

**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. The plaintext database is `~/.passwords` by default, and `~/.passwords.cpt` 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 zeros and ones before deleting it. The encrypted database can be edited directly with the standard text editor, *ed*, by invoking it with the `-x` flag.

**EXAMPLE**

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

**BUGS**

*pass* The method that *pass* uses to overwrite contents before deletion, and the method of encryption are arcane, crude and not at all secure in any sense of the word.

Your password is not double checked when encrypting the database, and there is no way to restore a corrupted database, so be sure to take regular backups.

**SEE ALSO**

*crypt*(1), *ed*(1)