



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

Linux Ubuntu 26.04 Manual Pages on command 'cbc_crypt.3'

\$ man cbc_crypt.3

des_crypt(3) Library Functions Manual des_crypt(3)

NAME

des_crypt, ecb_crypt, cbc_crypt, des_setparity, DES_FAILED - fast DES encryption

LIBRARY

Standard C library (libc, -lc)

SYNOPSIS

```
#include <rpc/des_crypt.h>
```

```
[[deprecated]] int ecb_crypt(unsigned int datalen;  
                             char *key, char data[datalen],  
                             unsigned int datalen, unsigned int mode);
```

```
[[deprecated]] int cbc_crypt(unsigned int datalen;  
                             char *key, char data[datalen],  
                             unsigned int datalen, unsigned int mode,  
                             char *ivec);
```

```
[[deprecated]] void des_setparity(char *key);
```

```
[[deprecated]] int DES_FAILED(int status);
```

DESCRIPTION

ecb_crypt() and cbc_crypt() 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. ecb_crypt() encrypts in ECB (Electronic Code Book) mode, which encrypts blocks of data independently. cbc_crypt() encrypts in CBC (Cipher Block Chaining) mode, which chains together successive blocks. CBC mode protects against insertions, deletions, and substitutions of blocks. Also, regularities in the clear text will not appear in

RETURN VALUE

DESERR NONE

DESERR NOHWDEVICE

DESERR HWERROR

DESERR BADPARAM

Given a result status `stat`, the macro `DES_FAILED(stat)` is false only for the first two statuses.

ATTRIBUTES

[illegible]

?	Interface	?	Attribute	?	Value	?
---	-----------	---	-----------	---	-------	---

[illegible]

? ecb crypt(), cbc crypt(), des setparity() ? Thread safety ? MT-Safe ?

[illegible]

STANDARDS

None.

HISTORY

Page 2/3

Because they employ the DES block cipher, which is no longer considered secure, these functions were removed. Applications should switch to a modern cryptography library, such as libgcrypt.

SEE ALSO

des(1), crypt(3), xcrypt(3)

Linux man-pages 6.17

2026-02-08

des_crypt(3)