# GPG Key Management and File Decryption Guide

## 1. Generate a New GPG Key

To generate a new GPG key pair, use the following command:  
  
gpg –full-generate-key

Follow the prompts to configure your key type, size, and expiration settings.

## 2. View Generated Keys

After generating a key, you can list your secret keys using:  
  
gpg –list-secret-keys

This will display the key ID and other details of your private key.

## 3. Export the Public Key (Optional)

To share your public key with others, export it using:  
  
gpg --armor --export <key\_id> > public-key.asc  
  
Replace `<key\_id>` with the actual key ID retrieved from the previous step.

## 4. Export the Private Key (Optional)

If you need to back up or transfer your private key, export it securely:  
  
gpg --armor --export-secret-keys <key\_id> > private-key.asc  
  
Ensure that you store the exported private key in a secure location.

## 5. Import a GPG Key File

To import a previously saved GPG key, use:  
  
gpg --import /path/to/private-key.gpg  
  
This will add the key to your keyring for further use.

## 6. Decrypt a File

To decrypt an encrypted file, run:  
  
gpg --output decrypted\_file --decrypt /path/to/encrypted\_file.gpg  
  
This command will prompt for the passphrase if required and output the decrypted content to `decrypted\_file`.

## 7. Decrypt Without Importing the Key

If you need to decrypt a file without permanently importing the key, use:  
  
gpg --homedir /custom/keyring --decrypt --output decrypted\_file encrypted\_file.gpg  
  
Replace `/custom/keyring` with the directory where your key is temporarily stored.

## Security Considerations

- Keep your private key secure and never share it.  
- Use a strong passphrase for added protection.  
- Consider using a key expiration date to limit risk.