Encrypt USB Drive partitions using LUKS.

LUKS, the **L**inux **U**nified **K**ey **S**etup, is a Linux standard for disk encryption. It adds a standardised header at the start of the device, a key-slot area directly behind the header and the bulk data area behind that. The whole set is called a 'LUKS container'. The device that a LUKS container resides on is called a 'LUKS device'.

Two tools are required.

cryptsetup for setting up encrypted filesystems (with the help from ***device mapper*** and ***dm-crypt*****)**.
gnome-disk-utility to create and encrypt partitions
I recommend that you read at least the intro to '**man cryptsetup'** before you start.

Install the tools.

```
sudo apt-get install -y gnome-disk-utility cryptsetup
```

Encrypting an existing partition.

The encryption will only be read/writable from Linux systems with ***cryptsetup*** installed.
The encryption process will destroy all the existing data on the USB so,
back up any data on drive that you need to keep before you start.

From your desktop menu launch the app labeled **Disks** or use the terminal command ***gnome-disks.***
Insert the USB drive.
Select the USB drive you want to format, then click on the partition you want to encrypt,

- Click on the gear (cog) icon
- Select "Format Partition"
- Select these two options:
  "Don’t overwrite existing data" *
  "Encrypted, compatible with Linux systems"
- Give the encrypted partition a name
- Click "Show Passphrases".
- Enter a strong encryption passphrase. **
- Verify the passphrase.
- Click **Format**.
- You will be prompted to verify.
- Check the "Affected Devices" list and if OK then,
- Click **Format** for a second time to verify.

When the process is completed a lock icon will appear in the lower right corner to indicate that you have created a 'LUKS device'.

Footnotes.
* Selecting "Don’t overwrite existing data" will speed up the formatting process, but any data originally on the USB drive is always lost because once the drive is encrypted that data is not retrievable.

** Do not use passphrases containing non-ASCII characters, because the non-ASCII characters may vary depending on the keymapping of the computer or the OS you are using.

LibreCrypt: Transparent on-the-fly disk encryption for Windows should be LUKS compatible.
https://n0where.net/open-source-disk-encryption-for-windows-librecrypt/