# Author: Trevor Perrin

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

"""Abstract class for 3DES."""

class TripleDES(object):

def \_\_init\_\_(self, key, mode, IV, implementation):

if len(key) != 24:

raise ValueError()

if mode != 2:

raise ValueError()

if len(IV) != 8:

raise ValueError()

self.isBlockCipher = True

self.block\_size = 8

self.implementation = implementation

self.name = "3des"

#CBC-Mode encryption, returns ciphertext

#WARNING: \*MAY\* modify the input as well

def encrypt(self, plaintext):

assert(len(plaintext) % 8 == 0)

#CBC-Mode decryption, returns plaintext

#WARNING: \*MAY\* modify the input as well

def decrypt(self, ciphertext):

assert(len(ciphertext) % 8 == 0)