

## Оглавление

Шифры моноалфавитной подстановки .....	2
Шифр Цезаря .....	3
Шифрование и расшифрование файла шифром Цезаря .....	4
Дешифрование текстового файла, зашифрованного шифром Цезаря .....	11
Дешифрование изображения, зашифрованного шифром Цезаря .....	12
Задание 1 .....	14
Задание 2 .....	14
Задание 3 .....	14
Афинный шифр .....	16
Задание 4 .....	18
Задание 5 .....	18
Задание 6 .....	19
Задание 7 .....	19
Дешифрование - частотный анализ .....	20
Задание 8 .....	21
Полиалфавитные подстановки .....	22
Задание 8 .....	24
Дешифрование - метод вероятных слов .....	24
Задание 9 .....	25
Задание 10 .....	25
Задание 11 .....	26
Шифры перестановки .....	27
Задание 12 .....	28
Литература .....	29

## Шифры моноалфавитной подстановки

Шифр моноалфавитной подстановки - это один из самых древних шифров на Земле. Частным случаем этого шифра для шифровки секретных сообщений пользовался еще Гай Юлий Цезарь.

Первая работа посвящена изучению моноалфавитных подстановок. Рассмотрим, как используют этот шифр.

Прежде всего выбирается *нормативный алфавит*, т.е. набор символов, которые будут использоваться при составлении сообщений, требующих зашифровки. Допустим, это будут прописные буквы русского алфавита (исключая буквы “Ё” и “Ъ”) и пробел. Таким образом, наш нормативный алфавит состоит из 32 символов. Затем выбирается *алфавит шифрования* и устанавливается взаимно однозначное соответствие между символами нормативного алфавита и символами алфавита шифрования. Алфавит шифрования может состоять из произвольных символов, в том числе и из символов нормативного алфавита.

Чтобы зашифровать исходное сообщение, каждый символ открытого текста заменяется на соответствующий ему символ алфавита шифрования.

Таблица 1

Нормативный алфавит	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	...
Алфавит шифрования	Н	К	А	Л	З	Т	П	И	О	Р	Б	Г	...

Зашифруем, например, слово “звезда”. Если использовать алфавиты, приведенные в таблице 1, то получится следующее:

Исходное сообщение:                   З В Е З Д А

Шифрованный текст:                   И А Т И З Н

Метод моноалфавитной подстановки можно представить как числовые преобразования символов исходного текста. Для этого каждой букве нормативного алфавита ставится в соответствие некоторое число,

называемое *числовым эквивалентом* этой буквы. Например, для букв русского алфавита и пробела это выглядит так:

Таблица 2

Нормативный алфавит	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
Числовые эквиваленты	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Таблица 2 (продолжение)

Нормативный алфавит	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	“ – ”
Числовые эквиваленты	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

## Шифр Цезаря

Простейшим примером моноалфавитных подстановок является шифр Цезаря. В этом шифре каждый символ открытого текста заменяется третьим после него символом в алфавите, замкнутом в кольцо, т.е. после пробела следует буква “А”. Таким образом, шифр Цезаря описывается так:

$$E_i = (M_i + S) \bmod L \quad (1)$$

где  $S$  - коэффициент сдвига, одинаковый для всех символов.

Цезарь использовал величину сдвига  $S=3$ , но, конечно, можно использовать любое целое  $S$ :  $1 \leq S \leq (L-1)$ .

Зашифруем, например, текст “ШИФР\_ЦЕЗАРЯ”, используя коэффициент сдвига  $S=2$ .

Открытый текст:	Ш	И	Ф	Р	_	Ц	Е	З	А	Р	Я
Шифрованный текст:	Ы	К	Ц	Т	Б	Ш	З	Й	В	Т	А

## Шифрование и расшифрование файла шифром Цезаря

1. Создаем файл Caesar.py
2. Вставляем в Caesar.py функцию шифрования одного числа:

```
def encrypt(m, key):  
    c = (m + key) % 256  
    return c
```

3. Проверяем: создаем файл main\_caesar.py (рис.1)

```
import Caesar  
  
def main():  
    m = 24  
    key = 37  
    c = Caesar.encrypt(m, key)  
    print('c=', c)  
  
if __name__ == '__main__':  
    main()
```

```
c= 61  
  
Process finished with exit code 0
```

Рисунок 1 – Вызов функции encrypt

4. Вставляем в caesar.py функцию расшифрования одного числа:

```
def decrypt(m, key):  
    c = (m - key) % 256  
    return c
```

5. Проверяем (рис.2)

```

import Caesar

def main():
    m = 24
    key = 37
    c = Caesar.encrypt(m, key)
    print('c=', c)
    m1 = Caesar.decrypt(c, key)
    print('m1=', m1)

if __name__ == '__main__':
    main()

```

```

c= 61
m1= 24

Process finished with exit code 0

```

Рисунок 2 – Вызов функции decrypt

6. Для шифрования массива (списка) чисел используем функцию:

```

def encrypt_data(data, key):
    cypher_data = []
    for m in data:
        c = encrypt(m, key)
        cypher_data.append(c)
    return cypher_data

```

7. Проверяем (рис. 3)

```

import Caesar

def main():
    m = 24
    key = 37
    c = Caesar.encrypt(m, key)
    print('c=', c)
    m1 = Caesar.decrypt(c, key)
    print('m1=', m1)
    data = [34, 67, 123, 79, 201]
    encrypt_data = Caesar.encrypt_data(data, key)
    print('encrypt_data =', encrypt_data)

if __name__ == '__main__':
    main()

```

```

c= 61
m1= 24
encrypt_data = [71, 104, 160, 116, 238]

Process finished with exit code 0

```

Рисунок 3 – Вызов функции encrypt\_data

8. Для расшифрования массива (списка) чисел используем функцию:

```

def decrypt_data(data_c, key):
    data = []
    for c in data_c:
        m = decrypt(c, key)
        data.append(m)
    return data

```

9. Проверяем (рис. 4)

```

import Caesar

def main():
    m = 24
    key = 37
    c = Caesar.encrypt(m, key)
    print('c=', c)
    m1 = Caesar.decrypt(c, key)
    print('m1=', m1)
    data = [34, 67, 123, 79, 201]
    encrypt_data = Caesar.encrypt_data(data, key)
    print('encrypt_data =', encrypt_data)
    decrypt_data = Caesar.decrypt_data(encrypt_data, key)
    print('decrypt_data =', decrypt_data)

if __name__ == '__main__':
    main()

```

```

c= 61
m1= 24
encrypt_data = [71, 104, 160, 116, 238]
decrypt_data = [34, 67, 123, 79, 201]

Process finished with exit code 0

```

Рисунок 4 – Вызов функции decrypt\_data

10. Теперь массив (список) чисел формируем не сами, а берем из файла. Формируем файл 'f1.txt'. В него заносим следующую информацию:

He was a burly man of an exceedingly dark complexion, with an exceedingly large head and a corresponding large hand. He took my chin in his large hand and turned up my face to have a look at me by the light of the candle. He was prematurely bald on the top of his head, and had bushy black eyebrows that wouldn't lie down but stood up bristling. His eyes were set very deep in his head, and were disagreeably sharp and suspicious. He had a large watchchain, and strong black dots where his beard and whiskers would have been if he had let them. He was nothing to me, and I could have had no foresight then, that he ever would be anything to me, but it happened that I had this opportunity of observing him well.

Подключаем модуль read\_write\_file (рис. 5).

```
import Caesar
import read_write_file

def main():
    data = read_write_file.read_data_1byte('f1.txt')
    print('data=', data[0:15])

if __name__ == '__main__':
    main()
```

```
data= [72, 101, 32, 119, 97, 115, 32, 97, 32, 98, 117, 114, 108, 121, 32]

Process finished with exit code 0
```

Рисунок 5 – Чтение файла “f1.txt”

Чтоб сделать код наглядней, можно импортировать функции для чтения и записи данных из файла так:

```
from read_write_file import read_data_1byte as read
from read_write_file import write_data_1byte as write
```

Тогда, прочитать данные из файла:

```
data = read('f1.txt')
```

11. Убедимся, что полученные числа – это наш текст (рис. 6):



```

import Caesar
import read_write_file

def main():
    data = read_write_file.read_data_1byte('f1.txt')
    print('data=', data[0:15])
    txt = ''
    for n in data[0:15]:
        txt += chr(n)
    print('text=', txt)

if __name__ == '__main__':
    main()

```

```

data= [72, 101, 32, 119, 97, 115, 32, 97, 32, 98, 117, 114, 108, 121, 32]
text= He was a burly

```

Рисунок 6

12. Или более коротко (рис. 7):

```

import Caesar
import read_write_file

def main():
    data = read_write_file.read_data_1byte('f1.txt')
    print('data=', data[0:15])
    txt = ''.join([chr(s) for s in data[0:15]])
    print('text=', txt)

if __name__ == '__main__':
    main()

```

```

data= [72, 101, 32, 119, 97, 115, 32, 97, 32, 98, 117, 114, 108, 121, 32]
text= He was a burly

```

Рисунок 7

13. Теперь зашифруем весь файл. Результат шифрования запишем в файл 'f1\_encrypt.txt' (Рис. 8)

```
import Caesar
import read_write_file

def main():
    data = read_write_file.read_data_1byte('f1.txt')
    print('data=', data[0:15])

    encrypt_data = Caesar.encrypt_data(data, key=67)
    print('encrypt_data=', encrypt_data[0:15])

    txt = ''.join([chr(s) for s in encrypt_data[0:15]])
    print('encrypt_text=', txt)

    read_write_file.write_data_1byte('f1_encrypt.txt', encrypt_data)

if __name__ == '__main__':
    main()

data= [72, 101, 32, 119, 97, 115, 32, 97, 32, 98, 117, 114, 108, 121, 32]
encrypt_data= [139, 168, 99, 186, 164, 182, 99, 164, 99, 165, 184, 181, 175, 188, 99]
encrypt_text= <"c°¤¶cxc¥,µ`¿c

Process finished with exit code 0
```

Рисунок 8 – Шифрование файла «f1.txt»

Содержимое файла 'fl\_encrypt.txt' показано на рис. 9.

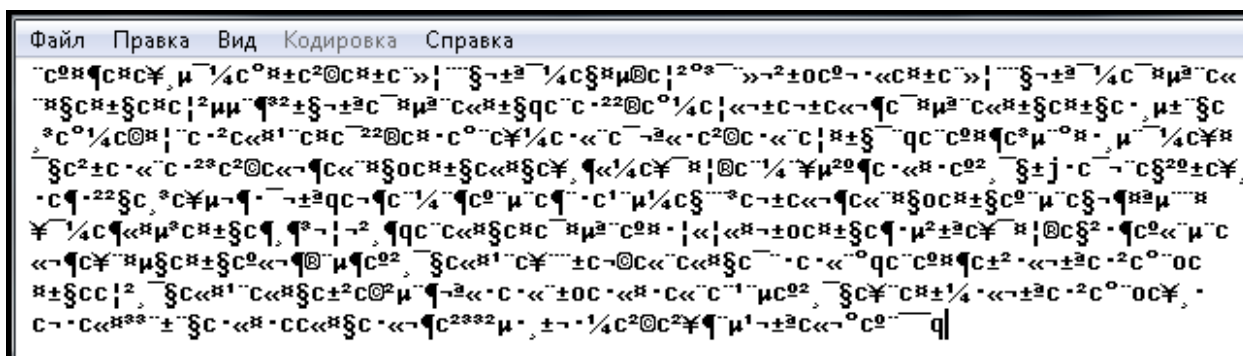


Рисунок 9 – Результат шифрования файла «f1.txt»

14. Теперь откроем зашифрованный файл 'f1\_encrypt.txt', расшифруем его и результат запишем в файл 'f1\_decrypt.txt' (рис. 10):

```

import Caesar
import read_write_file

def main():
    encrypt_data = read_write_file.read_data_1byte('f1_encrypt.txt')
    print('encrypt_data=', encrypt_data[0:15])

    decrypt_data = Caesar.decrypt_data(encrypt_data, key=67)
    print('decrypt_data=', decrypt_data[0:15])

    txt = ''.join([chr(s) for s in decrypt_data[0:15]])
    print('decrypt_data=', txt)

    read_write_file.write_data_1byte('f1_decrypt.txt', decrypt_data)

if __name__ == '__main__':
    main()

```

```

encrypt_data= [139, 168, 99, 186, 164, 182, 99, 164, 99, 165, 184, 181, 175, 188, 99]
decrypt_data= [72, 101, 32, 119, 97, 115, 32, 97, 32, 98, 117, 114, 108, 121, 32]
decrypt_data= He was a burly
Process finished with exit code 0

```

Рисунок 10 – Расшифрование зашифрованного файла

Исходный файл 'f1.txt' и 'f1\_decrypt.txt' совпадают.

## Дешифрование текстового файла, зашифрованного шифром Цезаря

Рассмотрим такую задачу: дан файл 'f1\_encrypt.txt' – зашифрованное шифром Цезаря текстовое сообщение. Ключ неизвестен. Надо дешифровать сообщение из этого файла.

Последовательность действий такая: перебираем все возможные ключи (от 0 до 255), т.е. расшифровываем сообщение на этих ключах, проверяем полученное текстовое сообщение: является оно написанным на английском языке. Если является, то нашли ключ и расшифровали сообщение. Чтобы

определить, что сообщение написано на английском языке используем модуль detectEnglish (рис.11).

На рисунке показан фрагмент программы, в котором выполняется расшифрование файла на очередном ключе k. Полученные данные преобразуются в текст и с помощью функции isEnglish из модуля detectEnglish проверяется является ли полученный текст, написанным на английском языке или нет. В функции isEnglish используется для этой цели словарь английский слов (файл “dictionary.txt”).

```
import Caesar
import read_write_file
import detectEnglish

# расшифровываем
decrypt_data = Caesar.decrypt_data(encrypt_data[0:15], key=k)
# смотрим, что получилось
txt = ''.join([chr(s) for s in decrypt_data])
print('decrypt_data=', txt)
# проверяем, полученный текст - английский или нет
is_english = detectEnglish.isEnglish(txt)
```

Рисунок 11 – В is\_english содержится true, если текст английский, false – в противном случае (Модуль detectEnglish.py вместе со словарем должен располагаться в папке вместе с программой)

## Дешифрование изображения, зашифрованного шифром Цезаря

Дан файл ‘f2.png’. В нем содержится следующее изображение (рис.12):



Рисунок 12

Содержимое этого файла в шестнадцатеричном виде показано на рис. 13.

Файл	Правка	Вид	Кодировка	Справка
00000000:	89	50	4E 47 0D 0A 1A 0A	00 00 00 0D 49 48 44 52   %PNG.....IHDR
00000010:	00	00	00 D5 00 00 00 00 EA	08 06 00 00 00 35 6C 00   ...X...к.....51.
00000020:	FB	00	00 00 01 73 52 47	42 00 AE CE 1C E9 00 00   ы....sRGB.00.й..
00000030:	00	04	67 41 4D 41 00 00	B1 8F 0B FC 61 05 00 00   ..gAMA..±U.ьa...
00000040:	00	09	70 48 59 73 00 00	0E C3 00 00 0E C3 01 C7   ..pHYs...Г...Г.3
00000050:	6F	A8	64 00 00 FF A5 49	44 41 54 78 5E EC BD 05   oËd..яГIDATx^mS.
00000060:	40	55	E9 F6 FF ED AD B9	D3 63 2B DD 48 29 D2 DD   @Uйцян-№Ус+ЭН)ТЭ
00000070:	AD	28	28 62 23 76 81 A2	74 87 20 20 22 20 DD DD   -( (b#vŕŷt# " 33
00000080:	2A	76	B7 63 CD CC 9D EE	B0 BB 03 41 44 9D EF BB   *v·сНМко°»..ADкп»
00000090:	D6	73	38 0E E3 F5 D6 FB	FF DD B9 33 F7 BA 66 96   Ц58.гхЦыяЭ№3чєf-
000000A0:	7B	9F	7D 36 FB EC 78 3E	7B C5 53 7D F0 52 FE 05   {ү}бѡмх>{ES}pRю.
000000B0:	79	0A	FC D8 2D 51 5A FF	91 FE 7D 44 FA 90 F4 41   у.ьШ-QZя`ю>DьђФА
000000C0:	2F	FF	CF DC 0D 0F 07 0F	60 07 4F 50 40 DD 50   /oPz4\$2wŕŷtŷmT.у

Рисунок 13

Видно, что первые два байта изображения имеют значения: 0x89, 0x50 в шестнадцатеричной системе счисления. Нетрудно убедиться, что у всех изображений в формате PNG первые два байта имеют данные значения. Зная эту информацию, можно выполнить дешифрование зашифрованного изображения в формате PNG.

Но прежде, зашифруем изображение (рис. 14):

```

import Caesar
import read_write_file
import detectEnglish

def main():
    data = read_write_file.read_data_1byte('f2.png')
    encrypt_data = Caesar.encrypt_data(data, key=143)
    read_write_file.write_data_1byte('f2_encrypt.png', encrypt_data)

```

Рисунок 14 – Шифрование изображения

Теперь задача: дан файл 'f2\_encrypt.png'. Считаем, что ключ не известен. Дешифровать.

### Задание 1

Дешифровать файл t3\_caesar\_c\_all.txt.

### Задание 2

Дешифровать файл c4\_caesar\_c\_all.bmp. Зашифровать, оставив первые 50 байт без изменения. Сравнить с оригинальным изображением.

### Задание 3

В общем случае ключом в моноалфавитном шифре является таблица замен. Таблицу замен можно сформировать следующим образом

```

k = list(range(256))
print(k)
random.shuffle(k)
print(k)

```

Само шифрование можно реализовать, например, так:

```

cypher_data = []
for m in data:
    c = k[m]
    cypher_data.append(c)

```

В модуле substitution.py реализовать функции шифрования и расшифрования данных. Известна таблица замен:

```
k=[179, 109, 157, 182, 126, 141, 251, 220, 169, 237, 188, 131, 207, 22, 32, 242, 208, 68, 216, 170, 249, 199, 44,
198, 206, 8, 148, 197, 136, 195, 159, 98, 175, 53, 123, 212, 233, 150, 6, 243, 38, 79, 156, 153, 2, 134, 47, 215, 102,
15, 57, 110, 236, 24, 184, 72, 137, 113, 171, 70, 161, 64, 252, 247, 49, 103, 105, 138, 119, 213, 87, 130, 203, 90,
167, 238, 231, 116, 78, 86, 173, 250, 200, 239, 178, 97, 114, 94, 166, 142, 104, 31, 75, 89, 106, 56, 128, 69, 164, 67,
26, 228, 61, 181, 125, 227, 54, 96, 168, 107, 17, 14, 37, 190, 219, 211, 121, 112, 35, 18, 143, 158, 193, 129, 71, 23,
101, 191, 41, 241, 82, 201, 223, 120, 59, 177, 58, 63, 151, 42, 36, 183, 226, 127, 172, 202, 84, 132, 3, 45, 73, 30,
235, 50, 189, 4, 1, 43, 221, 205, 83, 232, 46, 147, 93, 192, 124, 244, 12, 21, 80, 55, 160, 145, 245, 209, 88, 204, 176,
13, 253, 11, 99, 165, 140, 19, 224, 111, 27, 185, 65, 62, 16, 163, 210, 115, 217, 34, 92, 187, 152, 155, 108, 5, 122,
229, 174, 118, 162, 95, 100, 7, 66, 29, 230, 144, 149, 52, 9, 91, 117, 214, 76, 48, 33, 194, 254, 10, 234, 218, 40, 133,
196, 139, 135, 240, 60, 25, 225, 85, 255, 246, 51, 28, 146, 74, 222, 186, 39, 77, 0, 20, 180, 154, 81, 248]
```

Расшифровать файл c3\_subst\_c\_all.png.

Для обратной замены можно по значению в списке определить индекс этого значения. Если есть список:

```
k=[179, 109, 157, 182, 126, 141, 251]
```

то k.index(157) возвратит 2, k.index(182) возвратит 3, k.index(251) возвратит.

## Афинный шифр

Здесь буквы исходного сообщения преобразуются следующим образом:

$$E_i = (AM_i + B) \bmod L \quad (2)$$

где  $A, B$  – целые числа, причем  $A$  и  $L$  взаимно простые (наибольший общий делитель равен 1).

Зашифруем фразу КОРАБЛИ ОТПЛЫВАЮТ ВЕЧЕРОМ, используя афинную систему подстановок при  $A=13$ ,  $B=5$ . Размер алфавита  $L=32$  (будем считать, что в исходном алфавите в качестве буквы Й используется И, а в качестве Ё – Е, и добавим 32-ым символом пробел). В результате преобразований получим:

Сообщение К О Р А Б Л И   О Т П Л Ы В А Ю Т   В Е Ч Е Р О М  
Шифртекст Ы П И Е У З О   Щ П В Ъ З Ш   Е Я В Щ   Ж Г Ж И П Х

В нашем случае алфавит состоит из  $L=256$  элементов, следовательно, надо выбрать  $A$  таким образом, чтобы  $\text{НОД}(A, 256)=1$ .

Алгоритм Евклида поиска наибольшего общего делителя двух чисел приведен на рис.15:

```
EUCLID(a, b)
1.  A ← a; B ← b
2.  if B = 0 return A = gcd(a, b)
3.  R = A mod B
4.  A ← B
5.  B ← R
6.  goto 2
```

Рисунок 15 – Алгоритм Евклида [2]

Пример расчета. Найти  $\text{НОД}(1970, 1066)$ :



1970 = 1 × 1066 + 904	gcd(1066, 904)
1066 = 1 × 904 + 162	gcd(904, 162)
904 = 5 × 162 + 94	gcd(162, 94)
162 = 1 × 94 + 68	gcd(94, 68)
94 = 1 × 68 + 26	gcd(68, 26)
68 = 2 × 26 + 16	gcd(26, 16)
26 = 1 × 16 + 10	gcd(16, 10)
16 = 1 × 10 + 6	gcd(10, 6)
10 = 1 × 6 + 4	gcd(6, 4)
6 = 1 × 4 + 2	gcd(4, 2)
4 = 2 × 2 + 0	gcd(2, 0)

Следовательно, НОД(1970, 1066) = 2.

Ниже приведена функция gcd, которая реализует алгоритм Евклида для определения НОД.

```
def gcd(a, b):
    while a != 0:
        a, b = b % a, a
    return b
```

Обратное преобразование выглядит следующим образом:

$$M_i = (E_i - B) \cdot A^{-1} \bmod L$$

где  $A^{-1}$  - обратное значение по умножению:  $A \cdot A^{-1} \equiv 1 \bmod L$ .

Для поиска обратного значения по умножению применяют расширенный алгоритм Евклида рис.16.

```
EXTENDED EUCLID(m, b)
1. (A1, A2, A3) ← (1, 0, m); (B1, B2, B3) ← (0, 1, b)
2. if B3 = 0 return A3 = gcd(m, b); no inverse
3. if B3 = 1 return B3 = gcd(m, b); B2 = B-1 mod m

4.  $Q = \left\lfloor \frac{A3}{B3} \right\rfloor$ 

5. (T1, T2, T3) ← (A1 - QB1, A2 - QB2, A3 - QB3)
6. (A1, A2, A3) ← (B1, B2, B3)
7. (B1, B2, B3) ← (T1, T2, T3)
8. goto 2
```

Рисунок 16 – Расширенный алгоритм Евклида [2]

## Реализация в Python:

```
def findModInverse(a, m):  
    # Returns the modular inverse of a % m, which is  
    # the number x such that a*x % m = 1  
    if gcd(a, m) != 1:  
        return None # no mod inverse if a & m aren't relatively prime  
    # Calculate using the Extended Euclidean Algorithm:  
    u1, u2, u3 = 1, 0, a  
    v1, v2, v3 = 0, 1, m  
    while v3 != 0:  
        q = u3 // v3 # // is the integer division operator  
        v1, v2, v3, u1, u2, u3 = (u1 - q * v1), (u2 - q * v2), (u3 - q * v3), v1, v2, v3  
    return u1 % m
```

### Задание 4

В таблице показана пошаговая реализация алгоритма, приведенного на рис.16, для поиска обратного значения по умножению для 550 по mod 1759.

Q	A1	A2	A3	B1	B2	B3
	1	0	1759	0	1	550
3	0	1	550	1	3	109
5	1	3	109	5	16	5
21	5	16	5	106	339	4
1	106	339	4	111	355	1

Проверить полученный результат с помощью функции findModInverse.

### Задание 5

Расшифровать файл ff2\_affine\_c\_all.bmp. Шифр аффинный.  $a=167$   $b=35$ . Зашифровать, оставив первые 50 байт без изменения. Сравнить с оригинальным изображением.

### Задание 6

Дешифровать файл `text10_affine_c_all.txt`. Шифр аффинный. Подсчитать сколько перебрали вариантов ключей.

### Задание 7

Дешифровать файл `b4_affine_c_all.png`. Шифр аффинный. Подсчитать сколько перебрали вариантов ключей.

## Дешифрование - частотный анализ

Все естественные языки имеют характерное частотное распределение символов. Например, буква “О” \_ встречается в русском языке чаще других, а буква “Ф” – самая редкая (табл. 3).

Моноалфавитные подстановки обладают важным свойством: они не нарушают частот появления символов, характерных для данного языка. Это позволяет криптоаналитику легко получить открытый текст при помощи частотного анализа. Для этого нужно сопоставить частоты появления символов шифра с вероятностями появления букв используемого алфавита (в данном случае русского). После этого наиболее частые символы криптограммы заменяются на наиболее вероятные символы алфавита, остальные замены производятся на основе вероятных слов и знания синтаксических правил используемого языка.

Таблица 3. Вероятности встречаемости букв русского языка

Символ	вер_ть	символ	вер_ть	символ	вер_ть
Пробел	0.175	К	0.028	Ч	0.012
О	0.089	М	0.026	Й	0.010
Е	0.072	Д	0.025	Х	0.009
А	0.062	П	0.023	Ж	0.007
И	0.062	У	0.021	Ю	0.006
Н	0.053	Я	0.018	Ш	0.006
Т	0.053	Ы	0.016	Ц	0.004
С	0.045	З	0.016	Щ	0.003
Р	0.040	Ь	0.014	Э	0.003
В	0.038	Б	0.014	Ф	0.002
Л	0.035	Г	0.013		

## Задание 8

Используя частотный анализ, дешифровать криптограмму, зашифрованную методом моноалфавитных подстановок.

В табл.4 находятся результаты статистического анализа данной криптограммы. Сюда включены значения частот букв русского языка, а также частоты встречаемости символов для данной криптограммы.

Таблица 4. Статистика

Криптограмма		Русский язык	
Символ	Частота	Буква	Вероятность
А	0.121	Пробел	0.175
Щ	0.111	о	0.090
С	0.101	е	0.072
Й	0.091	а	0.062
Н	0.081	и	0.062
Ш	0.081	н	0.053
Т	0.071	т	0.053
Б	0.051	с	0.045
Р	0.040	р	0.040
Д	0.040	в	0.038
Ж	0.040	л	0.035
и т.д.		и т.д.	

Текст криптограммы:

КЩРНСЙШЩХДТАРБУТЦПФЮСНЫАШЙАЬЙЛБАНСЙСТНСТОБ  
НДЩМЩАЙШЙЖТЛЙАСЬДНСЙАШЩАСЩЖЕДЩАБНЖТАЩШАРЩН  
СЙСЩОЩЩАРЖТШШИГ

## Полиалфавитные подстановки

В случае моноалфавитных подстановок используется только один алфавит шифрования. Существуют шифры, где используется целый набор алфавитов шифрования. Такие шифры называются полиалфавитными и позволяют, в отличие от моноалфавитных подстановок, скрыть естественную частоту появления символов в тексте.

Простая полиалфавитная подстановка (или шифр Вижинера) последовательно и циклически меняет используемые алфавиты шифрования. Число используемых алфавитов называется периодом шифра. Для шифрования используется ключ - слово или бессмысленный набор символов нормативного алфавита. Каждая буква ключа определяет свой алфавит шифрования, который получается из нормативного циклическим сдвигом на количество символов, равное числовому эквиваленту буквы ключа (табл. 5). Очевидно, что длина ключа равна периоду шифра.

Таблица 5

Ключ	<u>А</u>	<u>Б</u>	<u>В</u>	<u>Г</u>	<u>Д</u>	...	<u>Э</u>	<u>Ю</u>	<u>Я</u>
0	А	Б	В	Г	Д	...	Э	Ю	Я
1	Б	В	Г	Д	Е	...	Ю	Я	А
2	В	Г	Д	Е	Ж	...	Я	А	Б
3	Г	Д	Е	Ж	З	...	А	Б	В
...	...	...	...	...	...	...	...	...	...
30	Ю	Я	А	Б	В	...	Ы	Ь	Э
31	Я	А	Б	В	Г	...	Ь	Э	Ю

Чтобы зашифровать сообщение шифром Вижинера, поступают следующим образом. Под каждой буквой открытого текста помещается буква ключа. Ключ циклически повторяется необходимое число раз. Чтобы вычислить числовой эквивалент буквы шифртекста, числовой эквивалент буквы ключа складывается по модулю  $L$  с числовым эквивалентом буквы открытого текста, где  $L$  - мощность нормативного алфавита. Т.е. шифр Вижинера описывается следующим выражением:

$$E_i = (M_i + K_{i \bmod U}) \bmod L \quad (3)$$

где

- $E_i, M_i$       числовые эквиваленты символов криптограммы и открытого текста соответственно,  
 $K_{i \bmod U}$     - числовой эквивалент буквы ключа,  
 $L$                 - мощность нормативного алфавита.  
 $U$                 - длина ключа или период шифра

Буквы ключа определяют величину смещения символов криптограммы относительно символов открытого текста.

Зашифруем, например, текст “полиалфавитная\_подстановка” с ключом “краб”. Будем использовать алфавит, приведенный в таблице 6. Процесс шифрования приведен в таблице 7.

Таблица 6

Нормативный Алфавит	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
Числовые Эквиваленты	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Таблица 6 (продолжение)

Нормативный Алфавит	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ы	Ь	Э	Ю	Я	“ _ ”
Числовые Эквиваленты	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Таблица 7

П	15	К	10	$(15 + 10) \bmod 32$	25	Щ
О	14	Р	16	$(14 + 16) \bmod 32$	30	Я
Л	11	А	0	$(11 + 0) \bmod 32$	11	Л
И	8	Б	1	$(8 + 1) \bmod 32$	9	Й
А	0	К	10	$(0 + 10) \bmod 32$	10	К
Л	11	Р	16	$(11 + 16) \bmod 32$	27	Ь
Ф	20	А	0	$(20 + 0) \bmod 32$	20	Ф
А	0	Б	1	$(0 + 1) \bmod 32$	1	Б
В	2	К	10	$(2 + 10) \bmod 32$	12	М
И	8	Р	16	$(8 + 16) \bmod 32$	24	Ш
Т	18	А	0	$(18 + 0) \bmod 32$	18	Т
Н	13	Б	1	$(13 + 1) \bmod 32$	14	О
А	0	К	10	$(0 + 10) \bmod 32$	10	К
Я	30	Р	16	$(30 + 16) \bmod 32$	14	О
_	31	А	0	$(31 + 0) \bmod 32$	31	_
П	15	Б	1	$(15 + 1) \bmod 32$	16	Р
О	14	К	10	$(14 + 10) \bmod 32$	24	Ш
Д	4	Р	16	$(4 + 16) \bmod 32$	20	Ф
С	17	А	0	$(17 + 0) \bmod 32$	17	С

Т	18	Б	1	$(18 + 1) \bmod 32$	19	У
А	0	К	10	$(0 + 10) \bmod 32$	10	К
Н	13	Р	16	$(13 + 16) \bmod 32$	29	Ю
О	14	А	0	$(14 + 0) \bmod 32$	14	О
В	2	Б	1	$(2 + 1) \bmod 32$	3	Г
К	10	К	10	$(10 + 10) \bmod 32$	20	Ф
А	0	Р	16	$(0 + 16) \bmod 32$	16	Р

В результате получилась криптограмма: “ЩЯЛЙКЬФБМШТОКО\_РШФСУКЮОГФР”.

### Задание 8

Расшифровать файл im6\_vigenere\_c\_all.bmp. Шифр Виженера. Ключ: magistr. Зашифровать, оставив первые 50 байт без изменения. Сравнить с оригинальным изображением.

Преобразовать ключ в численное значение:

```
key = 'magistr'
k = [ord(s) for s in key]
```

### Дешифрование - метод вероятных слов

Метод вероятных слов основан на том, что чаще всего заранее известна область применения криптограммы, а, значит, и слова, которые могут встретиться в тексте. Например, если известно, что в криптограмме зашифрован финансовый отчет, вероятно, в тексте встречаются слова “дебет”, “кредит”, “баланс” и т.п.

Т.к. в полиалфавитных подстановках криптограмма является суммой открытого текста и ключа по модулю L, то, чтобы проверить наличие вероятного слова в тексте, необходимо вычесть его из криптограммы по



модулю  $L$  во всех возможных позициях, где  $L$  - мощность исходного алфавита.

Если данное вероятное слово присутствует в тексте и вычитается в правильной позиции, то результатом такого вычитания будет ключ шифрования или его часть. Если слово испытывается в неправильной позиции, то результатом вычитания будет бессмысленный набор букв. Понятно, что, если этого слова нет в тексте, все позиции будут неправильными.

Полученная в результате вычитания хотя бы часть осмысленного слова - показатель успеха. Далее надо попытаться расширить открытый текст или ключ в этом направлении.

Конечно, будут возникать и “ложные тревоги”, особенно в случае коротких вероятных слов, но эти варианты будут легко отбрасываться в процессе продвижения анализа, т.к. они не дадут разумных расширений.

## Задание 9

Дешифровать `text4_vigener_c.txt` – зашифрованное шифром Вижинера текстовое сообщение. Известно, что сообщение начинается со строки из одних пробелов.

## Задание 10

Дешифровать этот же файл (`text4_vigener_c.txt`) – зашифрованное шифром Вижинера текстовое сообщение. Известно, что в сообщении присутствует слово `housewives`.

Надо взять первые `len(housewives)` значений зашифрованных данных. Вычесть из них численные значения `housewives`. Полученные 10 значений представить в виде текста и напечатать. Взять `len(housewives)` значений зашифрованных данных, но уже не с самого начала, а выполнить сдвиг на

```

+% 0 0 0+/"
, &000)0*000
-000/0+000
000!.0,0 0
000 /000)!
00/
,$0"00%0,!
+% 0 0 0+/"
, &000)0*000
-000/0+000
000!.0,0 0
000 /000)!
00/
,$0"00%000
+% 0 0 0+
0N
, &000)000\`
-000/ 0Kn`
000!00X|nb
0Jj|p!
&000\j_/w
,0 Nn\l0.b
00L`n^+tpn
0R^`p0 _|\
Yd^b/slkje
kd`!..^xYs0
kf0wpjfb)b
m%ub|Xo0pt

```

## Задание 11

Дешифровать файл (text1\_vigener\_c.txt) – зашифрованное шифром Вижинера текстовое сообщение. Известно, что в сообщении присутствуют слова it therefore.

## Шифры перестановки

Шифры замены относятся к т.н. поточным шифрам. В поточных шифрах шифрование происходит посимвольно. Если уподобить поточные шифры - а, вернее, шифраторы - черному ящику и подавать на вход поток символов открытого текста, то на выходе практически без задержек будут появляться соответствующие им символы криптограммы.

Кроме поточных, существуют еще блочные шифры. При использовании блочных шифров текст предварительно разбивается на блоки и шифрование происходит поблочно.

Перестановки относятся к блочным шифрам. Текст делится на блоки по  $N$  символов, и в каждом блоке символы переставляются в соответствии с некоторым правилом (ключом). Таким образом ключ задает порядок символов в блоке.

Кроме того, известны т.н. табличные перестановки. Например, исходный текст вписывают в таблицу по столбцам, а затем строки таблицы переставляются в соответствии с ключом. Размер таблицы оговаривается заранее.

### 1. Использование подстановки

Существует два способа использования ключа.

Пусть

$$\text{Ключ } K = k_1 k_2 \dots k_i \dots k_N$$

$$\text{Текст } M = m_1 m_2 \dots m_i \dots m_N$$

$$k_i - \text{целое число} : k_i \in [1, N].$$

#### Способ 1

Чтобы зашифровать  $M$ , нужно  $i$ -ый символ текста поставить на  $k_i$ -ое место. При расшифровке на  $i$ -ое место ставим  $k_i$ -ый символ криптограммы.

$N = 5$ ; Ключ 3-1-5-4-2

Исходный Текст : ИНФОР | МАЦИЯ

Криптограмма : НРИОФ | АЯМИЦ

### Способ 2

При шифровке на  $i$ -ое место ставим  $k_i$ -ый символ текста. При расшифровке  $i$ -ый символ криптограммы ставится на  $k_i$ -ое место.

$N = 5$ ; Ключ 3-1-5-4-2

Исходный Текст : ИНФОР | МАЦИЯ

Криптограмма : ФИРОН | ЦМЯИА

Такая таблица называется подстановкой степени  $n$ .

Зная подстановку, задающую преобразование, можно осуществить как зашифрование, так и расшифрование текста.

### Задание 12

Дешифровать `text2_permutation_c.txt` – зашифрованное шифром перестановки текстовое сообщение. Известно, что длина перестановки 6. Правило перестановки: на  $i$ -ю позицию ставится  $p(i)$  символ, где  $p$  – перестановка.

## Литература

- [1] Al Sweigart. Hacking Secret Ciphers with Python
- [2] Stallings W, “Cryptography And Network Security. Principles And Practice”, 5<sup>th</sup> Edition, 2011.