Program 21 ecb cbe ecb in c

from Crypto.Cipher import AES

from Crypto.Random import get\_random\_bytes

from Crypto.Util.Padding import pad

# ECB Mode Encryption

def ecb\_encrypt(plaintext, key):

cipher = AES.new(key, AES.MODE\_ECB)

ciphertext = cipher.encrypt(plaintext)

return ciphertext

# CBC Mode Encryption

def cbc\_encrypt(plaintext, key, iv):

cipher = AES.new(key, AES.MODE\_CBC, iv)

ciphertext = cipher.encrypt(plaintext)

return ciphertext

# CFB Mode Encryption

def cfb\_encrypt(plaintext, key, iv):

cipher = AES.new(key, AES.MODE\_CFB, iv)

ciphertext = cipher.encrypt(plaintext)

return ciphertext

def main():

key = get\_random\_bytes(16) # 128-bit key

iv = get\_random\_bytes(16) # Initialization vector

plaintext = b'This is a sample plaintext for encryption.'

block\_size = AES.block\_size

# Pad the plaintext to match the block size

plaintext = pad(plaintext, block\_size)

ecb\_ciphertext = ecb\_encrypt(plaintext, key)

cbc\_ciphertext = cbc\_encrypt(plaintext, key, iv)

cfb\_ciphertext = cfb\_encrypt(plaintext, key, iv)

print("Plaintext:", plaintext)

print("ECB Ciphertext:", ecb\_ciphertext.hex())

print("CBC Ciphertext:", cbc\_ciphertext.hex())

print("CFB Ciphertext:", cfb\_ciphertext.hex())

OUTPUT:

Plaintext: b'This is a sample plaintext for

encryption.\x06\x06\x06\x06\x06\x06'

ECBCiphertext:5d1a01bd38854fad7fed0f632471959f7c1866d12c2da92

28e21919244792872fb3a02f16dfae5811baf44a7e031711a

CBCCiphertext:

40cf1084f7f20deec9622dc9e354709626ee0c8edb483d0f950a9e656b3

121998be67be32c3aacafb6ae6fd3d31aa160

CFBCiphertext:

56ae78da72bc0b7ce7ec95cc45a30a212a428529ca9beea4ceb263593d3

3b0702a39a46e81da509704cd91683541bac7