Sicherheit durch Verschlüsselung: Das MCrypt-Modul

Hintergrund

In der Zeit des modernen Webs wird Sicherheit immer wichtiger. Immer mehr Programme und Websiten versuchen, durch die Cookies im Browser an sensible Daten ihres Besitzers zu gelangen. Noch Fataler als bei Passwörtern wird es, wenn Kontodaten oder -verbindungen abgespeichert werden- da muss schnell die Polizei eingeschaltet werden.

Doch je besser die Diebe werden, desto weiter entwickelt sich auch die Software, sich vor diesen Kriminellen zu schützen. Immer kompliziertere Verschlüsselungsverfahren mit eigenen Keys machen das Ausspionieren von Daten immer schwerer- eines dieser Verschlüsselungsmodule nennt sich MCrypt.

Inhaltsverzeichnis

Einsatz

Da dies ein Zusatzmodul zu PHP ist und bei den meisten nicht von Beginn an integriert ist, muss es noch im nachhinein installiert werden. Da es dazu eine gute, Deutschsprachige Anleitung auf PHP.net gibt, werde ich zur Installation hier nichts mehr beitragen.

Neues Modul initialisieren

Zur initialisierung dieses Moduls gibt es in PHP die Funktion *mcrypt_module_open*:

Quellcode

```
1. $mcrypt = mcrypt_module_open('blowfish', '', 'cfb', '');
```

Im ersten Parameter wird der Name des verwendeten Algorithmus eingefügt.
Beispiel:
mcrypt_module_open(**'blowfish'**, '', 'cfb', '');

Im zweiten Parameter wird der Pfad zur MCrypt-Installation eingegeben (üblicherweise /usr/local/lib/lib/mcrypt). Wird dieser Parameter nicht übergeben, so wird automatisch nach der Installation gesucht/die Einstellungen aus der php.ini übernommen.

Im dritten Parameter wird der verwendete Modus angegeben.
Beispiel:
mcrypt_module_open('blowfish', '', **'cfb'**, '');

Im dritten Parameter wird ebenfalls der Pfad zur MCrypt-Installation angegeben. Wird dieser Parameter leer gelassen, so wird ebenfalls nach dem Installationspfad gesucht.

Text verschlüsseln

Zur Verschlüsselung eines Textes werden nach der Initialisierung die Funktionen *mcrypt_create_iv*, *mcrypt_enc_get_iv_size*, *mcrypt_generic_init[i][i][i],* [/i][/i]mcrypt_generic [/i] und *mcrypt_generic_deinit* benötigt.
Beispiel für eine Verschlüsselung:

Quellcode

```
1. $key = 'Dies ist ein Key, mit dem der Text verschluesselt wird.';
2. $text = 'Dies ist der zu verschluesselnde Text.';
3. $iv = mcrypt_create_iv(mcrypt_enc_get_iv_size($mcrypt), MCRYPT_RAND);
4. mcrypt_generic_init($mcrypt, $key, $iv);
5. $crypted = mcrypt_generic($mcrypt, $text);
6. mcrypt_generic_deinit($mcrypt);
7. echo $crypted;
8. //Ausgabe bei der hier verwendeten Verschlüsselung: 0Î©Ä£Ó-`ì@6J 'º]Ã‰çØ©ì}m,•bRÖ¶—jÐ™¢(+
```

Mit jeder Anfrage wird der verschlüsselte Text ein anderer, da durch MCRYPT_RAND (Erklärung weiter hinten) zu dem Schlüssel ($key) ein Zufallswert hinzugefügt wird.

mcrypt_create_iv

Quellcode

```
1. mcrypt_create_iv($size, $source = MCRYPT_DEV_RANDOM);
```

Im ersten Parameter wird die Größe des MCrypts angegeben. Dieser kann optimalerweise mit mcrypt_get_iv_size($mcrypt); angegeben werden.

Der zweite Parameter ist optional. Hier wird ein Quellverzeichniss angegeben, wobei von mir **ausdrücklich empfohlen** wird, MCRYPT_RAND anzugeben, da die anderen möglichen Angaben (MCRYPT_DEV_RANDOM, MCRYPT_DEV_URANDOM) **nicht** von Windows-Servern unterstützt werden.

mcrypt_get_iv_size
Diese Funktion gibt die Größe von $mcrypt zurück.

Quellcode

```
1. mcrypt_get_iv_size($mcrypt);
```

mcypt_generic_init
Diese Funktion muss aufgerufen werden, bevor der Text verschlüsselt werden kann.

Quellcode

```
1. mcrypt_generic_init($mcrypt, $key, $iv);
```

$mcrypt: Der MCrypt-Handler (Rückgabewert der Funktion mcrypt_module_open()).

$key: Ein beliebiger Schlüssel, mit dem der Text verschlüsselt werden soll.

$iv: Das initialation vector- Objekt (Rückgabewert der Funktion mcrypt_create_iv()).

mcrypt_generic
Verschlüsselt den angegebenen Text.

Quellcode

1. $crypted = mcrypt_generic($mcrypt, $text);

$mcrypt: Der MCrypt-Handler (Rückgabewert der Funktion mcrypt_module_open()).

$text: Der zu verschlüsselnde Text (z.B. ein Passwort).

mcrypt_generic_deinit
Diese Funktion beendet den Verschlüsselungsvorgang.

Quellcode

1. mcrypt_generic_deinit($mcrypt);

$mcrypt: Der MCrypt-Handler (Rückgabewert der Funktion mcrypt_module_open()).

McryptUtil-Klasse

Für mein Framework habe ich eine eigene McryptUtil-Klasse definiert, die den Einsatz von Mcrypt erleichtert und den Code auf bis zu 3 Zeilen minimiert.

McryptUtil::open()

Diese Funktion öffnet ein neues Mcrypt-Modul.
Verwendungsweise:

Quellcode

1. McryptUtil::open($algorithmus = 'blowfish', $mode = 'cfb');

$algorithm: Der zu verwendende Verschlüsselungs-Algorithmus.

$mode: Der zu verwendende Verschlüsselungsmodus.

McryptUtil::encrypt()

Diese Funktion verschlüsselt einen Text.
Verwendungsweise:

Quellcode

1. $crypted = McryptUtil::encrypt($text, $key);

$text: Der zu verschlüsselnde Text.

$key: Der bei der Verschlüsselung verwendete Schlüssel.

Rückgabewert: Der verschlüsselte Text.

McryptUtil::decrypt()
Entschlüsselt einen verschlüsselten Text.
Verwendungsweise:
Quellcode

```
1. $encrypted = McryptUtil::decrypt($crypted, $key);
```

$crypted: Der verschlüsselte Text.

$key: Der bei der Verschlüsselung verwendete Schlüssel.

Rückgabewert: Der entschlüsselte Text.

Beispiele
=== Ohne McryptUtil ===
Quellcode

```
1. $text = 'Dieser Text soll verschlüsselt werden!';
2. $key = 'Dies ist der Schlüssel, der bei der Verschlüsselung verwendet werden soll!';
3. $mcrypt = mcrypt_module_open('blowfish', '', 'cfb', '');
4. $ivsize = mcrypt_get_iv_size($mcrypt);
5. //Verschlüsselung
6. $iv = mcrypt_create_iv($ivsize, MCRYPT_RAND);
7. mcrypt_generic_init($mcrypt, $key, $iv);
8. $crypted = mcrypt_generic($mcrypt, $text);
9. mcrypt_generic_deinit($mcrypt);
10. echo $iv.$crypted; //Unidentifizierbare Anreihung von Sonderzeichen
11. //Entschlüsselung
12. $iv = substr($crypted, 0, $ivsize);
13. $crypted = substr($crypted, $ivsize);
14. mcrypt_generic_init($mcrypt, $key, $iv);
15. $encrypted = mdecrypt_generic($mcrypt, $crypted);
16. mcrypt_generic_deinit($mcrypt);
17. echo $encrypted; //"Dieser Text soll verschlüsselt werden!"
```

Alles anzeigen

Mit McryptUtil
Quellcode

```
1. $text = 'Dieser Text soll verschlüsselt werden!';
```

```
2. $key = 'Dies ist der Schlüssel, der bei der Verschlüsselung verwendet werden soll!';
3. McryptUtil::open();
4. $crypted = McryptUtil::encrypt($text, $key);
5. echo $crypted; //Unidentifizierbare Anreihung von Sonderzeichen
6. $encrypted = McryptUtil::decrypt($crypted, $key);
7. echo $encrypted; //"Dieser Text soll verschlüsselt werden!"
```

Meine Verschlüsselung funktioniert nicht!

- Ist Mcrypt installiert?
- Ist der Key bei der Entschlüsselung identisch mit dem Key bei der Verschlüsselung?