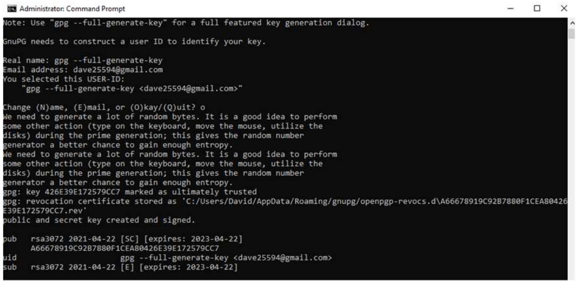
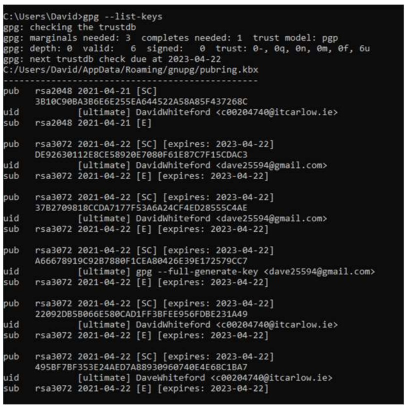
Lab 12

Creation of key



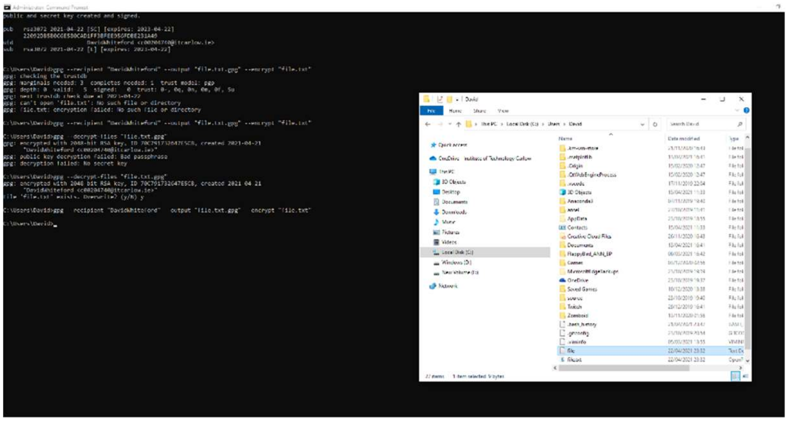
```
Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

GnuPG needs to construct a user ID to identify your key.

Real name: gpg --full-generate-key
Email address: dave25594@gmail.com
You selected this USER-ID:
    "gpg --full-generate-key <dave25594@gmail.com>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? o
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: key 426E39E172579CC7 marked as ultimately trusted
gpg: revocation certificate stored as 'C:/Users/David/AppData/Roaming/gnupg/openpgp-revocs.d\A66678919C92B7880F1CEA80426
E39E172579CC7.rev'
public and secret key created and signed.

pub   rsa3072 2021-04-22 [SC] [expires: 2023-04-22]
      A66678919C92B7880F1CEA80426E39E172579CC7
uid                      gpg --full-generate-key <dave25594@gmail.com>
sub   rsa3072 2021-04-22 [E] [expires: 2023-04-22]
```

Lists of keys



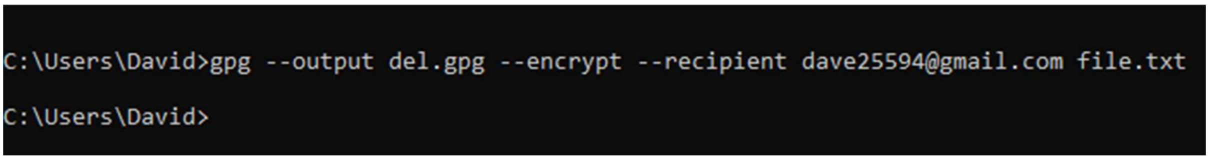
```
C:\Users\David>gpg --list-keys
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   6  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 6u
gpg: next trustdb check due at 2023-04-22
C:/Users/David/AppData/Roaming/gnupg/pubring.kbx
------------------------------------------------
pub   rsa2048 2021-04-21 [SC]
      3B10C90BA3B6E6E255EA644522A58A85F437268C
uid           [ultimate] DavidWhiteford <c00204740@itcarlow.ie>
sub   rsa2048 2021-04-21 [E]

pub   rsa3072 2021-04-22 [SC] [expires: 2023-04-22]
      DE92630112E8CE58920E7080F61E87C7F15CDAC3
uid           [ultimate] DavidWhiteford <dave25594@gmail.com>
sub   rsa3072 2021-04-22 [E] [expires: 2023-04-22]

pub   rsa3072 2021-04-22 [SC] [expires: 2023-04-22]
      37B2709818CCDA7177F53A6A24CF4ED28555C4AE
uid           [ultimate] DavidWhiteford <dave25594@gmail.com>
sub   rsa3072 2021-04-22 [E] [expires: 2023-04-22]

pub   rsa3072 2021-04-22 [SC] [expires: 2023-04-22]
      A66678919C92B7880F1CEA80426E39E172579CC7
uid           [ultimate] gpg --full-generate-key <dave25594@gmail.com>
sub   rsa3072 2021-04-22 [E] [expires: 2023-04-22]

pub   rsa3072 2021-04-22 [SC] [expires: 2023-04-22]
      22092DB5B066E580CAD1FF3BFEE956FDBE231A49
uid           [ultimate] DavidWhiteford <c00204740@itcarlow.ie>
sub   rsa3072 2021-04-22 [E] [expires: 2023-04-22]

pub   rsa3072 2021-04-22 [SC] [expires: 2023-04-22]
      495BF7BF353E24AED7A88930960740E4E68C1BA7
uid           [ultimate] DaveWhiteford <c00204740@itcarlow.ie>
sub   rsa3072 2021-04-22 [E] [expires: 2023-04-22]
```

File Encryption



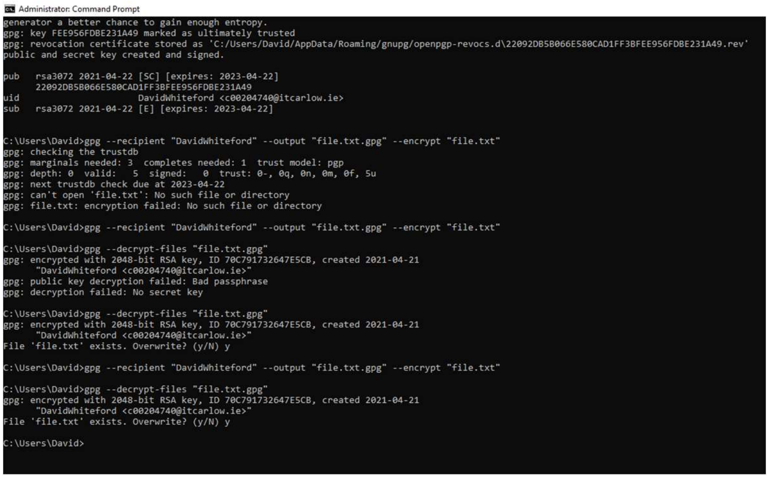
```
public and secret key created and signed.

pub   rsa3072 2021-04-22 [SC] [expires: 2023-04-22]
      22092DB5B066E580CAD1FF3BFEE956FDBE231A49
uid                      DavidWhiteford <c00204740@itcarlow.ie>
sub   rsa3072 2021-04-22 [E] [expires: 2023-04-22]

C:\Users\David>gpg --recipient "DavidWhiteford" --output "file.txt.gpg" --encrypt "file.txt"
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   5  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 5u
gpg: next trustdb check due at 2023-04-22
gpg: can't open 'file.txt': No such file or directory
gpg: file.txt: encryption failed: No such file or directory

C:\Users\David>gpg --recipient "DavidWhiteford" --output "file.txt.gpg" --encrypt "file.txt"

C:\Users\David>gpg --decrypt-files "file.txt.gpg"
gpg: encrypted with 2048-bit RSA key, ID 70C791732647E5C8, created 2021-04-21
      "DavidWhiteford <c00204740@itcarlow.ie>"
gpg: public key decryption failed: Bad passphrase
gpg: decryption failed: No secret key

C:\Users\David>gpg --decrypt-files "file.txt.gpg"
gpg: encrypted with 2048 bit RSA key, ID 70C791732647E5C8, created 2021 04 21
      "DavidWhiteford <c00204740@itcarlow.ie>"
File 'file.txt' exists. Overwrite? (y/N) y

C:\Users\David>gpg   recipient "DavidWhiteford"   output "file.txt.gpg"   encrypt "file.txt"

C:\Users\David>_
```

File Sent to other email



```
C:\Users\David>gpg --output del.gpg --encrypt --recipient dave25594@gmail.com file.txt

C:\Users\David>
```

File Decryption



```
generator a better chance to gain enough entropy.
gpg: key FEE956FDBE231A49 marked as ultimately trusted
gpg: revocation certificate stored as 'C:/Users/David/AppData/Roaming/gnupg/openpgp-revocs.d\22092DB5B066E580CAD1FF3BFEE956FDBE231A49.rev'
public and secret key created and signed.

pub   rsa3072 2021-04-22 [SC] [expires: 2023-04-22]
      22092DB5B066E580CAD1FF3BFEE956FDBE231A49
uid                      DavidWhiteford <c00204740@itcarlow.ie>
sub   rsa3072 2021-04-22 [E] [expires: 2023-04-22]


C:\Users\David>gpg --recipient "DavidWhiteford" --output "file.txt.gpg" --encrypt "file.txt"
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   5  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 5u
gpg: next trustdb check due at 2023-04-22
gpg: can't open 'file.txt': No such file or directory
gpg: file.txt: encryption failed: No such file or directory

C:\Users\David>gpg --recipient "DavidWhiteford" --output "file.txt.gpg" --encrypt "file.txt"

C:\Users\David>gpg --decrypt-files "file.txt.gpg"
gpg: encrypted with 2048-bit RSA key, ID 70C791732647E5CB, created 2021-04-21
      "DavidWhiteford <c00204740@itcarlow.ie>"
gpg: public key decryption failed: Bad passphrase
gpg: decryption failed: No secret key

C:\Users\David>gpg --decrypt-files "file.txt.gpg"
gpg: encrypted with 2048-bit RSA key, ID 70C791732647E5CB, created 2021-04-21
      "DavidWhiteford <c00204740@itcarlow.ie>"
File 'file.txt' exists. Overwrite? (y/N) y

C:\Users\David>gpg --recipient "DavidWhiteford" --output "file.txt.gpg" --encrypt "file.txt"

C:\Users\David>gpg --decrypt-files "file.txt.gpg"
gpg: encrypted with 2048-bit RSA key, ID 70C791732647E5CB, created 2021-04-21
      "DavidWhiteford <c00204740@itcarlow.ie>"
File 'file.txt' exists. Overwrite? (y/N) y

C:\Users\David>
```