CryptoParty!!

Here are some notes to help you along the way.

1 Installing Gnu Privacy Guard (GPG)

```
sudo apt-get install gnupg2 gnupg-agent pinentry-gtk2
```

2 Installing a friendly GUI for GPG

```
sudo apt-get install gpa
```

3 Generate a key

`gpg2 --full-gen-key` or `gpg2 --gen-key`

Recommended options

- Encryption/Signing type = RSA and RSA
- RSA key size = 2048 ("4096 gives us almost nothing, while costing us quite a lot")
- Key expiration date = 1y (One year. You can easily extend this later.)
- You can also add new email addresses to the same key later
- Leave the comment blank
- Choose a **secure** password

4 GPG commands

Encrypt a file: `gpg2 --encrypt --armor secretstuff.txt`
Decrypt a file: `gpg2 --decrypt secretstuff.txt`
Copy your privatekey: `gpg2 --export-secret-keys --armor <email> > privkey.asc`
Copy your publickey: `gpg2 --armor --output public.key --export <email>`
List publickeys: `gpg2 --list-keys`
List privatekeys: `gpg2 --list-secret-keys`

5 More fun places to go

Send encrypted chat messages from your phone
https://whispersystems.org/

Encrypt your text messages
https://smssecure.org/

Encrypt a folder on your Linux computer
https://github.com/vgough/encfs/

Use HTTPS by default where available
https://www.eff.org/Https-everywhere/

Get a free signed SSL certificate
https://letsencrypt.org/

Manage your passwords with gpg and git
https://www.passwordstore.org/