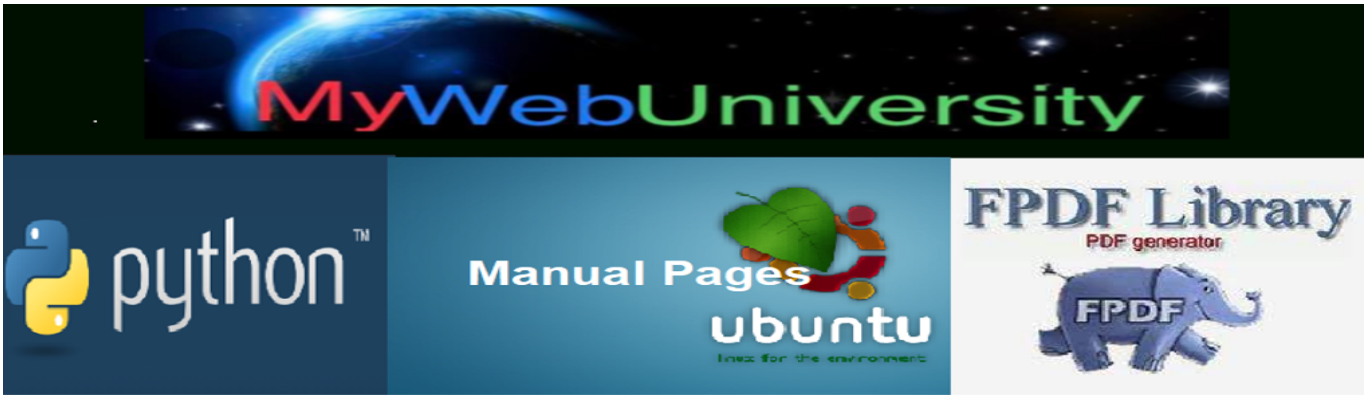

Full credit is given to the above companies including the Operating System (OS) that this PDF file was generated!

Rocky Enterprise Linux 9.2 Manual Pages on command 'des_crypt.3t'

$ man des_crypt.3t

DES_CRYPT(3) BSD Library Functions Manual DES_CRYPT(3)

NAME

des_crypt, ecb_crypt, cbc_crypt, des_setparity ? fast DES encryption

SYNOPSIS

#include <rpc/des_crypt.h>

int

ecb_crypt(char *key, char *data, unsigned datalen, unsigned mode);

int

cbc_crypt(char *key, char *data, unsigned datalen, unsigned mode, char *ivec);

void

des_setparity(char *key);

DESCRIPTION

The ecb_crypt() and cbc_crypt() functions implement the NBS DES (Data Encryption Standard). These routines are faster and more general purpose than crypt(3). They also are able to utilize DES hardware if it is available. The ecb_crypt() function encrypts in ECB (Elec? tronic Code Book) mode, which encrypts blocks of data independently. The cbc_crypt() func? tion encrypts in CBC (Cipher Block Chaining) mode, which chains together successive blocks.

CBC mode protects against insertions, deletions and substitutions of blocks. Also, regular?
ities in the clear text will not appear in the cipher text.

Here is how to use these routines. The first argument, key, is the 8-byte encryption key
with parity. To set the key's parity, which for DES is in the low bit of each byte, use
des_setparity(). The second argument, data, contains the data to be encrypted or decrypted.
The third argument, datalen, is the length in bytes of data, which must be a multiple of 8.
The fourth argument, mode, is formed by OR'ing together some things. For the encryption di?
rection OR in either DES_ENCRYPT or DES_DECRYPT. For software versus hardware encryption,
OR in either DES_HW or DES_SW. If DES_HW is specified, and there is no hardware, then the
encryption is performed in software and the routine returns DESERR_NOHWDEVICE. For
cbc_crypt(), the ivec argument is the 8-byte initialization vector for the chaining. It is
updated to the next initialization vector upon return.

ERRORS

[DESERR_NONE] No error.

[DESERR_NOHWDEVICE] Encryption succeeded, but done in software instead of the requested
hardware.

[DESERR_HWERR] An error occurred in the hardware or driver.

[DESERR_BADPARAM] Bad argument to routine.

Given a result status stat, the macro DES_FAILED(stat) is false only for the first two sta?
tuses.

AVAILABILITY

The ecb_crypt(), cbc_crypt(), and des_setparity() functions are part of libtirpc.

SEE ALSO

crypt(3)

RESTRICTIONS

These routines are not available in RPCSRC 4.0. This information is provided to describe
the DES interface expected by Secure RPC.