# Author: Trevor Perrin

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

"""Pure-Python RC4 implementation."""

from .rc4 import RC4

from .cryptomath import \*

def new(key):

return Python\_RC4(key)

class Python\_RC4(RC4):

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

RC4.\_\_init\_\_(self, keyBytes, "python")

S = [i for i in range(256)]

j = 0

for i in range(256):

j = (j + S[i] + keyBytes[i % len(keyBytes)]) % 256

S[i], S[j] = S[j], S[i]

self.S = S

self.i = 0

self.j = 0

def encrypt(self, plaintextBytes):

ciphertextBytes = plaintextBytes[:]

S = self.S

i = self.i

j = self.j

for x in range(len(ciphertextBytes)):

i = (i + 1) % 256

j = (j + S[i]) % 256

S[i], S[j] = S[j], S[i]

t = (S[i] + S[j]) % 256

ciphertextBytes[x] ^= S[t]

self.i = i

self.j = j

return ciphertextBytes

def decrypt(self, ciphertext):

return self.encrypt(ciphertext)