SА 5/1  
Код:

# from bit import BitArray

import re

for\_big\_text = "АБВГДЕёЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ".lower() + "АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ"  + " !\"#$%-'()\*+,—–./:;<=>?@[\]^\_`{|}"

mode = int(input("выберите режим (1 - карточка, 2 - большой текст): "))

if mode == 1:

    text = input("Введите текст: ").upper()

else:

    text = input("Введите текст: ")

text\_reg = ''

for i in text:

    c = str(bin(for\_big\_text.find(i)+1))[2:]

    while len(c) != 8: c = '0' + c

    text\_reg += c

key = [1] \* 64

x = [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

y = [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

z = [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

gamma = ''

def F(x, y, z):

    return (x & y) or (x & z) or (y & z)

for i in range(64):

    x.append(x[1] ^ x[2] ^ x[5] ^ x.pop(0) ^ key[i])

    y.append(y[1] ^ y.pop(0) ^ key[i])

    z.append(z[1] ^ z[2] ^ z[15] ^ z.pop(0) ^ key[i])

    # print(\*x)

    # print(\*y)

    # print(\*z)

    # print("------------------------------------------")

for i in range(100):

    f = F(x[10], y[11], z[12])

    if x[10] == f:

        x.append(x[1] ^ x[2] ^ x[5] ^ x.pop(0))

    if y[11] == f:

        y.append(y[1] ^ y.pop(0))

    if z[12] == f:

        z.append(z[1] ^ z[2] ^ z[15] ^ z.pop(0))

for i in range(114):

    gamma += str(x[0] ^ y[0] ^ z[0])

    f = F(x[10], y[11], z[12])

    if x[10] == f:

        x.append(x[1] ^ x[2] ^ x[5] ^ x.pop(0))

    if y[11] == f:

        y.append(y[1] ^ y.pop(0))

    if z[12] == f:

        z.append(z[1] ^ z[2] ^ z[15] ^ z.pop(0))

gamma = gamma\*500

text\_enc = ''

for i in range(len(text\_reg)):

    text\_enc += str(int(text\_reg[i]) ^ int(gamma[i]))

text\_dec = ''

text\_dec\_res = ''

for i in range(len(text\_enc)):

    text\_dec += str(int(text\_enc[i]) ^ int(gamma[i]))

text\_dec\_sub = re.findall(".{8}", text\_dec)

# print(text\_dec\_sub)

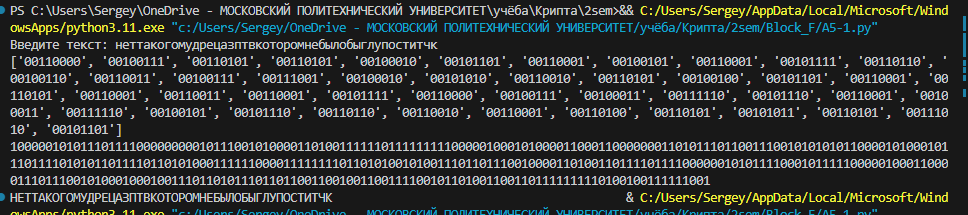
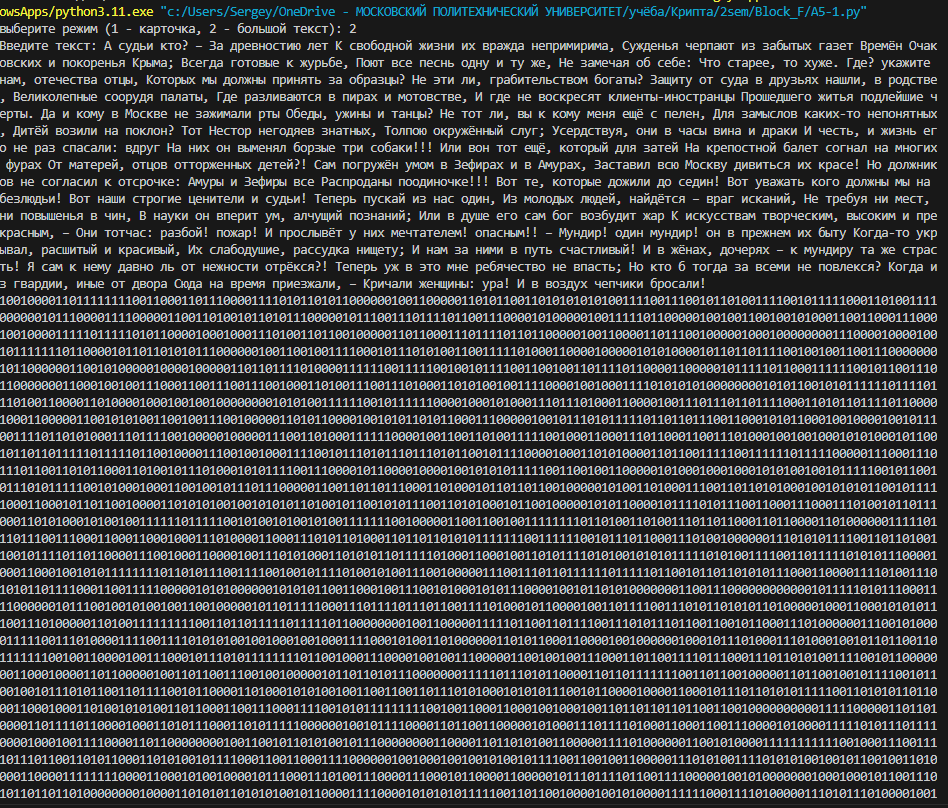
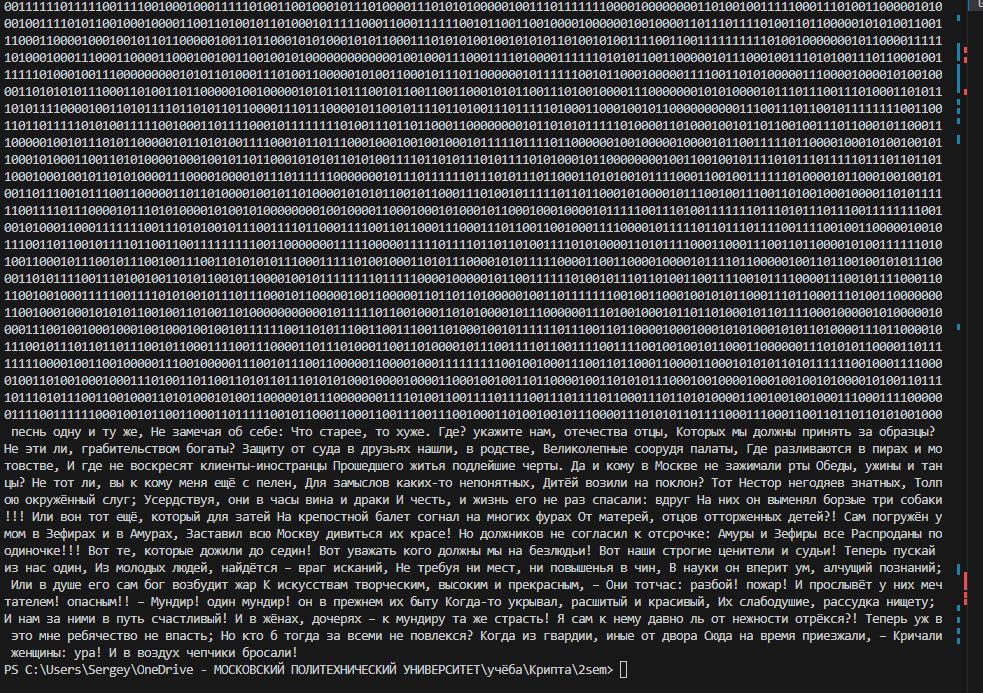
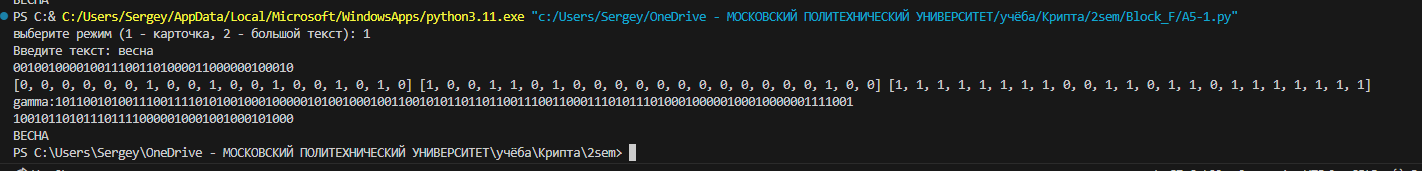
for i in text\_dec\_sub:

    text\_dec\_res += for\_big\_text[int(i, 2)-1]

print(text\_enc)

print(text\_dec\_res)

Пример работы:

  
  
  
Ручная проверка:  


A5/2

Код:

# from bit import BitArray

import re

for\_big\_text = "АБВГДЕёЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ".lower() + "АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ"  + " !\"#$%-'()\*+,—–./:;<=>?@[\]^\_`{|}"

mode = int(input("выберите режим (1 - карточка, 2 - большой текст): "))

if mode == 1:

    text = input("Введите текст: ").upper()

else:

    text = input("Введите текст: ")

text\_reg = ''

for i in text:

    c = str(bin(for\_big\_text.find(i)+1))[2:]

    while len(c) != 8: c = '0' + c

    text\_reg += c

key = [1] \* 64

print(text\_reg)

x = [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

y = [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

z = [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

r4 = [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]

gamma = ''

def F(x, y, z):

    return (x & y) or (x & z) or (y & z)

for i in range(64):

    x.append(x[1] ^ x[2] ^ x[5] ^ x.pop(0) ^ key[i])

    y.append(y[1] ^ y.pop(0) ^ key[i])

    z.append(z[1] ^ z[2] ^ z[15] ^ z.pop(0) ^ key[i])

    r4.append(r4[5] ^ key[i] ^ r4.pop(0))

    # print(\*x)

    # print(\*y)

    # print(\*z)

    # print("------------------------------------------")

r4[6], r4[9], r4[13] = 0, 0, 0

for i in range(99):

    if r4[6]:

        x.append(x[1] ^ x[2] ^ x[5] ^ x.pop(0))

    if r4[9]:

        y.append(y[1] ^ y.pop(0))

    if r4[13]:

        z.append(z[1] ^ z[2] ^ z[15] ^ z.pop(0))

    r4.append(r4[5] ^ r4.pop(0))

for i in range(114):

    f1 = x[3] ^ x[4] ^ x[6]

    f2 = y[6] ^ y[9] ^ y[13]

    f3 = z[4] ^ z[6] ^ z[9]

    gamma += str(x[0] ^ y[0] ^ z[0] ^ f1 ^ f2 ^ f3)

    if r4[6]:

        x.append(x[1] ^ x[2] ^ x[5] ^ x.pop(0))

    if r4[9]:

        y.append(y[1] ^ y.pop(0))

    if r4[13]:

        z.append(z[1] ^ z[2] ^ z[15] ^ z.pop(0))

    r4.append(r4[5] ^ r4.pop(0))

print(x, y, z)

print("gamma:" + gamma)

gamma = gamma\*500

text\_enc = ''

for i in range(len(text\_reg)):

    text\_enc += str(int(text\_reg[i]) ^ int(gamma[i]))

text\_dec = ''

text\_dec\_res = ''

for i in range(len(text\_enc)):

    text\_dec += str(int(text\_enc[i]) ^ int(gamma[i]))

text\_dec\_sub = re.findall(".{8}", text\_dec)

# print(text\_dec\_sub)

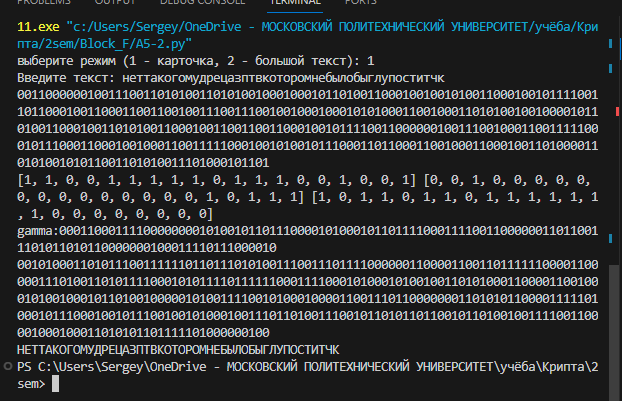
for i in text\_dec\_sub:

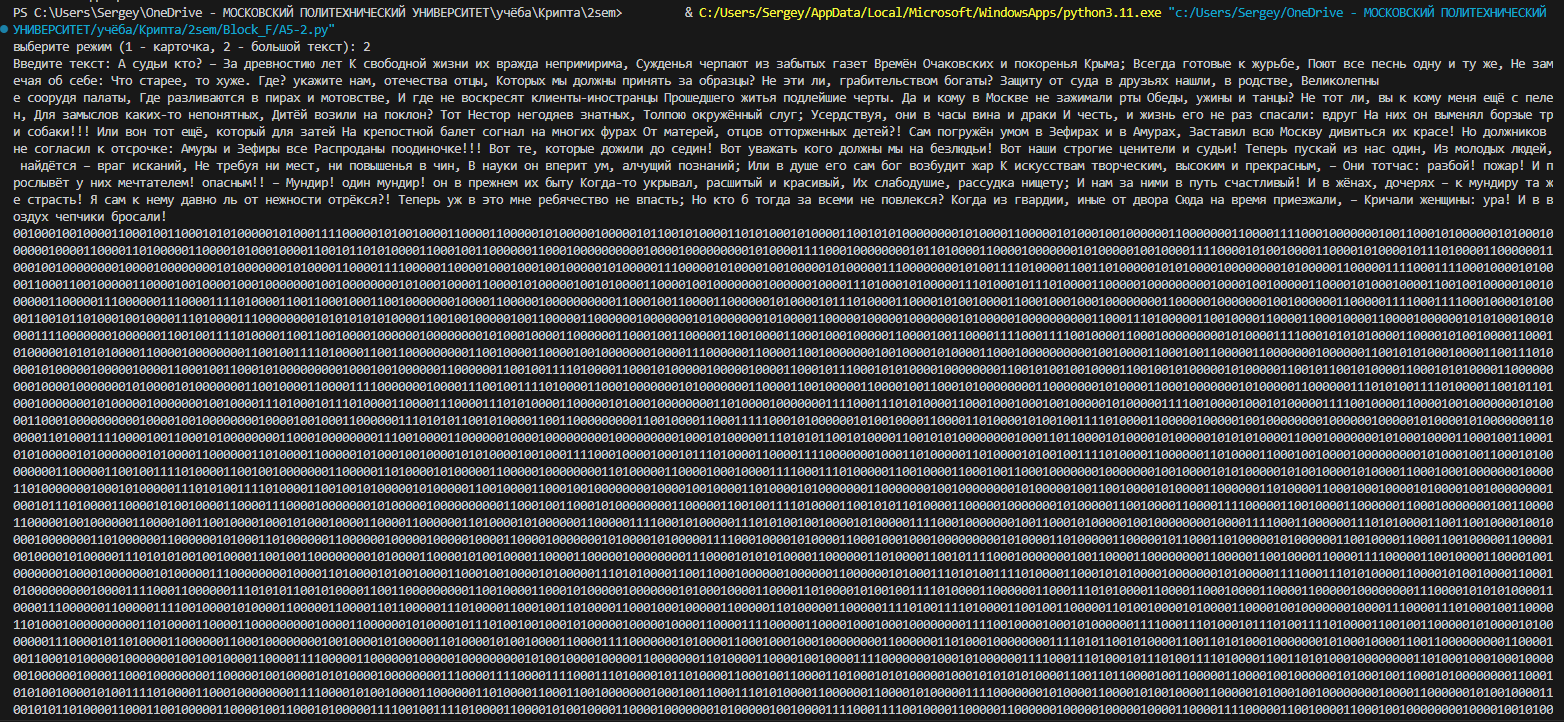
    text\_dec\_res += for\_big\_text[int(i, 2)-1]

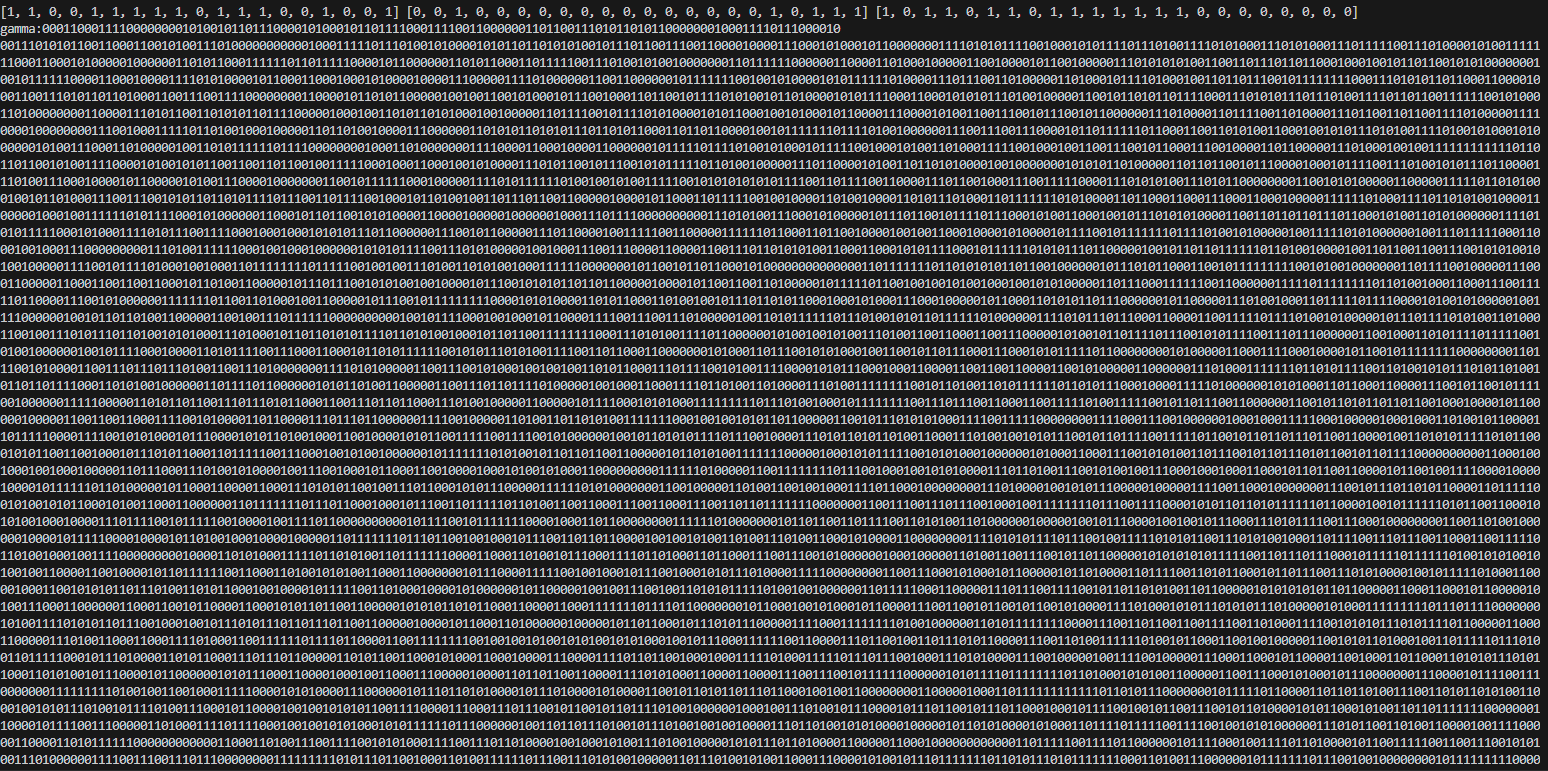
print(text\_enc)

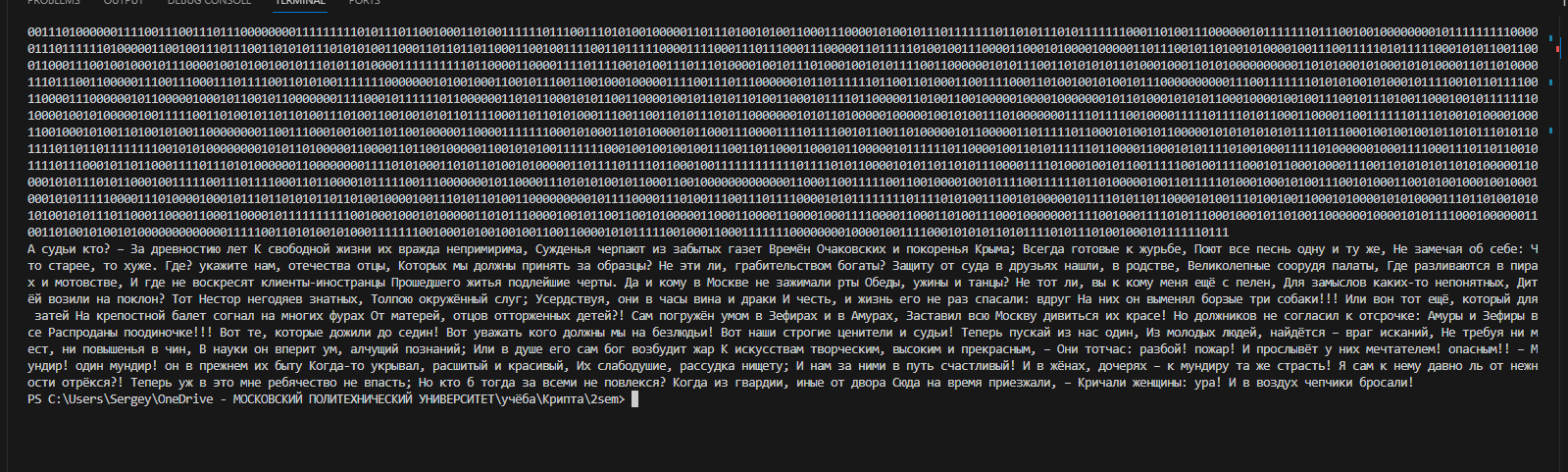
print(text\_dec\_res)

Пример работы:









Для ручной проверки  
