Rocky Enterprise Linux 9.2 Manual Pages on command 'RC4_set_key.3ossl'

$ man RC4_set_key.3ossl

RC4_SET_KEY(3ossl) OpenSSL RC4_SET_KEY(3ossl)

NAME

RC4_set_key, RC4 - RC4 encryption

SYNOPSIS

#include <openssl/rc4.h>

The following functions have been deprecated since OpenSSL 3.0, and can be hidden entirely by defining OPENSSL_API_COMPAT with a suitable version value, see openssl_user_macros(7):

void RC4_set_key(RC4_KEY *key, int len, const unsigned char *data);

void RC4(RC4_KEY *key, unsigned long len, const unsigned char *indata,
unsigned char *outdata);

DESCRIPTION

All of the functions described on this page are deprecated.
Applications should instead use EVP_EncryptInit_ex(3),
EVP_EncryptUpdate(3) and EVP_EncryptFinal_ex(3) or the equivalently
named decrypt functions.

This library implements the Alleged RC4 cipher, which is described for
example in Applied Cryptography. It is believed to be compatible with
RC4[TM], a proprietary cipher of RSA Security Inc.

RC4 is a stream cipher with variable key length. Typically, 128 bit
(16 byte) keys are used for strong encryption, but shorter insecure key
sizes have been widely used due to export restrictions.

RC4 consists of a key setup phase and the actual encryption or
decryption phase.

RC4_set_key() sets up the RC4_KEY key using the len bytes long key at
data.

RC4() encrypts or decrypts the len bytes of data at indata using key
and places the result at outdata. Repeated RC4() calls with the same
key yield a continuous key stream.

Since RC4 is a stream cipher (the input is XORed with a pseudo-random
key stream to produce the output), decryption uses the same function
calls as encryption.

RETURN VALUES

RC4_set_key() and RC4() do not return values.

NOTE

Applications should use the higher level functions EVP_EncryptInit(3)
etc. instead of calling these functions directly.

It is difficult to securely use stream ciphers. For example, do not perform multiple encryptions using the same key stream.

SEE ALSO

EVP_EncryptInit(3)

HISTORY

All of these functions were deprecated in OpenSSL 3.0.

COPYRIGHT

Copyright 2000-2021 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>.