

Блокнот Шеннона

```
alp = "АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ".lower()
for_big_text = "АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ".lower() +
"АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ" + " !\"#$%&'()*+,-./:;<=>?@[\\]^_`{|}"
# print(alp.index("А"))
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:

```

TET\учеба\Крипта\2sem\B1ock_E\shannon.py" ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ\учеба\Крипта\2sem>
Выберите задание (1 - карточка, 2 - текст): 1
a = 9
c = 7
T0 = 4
Введите текст: неттакогомудрецаптвокоторомнебылобыглупоститчк
[24, 15, 19, 2, 23, 0, 27, 31, 17, 14, 12, 12, 31, 19, 27, 20, 2, 9, 3, 2, 17, 20, 15, 26, 3, 0, 21, 5, 4, 31, 16, 15, 25, 11, 28, 19, 2, 9, 28, 10, 20, 20, 1, 26, 6, 24]
Зашифрованный текст: шлувачьясоммууфйгвсфпгакедярпцльувйкфбъш
Дешифрованный текст: неттакогомудрецаптвокоторомнебылобыглупоститчк
PS C:\Users\Sergey\OneDrive - МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ\учеба\Крипта\2sem>

```

