Rocky Enterprise Linux 9.2 Manual Pages on command 'EVP_rc5_32_12_16_cfb.3ossl'

$ man EVP_rc5_32_12_16_cfb.3ossl

EVP_RC5_32_12_16_CBC(3ossl) OpenSSL EVP_RC5_32_12_16_CBC(3ossl)

NAME

EVP_rc5_32_12_16_cbc, EVP_rc5_32_12_16_cfb, EVP_rc5_32_12_16_cfb64,

EVP_rc5_32_12_16_ecb, EVP_rc5_32_12_16_ofb - EVP RC5 cipher

SYNOPSIS

#include <openssl/evp.h>

const EVP_CIPHER *EVP_rc5_32_12_16_cbc(void);

const EVP_CIPHER *EVP_rc5_32_12_16_cfb(void);

const EVP_CIPHER *EVP_rc5_32_12_16_cfb64(void);

const EVP_CIPHER *EVP_rc5_32_12_16_ecb(void);

const EVP_CIPHER *EVP_rc5_32_12_16_ofb(void);

DESCRIPTION

The RC5 encryption algorithm for EVP.

EVP_rc5_32_12_16_cbc(), EVP_rc5_32_12_16_cfb(),

EVP_rc5_32_12_16_cfb64(), EVP_rc5_32_12_16_ecb(),

EVP_rc5_32_12_16_ofb()

RC5 encryption algorithm in CBC, CFB, ECB and OFB modes respectively. This is a variable key length cipher with an additional "number of rounds" parameter. By default the key length is set to 128 bits and 12 rounds. Alternative key lengths can be set using EVP_CIPHER_CTX_set_key_length(3). The maximum key length is 2040 bits.

The following rc5 specific ctrls are supported (see EVP_CIPHER_CTX_ctrl(3)).

EVP_CIPHER_CTX_ctrl(ctx, EVP_CTRL_SET_RC5_ROUNDS, rounds, NULL)

Sets the number of rounds to rounds. This must be one of RC5_8_ROUNDS, RC5_12_ROUNDS or RC5_16_ROUNDS.

EVP_CIPHER_CTX_ctrl(ctx, EVP_CTRL_GET_RC5_ROUNDS, 0, &rounds)

Stores the number of rounds currently configured in *rounds where *rounds is an int.

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

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>.