NAME

EVP_des_cbc, EVP_des_cfb, EVP_des_cfb1, EVP_des_cfb8, EVP_des_cfb64, EVP_des_ecb, EVP_des_ofb, EVP_des_ede, EVP_des_ede_cbc, EVP_des_ede_cfb, EVP_des_ede_cfb64, EVP_des_ede_ecb, EVP_des_ede_ofb, EVP_des_ede3, EVP_des_ede3_cbc, EVP_des_ede3_cfb, EVP_des_ede3_cfb1, EVP_des_ede3_cfb8, EVP_des_ede3_cfb64, EVP_des_ede3_ecb, EVP_des_ede3_ofb, EVP_des_ede3_wrap − EVP DES cipher

SYNOPSIS

```
#include <openssl/evp.h>

const EVP_CIPHER *EVP_ciphername(void)
```

EVP_ciphername is used a placeholder for any of the described cipher functions, such as *EVP_des_cbc*.

DESCRIPTION

The DES encryption algorithm for EVP.

EVP_des_cbc(), **EVP_des_ecb()**, **EVP_des_cfb()**, **EVP_des_cfb1()**, **EVP_des_cfb8()**, **EVP_des_cfb64()**, **EVP_des_ofb()**

DES in CBC, ECB, CFB with 64−bit shift, CFB with 1−bit shift, CFB with 8−bit shift and OFB modes.

None of these algorithms are provided by the OpenSSL default provider. To use them it is necessary to load either the OpenSSL legacy provider or another implementation.

EVP_des_ede(), **EVP_des_ede_cbc()**, **EVP_des_ede_cfb()**, **EVP_des_ede_cfb64()**, **EVP_des_ede_ecb()**, **EVP_des_ede_ofb()**

Two key triple DES in ECB, CBC, CFB with 64−bit shift and OFB modes.

EVP_des_ede3(), **EVP_des_ede3_cbc()**, **EVP_des_ede3_cfb()**, **EVP_des_ede3_cfb1()**, **EVP_des_ede3_cfb8()**, **EVP_des_ede3_cfb64()**, **EVP_des_ede3_ecb()**, **EVP_des_ede3_ofb()**

Three−key triple DES in ECB, CBC, CFB with 64−bit shift, CFB with 1−bit shift, CFB with 8−bit shift and OFB modes.

EVP_des_ede3_wrap()

Triple−DES key wrap according to RFC 3217 Section 3.

NOTES

Developers should be aware of the negative performance implications of calling these functions multiple times and should consider using **EVP_CIPHER_fetch**(3) with **EVP_CIPHER−DES**(7) instead. See "Performance" in **crypto**(7) for further information.

RETURN VALUES

These functions return an **EVP_CIPHER** structure that contains the implementation of the symmetric cipher. See **EVP_CIPHER_meth_new**(3) for details of the **EVP_CIPHER** structure.

SEE ALSO

evp(7), **EVP_EncryptInit**(3), **EVP_CIPHER_meth_new**(3)

COPYRIGHT