To set things up, you will need to get your RPi Zero connected to the Internet and some very light soldering to put everything together will be necessary. Neither of these topics will be covered here.

**Software**

* Get the latest Raspbian image. The one I used was **2017-09-07-raspbian-stretch-lite**.
* Connect via SSH (or otherwise) to your RPi.
* sudo apt-get update --fix-missing
* Install pip for Python 3:
  + sudo apt-get install python3-pip
* Install the Python 3 dependencies. Expect this to take way more time than it does on your own computer:
  + pip3 install pycrypto
  + pip3 install pyinotify
  + pip3 install RPi.GPIO
* Install udiskie which will help us automount the removable drives:
  + sudo apt-get install python3-udiskie
* udiskie will not allow you to mount disks as a non-root user. That is technically not necessary, but I did not like it, so I made some changes in the configuration files.
  + sudo nano /usr/share/polkit-1/actions/org.freedesktop.udisks2.policy
  + Change all <allow\_any>auth\_admin</allow\_any><allow\_inactive>auth\_admin</allow\_inactive> to:
  + <allow\_any>yes</allow\_any><allow\_inactive>yes</allow\_inactive>
* Use RPi's hardware random number generator to generate entropy.
  + Install rng-tools:
    - sudo apt-get install rng-tools
  + Enable the use of /dev/hwrng by editing /etc/default/rng-tools:
    - sudo nano /etc/default/rng-tools
    - Add HRNGDEVICE=/dev/hwrng to the file (or uncomment the existing entry)
* Launch the script on start-up as non-root user by adding it before exit 0 in /etc/rc.local:
  + sudo nano /etc/rc.local
  + Add the following lines:

# Run udiskie

su pi -c '/usr/bin/udiskie --no-notify --no-file-manager &'

# Create mountpoint if it does not exist so we can monitor it with the Python script

su pi -c '/bin/mkdir -p /media/pi'

# Run Cryptopuck and save logs

su pi -c '/usr/bin/python3 /home/pi/cryptopuck/cryptopuck.py --mountpoint=/media/pi/ --public-key=/home/pi/cryptopuck/key.public >> /home/pi/cryptopuck.log 2>&1 &'

* Transfer this repository to RPi's /home/pi folder. You can either use git or copy the files directly to the microSD card.
* Generate the public and private key pair:
  + python3 generate\_keys.py
* Move the private key (key.private) off the Cryptopuck. **You should never use Cryptopuck with the private key stored on the Raspberry Pi as if the perpetrator discovers it, they will be able to decrypt your files.**
* If you wish to never have stored the private key on the Cryptopuck, do the above process on your own computer and transfer **the public key** to the Cryptopuck.
* That was about it! After you have encrypted the drive, you can plug it into your computer where the private key is stored to decrypt your files. To achieve that, you should install the Python 3 and PyCrypto on your computer and use the decrypt.py script:
  + python3 decrypt.py --source=/path/to/your/drive/ --destination=/path/to/your/drive/ --private-key=/path/to/your/key.private