

**NAME**

`pass` - a simple password manager

**SYNOPSIS**

```
pass [ -de ] [ keywords... ]
```

**DESCRIPTION**

`pass` manages a plaintext database of passwords, letting you encrypt/decrypt or search the encrypted database using GnuPG. The plaintext database is `~/.passwords` by default, and `~/.passwords.gpg` if it is encrypted. With no arguments, `pass` will simply print the database. If you supply keyword arguments, it will search for lines in the database containing those keywords. (in both cases this will only work if you actually have an encrypted database)

There are two flags, `-d` will decrypt the password database, and `-e` will copy the plaintext file into an encrypted database, then overwrite the plaintext file with garbage before deleting it.

**EXAMPLE**

```
pass -d
echo Bank Pincode 12345 >> ~/.passwords
pass -e
pass bank
Bank Pincode 12345
```

**BUGS**

`pass` tries to purge the plaintext passwords from disk when encrypting the database, but it is technically impossible to guarantee that this is done. Filesystems and harddisks often do their own internal caching, which the script has no control over. Additionally no attempt is made to purge the plaintext passwords from system memory. `pass` makes it more difficult to recover your plaintext passwords, but not impossible.

Make sure that the text editor you are using doesn't make automatic backups, otherwise your passwords will be saved as plaintext in those backup files.

There is no way to restore a corrupted database, so its wise to backup the encrypted database before making adjustments to it.

**SEE ALSO**

`gpg2(1)`