

## 4.8.V Datenträger/Verschlüsselung – Versuch

### 4.8.V.1 Beispiel anhande der Verschlüsselung einer 1 GiB großen Datei

- a) Datei erstellen (ca. 30 MiB für Header, daher mind. 64 MiB):

```
Terminal
root@debian964:~# dd if=/dev/zero bs=1M count=1024 of=cont.txt
root@debian964:~# ls -ltrh cont.txt
```

- b) Verschlüsselung bewirken, vorher Passwort wählen:

```
Terminal
root@debian964:~# /sbin/cryptsetup luksFormat -c aes-xts-plain64\
-s 512 -h sha512 -y cont.txt
```

- c) Entschlüsselt öffnen und geöffnetem Gerät zuweisen, dazu vorher gewähltes Passwort eingeben:

```
Terminal
root@debian964:~# /sbin/cryptsetup luksOpen cont.txt contdat
```

- d) Geöffnetes Gerät formatieren:

```
Terminal
root@debian964:~# /sbin/mkfs.ext3 /dev/mapper/contdat
root@debian964:~# /sbin/tune2fs -L conti /dev/mapper/contdat
```

- e) Und mounten (einhängen):

```
Terminal
schueler@debian964:~$ /bin/mount /dev/mapper/contdat /mnt
schueler@debian964:~$ ls -l /mnt
schueler@debian964:~$ df -h
```

- f) Und nutzen:

```
Terminal
schueler@debian964:~$ echo 123 > /mnt/datei.txt
schueler@debian964:~$ ls -l /mnt
schueler@debian964:~$ df -h
```

- g) Ende der Nutzung, aushängen:

```
Terminal
schueler@debian964:~$ umount /mnt
```

- h) Gerätezuweisung beenden (geöffnetes Gerät schließen):

```
Terminal
schueler@debian964:~$ /sbin/cryptsetup luksClose contdat
schueler@debian964:~$ ls -l /dev/mapper/c* # nicht mehr sichtbar
```

- i) Geschlossenes Gerät hat nur lesbaren Header, den anzeigen:

```
Terminal
schueler@debian964:~$ /sbin/cryptsetup luksDump cont.txt
schueler@debian964:~$ ls -l cont.txt
```