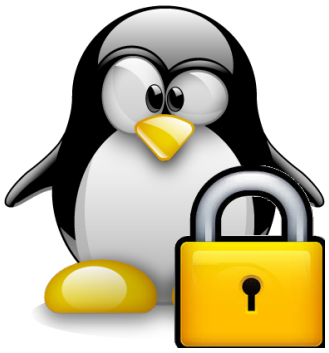
How to password encrypt / decrypt files on Linux to keep and pass your data private

Author : admin



If you have a sensitive data like a scan copy of your *ID card, Driving License, Birth Certificate, Marriage Certificate* or *some revolutionary business / idea or technology* and you want to transfer that over some kind of network lets say Internet vie some public unencrypted e-mail service like (Gmail.com / Yahoo Mail / Mail.com / (Bulgarian Mail Abv.bg)) etc. you will certainly want to transfer the file in encrypted form to prevent, someone sniffing your Network or someone having administrative permissions to servers of free mail where your mail data is stored.

Transferring your files in encrypted form become very important these days especially after recent **Edward Snowden** disclosures about American Mass Surveilance program PRISM - for those who didn't yet hear of ***PRISM*** (this *is a American of America's NSA - National Security Agency aiming to sniff and log everyone's information transferred in digital form via the Internet and even Mobile Phone conversations*)...

First step to mitigate surveilance is to use *fully free software (100% free software) OS* distribution like Trisquel GNU / Linux.
Second is to encrypt to **use encryption** - *the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key*.
There are many ways to **encrypt your data on Linux** and to later decrpyt it, I've earlier blogged about encryping files with GPG and OpenSSL on Linux, however encryption with GPG and OpenSSL is newer as concept than the **old-school way to encrypt files on UNIX** with **crypt** command which in Linux is replaced by **mcrypt** command.

mcrypt is provided by *mcrypt* package by default on most if not all Linux distributions, however mcrypt is not installed by default so to start using it you have to install it first.

1. Install mcrypt on Debian / Ubuntu / Mint (deb based) Linux

```
apt-get install --yes mcrypt
```

2. Install mcrypt on Fedora / CentOS rest of RPM bases Linux

```
yum -y install libmcrypt
```

3. Encrypting file with *mcrypt*

To get a list with all supported algorithms by mcrypt:

```
mcrypt --list
cast-128 (16): cbc cfb ctr ecb ncfb nofb ofb
gost (32): cbc cfb ctr ecb ncfb nofb ofb
rijndael-128 (32): cbc cfb ctr ecb ncfb nofb ofb
twofish (32): cbc cfb ctr ecb ncfb nofb ofb
arcfour (256): stream
cast-256 (32): cbc cfb ctr ecb ncfb nofb ofb
loki97 (32): cbc cfb ctr ecb ncfb nofb ofb
rijndael-192 (32): cbc cfb ctr ecb ncfb nofb ofb
saferplus (32): cbc cfb ctr ecb ncfb nofb ofb
wake (32): stream
blowfish-compat (56): cbc cfb ctr ecb ncfb nofb ofb
des (8): cbc cfb ctr ecb ncfb nofb ofb
rijndael-256 (32): cbc cfb ctr ecb ncfb nofb ofb
serpent (32): cbc cfb ctr ecb ncfb nofb ofb
xtea (16): cbc cfb ctr ecb ncfb nofb ofb
blowfish (56): cbc cfb ctr ecb ncfb nofb ofb
enigma (13): stream
rc2 (128): cbc cfb ctr ecb ncfb nofb ofb
```

tripledes (24): cbc cfb ctr ecb ncfb nofb ofb

mcrypt File-To-Crypt.PDF.cpy

Enter the passphrase (maximum of 512 characters)
Please use a combination of upper and lower case letters and numbers.
Enter passphrase:
Enter passphrase:

If crypt is invoked to create the encrypted file without OS redirects (), i.e.:

mcrypt -a blowfish File-To-Crypt.PDF

Please use a combination of upper and lower case letters and numbers.
Enter passphrase:
Enter passphrase:

File File-To-Crypt was encrypted.

mcrypt outputs encrypted file in **.nc** extension and the new file and file default mode of 0600 (read write only for root user) are set, while new file keeps the modification date of the original.

4. Decrypting file with *mcrypt*

Decryption of files is done ***mdecrypt***

```
mdecrypt File-To-Crypt.PDF.cpy
```

```
Enter passphrase:
File File-To-Crypt.PDF.cpy was decrypted.
```

To make mcrypt behave in a certain way when invoked modify **~/.mcryptrd**

mcrypt is also available as a module for php5 (**php5-mcrypt**).