

encrypt - Man Page

encoding function (CRYPT)

Prolog

This manual page is part of the POSIX Programmer's Manual. The Linux implementation of this interface may differ (consult the corresponding Linux manual page for details of Linux behavior), or the interface may not be implemented on Linux.

Synopsis

```
#include <unistd.h>
```

```
void encrypt(char block[64], int edflag);
```

Description

The *encrypt()* function shall provide access to an implementation-defined encoding algorithm. The key generated by *setkey()* is used to encrypt the string *block* with *encrypt()*.

block *encrypt()* shall be an array of length 64 bytes containing only the bytes with values of 0 and 1. The array is modified in place to a similar array using the key set by *setkey()*. If *edflag* is 0, the argument is encoded. If *edflag* is 1, the argument may be decoded (see the section); if the argument is not decoded, *errno* shall be set to **[ENOSYS]**.

The *encrypt()* function shall not change the setting of *errno* if successful. An application wishing to check for error situations should set *errno* to 0 before calling *encrypt()*. If *errno* is non-zero on return, an error has occurred.

The *encrypt()* function need not be thread-safe.

Return Value

The *encrypt()* function shall not return a value.

Errors

The *encrypt()* function shall fail if:

ENOSYS

The functionality is not supported on this implementation.

The following sections are informative.

encrypt - Man Page

None.

Application Usage

Historical implementations of the *encrypt()* function used a rather primitive encoding algorithm.

In some environments, decoding might not be implemented. This is related to some Government restrictions on encryption and decryption routines. Historical practice has been to ship a different version of the encryption library without the decryption feature in the routines supplied. Thus the exported version of *encrypt()* does encoding but not decoding.

Rationale

None.

Future Directions

A future version of the standard may mark this interface as obsolete or remove it altogether.

See Also

[crypt\(\)](#), [setkey\(\)](#)

The Base Definitions volume of POSIX.1-2017, [<unistd.h>](#)

Copyright

Portions of this text are reprinted and reproduced in electronic form from IEEE Std 1003.1-2017, Standard for Information Technology -- Portable Operating System Interface (POSIX), The Open Group Base Specifications Issue 7, 2018 Edition, Copyright (C) 2018 by the Institute of Electrical and Electronics Engineers, Inc and The Open Group. In the event of any discrepancy between this version and the original IEEE and The Open Group Standard, the original IEEE and The Open Group Standard is the referee document. The original Standard can be obtained online at <http://www.opengroup.org/unix/online.html> .

Any typographical or formatting errors that appear in this page are most likely to have been introduced during the conversion of the source files to man page format. To report such errors, see https://www.kernel.org/doc/man-pages/reporting_bugs.html .

encrypt - Man Page

`crypt(3p)`, `setkey(3p)`, `unistd.h(0p)`.

2017 IEEE/The Open Group POSIX Programmer's Manual