

# LUKS

## Mount encrypted partition

```
cryptsetup luksOpen /dev/mmcblk1p3 mmcblk2p3_crypt  
mount /dev/vgkubuntu/root /target # use lvdisplay to find the volume
```

## Change key of encrypted partition

```
cryptsetup luksChangeKey /dev/sdX
```

## Extend encrypted partition

- <https://unix.stackexchange.com/a/322631>

## Setup automatic unlock

```
apt install -y clevis clevis-luks clevis-udisks2 clevis-systemd clevis-tpm2  
clevis-initramfs  
clevis luks bind -d /dev/mmcblkp3 tpm2 '{"pcr_ids":"1,7","key":"rsa"}'  
systemctl enable clevis-luks-askpass.path  
update-initramfs -u -k all
```

## Regenerate

If automatic unlock does not work anymore it needs to be regenerated. First list the used slots:

```
clevis luks list -d /dev/nvme0n1p3
```

Then regenerate the used slot:

```
clevis luks regen -d /dev/nvme0n1p3 -s 1
```

## References

- <https://tqdev.com/2023-luks-recovery-from-initramfs-shell>
- <https://fedoramagazine.org/automatically-decrypt-your-disk-using-tpm2/>
- <https://github.com/latchset/clevis/issues/165>
- <https://unix.stackexchange.com/questions/704813/ubuntu-20-04-clevis-luks-setup-auto-unlockin>

### g-not-working

- <https://wiki.archlinux.org/title/Clevis>
- [https://wiki.archlinux.org/title/Trusted\\_Platform\\_Module#Accessing\\_PCR\\_registers](https://wiki.archlinux.org/title/Trusted_Platform_Module#Accessing_PCR_registers)
- <https://www.tuxedocomputers.com/en/Infos/Help-Support/Instructions/Change-LUKS-encryption-password.tuxedo>

From:  
<https://wiki.web.home.dark-link.info/> - **Patchouli's Library**

Permanent link:  
<https://wiki.web.home.dark-link.info/doku.php?id=tech:cheatsheets:linux:luks&rev=1712066818>

Last update: **2024/04/02 14:06**

