

**NAME**

EVP\_des\_cbc, EVP\_des\_cfb, EVP\_des\_cfb1, EVP\_des\_cfb8, EVP\_des\_cfb64, EVP\_des\_ecb, EVP\_des\_ofb, EVP\_des\_edc, EVP\_des\_edc\_cbc, EVP\_des\_edc\_cfb, EVP\_des\_edc\_cfb64, EVP\_des\_edc\_ecb, EVP\_des\_edc\_ofb, EVP\_des\_edc3, EVP\_des\_edc3\_cbc, EVP\_des\_edc3\_cfb, EVP\_des\_edc3\_cfb1, EVP\_des\_edc3\_cfb8, EVP\_des\_edc3\_cfb64, EVP\_des\_edc3\_ecb, EVP\_des\_edc3\_ofb, EVP\_des\_edc3\_wrap - EVP DES cipher

**SYNOPSIS**

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

```
const EVP_CIPHER *EVP_ciphernam(void)
```

*EVP\_ciphernam* 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\_edc(), EVP\_des\_edc\_cbc(), EVP\_des\_edc\_cfb(), EVP\_des\_edc\_cfb64(),  
EVP\_des\_edc\_ecb(), EVP\_des\_edc\_ofb()**

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

**EVP\_des\_edc3(), EVP\_des\_edc3\_cbc(), EVP\_des\_edc3\_cfb(), EVP\_des\_edc3\_cfb1(),  
EVP\_des\_edc3\_cfb8(), EVP\_des\_edc3\_cfb64(), EVP\_des\_edc3\_ecb(), EVP\_des\_edc3\_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\_edc3\_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)** 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

Copyright 2017-2023 The OpenSSL Project Authors. All Rights Reserved.

Licensed under the Apache License 2.0 (the "License"). You may not use this file except in compliance with the License. You can obtain a copy in the file LICENSE in the source distribution or at <https://www.openssl.org/source/license.html>.