Rocky Enterprise Linux 9.2 Manual Pages on command 'EVP_sm4_ofb.3ossl'

$ man EVP_sm4_ofb.3ossl

EVP_SM4_CBC(3ossl) OpenSSL EVP_SM4_CBC(3ossl)

NAME

EVP_sm4_cbc, EVP_sm4_ecb, EVP_sm4_cfb, EVP_sm4_cfb128, EVP_sm4_ofb,

EVP_sm4_ctr - EVP SM4 cipher

SYNOPSIS

#include <openssl/evp.h>

const EVP_CIPHER *EVP_sm4_cbc(void);

const EVP_CIPHER *EVP_sm4_ecb(void);

const EVP_CIPHER *EVP_sm4_cfb(void);

const EVP_CIPHER *EVP_sm4_cfb128(void);

const EVP_CIPHER *EVP_sm4_ofb(void);

const EVP_CIPHER *EVP_sm4_ctr(void);

DESCRIPTION

The SM4 blockcipher (GB/T 32907-2016) for EVP.

All modes below use a key length of 128 bits and acts on blocks of 128 bits.

EVP_sm4_cbc(), EVP_sm4_ecb(), EVP_sm4_cfb(), EVP_sm4_cfb128(), EVP_sm4_ofb(), EVP_sm4_ctr()

The SM4 blockcipher with a 128-bit key in CBC, ECB, CFB, OFB and CTR modes respectively.

RETURN VALUES

These functions return a 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