# Chiffrement à clé symétrique

Le chiffrement symétrique utilise la même clé pour le chiffrement et le déchiffrement.   
Ceci nécessite que l’émetteur et le récepteur du message partagent la même clé privée.

# Chiffrement de fichiers

## mcrypt

mcrypt est un **utilitaire de chiffrement simple**.

Lors du chiffrement et du déchiffrement d'un fichier, un **nouveau fichier est créé avec le suffixe .nc** et les **permissions 0600 (-rw-) sont attribuées**.   
(Lecture et écriture pour le propriétaire et aucune permission pour les autres).   
Le **nouveau fichier conserve la date de modification de l'original**.   
Le **fichier d'origine peut être supprimé en spécifiant le paramètre --unlink** (-u).

### Installation

Pour **installer mcrypt** …  
**>> sudo apt install mcrypt**

Pour **connaître la version installée** …  
**>> mcrypt --version  
Mcrypt v.2.6.8 (x86\_64-pc-linux-gnu)  
Linked against libmcrypt v.2.5.8  
Copyright (C) 1998-2002 Nikos Mavroyanopoulos (nmav@gnutls.org)**

Pour un peu d’aide …  
**>> mcrypt --help | less  
Mcrypt encrypts and decrypts files with symmetric encryption algorithms.  
Usage: mcrypt [-dFusgbhLvrzp] [-f keyfile] [-k key1 key2 ...] [-m mode] [-o keymode] [-s keysize] [-a algorithm] [-c config\_file] [file ...]  
…**

### Chiffrement d’un fichier

Pour chiffrer un fichier …  
**>> echo Ceci est un fichier chiffré > data.texte  
>> mcrypt data.texte  
Enter the passphrase (maximum of 512 characters)  
Please use a combination of upper and lower case letters and numbers.  
Enter passphrase: …  
Enter passphrase: …  
File data.texte was encrypted.**

Un nouveau fichier est créé avec l'extension .nc …  
**>> ls**   
**data.texte data.texte.nc**

**>> cat data.texte.nc  
m@rijndael-128 cbcmcrypt-sha1 ��29��>l��Ϯ�G�9sha1�X�eE�xӺ�i�,�4ՐN#xş����m#I�I&�7K��++��NG��M�I�eenR� �bCY�1�$��**

**Remarque** …  
Le **fichier original n’est pas supprimé**.

Pour supprimer le fichier d'entrée si l'ensemble du processus de chiffrement/déchiffrement réussit …  
**>> ls**  
**data.texte  
>> mcrypt -u data.texte  
>> mcrypt --unlink data.texte**  
**Enter the passphrase (maximum of 512 characters)  
Please use a combination of upper and lower case letters and numbers.  
Enter passphrase:   
Enter passphrase:   
File data.texte was encrypted.**  
**>>**  **ls**  
**data.texte.nc**

### Déchiffrement d’un fichier

Pour déchiffrer un fichier …  
**>> mcrypt -d data.texte.nc  
>> mcrypt --decrypt data.texte.nc   
mcrypt: data.texte already exists; do you wish to overwrite (y or n)?y  
Enter passphrase:   
File data.texte.nc was decrypted.**

## GPG (

L'utilitaire **GNU Privacy Guard** (GPG ou gpg) est un **outil de sécurité natif pour chiffrer les fichiers**.   
gpg est la **partie OpenPGP** (*Pretty Good Privacy*) de **GNU Privacy Guard** (GnuPG).   
Il s'agit d'un outil permettant de fournir des **services de chiffrement et de signature numériques** utilisant la norme OpenPGP.

GnuPG, est un outil **conforme à la norme Internet OpenPGP** qui est **utilisé pour la communication sécurisée** et le **stockage de données**. Il dispose d'un **système de gestion de clés robuste** et **s'intègre facilement à d'autres applications**.   
gpg propose une gestion complète des clés et toutes les fonctionnalités que l’on attend d'une implémentation complète d'OpenPGP.

L'utilitaire gpg possède beaucoup d'options.   
Toutefois, le **chiffrement et le déchiffrement sont faciles à faire** et nécessitent seulement que l'on connaisse trois options pour une utilisation rapide …

* **Créer ou chiffrer** (-c) ;
* **Déchiffrer** (-d)   
  et
* **Extraire et déchiffrer** (pas d'option).

### Installation de gpg

Pour **installer gpg** …  
**>> sudo apt install gpg**

Pour **connaître la version installée** …  
**>> gpg --version  
gpg (GnuPG) 2.2.27  
libgcrypt 1.8.8  
Copyright (C) 2021 Free Software Foundation, Inc.  
License GNU GPL-3.0-or-later** [**https://gnu.org/licenses/gpl.html**](https://gnu.org/licenses/gpl.html) **…**

Pour un peu d’**aide** …  
**>> gpg --help | less  
gpg –help  
gpg (GnuPG) 2.2.12  
libgcrypt 1.8.4  
...  
Commandes :  
-s, --sign faire une signature  
 --clear-sign faire une signature en texte clair  
 -b, --detach-sign faire une signature détachée  
 -e, --encrypt chiffrer les données  
…**

### Chiffrement d'un fichier

Il suffit d'avoir installé GnuPG pour chiffrer ou déchiffrer un fichier avec un secret partagé.

Pour **spécifier le chiffrement symétrique**, on utilise l'**option** **-c** ou **--symmetric** et on indique le fichier que l'on souhaite chiffrer.

La méthode rapide pour chiffrer un fichier consiste à exécuter la commande gpg avec l'option --symmetric ou -c (créer) …  
**>> echo Ceci est un test de chiffrement > fichier01.texte  
>> gpg --symmetric fichier01.texte**ou  
**>> gpg -c fichier01.texte   
<On saisit la phrase secrète et répéter la phrase secrète>**

Le chiffrement d'un fichier avec gpg **laisse le fichier d'origine intact** (fichier01.texte) et **ajoute le suffixe .gpg au fichier nouvellement chiffré**.   
On peut **supprimer le fichier d'origine** (fichier01.texte) afin que le **fichier chiffré soit la seule source d'informations qu'il contient**.   
Alternativement, si on souhaite partager la version chiffrée, on peut la renommer avant de la partager.

Le **suffixe .gpg n'est pas requis**.

Néanmoins, il permet à l'utilisateur de savoir quel outil de déchiffrement utiliser pour lire le fichier.   
On peut renommer le fichier comme on le souhaite …  
**>>** **file fichier01.texte.gpg  
fichier01.texte.gpg : GPG symmetrically encrypted data (AES256 cipher)  
>> mv fichier01.texte.gpg fichier01.doc  
>>** **file fichier01.doc  
fichier01.doc : GPG symmetrically encrypted data (AES256 cipher)**

### Déchiffrement d’un fichier

**Déchiffrer** un fichier signifie que l'on **élimine la notion de chiffrement afin de lire le contenu du fichier**.

**Remarque** …  
La valeur par défaut est d'**afficher** **le contenu sur la sortie standard et de laisser le fichier déchiffré en place**.  
Il n'y a **pas d'extraction de contenu ou de création du fichier d'origine lors du déchiffrement**.

Pour déchiffrer un fichier …  
**>> gpg --decrypt fichier01.doc**ou **>> gpg -d fichier01.doc   
gpg: chiffré avec 1 phrase secrète  
Ceci est un test de chiffrement**

**Remarque** …  
GnuPG **essaie d'utiliser ses mots de passe mis en cache** pour déchiffrer **avant de demander le secret partagé**.   
Le cache est basé sur une valeur salt spécifique au message, mais on peut utiliser l'**option** **--no-symkey-cache** pour que **gpg ignore le cache**.

La **valeur de délai d'attente par défaut est de 10 minutes**.

## openSSL

openSSL est une **boîte à outils de cryptographie** mettant en œuvre les protocoles réseau **Secure Sockets Layer**   
(SSL v2/v3) et **Transport Layer Security** (TLS v1) et les **normes de cryptographie connexes requises** par ceux-ci.

On peut utiliser le programme openssl qui est un **outil en ligne de commande pour utiliser les différentes fonctions de cryptographie** de la bibliothèque cryptographique d'OpenSSL à partir du shell.

Il peut être utilisé pour **chiffrer et déchiffrer des fichiers avec un mot de passe**.

### Chiffrement d'un fichier

Pour chiffrer le fichier **document.texte** en **document.out** en utilisant **AES 256 bits** en mode CBC …  
**>> echo Ceci est un test de chiffrement et de déchiffrement > document.texte  
>> openssl enc -aes-256-cbc -md sha512 -pbkdf2 -iter 100000 -salt -in document.texte -out document.aes  
Enter aes-256-cbc encryption password:  
Verifying - enter aes-256-cbc encryption password:**

Commutateurs de la commande ...

* **-aes-256-cbc** est ce que l’algorithme à utiliser pour une protection maximale.  
  La version 128 bits, le 3DES (Triple DES) a été abandonné il y a quelque temps.  
  AES est accéléré par tous processeurs modernes ;
* **-md sha512** est la variante la plus rapide de la famille de fonctions de hachage de la famille SHA-2 ;
* **-pbkdf2** permet d’utiliser l'algorithme PBKDF2 (Password-Based Key Derivation Function 2) ;
* **-iter** 100000 remplace le nombre d'itérations par défaut pour le mot de passe.  
  On utilise un nombre donné d'itérations sur le mot de passe pour dériver la clé de chiffrement. Des valeurs élevées augmentent le temps requis pour augmenter le déchiffrement par force brute Du fichier résultant.  
  Cette option permet d'utiliser l'algorithme PBKDF2 pour dériver la clé.

Pour vérifier le chiffrement …  
**>> diff document.texte document.aes**

### Déchiffrement d’un fichier

Pour déchiffrer un fichier à l’aide de openSSL …  
**>> openssl enc -d -aes-256-cbc -in document.aes**

### Autre algorithme de chiffrement

Pour chiffrer le fichier document.texte avec l’algorithme Blowfish en mode CBC, avec une clé générée par mot de passe, le chiffré étant stocké dans le fichier document.chiffré …  
**>> openssl enc -bf-cbc -pbkdf2 -in document.texte -out document.bf**

Pour déchiffrer le même message, on utilise la commande …  
**>> openssl enc -bf-cbc -d -in document.bf -out document.texte**

Pour vérifier le chiffrement …  
**>> diff document.texte document.bf**