Блокнот Шеннона

alp = "АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ".lower()

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

# print(alp.index("A"))

def gamma(mes, a, c, T0, mode):

    if mode == 1:

        alp\_arr = []

        for i in mes.lower():

            alp\_arr.append(alp.index(i))

        arr = [T0]

        for i in range(len(mes)):

            t = (a\*arr[-1]+c) % 32

            arr.append(t)

        arr.pop(0)

        return arr, alp\_arr

    else:

        alp\_arr = []

        for i in mes:

            alp\_arr.append(for\_big\_text.index(i)+1)

        arr = [T0]

        for i in range(len(mes)):

            t = (a\*arr[-1]+c) % 98

            arr.append(t)

        arr.pop(0)

        return arr, alp\_arr

def encrypt(message, one\_time\_pad, mode):

    if mode == 1:

        arr = []

        for i in range(len(message)):

            arr.append((message[i]+one\_time\_pad[i]) % 32)

        print(arr)

        return "".join([alp[i] for i in arr])

    else:

        arr = []

        for i in range(len(message)):

            arr.append((message[i]+one\_time\_pad[i]) % 98)

        print(arr)

        return "".join([for\_big\_text[i] for i in arr])

def decrypt(ciphertext, one\_time\_pad, mode):

    if mode == 1:

        arr = []

        for i in range(len(ciphertext)):

            shift = (alp.index(ciphertext[i])-one\_time\_pad[i]+1) % 32

            arr.append(shift)

        return "".join([alp[i-1] for i in arr])

    else:

        arr = []

        for i in range(len(ciphertext)):

            shift = (for\_big\_text.index(ciphertext[i])-one\_time\_pad[i]) % 98

            arr.append(shift)

        return "".join([for\_big\_text[i-1] for i in arr])

from math import gcd

mode = int(input("Выберите задание (1 - карточка, 2 - текст): "))

a = int(input("a = "))

if mode == 1:

    check = 32

else:

    check = 99

if a%2 != 0 and a%4 == 1 and a > 1:

    x = 32 if mode == 1 else 98

    c = int(input("c = "))

    if gcd(c, x) == 1:

        T0 = int(input("T0 = "))

        if 0<T0<check:

            message = str(input("Введите текст: "))

            one\_time\_pad, msg = gamma(message, a, c, T0 , mode)

            ciphertext = encrypt(msg, one\_time\_pad, mode)

            print("Зашифрованный текст:", ciphertext)

            decrypted\_message = decrypt(ciphertext, one\_time\_pad, mode)

            print("Дешифрованный текст:", decrypted\_message)

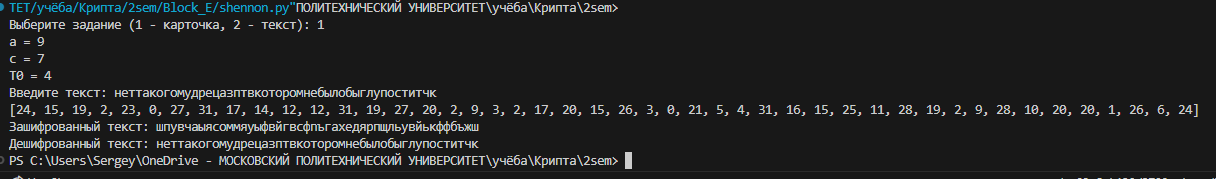
    else:

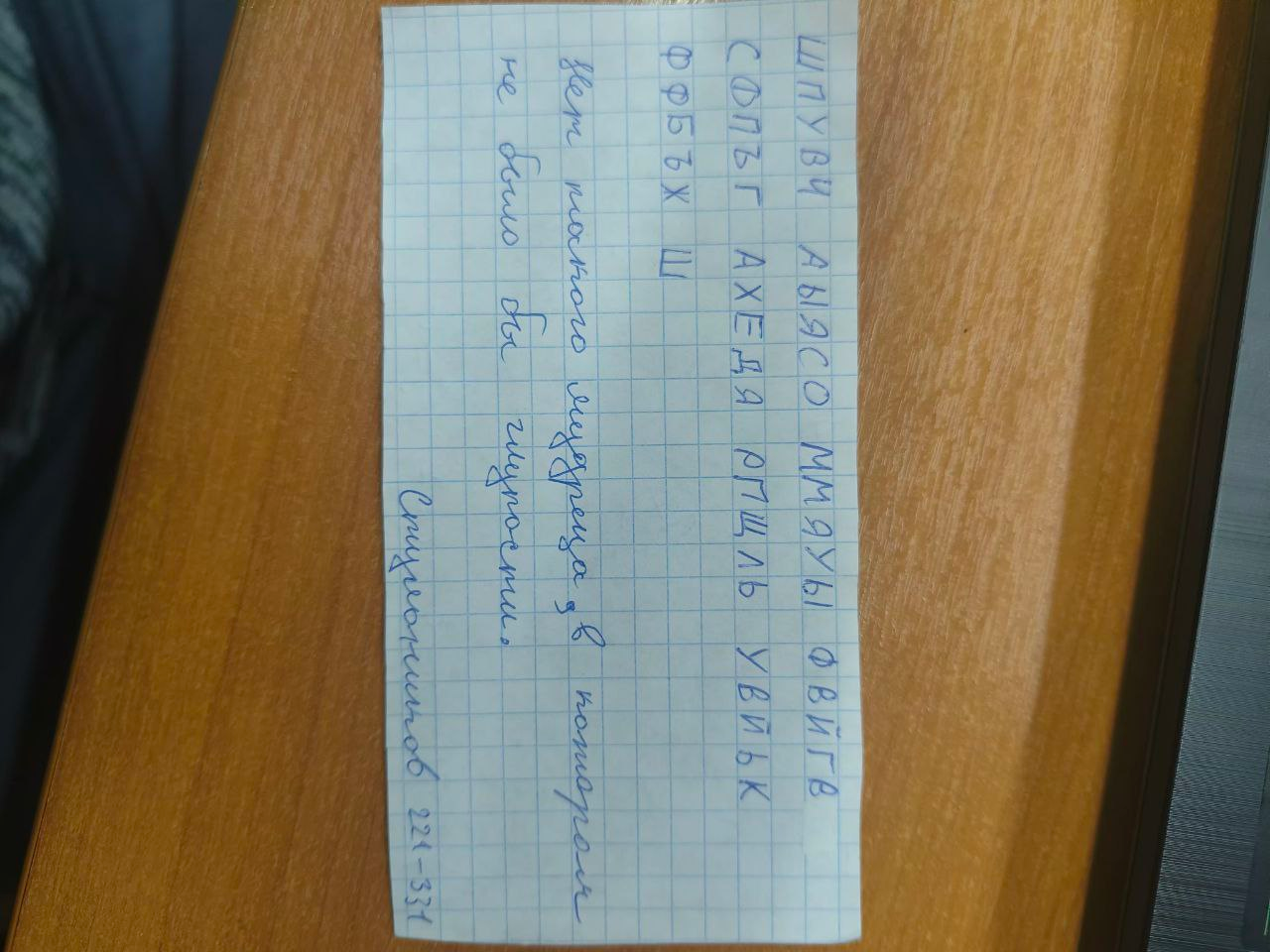
        print("c не взаимно прост с модулем m")

else:

    print("неверные значения. a должно быть нечётным, больше 1 и меньше 32; T0 должно быть больше 1 и меньше мощности алфавита")

Тест работы:





Тест на тексте > 1000 символов:

