，这点很像 Blowfish 算法

	的 cost 参数。默认的循环次数是 5000，最小是 1000，最大是 999,999,999。超出这个范围的 N 将会被转换为最接近的值。
CRYPT_SHA512	SHA-512 算法使用一个以 6 开头的 16 字符字符串盐值进行散列。如果盐值字符串以 "rounds=<N>$" 开头，N 的数字值将被用来指定散列循环的执行次数，这点很像 Blowfish 算法的 cost 参数。默认的循环次数是 5000，最小是 1000，最大是 999,999,999。超出这个范围的 N 将会被转换为最接近的值。

在该函数支持多种算法的系统上，如果支持上述常量则设置为 "1"，否则设置为 "0"。

注释：没有相应的解密函数。crypt() 函数使用一种单向算法。

语法

```
crypt(str,salt)
```

参数	描述
str	必需。规定要编码的字符串。
salt	可选。用于增加被编码字符数目的字符串，以使编码更加安全。如果未提供 salt 参数，则每次调用该函数时 PHP 会随机生成一个。

技术细节

返回值：	返回加密后的字符串或一个少于 13 字符的字符串，从而保证在失败时与盐值区分开来。
PHP 版本：	4+

更新日志

版本	说明
5.3.2	基于 Ulrich Drepper 的实现，新增基于 SHA-256 算法和 SHA-512 算法的 crypt。
5.3.2	修正了 Blowfish 算法由于非法循环导致的问题，返回"失败"字符串（"*0" 或 "*1"）而不是转而使用 DES 算法。
5.3.0	PHP 现在包含了它自己的 MD5 Crypt 实现，包括标准 DES 算法，扩展的 DES 算法以及 Blowfish 算法。如果系统缺乏相应的实现，那么 PHP 将使用它自己的实现。

实例

例子 **1**

在本实例中，我们将测试不同的算法：

```
<?php
// 两字符 salt
if (CRYPT_STD_DES == 1)
{
echo "Standard DES: ".crypt('something','st')."\n<br>";
}
else
{
echo "Standard DES not supported.\n<br>";
}

// 4 字符 salt
if (CRYPT_EXT_DES == 1)
{
echo "Extended DES: ".crypt('something','_S4..some')."\n<br>";
}
else
{
echo "Extended DES not supported.\n<br>";
}

//以 $1$ 开始的 12 字符
if (CRYPT_MD5 == 1)
{
echo "MD5: ".crypt('something','$1$somethin$')."\n<br>";
}
else
{
echo "MD5 not supported.\n<br>";
}

// 以 $2a$ 开始的 Salt。双数字的 cost 参数: 09. 22 字符
if (CRYPT_BLOWFISH == 1)
{
echo "Blowfish: ".crypt('something','$2a$09$anexamplestringforsalt$')."\n<br>";
}
else
{
echo "Blowfish DES not supported.\n<br>";
}

// 以 $5$ 开始的 16 字符 salt。周长的默认数是 5000。
if (CRYPT_SHA256 == 1)
{
echo "SHA-256: ".crypt('something','$5$rounds=5000$anexamplestringforsalt$')."\n<br>"; }
else
{
echo "SHA-256 not supported.\n<br>";
}
```

```
// 以 $5$ 开始的 16 字符 salt。周长的默认数是 5000。
if (CRYPT_SHA512 == 1)
{
echo "SHA-512: ".crypt('something','$6$rounds=5000$anexamplestringforsalt$');
}
else
{
echo "SHA-512 not supported.";
}
?>
```

上面的代码的输出（取决于操作系统）：

```
Standard DES: stqAdD7zlbByI
Extended DES: _S4..someQXidlBpTUu6
MD5: $1$somethin$4NZKrUlY6r7K7.rdEOZ0w.
Blowfish: $2a$09$anexamplestringforsaleLouKejcjRlExmf1671qw3Khl49R3dfu
SHA-256: $5$rounds=5000$anexamplestringf$KIrctqsxo2wrPg5Ag/hs4jTi4PmoNKQUGWFXlVy9vu9
SHA-512: $6$rounds=5000$anexamplestringf$Oo0skOAdUFXkQxJpwzO05wgRHG0dhuaPBaOU/
oNbGpCEKlf/7oVM5wn6AN0w2vwUgA0O24oLzGQpp1XKI6LLQ0.
```

PHP String 函数