# Author: Trevor Perrin

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

"""PyCrypto AES implementation."""

from .cryptomath import \*

from .aes import \*

if pycryptoLoaded:

import Crypto.Cipher.AES

def new(key, mode, IV):

return PyCrypto\_AES(key, mode, IV)

class PyCrypto\_AES(AES):

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

AES.\_\_init\_\_(self, key, mode, IV, "pycrypto")

key = bytes(key)

IV = bytes(IV)

self.context = Crypto.Cipher.AES.new(key, mode, IV)

def encrypt(self, plaintext):

plaintext = bytes(plaintext)

return bytearray(self.context.encrypt(plaintext))

def decrypt(self, ciphertext):

ciphertext = bytes(ciphertext)

return bytearray(self.context.decrypt(ciphertext))