

# Présentation de la librairie Mcrypt pour chiffrer/déchiffrer ses données en PHP

par maxime.ohayon ([Site Perso](#))

Date de publication : 6/3/2008

Dernière mise à jour : 11/3/2008

La Bibliothèque Mcrypt offre la possibilité de chiffrer/déchiffrer des données en PHP via les algorithmes de chiffrement les plus utilisés (Blow Fish, Triplées, Saferplus, Enigma ...) et selon la plupart des modes de chiffrements (CBC, EBC, OFB ...).

- I - Cryptographie
  - I-A - Pourquoi crypter ?
  - I-B - Principes et Notions de la cryptographie à clé secrète
- II - Mcrypt
  - II-A - Qu'est-ce que Mcrypt ?
  - II-B - Pré-requis
  - II-C - Avec un exemple
- III - Conclusion

## I - Cryptographie

### I-A - Pourquoi crypter ?

La cryptographie est la discipline visant à protéger des messages via différentes opérations arithmétiques. Même si cette discipline est souvent rattachée à "une arme de guerre", elle permet d'assurer la confidentialité des messages.

La cryptographie se divise en deux parties:

- La cryptographie à clé secrète (dit chiffrement symétrique)
- La cryptographie à clé publique (dit chiffrement asymétrique)

Même si les deux concepts sont entièrement différents et très intéressants, dans le cadre de la librairie Mcrypt nous nous focaliserons sur le chiffrement symétrique.

### I-B - Principes et Notions de la cryptographie à clé secrète

Le concept fondamentale du chiffrement symétrique réside dans la clé, en effet c'est grâce à cet clé que l'on peut chiffrer et déchiffrer le message. Bien que ce procédé soit très ancien (on pourrait remonter jusqu'à l'Egypte), les techniques modernes ont apporté sécurité et performance dans ce domaine.

On distingue deux procédés de chiffrement symétrique :

- Le chiffrement par blocs, découpage des données en blocs de taille généralement fixe, les blocs sont chiffrés les uns après les autres.
- Le chiffrement par flots ou flux, traitement des données de longueur quelconque.

Je ne détaillerai pas plus ces deux procédés mais il est important de connaître leur principe.


De plus, on distingue la manière de traiter les blocs de textes clairs et chiffrés au sein d'un algorithme de chiffrement par blocs :

- (ECB), Dictionnaire de codes : il s'agit du mode le plus simple, le message est découpé en blocs qui sont chiffrés séparément les uns après les autres. Le gros désavantage réside dans le fait que deux blocs identiques auront leurs homologues chiffrés identiques.
- (CBC), Enchaînement des blocs : on applique sur chaque block un '#OU exclusif' avec le chiffrage du bloc précédent avant qu'il soit lui-même chiffré. De plus, afin de rendre chaque message unique, un vecteur d'initialisation est utilisé.
- (CFB), Chiffrement à rétroaction : il agit comme un chiffrement par flux, il génère un flux de clés qui est ensuite appliqué au document original, le flux de clé est obtenu en chiffrant le précédent blocs chiffré. Nécessite aussi un vecteur d'initialisation.
- (OFB), Chiffrement à rétroaction de sortie : similaire à CFB, le flux de clé est obtenu en chiffrant le précédent flux de clé. Nécessite aussi un vecteur d'initialisation.
- (CTR), Chiffrement basé sur compteur : similaire à CFB, le flux de clé est obtenu en chiffrant les valeurs successives d'un compteur. Nécessite aussi un vecteur d'initialisation.

Un vecteur d'initialisation est un bloc de données aléatoires qui permet de démarrer le chiffrement du premier bloc et fournir ainsi une forme de hasard indépendant des messages à chiffrer. Il n'a pas besoin d'être lui-même chiffré lors de la transmission, mais il ne doit jamais être réemployé avec la même clé.

## II - Mcrypt

### II-A - Qu'est-ce que Mcrypt ?

Mcrypt est une librairie écrite en C et en Assembleur qui implémente la majeure partie des algorithmes de chiffrement dans la plupart des modes de chiffrement. Cette librairie a été portée sur les plateformes Unix et Windows via des primitives PHP. Pour plus d'informations et installation veuillez vous référer à la  **doc**, cependant elle est fournie en standard avec Apache.

### II-B - Pré-requis

Les exemples de l'article, les modes et les algorithmes de chiffrement utilisés dans cet article sont présents à partir de la version 2.5.6 de Mcrypt.

Les modes de chiffrement sont représentés par les constantes PHP suivantes :

- MCRYPT\_MODE\_ECB
- MCRYPT\_MODE\_CBC
- MCRYPT\_MODE\_CFB
- MCRYPT\_MODE\_OFB
- MCRYPT\_MODE\_NOFB (comme OFB mais plus sûre)
- MCRYPT\_MODE\_STREAM

Les algorithmes de chiffrement sont représentés par les constantes PHP suivantes :

- MCRYPT\_3DES
- MCRYPT\_ARCFOUR\_IV
- MCRYPT\_ARCFOUR
- MCRYPT\_BLOWFISH
- MCRYPT\_CAST\_128
- MCRYPT\_CAST\_256
- MCRYPT\_CRYPT
- MCRYPT\_DES
- MCRYPT\_DES\_COMPAT
- MCRYPT\_ENIGMA
- MCRYPT\_GOST
- MCRYPT\_IDEA
- MCRYPT\_LOKI97
- MCRYPT\_MARS
- MCRYPT\_PANAMA
- MCRYPT\_RIJNDAEL\_128
- MCRYPT\_RIJNDAEL\_192

- MCRYPT\_RIJNDAEL\_256
- MCRYPT\_RC2
- MCRYPT\_RC4
- MCRYPT\_RC6
- MCRYPT\_RC6\_128
- MCRYPT\_RC6\_192
- MCRYPT\_RC6\_256
- MCRYPT\_SAFER64
- MCRYPT\_SAFER128
- MCRYPT\_SAFERPLUS
- MCRYPT\_SERPENT
- MCRYPT\_SERPENT\_128
- MCRYPT\_SERPENT\_192
- MCRYPT\_SERPENT\_256
- MCRYPT\_SKIPJACK
- MCRYPT\_TEAN
- MCRYPT\_THREEWAY
- MCRYPT\_TRIPLEDES
- MCRYPT\_TWOFISH
- MCRYPT\_TWOFISH128
- MCRYPT\_TWOFISH192
- MCRYPT\_TWOFISH256
- MCRYPT\_WAKE
- MCRYPT\_XTEA

Pour tous les modes sauf ECB, on utilisera un vecteur d'initialisation.

## II-C - Avec un exemple

Il existe plusieurs fonctions pour crypter/décrypter vos messages, certaines sont obsolètes, d'autres sont plus difficiles à employer pour un résultat similaire. Je vous présenterai ici la méthode générique qui fonctionne pour la majorité des algorithmes et des modes de chiffrements.

### Cryptage/Décryptage par l'algorithme triple Des

```
<?php
// On calcule la taille de la clé pour l'algo triple des
$cle_taille = mcrypt_module_get_algo_key_size(MCRYPT_3DES);
// On calcule la taille du vecteur d'initialisation pour l'algo triple des et pour le mode NOFB
$iv_taille = mcrypt_get_iv_size(MCRYPT_3DES, MCRYPT_MODE_NOFB);
//On fabrique le vecteur d'initialisation, la constante MCRYPT_RAND permet d'initialiser un vecteur
aléatoire
$iv = mcrypt_create_iv($iv_taille, MCRYPT_RAND);

$cle = "Ceci est une clé censé crypter un message mais à mon avis elle est beaucoup trop longue";
// On retaille la clé pour qu'elle ne soit pas trop longue
$cle = substr($cle, 0, $cle_taille);
```

### Cryptage/Décryptage par l'algorithme triple Des

```
// Le message à crypter
$message = "Voici mon super message que je dois crypter";
// On le crypte
$message_crypte = mcrypt_encrypt(MCRYPT_3DES, $cle, $message, MCRYPT_MODE_NOFB, $iv);
// On le décrypte
$message_decrypte = mcrypt_decrypt(MCRYPT_3DES, $cle, $message_crypte, MCRYPT_MODE_NOFB, $iv);

echo "Message en clair : $message <br/> Message crypté : $message_crypte <br /> Message décrypté :
$message_decrypte";
?>
```

Il vous suffira ensuite de changer les constantes d'algorithmes et de modes de chiffrement. Si vous utilisez toujours le même couple algorithme/mode de chiffrement, vous connaîtrez ainsi les bonnes longueurs de la clé et du vecteur d'initialisation.

Il ne vous reste plus qu'à faire votre propre fonction qui regroupe toutes ces primitives.

### III - Conclusion

Mcrypt est donc la solution pour crypter/décrypter en PHP, elle est très complète et robuste ; si on comptabilise le tout, on a une quarantaine d'algorithmes fonctionnant sur environ cinq modes de chiffrement, qui sont initialisables par un vecteur aléatoire, et par une clé secrète. En d'autres termes, il devient très difficile de casser vos messages !

