SA 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, 0, 0]
y = [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]

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:


PS C:\Users\Sergey\OneDrive - МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ\учёба\Крипта\2sem>& C:/Users/Sergey/AppData/Local/Microsoft/WindowsApps/python3.11.exe "c:/Users/Sergey/OneDrive - МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ/учёба/Крипта/2sem/Block_F/A5-1.py"
Введите текст: неттакогомудрецазптвкоторомнебылобыглупоститчк
['00110000', '00100111', '00110101', '00110101', '00100010', '00101101', '00110001', '00100101', '00110001', '00101111', '00110110', '00100110', '00110011', '00100111', '00111001', '00100010', '00101010', '00110010', '00110101', '00100100', '00101101', '00110001', '00110101', '00110001', '00110011', '00110001', '00101111', '00110000', '00100111', '00100011', '00111110', '00101110', '00110001', '00100011', '00111110', '00100101', '00101110', '00110110', '00110010', '00110001', '00110100', '00110101', '00101011', '00110101', '00111010', '00101101']
НЕТТАКОГОМУДРЕЦАЗПТВКОТОРОМНЕБЫЛОБЫГЛУПОСТИТЧК
& C:/Users/Sergey/AppData/Local/Microsoft/WindowsApps/python3.11.exe "c:/Users/Sergey/OneDrive - МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ/учёба/Крипта/2sem/Block_F/A5-1.py"
Выберите режим (1 - карточка, 2 - большой текст): 2
Введите текст: А судьи кто? – За древностию лет К свободной жизни их вражда непримирима, Сужденья черпают из забытых газет Времён Очаковских и покоренья Крыма; Всегда готовые к журьбе, Поют все песнь одну и ту же, Не замечая об себе: Что старее, то хуже. Где? укажите нам, отечества отцы, Которых мы должны принять за образцы? Не эти ли, грабительством богаты? Защиту от суда в друзьях нашли, в родстве , Великолепные соорудя палаты, Где разливаются в пирах и мотовстве, И где не воскресят клиенты-иностранцы Прошедшего житья подлейшие черты. Да и кому в Москве не зажимали рты Обеды, ужины и танцы? Не тот ли, вы к кому меня ещё с пелен, Для замыслов каких-то непонятных , Дитёй возили на поклон? Тот Нестор негодяев знатных, Толпою окружённый слуг; Усердствуя, они в часы вина и драки И честь, и жизнь его не раз спасали: вдруг На них он выменял борзые три собаки!!! Или вон тот ещё, который для затей На крепостной балет согнал на многих фурах От матерей, отцов отторженных детей?! Сам погружён умом в Зефирах и в Амурах, Заставил всю Москву дивиться их красе! Но должник ов не согласил к отсрочке: Амуры и Зефиры все Распроданы поодиночке!!! Вот те, которые дожили до седин! Вот уважать кого должны мы на безлюдьи! Вот наши строгие ценители и судьи! Теперь пускай из нас один, Из молодых людей, найдётся – враг исканий, Не требуя ни мест, ни повышенья в чин, В науки он вперит ум, алчущий познаний; Или в душе его сам бог возбудит жар К искусствам творческим, высоким и прекрасным, – Они тотчас: разбой! пожар! И прослывёт у них мечтателем! опасным!! – Мундир! один мундир! он в прежнем их быту Когда-то укрывал, расшитый и красивый, Их слабодушие, рассудка нищету; И нам за ними в путь счастливый! И в жёнах, дочерях – к мундиру та же страсть! Я сам к нему давно ль от нежности отрёкся?! Теперь уж в это мне ребячество не впасть; Но кто б тогда за всеми не повлекся? Когда и в гвардии, иные от двора Сюда на время приезжали, – Кричали женщины: ура! И в воздух чепчики бросали!

Ручная проверка:

A5/2

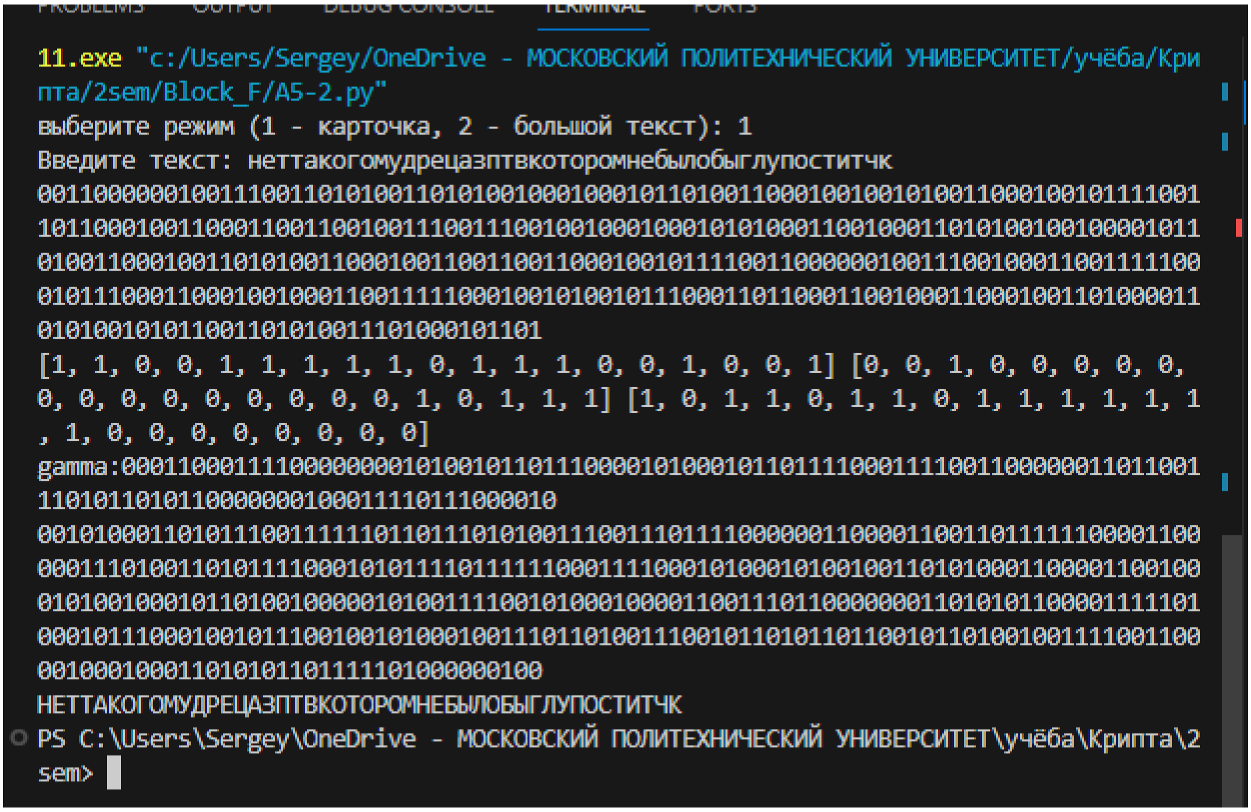
Код:

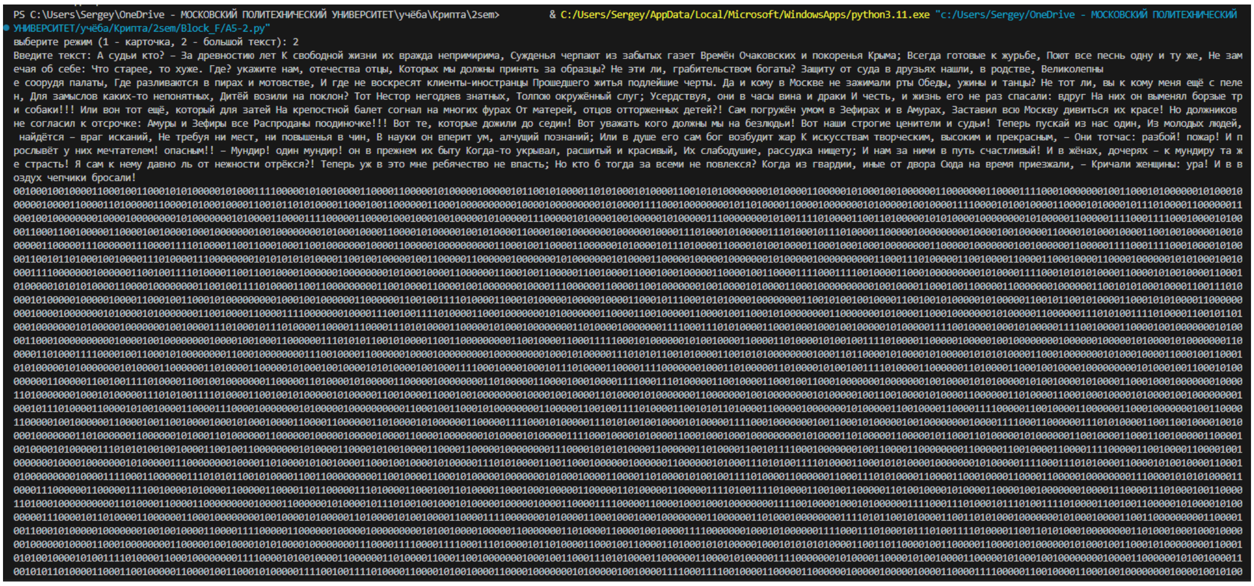
```
# from bit import BitArray
import re
for_big_text = "АБВГДЕёЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ".lower() +
"АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ"  + " !\"#$%-'()*+,—–
./:;<=>?@[\]^_`{|}"

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:]
```

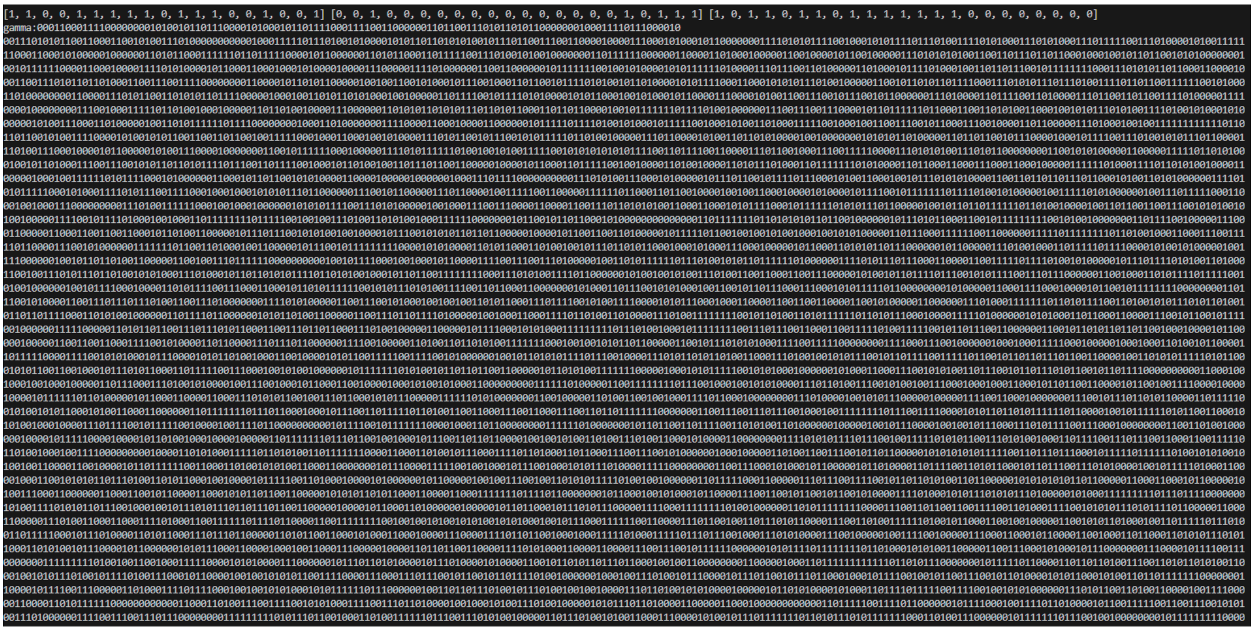
```
    while len(c) != 8: c = '0' + c
    text_reg += c
key = [1] * 64
print(text_reg)

x = [0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
y = [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]
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]:
```

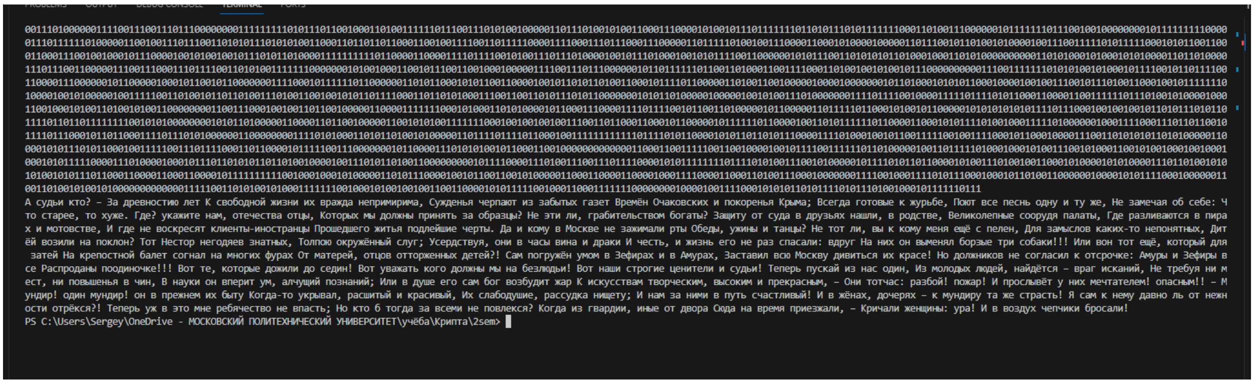
```
        y.append(y[1] ^ y.pop(0))
    if r4[13]:
        z.append(z[1] ^ z[2] ^ z[15] ^ z.pop(0))
    r4.append(r4[5] ^ r4.pop(0))
print(x, y, z)
print("gamma:" + gamma)

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:


PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
11.exe "c:/Users/Sergey/OneDrive - МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ/учёба/Крипта/2sem/Block_F/A5-2.py"
выберите режим (1 - карточка, 2 - большой текст): 1
Введите текст: неттакогомудрецазптвкоторомнебылобыглупоститчк
0011000000100111001101010011010100100010001011010011000100100101001100010010111100110110001001100011001100100111001110010010001000101010001100100011010100100100001011010011000100110101001100010011001100110001001011110011000000100111001000110011111000101110001100010010001000110011111000100101001011100011011000110010001100010011010000110101001010110011010100111010001011
[1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 0, 0, 1] [0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1] [1, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0]
gamma:00011000111100000000101001011011100001010001011011110001111001100000011011001110101101011000000010001111011110000100010100011010111001111110110111010100111001110111100000011000011001101111111000011000000111010011010111100010101111011111110001111000101000101001001101010001100001100100010100100010110100100000101001111001010001000011001110110000000110101011000011111010001011100010010111001001010001001110110100111001011010110110010110100100111100110000100010001101010110111110100000010
НЕТТАКОГОМУДРЕЦАЗПТВКОТОРОМНЕБЫЛОБЫГЛУПОСТИТЧК
PS C:\Users\Sergey\OneDrive - МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ\учёба\Крипта\2sem>


PS C:\Users\Sergey\OneDrive - МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ\учёба\Крипта\2sem> & C:/Users/Sergey/AppData/Local/Microsoft/WindowsApps/python3.11.exe "c:/Users/Sergey/OneDrive - МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ/учёба/Крипта/2sem/Block_F/A5-2.py"
выберите режим (1 - карточка, 2 - большой текст): 2
Введите текст: А судьи кто? – За древностию лет К свободной жизни их вражда непримирима, Сужденья черпают из забытых газет Времён Очаковских и покоренья Крыма; Всегда готовые к журьбе, Поют все песнь одну и ту же, Не замечая об себе: Что старее, то хуже. Где? укажите нам, отечества отцы, Которых мы должны принять за образцы? Не эти ли, грабительством богаты? Защиту от суда в друзьях нашли, в родстве, Великолепные соорудя палаты, Где разливаются в пирах и мотовстве, И где не воскресят клиенты-иностранцы Прошедшего житья подлейшие черты. Да и кому в Москве не зажимали рты Обеды, ужины и танцы? Не тот ли, вы к кому меня ещё с пеленн, Для замыслов каких-то непонятных, Дитёй возили на поклон? Тот Нестор негодяев знатных, Толпою окружённый слуг; Усердствуя, они в часы вина и драки И честь, и жизнь его не раз спасали: вдруг На них он выменял борзые три собаки!!! Или вон тот ещё, который для затей На крепостной балет согнал на многих фурах От матерей, отцов отторженных детей?! Сам погружён умом в Зефирах и в Амурах, Заставил всю Москву дивиться их красе! Но должников не согласил к отсрочке: Амуры и Зефиры все Распроданы поодиночке!!! Вот те, которые дожили до седин! Вот уважать кого должны мы на безлюдьи! Вот наши строгие ценители и судьи! Теперь пускай из нас один, Из молодых людей, найдётся – враг исканий, Не требуя ни мест, ни повышенья в чин, В науки он вперит ум, алчущий познаний; Или в душе его сам бог возбудит жар К искусствам творческим, высоким и прекрасным, – Они тотчас: разбой! пожар! И прослывёт у них мечтателем! опасным!! – Мундир! один мундир! он в прежнем их быту Когда-то укрывал, расшитый и красивый, Их слабодушие, рассудка нищету; И нам за ними в путь счастливый! И в жёнах, дочерях – к мундиру та же страсть! Я сам к нему давно ль от нежности отрёкся?! Теперь уж в это мне ребячество не впасть; Но кто б тогда за всеми не повлекся? Когда из гвардии, иные от двора Сюда на время приезжали, – Кричали женщины: ура! И в воздух чепчики бросали!





Для ручной проверки

```
PS C:\Users\Sergey\OneDrive - МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ\учёба\Крипта\2sem> & C:/Users/Sergey/AppData/Local/Mic
TET/учёба/Крипта/2sem/Block_F/A5-2.py"
выберите режим (1 - карточка, 2 - большой текст): 1
Введите текст: осень
0011000100110100001001110011000000111111
gamma:11100011011001011001110111111001110101001110101101010111001011100110010101010010011110111100011011101111000001000
1101001001010001101110101100100111101011
ОСЕНЬ
PS C:\Users\Sergey\OneDrive - МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ\учёба\Крипта\2sem>
```