## 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 Е: ШИФРЫ ГАММИРОВАНИЯ

• Гаммирование ГОСТ 28147-89

## Код программы:

```
# -*- coding:utf-8 -*-
import sys
import numpy.random
import itertools
from demo import alphabet, input_for_cipher_short, input_for_cipher_long,
output_from_decrypted
import binascii
class GostCrypt(object):
   def __init__(self, key, sbox):
       self._key = None
       self._subkeys = None
        self.key = key
        self.sbox = sbox
   @staticmethod
    def _bit_length(value):
       return len(bin(value)[2:])
    @property
    def key(self):
        return self._key
    @key.setter
    def key(self, key):
        self. key = key
       self._subkeys = [(key >> (32 * i)) & 0xFFFFFFFF for i in range(8)] #8
кусков
    def _f(self, part, key):
       temp = part ^ key
        output = 0
        for i in range(8):
            output |= ((self.sbox[i][(temp >> (4 * i)) & 0b1111]) << (4 * i))
        return ((output >> 11) | (output << (32 - 11))) & 0xFFFFFFFF
    def _decrypt_round(self, left_part, right_part, round_key):
        return left part, right part ^ self. f(left part, round key)
    def encrypt(self, plain_msg):
        def _encrypt_round(left_part, right_part, round_key):
           return right_part, left_part ^ self._f(right_part, round_key)
```

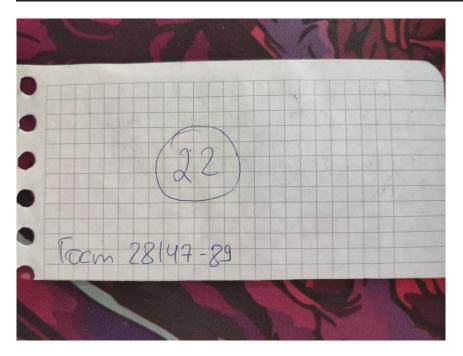
```
left_part = plain_msg >> 32
        right_part = plain_msg & 0xFFFFFFFF
        for i in range(24):
            left_part, right_part = _encrypt_round(left_part, right_part,
self._subkeys[i % 8])
        for i in range(8):
            left_part, right_part = _encrypt_round(left_part, right_part,
self._subkeys[7 - i])
        return (left_part << 32) | right_part</pre>
    def decrypt(self, crypted_msg):
        def _decrypt_round(left_part, right_part, round_key):
            return right_part ^ self._f(left_part, round_key), left_part
        left_part = crypted_msg >> 32
        right_part = crypted_msg & 0xFFFFFFFF
        for i in range(8):
            left_part, right_part = _decrypt_round(left_part, right_part,
self._subkeys[i])
        for i in range(24):
            left_part, right_part = _decrypt_round(left_part, right_part,
self._subkeys[(7 - i) % 8])
        return (left_part << 32) | right_part</pre>
sbox = [numpy.random.permutation(1) for 1 in itertools.repeat(list(range(16)),
8)]
sbox = (
    (4, 10, 9, 2, 13, 8, 0, 14, 6, 11, 1, 12, 7, 15, 5, 3),
    (14, 11, 4, 12, 6, 13, 15, 10, 2, 3, 8, 1, 0, 7, 5, 9),
    (5, 8, 1, 13, 10, 3, 4, 2, 14, 15, 12, 7, 6, 0, 9, 11),
    (7, 13, 10, 1, 0, 8, 9, 15, 14, 4, 6, 12, 11, 2, 5, 3),
    (6, 12, 7, 1, 5, 15, 13, 8, 4, 10, 9, 14, 0, 3, 11, 2),
    (4, 11, 10, 0, 7, 2, 1, 13, 3, 6, 8, 5, 9, 12, 15, 14),
    (13, 11, 4, 1, 3, 15, 5, 9, 0, 10, 14, 7, 6, 8, 2, 12),
    (1, 15, 13, 0, 5, 7, 10, 4, 9, 2, 3, 14, 6, 11, 8, 12),
key =
18318279387912387912789378912379821879387978238793278872378329832982398023031
text_short = input_for_cipher_short().encode().hex()
text short = int(text short, 16)
gost_short = GostCrypt(key, sbox)
enc_txt = gost_short.encrypt(text_short)
dec_txt = gost_short.decrypt(enc_txt)
dec txt = bytes.fromhex(hex(dec txt)[2::]).decode('utf-8')
```

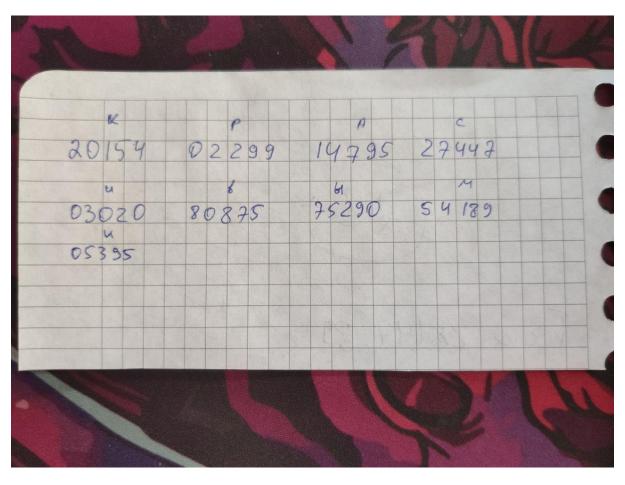
```
text_long = input_for_cipher_long().encode().hex()
text_long = int(text_long, 16)

print(f'''
Зашифрованный текст:
{enc_txt}
Расшифрованный текст:
{output_from_decrypted(dec_txt)}
''')
```

## Тестирование:

```
PS C:\Users\xiaomi\Desktop\cryptography_ciphers\lab_5\gost89> python3 .\gost89.py
Введите текст
Красивыми словами пастернак не помаслишь
Зашифрованный текст:
201540229914795274470302080875752905418905395191770125716947353830703838459216489491995987139374943186403280256065931194756968616301154931354263908686151430859726366026252421
Расшифрованный текст:
Красивымисловамипастернакнепомаслишь
```





PS C:\Users\xiaomi\Desktop\cryptography\_ciphers\lab\_5\gost89> python3 .\gost89.py

Введите текст

Вот пример статъм на тыслеу символива. Это достаточно маленький текст, отгимально подходящий для королька товаров в интернет или магазинах или для небольших информационных публикаций. В таком тексте редух или трех абзацие и обычно один подаголовок. Но можно и без него. В тыслеу смеюлов ресконендовани кололовать один или дая илеле и одру жартиру. Текст на тыслеу сменелов это стокомых отриченного колоновать один или дая сменелов, а ток подаголовать один или дая сменелов, а ток поличество слов неизменен верыствет. В колиратерской делегемьоги принято считать тыслеч с пробелам или без. Учет пробелов увеличенняем ет быть стать пробела и должного делегемьоги принято считать тыслеч с пробелам или без. Учет пробелов увеличенняем ет быть от сотоком раз на разделяем слова свободьям пространством. Считать пробела заказчим иле либе. Ток пробелами, считам последии важного пробелами, считам последии важного пробелами, считам последии важного пробелами. В пробелами от пробелами или простем учети на пробела учет пробелами или пространительного восприятил. Осгласитесь, читать слитный текст без с циного прогуссе, инсто не будет. Но большимству муни цена за тыслеу заково без пробелами.

### ашифпованный текст:

Расшифрованый текст:
В отприем станующенного в эторостаточемаленькийтекст, оттичальногододяцийдлякарточектоварованитернетилимагазинахилидлянебольшкоинформационныхтубликаций. Втакситекстередкобываетболеедвухилитрёхабзацевнобычносодингодзаго вок. Начинаться по предераты и предераты и предераты предераты предераты предераты и предераты предераты

# • Одноразовый блокнот К.Шеннона

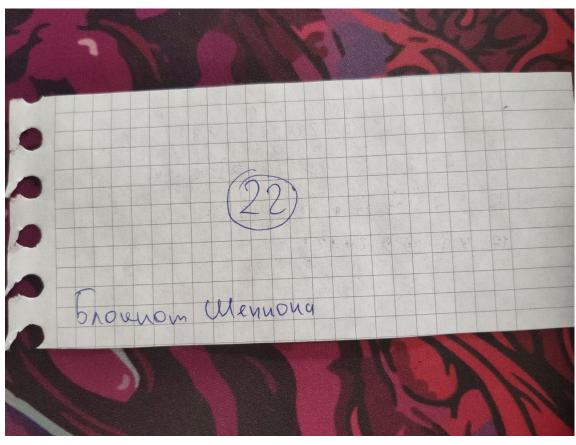
## Код программы:

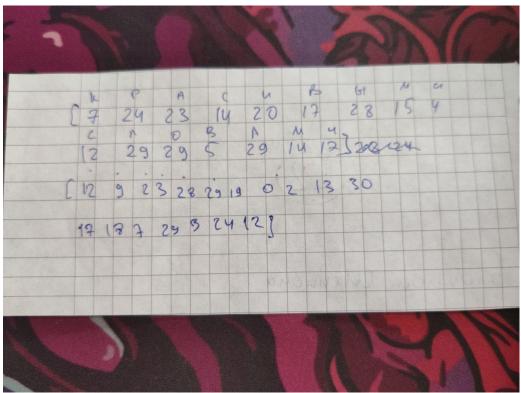
```
import random
alphabet = "абвгдеёжзийклмнопрстуфхцчшщьыьэюя "
alphabet = alphabet.replace(' ', '')
alphabet_lower = {}
```

```
i = 0
while i < (len(alphabet)):</pre>
    alphabet_lower.update({alphabet[i]: i})
    i += 1
def get_key(d, value):
    for k, v in d.items():
        if v == value:
            return k
def encode(msg):
    msg_list = list(msg)
    msg_list_len = len(msg_list)
    msg_code_bin_list = list()
    for i in range(len(msg_list)):
        msg_code_bin_list.append(alphabet_lower.get(msg_list[i]))
    key_list = list()
    for i in range(msg_list_len):
        key_list.append(random.randint(0, 32))
    cipher_list = list()
    for i in range(msg_list_len):
        m = int(msg_code_bin_list[i])
        k = int(key_list[i])
        cipher_list.append(int(bin(m ^ k), base=2))
    return cipher_list, key_list
def decode(msg, key_list):
    decipher_list = list()
    msg_list_len = len(msg)
    for i in range(msg_list_len):
        c = int(msg[i])
        k = int(key_list[i])
        decipher_list.append(int(bin(c ^ k), base=2))
    deciphered str = ""
    for i in range(len(decipher_list)):
        deciphered_str += get_key(alphabet_lower, decipher_list[i])
    return deciphered str
```

## Тестирование:

```
Ведите текст
Красиваем словаем пастернак не помасливь
Завифольный текст:
(7, 24, 23, 14, 26, 17, 28, 15, 4, 12, 29, 29, 5, 29, 14, 17, 28, 24, 28, 0, 20, 16, 22, 20, 7, 18, 8, 16, 2, 11, 0, 12, 28, 1, 12, 17], [12, 9, 23, 28, 29, 19, 0, 2, 13, 30, 17, 18, 7, 29, 3, 24, 12, 24, 14, 19, 17, 1, 24, 20, 12, 28, 13, 0, 13, 6, 0, 30, 16, 8, 21, 12])
Расмефотоваемый текст:
Красиваемостоваемый текст:
```





#### Ввелите текст

ВОТ пример СТЕТИМ НЕ ТЕСНУИ СМИСТИЛЬ ТО ТЕСТИТИ НЕ ТЕСНУИ СТЕТИМ НЕ ТЕСНИИ ТЕСНУИ СТЕТИМ НЕ ТЕСНУИ ТЕСНИИ ТЕ

#### Зашифрованный текст:

вотристительные со пожодые по применения и померанизации по померани по померанизации по померанизации по п