Rocky Enterprise Linux 9.2 Manual Pages on command 'passwd2des.3'

$ man passwd2des.3

XCRYPT(3)   Linux Programmer's Manual   XCRYPT(3)

NAME

   xencrypt, xdecrypt, passwd2des - RFS password encryption

SYNOPSIS

   #include <rpc/des_crypt.h>

   void passwd2des(char *passwd, char *key);

   int xencrypt(char *secret, char *passwd);

   int xdecrypt(char *secret, char *passwd);

DESCRIPTION

   WARNING: Do not use these functions in new code. They do not achieve

   any type of acceptable cryptographic security guarantees.

   The function passwd2des() takes a character string passwd of arbitrary

   length and fills a character array key of length 8. The array key is

   suitable for use as DES key. It has odd parity set in bit 0 of each

   byte.   Both other functions described here use this function to turn

   their argument passwd into a DES key.

   The xencrypt() function takes the ASCII character string secret given

   in hex, which must have a length that is a multiple of 16, encrypts it

using the DES key derived from passwd by passwd2des(), and outputs the result again in secret as a hex string of the same length.

The xdecrypt() function performs the converse operation.

RETURN VALUE

The functions xencrypt() and xdecrypt() return 1 on success and 0 on error.

VERSIONS

These functions are available in glibc since version 2.1.

ATTRIBUTES

For an explanation of the terms used in this section, see at?

tributes(7).

???

| ?Interface | ? Attribute | ? Value | ? |

???

| ?passwd2des(), xencrypt(), xdecrypt() | ? Thread safety | ? MT-Safe | ? |

???

BUGS

The prototypes are missing from the abovementioned include file.

SEE ALSO

cbc_crypt(3)

COLOPHON

This page is part of release 5.10 of the Linux man-pages project. A description of the project, information about reporting bugs, and the latest version of this page, can be found at https://www.kernel.org/doc/man-pages/.

                    2019-03-06   XCRYPT(3)