

Encrypted File Systems

Encrypting your USB stick

Reference: <http://emcken.dk/weblog/archives/164-encrypted-usb-drive-in-ubuntu.html>

GUI (Which doesn't work! plus it automatically selects a filesystem you may not want):
<http://mandalka.name/usbcryptformat/index.html.en>

cryptkeeper - gnome GUI app for encrypting directories.

Before encryption

Backup data
Double check your USB stick device name using: 'df -h'
Unmount drive

Encryption

Install crypt package and load.

```
sudo apt-get install cryptsetup  
sudo modprobe dm-crypt
```

Setup Encryption

```
$ sudo cryptsetup --verbose --verify-passphrase luksFormat /dev/sdd1
```

Connect to the encrypted partition

```
$ sudo cryptsetup luksOpen /dev/sdd1 sdd1
```

Make the filesystem

```
$ sudo mkfs.ext4 /dev/mapper/sdd1
```

Close link to encrypted partition.

```
sudo cryptsetup luksClose sdd1
```

After encryption

When you enter the drive in Ubuntu 8.10 or greater it will automatically ask you for a password.

Allow write/read access to the USB

```
$ sudo chmod 777 /media/disk
```

Copy your data back.

Other computers

If you want to read your memory stick on other computers you will need to install the **cryptsetup** package.

Windows reference: <http://www.mayrhofer.eu.org/Default.aspx?pageid=34>