

GPG Cheatsheet

Create a key:

```
gpg --gen-key
```

You may either select the defaults (RSA and RSA with GPG2) or use the more widespread DSA and Elgamal.

List private keys:

```
gpg --list-secret-keys
```

List public keys:

```
gpg --list-keys
```

Delete an private key:

```
gpg --delete-secret-key "username"
```

This deletes the secret key from your secret key ring.

Delete a public key:

```
gpg --delete-key "username"
```

Removes the public key associated with 'username' from your public key ring, but only if there is no associated private key.

Export a private key into file:

```
gpg -a --export-secret-keys XXXXXXXXX | gpg -aco privatekey.pgp.asc
```

Creates a file called 'privatekey.pgp.asc' with the encrypted and ASCII armored representation of the private key for the entered ID (XXXXXXX).

Export a public key into file:

```
gpg -ao publickey.asc --export name@domain.com
```

Outputs your public key as an ASCII armored file 'publickey.asc' (replacing 'name@domain.com' with the email address for your key).

Import a private key:

```
gpg --allow-secret-key-import --import private.key
```

Adds the private key in the file 'private.key' to your private key ring.

Import a public key:

```
gpg --import public.key
```

Adds the public key in the file 'public.key' to your public key ring.

Encrypt data:

```
gpg -e -u "sender username" -r "receiver username" somefile
```

Options:

```
-u
```

Specifies the secret key to be used.

```
-r
```

Specifies the public key of the recipient.

Example:

```
gpg -e -u "yourname" -r "receivename" yourfile.zip
```

Creates a file called 'yourfile.zip.gpg' that contains the encrypted data.

Decrypt data:

```
gpg -d yourfile.zip.gpg
```

You will be asked to enter your passphrase.

Generate a revocation certificate:

```
gpg -ao certificate.asc --gen-revoke XXXXXXXXX
```

Starts the process for creating a revocation certificate for the entered ID (XXXXXXX).

Send public key to a keyserver:

```
gpg --keyserver serverurl --send-keys XXXXXXXXX
```

Sends a key with the ID 'XXXXXXX' to a keyserver with the optional URL 'serverurl' (for example <http://pool.sks-key-servers.net>).

Get public key from a keyserver:

```
gpg --keyserver serverurl --recv-key XXXXXXXXX
```

Gets a key with the ID 'XXXXXXX' from a keyserver with the URL 'serverurl' (for example <http://pool.sks-key-servers.net>).