**МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАНА**

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

***Практическая работа 5***

*по предмету* ***«Криптография»***

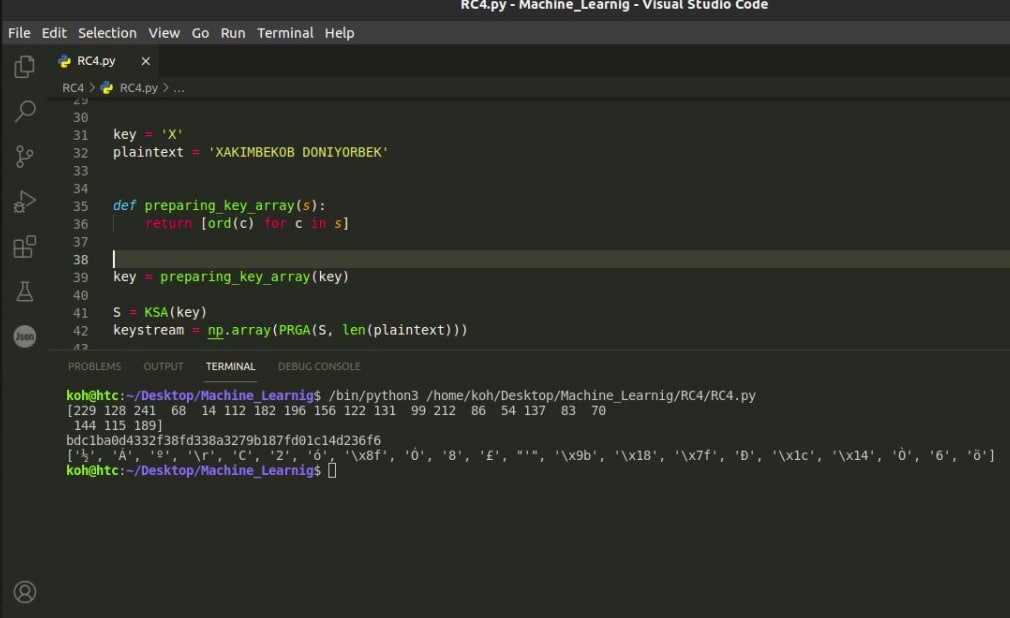
#### На тему: **«Разработка программу шифрования и дешифрования данных на основе алгоритма шифрования RC4»**

Группа: 721-19

Выполнил: Хакимбеков Дониёрбек

Принял: Хамидов Шерзод

***Ташкент 2021***



import numpy as np

def KSA(key):

key\_length = len(key)

S = list(range(256))

j = 0

for i in range(256):

j = (j + S[i] + key[i % key\_length]) % 256

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

# swap

return S

def PRGA(S, n):

i = 0

j = 0

key = []

while n > 0:

n = n-1

i = (i+1) % 256

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

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

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

key.append(K)

return key

key = 'X'

plaintext = ‘XAKIMBEKOV DONIYORBEK’

def preparing\_key\_array(s):

return [ord(c) for c in s]

key = preparing\_key\_array(key)

S = KSA(key)

keystream = np.array(PRGA(S, len(plaintext)))

print(keystream)

plaintext = np.array([ord(i) for i in plaintext])

cipher = keystream ^ plaintext # xor two numpy arrays

print(cipher.astype(np.uint8).data.hex()) # print hex cipher values

print([chr(c) for c in cipher]) # print unicode