Installing PGP

1. sudo apt update
2. sudo apt install gnupg

Creating the Keys

1. Open the terminal
2. gpg --generate-key
3. Enter your name
4. Enter your email
5. Select o
6. Enter a Private Shared Key (Don't lose this) – Needed to decrypt

Uploading the key

1. Export your key by issuing this command (where GPGKEY is defined above) : gpg --export -a $GPGKEY > mykey.asc.
2. Upload the file mykey.asc to https://keys.openpgp.org/upload

Encrypt Message to someone with a public key

1. Get public key from keys.openpgp.org
2. Import key with gpg --import keyname.asc
3. Create message
4. Encrypt message with gpg --encrypt --armor -r ssteiner@ewu.edu --output message.enc message.txt
5. You will get the warning
   It is NOT certain that the key belongs to the person named
   in the user ID. If you *really* know what you are doing,
   you may answer the next question with yes.

   Use this key anyway? (y/N) y

Decrypt Message from someone who has your public key

1. Save the message
2. Open your terminal and navigate to the message
3. gpg --decrypt message.enc
4. Enter your Private Shared Key from when you created your keys.
5. Message is displayed

Encrypt Message to someone with a public key with no warning

1. Get public key from keys.openpgp.org
2. Import key with gpg --import keyname.asc
3. Edit the trust of the public key
4. gpg –edit-key key email address
5. Enter trust
6. Select option 5
7. Encrypt message with gpg --encrypt --armor -r ssteiner@ewu.edu --output message.enc message.txt