NAME

bfed — perform blowfish encryption/decryption

SYNOPSIS

bfed [**-deh**] **-k** *key*

DESCRIPTION

The **bfed** utility can be used to perform symmetric encryption/decryption of the input stream using the blowfish(3) block cipher.

OPTIONS

bfed supports the following command-line options:

-d Perform decryption of the input stream.

-e Perform encryption of the input stream.

-h Print a short usage and exit.

-k *key* Use the given string as the symmetric key. *key* must be exactly 16 hexadecimal characters.

DETAILS

bfed reads data from stdin and either encrypts or decrypts it (depending on the **-d** or **-e** flag). It uses OpenSSL's blowfish(3) cipher using a 128 bit (16 byte) key (specified via the **-k** flag) and an **ivec** initialized to zero.

Since the *key* is given on the command-line, **bfed** prevents leaking the secret into the process table by using setproctitle(3) (where available) or by manipulating **argv**.

Output is written to stdout.

EXAMPLES

The following examples show common usage.

To encrypt the contents of the file 'file' using the key 'cafefacedeadbeef' and storing the encrypted output in 'file.enc':

```
bfed -e -k 'cafefacedeadbeef' <file >file.enc
```

To decrypt the contents of that file again:

```
bfed -d -k 'cafefacedeadbeef' <file.enc
```

EXIT STATUS

bfed exits 0 on success, and >0 if an error occurred.

SEE ALSO

blowfish(3), EVP_EncryptInit(3)

HISTORY

The **bfed** program was first assigned as a stand-alone programming assignment for the class “Advanced Programming in the UNIX Environment” at Stevens Institute of Technology in the Fall of 2012.

BUGS

Well, let's see...