

GPG Quick Reference Guide

Installation & Setup

```
bash

# Check if GPG is installed
gpg --version

# Install GPG (if needed)
sudo apt-get install gnupg

# Get help
gpg --help
man gpg
```

Basic File Encryption

Create Test File

```
bash

echo "This is a sensitive message" > sensitive.txt
cat sensitive.txt
```

Encrypt File (Symmetric)

```
bash

gpg --symmetric sensitive.txt
# Creates: sensitive.txt.gpg
```

Decrypt File

```
bash

gpg --output decrypted.txt --decrypt sensitive.txt.gpg
cat decrypted.txt
```

List Files

```
bash
```

```
ls
```

```
# Shows: sensitive.txt, sensitive.txt.gpg, decrypted.txt
```

Common Issues & Solutions

Incorrect passphrase:

- Error: `gpg: decryption failed: bad key`
- Solution: Enter correct passphrase

File not found:

- Check file paths are correct
- Use `ls` to verify files exist

Permission issues:

- Run with `sudo` if needed
- Check file permissions

Command Breakdown

`gpg --symmetric filename`

- `gpg` = calls GPG tool
- `--symmetric` = uses same password for encrypt/decrypt
- `filename` = file to encrypt

`gpg --output newfile --decrypt encrypted.gpg`

- `--output newfile` = where to save decrypted data
- `--decrypt` = tells GPG to decrypt
- `encrypted.gpg` = encrypted file to decrypt