МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

**«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

**ЛАБОРАТОРНЫЕ РАБОТЫ ПО ПРЕДМЕТУ**

«Программирование криптографических алгоритмов»

**Выполнил:**

Барышников С.С. гр. 191-351

**Преподаватель:**

Бутакова Н.Г.

Москва 2021 г.

**Содержание**

[Аннотация 3](#_Toc84963116)

[Постоянный модуль 4](#_Toc84963117)

[F: ПОТОЧНЫЕ ШИФРЫ 5](#_Toc84963118)

[15. А5 /1 5](#_Toc84963119)

# Аннотация

**Среда программирования:** Visual Studio Code

**Язык программирования:** Python 3

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

**Пословица-тест:** Время, приливы и отливы не ждут человека.

**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#

# Постоянный модуль

Код модуля base.py используемый для предотвращения дублирования кода, используется во всех последующих программах:

import re

alphabet = "абвгдеёжзийклмнопрстуфхцчшщъыьэюя"

dict = {'.': 'тчк', ',': 'зпт'}

def replace\_all\_to(input\_text, dict):

    input\_text = input\_text.replace(' ', '')

    for i, j in dict.items():

        input\_text = input\_text.replace(i, j)

    return input\_text

def replace\_all\_from(input\_text, dict):

    for i, j in dict.items():

        input\_text = input\_text.replace(j, i)

    return input\_text

def file\_to\_string(name):

    with open(name) as f:

        input\_short\_text = " ".join([l.rstrip() for l in f]) + ' '

    return input\_short\_text.lower()

def input\_for\_cipher\_short():

    return replace\_all\_to(file\_to\_string('short.txt'), dict)

def input\_for\_cipher\_long():

    return replace\_all\_to(file\_to\_string('long.txt'), dict)

def output\_from\_decrypted(decrypted\_text):

    return replace\_all\_from(decrypted\_text, dict)

# F: ПОТОЧНЫЕ ШИФРЫ

# 

# 

# 

# 

# 

# 

# 

## А5 /1

А5 — это поточный алгоритм шифрования, используемый для обеспечения конфиденциальности передаваемых данных между телефоном и базовой станцией в европейской системе мобильной цифровой связи GSM (Groupe Spécial Mobile).

Шифр основан на побитовом сложении по модулю два (булева операция «исключающее или») генерируемой псевдослучайной последовательности и шифруемой информации. В A5 псевдослучайная последовательность реализуется на основе трёх линейных регистров сдвига с обратной связью. Регистры имеют длины 19, 22 и 23 бита соответственно. Сдвигами управляет специальная схема, организующая на каждом шаге смещение как минимум двух регистров, что приводит к их неравномерному движению. Последовательность формируется путём операции «исключающее или» над выходными битами регистров.

**Код программы:**

# -\*- coding:utf-8 -\*-

from base import alphabet, input\_for\_cipher\_short, input\_for\_cipher\_long, 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 encrypt(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 decrypt(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'''

A5/1:

КОРОТКИЙ ТЕКСТ:

Зашифрованный текст:

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

Расшифрованный текст:

{output\_from\_decrypted(decrypt(encrypt(

    input\_for\_cipher\_short())))}

ДЛИННЫЙ ТЕКСТ:

Зашифрованный текст:

{encrypt(input\_for\_cipher\_long())}

Расшифрованный текст:

{output\_from\_decrypted(decrypt(encrypt(

    input\_for\_cipher\_long())))}

''')

**Тестирование:**

/bin/python3 /root/mospolytech-education-crypt-dev-2021-1/lab06\_15\_a51.py

Введите 64-bit ключ: 0101001000011010110001110001100100101001000000110111111010110111

A5/1:

КОРОТКИЙ ТЕКСТ:

Зашифрованный текст:

110110111010111010100001110101110010000011100101011111001001110110010010101100000101101110000111110111101000110110110011011100000100010011000101110011111100110001110110110111110101101011100011111101001110011000001001101010010111101100100011001101010010111010010100100010001000010101100101001011111011001010111110001000101001010011111101100001100000010100001001101001100010000101010111100110000100110110111000011011100100001000010001000011010111011101100111101011111000

Расшифрованный текст:

время,приливыиотливынеждутчеловека.

ДЛИННЫЙ ТЕКСТ:

Зашифрованный текст:

110110111010111011011111110100000101000011100110011111000110110110011101101100000110101111110000110110010111110110110010011101111110010011001110110010000110110000001000110110000110101011100110111101000000011000001001101011100111101101011010001100101111111010011000100011110110010100010001001011110101001010110110001001011000010010000001100000011100010100000010101001101011000100101011100111110001110110110111011010010011001001100011000010101011011100010100101011111100100110111000000101001101100011111011011110011101111110101101001011101000101010111010110100011100110000110111011001110010010001111101010000101101101000111100011011100001111110100111000101101000101001110010101100011011111110001111001100010110001011000000101101100010011100100001110010010010111011101010100011001110110111000000010100111001110101010011110000101100000100111101100000100010001111111111110011010000110000000001101110000000010110111100001011011111000111001001001001011000111011000100000000101011100110101010111111110111100101100111010011000010010111100000110101010010010110110000101010100100010101110100010010000000001010011010110010110101110101111011010101101000001101111100011000101100110001110110111100000010000000011001101000111100110010111110111101101111100011000010011100000011010111011011100010101100110100100101111001110000111010111010110001001011011111101011100011110000101000001010000011000100010101001100100000100101111000111100000000010100000001011001110111000111011010101001100110011100111011100101000101001010011011001011000110001101110001110110110100000010101000111110100100110011001100110011011010000101011011010111100100100000110000100111011001001110000100010011011110000110010010000000000101111010101110001000110101111001011100110001101011000111100011000000010001111010110001100111001111100000010011101001000101011001100101000010010010111010010101011000100111011000100010111110111111110110000010100100000111000001010000110001011011010010001110011111111101011000011000111110000011100101011101101011111110100111011010001001111110000001010101011100000011011111010110000110111101100110100000100110000011111001010110101111000001110111011000000100111101001010000101100101011001010001100111111010011110101011001110111101110101110010101100011100000011010011011100110101000110111000101000100001001001100010000011100111111011011001011010100001110011011001101001000000111100000100000001001010110011001001111110001111001101101010000100001001010010001110100010101001011001010111110001011011100100010110011100100011101110101101010011001101110111010000111100000011010100110100101101110010101101000000000101101000100110010111011101010100101110100101010110011101011011000001101001101101010111010110011111111000001001101011111000101101111010010111010011111111001111010111100111101001110101010000000011011100111000110010010100001111110010011011100001100011100010000000100000000110001011010111110110000000001010000001010111000001010100111001110010100010011011000011111000000011110110100000101001101100111001000010110110111001101111011000011100110011111100010101100010101101011000110110001010110110101100111111010100000101111011101111101001101111011011000100110100110011001001010011101000110101010101110100101100010011111011010101001111010100111100010001001110110010100011011001011000110111100111100010110010010001000110100101111110100111001001110001100011000101011111010111101101001101001011011100001111110111111011001101000011001001001100101010011101110010011111101001000100110110011110010100101010000000101101011010111001110110110100001000000100000011010111010001111111110100101110101111011110000111000000100011111100010000000110100000101010001101000011110010001000111100011000111001000111110010010000101001111011100011111000010100010111111010111011000101011001011111010110101011011001110000001111010000101011110100011001010011100000010011011110110111100011101001010111011110110000111010101010110001111000000010100100110010101110001101101110000000000101001111000010010111001010101111111110100011101000011001101110101011101110001110101011101010110110111110001010101100110001101011101111101011011011011011010011100000001111111101000101010010110001011111000010110111000010011001010010110100111011000010010010010011110110010110100100001001111100101001101111010011011101010101100000100001011100001011001000000001000110101110000011100011011011000000110001100011001110010001000000100011111001100011000011011010011110000000001001001011100000101000110110000010001100011001000010011000011100101100011010110111010001110011011000110011100001001001011010110110101011001110011111000101100011000110000101101001011100111100010001101001110011010110111100110001000111110011001000101001100010101101011111100010011001000100001110000111111010011011111001001001000011110001000011000100100110000001001111001110111001110011011001010100000010101001110000110010111000001001110111000001100100100000001010011111011100101000110000110000100011001101010000111111000111101000100101110110100000001000011110111110011000010110000100100110011100001001100101001110000111111101011000001110100000100101101101010001000111111001100010011011100110101011110111010000111110111110111010101100000110001110000001110001001001101001011111011100111010010100101110101111110001101111110110110111011111000000100101011010111110111010000110101010100001100101111011001000000111100110000011111101101111100111000111000001100110110010010101110000000010000111001100011011011000110101101011011100000001110000000110111010110111000101111001010000101010010010000000111001001101010101000101011001000010110011111010001110100110011010110111111000110000010010100110111110100010000010100111010110011111000001111110001011110010100101011011011100111100000010000101100101000100010001011011010111010110110111010010110101100001100111101011010000101000000000100101100111100101101011100001011111010011011000000101001111110111001000100000001111000001011110100111011101000101101001101001110101010011110111100000100001100100111111101101010110010101001110001110111000010011011000110011000011101000001000110111110010010101001000111111111011001011110110110000011011100111011101001111000110110111011100101011010101100110011010000010010111001010101101110101011101101101111001001011110100010101011110011001010010010111000111010110000011111111111001111100100000100001111101000110000010111000111001001010010010010101111101110111011001011010101101100101100001001011111101000010001111100000110110110000010011111100001010001010000101010100011110111000001110000100101101010111100010111000010010010000011000001111011111100011111110011011101010011111111010101101110101100110011100110100010011110111100010010000010010011110000101011100101011011100111000000110010010100011000010101101110011101011111010000000010010001111011101001000110110111001111001000011011101001001100110100000111010011010110000000111011111100011011010010010011000010000110101001110000101110100011011000000100110001000111011001101100010100111111100000000010110111011010011101110001010100010000111100011010100000100101110110001000110010101111100101101000011010010011000111011000010001100001001101100000100000110101001100000110010010011111011011100111011001001000111111011001011101101011100100100111110010001001101110110100100011110000100011101100111000000011011000011110001110011010000001011010100000110011110100101110100001110111111101000101010110011101111101100111000110001001101001001000000000001110010011111010110000011010010010100110011111000000101010001101100111101100010111010111011000110001001011000110011110100010011010001101101011001000101111101000101001010100011011111011011000011010010000011111110011000100100101000000100101000011100111100001110110011111001000111100110000001010001100001011011100110011101100110100000000100101001111011101111110000100100011000011011110001000011110110100010100101101010000101001001110001011001111000101001100010000010100001011000101100101100101011000001110100001101001100011011110100000000111011100001010001101010110101001111100000101110010011110110000100010011110001100010010100111100101100001011011000011001010011110110100111000000111100100111001001010100000111101010010100111010101001100111111100001000110101101100000110100010100110011011111011010101001110101011000001000011111000001001110000101010010000000111000101101110011110100001001001111011111010101110001001010111111001110001100110010110100111000001110010000111011001100101111001000000111011110011000011001010101000000010110010100001011010101111010101010001111111011101101001000010011110111100011100011100111010100110101110011101101101111111001110011010100001010101110100011110111011100000110011010110000001110100011001100110111010100010101011001010110101110000000010001001110010001111010001111000010000100010000111100101011010001100110010001010010000010101001011101111111111011011110110001101010010011110101010101001011100011011110100110001110101100000110111000000100111101011111101001000011000110011111000001010110110011001010010001010101010111011110110100101000010111010101110101101001000001000000110101100000101101100011000000001001011101101001001111111001011011001100010011101011010000001111000101100000101010000111100100111101101001000000000111000001100001101001000011011111010101100111110111010111111111011001111100010111010000010111111110000011000001001111110101000001100110111101011101101010011000111100111111011100001011000011001001100000000001111011111001010010101011001110010010000110011001011111001110011011111000000011000001000001001000010001111101011100011100100110101101110001000100101100100110000000001000111111100001110011001111111111010010110110010100000010101000100000101010001000010011100100110110111000010011010110110110100001000011110111000110001000011101000101100000000011001001111111101001111100100001110001010000010110101111010100010000111111010011010101110100001001010100110010100000001100011100001110011001101011010000000010100010100010000101111011011101101000110100101110010010110111011010010001110110001111100100010011111110000000110000011000010111001000100111001000100000011011101011110101101100110100110111011110000111110010001100000100001010101011100111001111010111110100101101000110111011111111001000110001000100111001100111010111100011001101001101101101101101001001101001111011111100000101001001110000100110101110011010001111110110000011110101010101000011101011111100110000000001010101011010110011100100111001001101100010101110101110100000010010001100100111000111011100001111000100111111001110000001000010000111001110001010001010000111001110110111000000100110101100111001110011110101011101001101101000001010101000011100010010010100000011011011111010101101100101100001010011110000110011000111111010000100100111000111101100110101010010100000111000010100101001110101010000011011100110000010110100010011000101000110001111110100101111010000100100010001110010110101000111011111111000011011100100111111110101010111100000010110000111011100001010011010101000000010011001101101101010001101100010111010001111001000000100010000110101110111111100100100011010001100111110110101110011000001110110111011110100010110110011111000110111100100111011011100000001000011000010000011001001111010001111001001011011111111001011010010101111100010000101010100010000001010000101101110111111111101101110011000000000101110000011110011111111111110101110111010010001111000110010101010001101110001011011111001010011001101110011001111000110011001011001000100001011011011111100000000100011011110000110001001111111000001000100101110010100000000001010100000010111101100101111011010001010110011100100010010000011111100100010001111011001001000011110100001000001011001010111101100011011110010100011100100111110000110010001110110000001101101011111110101111101011111110011001011011101100111011100110111100001000001010101000110100000111101111001011000100011111001000111001000000110011101101010100111010100110001001101001010000010111111000111000010100010101010111010010110000010100110010011110111101010100011010010110010110110010100110010100000000010111001110101010111101100110101001001000010101100010010111010110110100110100000011010100000111100100000100001001011001101100011100010011011001011111011000000101111111111100010010110011001001111110101111010000110010010011000111010011001100111111110010101111110110000011000100001000100110100011110010101101010111000001001010001110000111001000011110111000111010110011110100001010001010101100010010001111011110010001011001001011001101100001100000010001110001011001101001100110000111101101000101001100010010111111100010010100000110110100111100011000111001011101010010101110001010110011111111101000110111000011101010010110001101110011110111000001001001001101010011111101001000111100010000010110111110111001000101000001100011110100101010100111001001000101111000100101100011001011101111001110100101010000001000000100010101101011011101001011000000111111010111000100101110001110110000101011001000010101100110000001101111001100111100000100110011111110011011100100011011110011011010110010011101010001101100111000101111010100000111001000100101101111000110001001101101000100110001000001101001110111010111011010111011101001001100110000110010011111101010101011011010

Расшифрованный текст:

вотпримерстатьинатысячусимволов.этодостаточномаленькийтекст,оптимальноподходящийдлякарточектовароввинтернетилимагазинахилидлянебольшихинформационныхпубликаций.втакомтекстередкобываетболеедвухилитрёхабзацевиобычноодинподзаголовок.номожноибезнего.натысячусимволоврекомендованоиспользоватьодинилидваключаиоднукартину.текстнатысячусимволовэтосколькопримернослов.статистикапоказывает,чтотысячавключаетвсебястопятьдесятилидвестисловсреднейвеличины.но,еслизлоупотреблятьпредлогами,союзамиидругимичастямиречинаодинилидвасимвола,токоличествословнеизменновозрастает.вкопирайтерскойдеятельностипринятосчитатьтысячиспробеламиилибез.учетпробеловувеличиваетобъемтекстапримернонастоилидвестисимволовименностолькоразмыразделяемсловасвободнымпространством.считатьпробелызаказчикинелюбят,таккакэтопустоеместо.однаконекоторыефирмыибирживидятсправедливымставитьстоимостьзатысячусимволовспробелами,считаяпоследниеважнымэлементомкачественноговосприятия.согласитесь,читатьслитныйтекстбезединогопропуска,никтонебудет.нобольшинствунужнаценазатысячузнаковбезпробелов.