



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

C:\>man xdecrypt.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.

