NAME

enigma, **crypt** - very simple file encryption

SYNOPSIS

enigma [**-s**] [**-k**] [*password*]
crypt [**-s**] [**-k**] [*password*]

DESCRIPTION

The **enigma** utility, also known as **crypt** is a *very* simple encryption program, working on a "secret-key" basis. It operates as a filter, i.e., it encrypts or decrypts a stream of data from standard input, and writes the result to standard output. Since its operation is fully symmetrical, feeding the encrypted data stream again through the engine (using the same secret key) will decrypt it.

There are several ways to provide the secret key to the program. By default, the program prompts the user on the controlling terminal for the key, using getpass(3). This is the only safe way of providing it.

Alternatively, the key can be provided as the sole command-line argument *password* when starting the program. Obviously, this way the key can easily be spotted by other users running ps(1). As yet another alternative, **enigma** can be given the option **-k**, and it will take the key from the environment variable CrYpTkEy. While this at a first glance seems to be more secure than the previous option, it actually is not since environment variables can also be examined with ps(1). Thus this option is mainly provided for compatibility with other implementations of **enigma**.

When specifying the option **-s**, **enigma** modifies the encryption engine in a way that is supposed to make it a little more secure, but incompatible with other implementations.

Warning

The cryptographic value of **enigma** is rather small. This program is only provided here for compatibility with other operating systems that also provide an implementation (usually called crypt(1) there). For real encryption, refer to openssl(1), or gpg(1) (*ports/security/gnupg1*).

ENVIRONMENT

CrYpTkEy used to obtain the secret key when option **-k** has been given

EXAMPLES

```
man enigma | enigma > encrypted
Enter key: (XXX -- key not echoed)
```

This will create an encrypted form of this man page, and store it in the file *encrypted*.

```
enigma XXX < encrypted
```

This displays the previously created file on the terminal.

SEE ALSO

gpg(1) (*ports/security/gnupg1*), openssl(1), ps(1), getpass(3)

HISTORY

Implementations of **crypt** are very common among UNIX operating systems. This implementation has been taken from the *Cryptbreakers Workbench* which is in the public domain.