# Аннотация

**Среда программирования:** Visual Studio Code

**Язык программирования:** Python 3

**Процедуры для запуска программы:** $ python3 <имя\_файла>.py

**Пословица-тест:** Красивыми словами пастернак не помаслишь

**Текст для проверки работы:** Вот пример статьи на тысячу символов. Это достаточно маленький текст, оптимально подходящий для карточек товаров в интернет или магазинах или для небольших информационных публикаций. В таком тексте редко бывает более двух или трёх абзацев и обычно один подзаголовок. Но можно и без него. На тысячу символов рекомендовано использовать один или два ключа и одну картину. Текст на тысячу символов это сколько примерно слов? Статистика показывает, что тысяча включает в себя сто пятьдесят или двести слов средней величины. Но, если злоупотреблять предлогами, союзами и другими частями речи на один или два символа, то количество слов неизменно возрастает. В копирайтерской деятельности принято считать тысячи с пробелами или без. Учет пробелов увеличивает объем текста примерно на сто или двести символов именно столько раз мы разделяем слова свободным пространством. Считать пробелы заказчики не любят, так как это пустое место. Однако некоторые фирмы и биржи видят справедливым ставить стоимость за тысячу символов с пробелами, считая последние важным элементом качественного восприятия. Согласитесь, читать слитный текст без единого пропуска, никто не будет. Но большинству нужна цена за тысячу знаков без пробелов.

**Интерфейс:** #в разработке#

**Блок F: ПОТОЧНЫЕ ШИФРЫ**



## 

* **A5/1**

**Код программы:**

# -\*- coding:utf-8 -\*-

from demo import alphabet, input\_for\_cipher\_short, output\_from\_decrypted

import re

import copy

reg\_x\_length = 19

reg\_y\_length = 22

reg\_z\_length = 23

key\_one = ""

reg\_x = []

reg\_y = []

reg\_z = []

def loading\_registers(key):

    i = 0

    while(i < reg\_x\_length):

        reg\_x.insert(i, int(key[i]))

        i = i + 1

    j = 0

    p = reg\_x\_length

    while(j < reg\_y\_length):

        reg\_y.insert(j, int(key[p]))

        p = p + 1

        j = j + 1

    k = reg\_y\_length + reg\_x\_length

    r = 0

    while(r < reg\_z\_length):

        reg\_z.insert(r, int(key[k]))

        k = k + 1

        r = r + 1

def set\_key(key):

    if(len(key) == 64 and re.match("^([01])+", key)):

        key\_one = key

        loading\_registers(key)

        return True

    return False

def get\_key():

    return key\_one

def to\_binary(plain):

    s = ""

    i = 0

    for i in plain:

        binary = str(' '.join(format(ord(x), 'b') for x in i))

        j = len(binary)

        while(j < 12):

            binary = "0" + binary

            s = s + binary

            j = j + 1

    binary\_values = []

    k = 0

    while(k < len(s)):

        binary\_values.insert(k, int(s[k]))

        k = k + 1

    return binary\_values

def get\_majority(x, y, z):

    if(x + y + z > 1):

        return 1

    else:

        return 0

def get\_keystream(length):

    reg\_x\_temp = copy.deepcopy(reg\_x)

    reg\_y\_temp = copy.deepcopy(reg\_y)

    reg\_z\_temp = copy.deepcopy(reg\_z)

    keystream = []

    i = 0

    while i < length:

        majority = get\_majority(reg\_x\_temp[8], reg\_y\_temp[10], reg\_z\_temp[10])

        if reg\_x\_temp[8] == majority:

            new = reg\_x\_temp[13] ^ reg\_x\_temp[16] ^ reg\_x\_temp[17] ^ reg\_x\_temp[18]

            reg\_x\_temp\_two = copy.deepcopy(reg\_x\_temp)

            j = 1

            while(j < len(reg\_x\_temp)):

                reg\_x\_temp[j] = reg\_x\_temp\_two[j-1]

                j = j + 1

            reg\_x\_temp[0] = new

        if reg\_y\_temp[10] == majority:

            new\_one = reg\_y\_temp[20] ^ reg\_y\_temp[21]

            reg\_y\_temp\_two = copy.deepcopy(reg\_y\_temp)

            k = 1

            while(k < len(reg\_y\_temp)):

                reg\_y\_temp[k] = reg\_y\_temp\_two[k-1]

                k = k + 1

            reg\_y\_temp[0] = new\_one

        if reg\_z\_temp[10] == majority:

            new\_two = reg\_z\_temp[7] ^ reg\_z\_temp[20] ^ reg\_z\_temp[21] ^ reg\_z\_temp[22]

            reg\_z\_temp\_two = copy.deepcopy(reg\_z\_temp)

            m = 1

            while(m < len(reg\_z\_temp)):

                reg\_z\_temp[m] = reg\_z\_temp\_two[m-1]

                m = m + 1

            reg\_z\_temp[0] = new\_two

        keystream.insert(i, reg\_x\_temp[18] ^ reg\_y\_temp[21] ^ reg\_z\_temp[22])

        i = i + 1

    return keystream

def convert\_binary\_to\_str(binary):

    s = ""

    length = len(binary) - 12

    i = 0

    while(i <= length):

        s = s + chr(int(binary[i:i+12], 2))

        i = i + 12

    return str(s)

def encode(plain):

    s = ""

    binary = to\_binary(plain)

    keystream = get\_keystream(len(binary))

    i = 0

    while(i < len(binary)):

        s = s + str(binary[i] ^ keystream[i])

        i = i + 1

    return s

def decode(cipher):

    s = ""

    binary = []

    keystream = get\_keystream(len(cipher))

    i = 0

    while(i < len(cipher)):

        binary.insert(i, int(cipher[i]))

        s = s + str(binary[i] ^ keystream[i])

        i = i + 1

    return convert\_binary\_to\_str(str(s))

def user\_input\_key():

    tha\_key = str(input('Введите 64-bit ключ: '))

    if (len(tha\_key) == 64 and re.match("^([01])+", tha\_key)):

        return tha\_key

    else:

        while(len(tha\_key) != 64 and not re.match("^([01])+", tha\_key)):

            if (len(tha\_key) == 64 and re.match("^([01])+", tha\_key)):

                return tha\_key

            tha\_key = str(input('Введите 64-bit ключ: '))

    return tha\_key

# 0101001000011010110001110001100100101001000000110111111010110111

key = str(user\_input\_key())

set\_key(key)

print(f'''

Зашифрованный текст:

{encode(input\_for\_cipher\_short())}

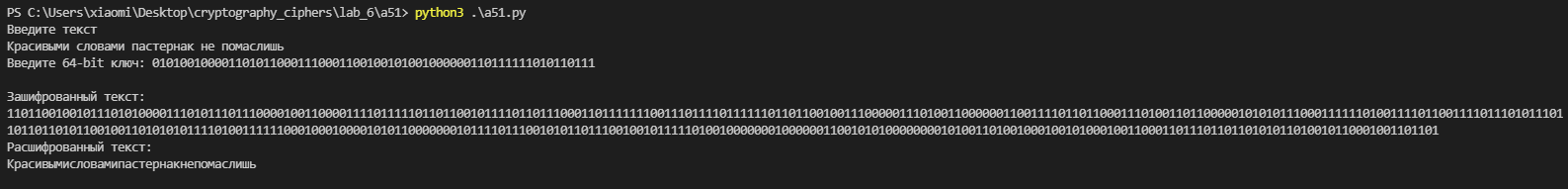
Расшифрованный текст:

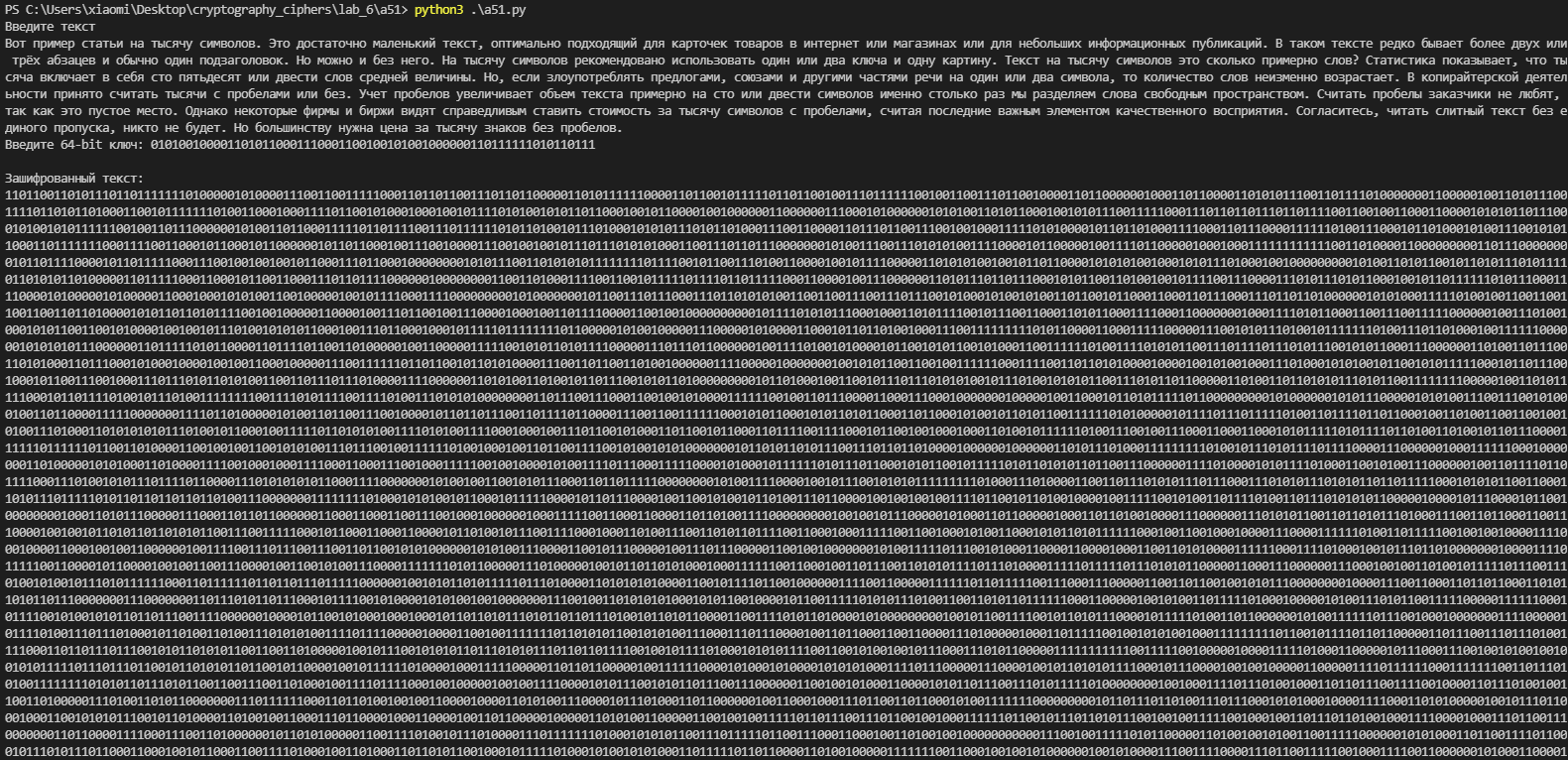
{output\_from\_decrypted(decode(encode(

    input\_for\_cipher\_short())))}

''')

**Тестирование:**



****

****