# Author: Trevor Perrin

# See the LICENSE file for legal information regarding use of this file.

"""OpenSSL/M2Crypto RC4 implementation."""

from .cryptomath import \*

from .rc4 import RC4

if m2cryptoLoaded:

def new(key):

return OpenSSL\_RC4(key)

class OpenSSL\_RC4(RC4):

def \_\_init\_\_(self, key):

RC4.\_\_init\_\_(self, key, "openssl")

self.rc4 = m2.rc4\_new()

m2.rc4\_set\_key(self.rc4, key)

def \_\_del\_\_(self):

m2.rc4\_free(self.rc4)

def encrypt(self, plaintext):

return bytearray(m2.rc4\_update(self.rc4, plaintext))

def decrypt(self, ciphertext):

return bytearray(self.encrypt(ciphertext))