Шифрование данных с помощью EncFS


Зачем нужно шифровать данные это всем понятно. Моя цель будет показать простой способ шифрования с автоматическим закачиванием в интернет зашифрованных файлов на примере Dropbox.

Где именно будут храниться зашифрованные файлы это не важно. Будь то Dropbox, ubuntuone или просто папка на своём же винчестере, нам надо чтобы шифровка/расшифровка происходила мгновенно и чтобы расшифрованные файлы были под рукой.

Для начала установим саму систему шифрования:

```
sudo apt-get install encfs libpam-mount
```

Следующим шагом нам нужно добавить себя в группу пользователей fuse

```
sudo adduser username fuse
```

заместо username пишем свой логин от входа в систему.
Что бы изменения вступили в силу завершаем сеанс и заходим заново.

Теперь нам надо создать 2 папки. Первая будет с не зашифрованными данными, вторая зашифрованная. Где их создавать и как называть не суть важно, но если будете их делать вне папки /home незабудьте дать права на запись.
Я помещу зашифрованную папку в Dropbox, а не зашифрованную в корень домашней папке.

```
mkdir ~/unencfs
mkdir ~/Dropbox/encfs
```

Теперь настроим само шифрование, вставляем в терминале следующую строчку заменив пути к папкам и username на свои

```
encfs /home/username/Dropbox/encfs /home/username/unencfs
```

Нажимаем энтер и отвечаем навопросы. Если не хотите заворачиваться жмите:

1. «x» для выбора режима эксперта.
2. «1» для выбора алгоритма шифрования «AES»

3. «256» для задания размера ключа в битах.
4. «1024» для задания размера блока файловой системы.
5. «1» для выбора алгоритма зашифровки «Block».
6. «y» для опции «Enable filename initialization vector chaining?»
7. «n» для опции «Enable per-file initialization vectors?»
8. «n» для опции «Enable block authentication code headers on every block in a file?»
9. «y» для опции «Enable file-hole pass-through?»
10. Вводим пароль. Если хотим чтобы расшифровка происходила сразу же после запуска системы, то вводим тотже пароль что у нас стоит на вход в систему
11. Подтверждаем пароль

При следующем выполнение команды нам нужно будет ввести только пароль.

Команда, по сути, монтирует папку как новую файловую систему и если отмонтировать, то папка с расшифрованными данными очиститься:

```
sudo umount ~/unencfs
```

Что бы настроить авто-монтирование при запуске то открываем файл pam_mount.conf.xml

```
sudo gedit /etc/security/pam_mount.conf.xml
```

Находим в нём строчку *<!— Volume definitions —>* и вставляем после неё :

```
<volume user="username" fstype="fuse"
path="encfs#/home/username/Dropbox/encfs"
mountpoint="/home/username/unencfs" />
```

Заменив username и пусть к папкам на свои.

ВНИМАНИЕ! У некоторых автомонтирование не работает и система после этого вообще не грузится. У меня так и случилось. Паниковать не стоит. Если в течении 5 минут у нас только тёмный экран после загрузки, то нажимаем Alt-Ctrl-F1, вводим свой логин и пароль и нажимаем стрелку вверх пока не дойдём до команды с открытием файла pam_mount.conf.xml. Слегка изменим её:

```
sudo nano /etc/security/pam_mount.conf.xml
```

nano это консольный редактор. Сотрём то что мы в нём изменили и сохраняем: Ctrl-X на вопрос сохранении отвечаем Y, и оставляем тоже имя.

Но такая проблема только у единиц, практически у всех автомонтирование работает без проблем.
Что бы упростить процесс монтирования можно создать текстовый файл:

```
#!/bin/bash
encfs /home/zegi/Dropbox/encfs /home/zegi/unencfs
```

и запускать его в терминале. Или упростить команду с помощью алиасов

Как работает шифрование: всё что мы закидываем в папку ~/unencfs автоматически шифруется и помещается в ~/Dropbox/encfs. Папки абсолютно синхронизированы. В зашифрованной папке будет файл .encfs6.xml НЕ УДАЛЯЙТЕ его. В нём хранятся данные о шифровке.

Чтобы изменить пароль вводим команду:

```
encfsctl passwd путь_к_зашифрованной_папке
```

Но для этого надо помнить старый пароль ;)