Отчёт по лабораторной работе 2

Ильин Никита Евгеньевич

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Цель данной работы - научиться программировать шифры перестановки, такие как: маршрутное шифрование, шифрование с помощью решеток и таблица Виженера.

2 Задание

1. Реализовать представленные в задании шифры.

3 Теоретическое введение

Шифры перестановки преобразуют открытый текст в криптограмму путем перестановки его символов. Способ, каким при шифровании переставляются буквы открытого текста, и является ключом шифра. Важным требованием является равенство длин ключа и исходного текста. Существует два широко распространенных метода перестановок: 1. Маршрутное шифрование. Данный способ шифрования разработал французский математик Франсуа Виет. Открытый текст записывают в некоторую геометрическую фигуру (обычно прямоугольник) по некоторому пути, а затем, выписывая символы по другому пути, получают шифртекст. Пусть т и п - целые положительные числа, большие 1. Открытый текст разбивается на блоки равной длины, состоящие из числа символов, равному произведению тп. Если последний блок получится меньше остальных, то в него следует дописать требуемое количество произвольных символов. Составляется таблица размерности тп. Блоки вписывается построчно в таблицу. КриптограммаК получается выписыванием букв из таблицы в соответствии с некоторым маршрутом. Ключом такой криптограммы является маршрут и числа т и п. Обычно буквы выписывают по столбцам, которые упорядочивают согласно паролю: внизу таблицы приписывается слово из n неповторяющихся букв и столбцы нумеруются по алфавитному порядку букв пароля. Например, для шифрования текста нельзя недооценивать противника, разобьем его на блоки длины n = 6. Блоков получится т = 5. К последнему блоку припишем букву а. В качестве пароля выберем слово пароль. Теперь будем выписывать буквы по столбцам в соответствии с алфавитным порядком букв пароля и получим следующую криптограмму:

ЕЕНПНЗОАТАБОВОКННЕЬВЯЦТИА. 8

•аратовсь ствен нельзя недооц ени ват вникаа парол в Рассмотренный способ шифрования (столбцовая перестановка) в годы первой мировой войны использовала легендарная немецкая шпионка Мата Хари. 2. Шифрование спомощью решеток. о l Данный способ шифрования предложил австрийский криптограф Эдуард Флейснер в 181 году. Суть этого способа заключается в следующем. Выбирается натуральное число k > ,1 строится квадрат размерности k и построчно заполняется числами 1,2,..., k?. В качестве примера рассмотри квадрат размерности k = .2 R2 4 Повернем его по часовой стрелке на 90° и присоединим к исходному квадрату справа. 1123 1 34 42 Проделаем еще дважды такую процедуру и припишем получившиеся квадраты снизу. Получился большой квадрат размерности 2k. 1 1 32 23 1321 Далее из большого квадрата вырезаются клетки, содержащие числа от 1 до k7. В каждой клетке должно быть только одно число. Получается своего рода решето. Шифрование осуществляется следующим образом. Решето накладывается на чистый квадрат 2k × 2k и в прорези вписываются буквы 9

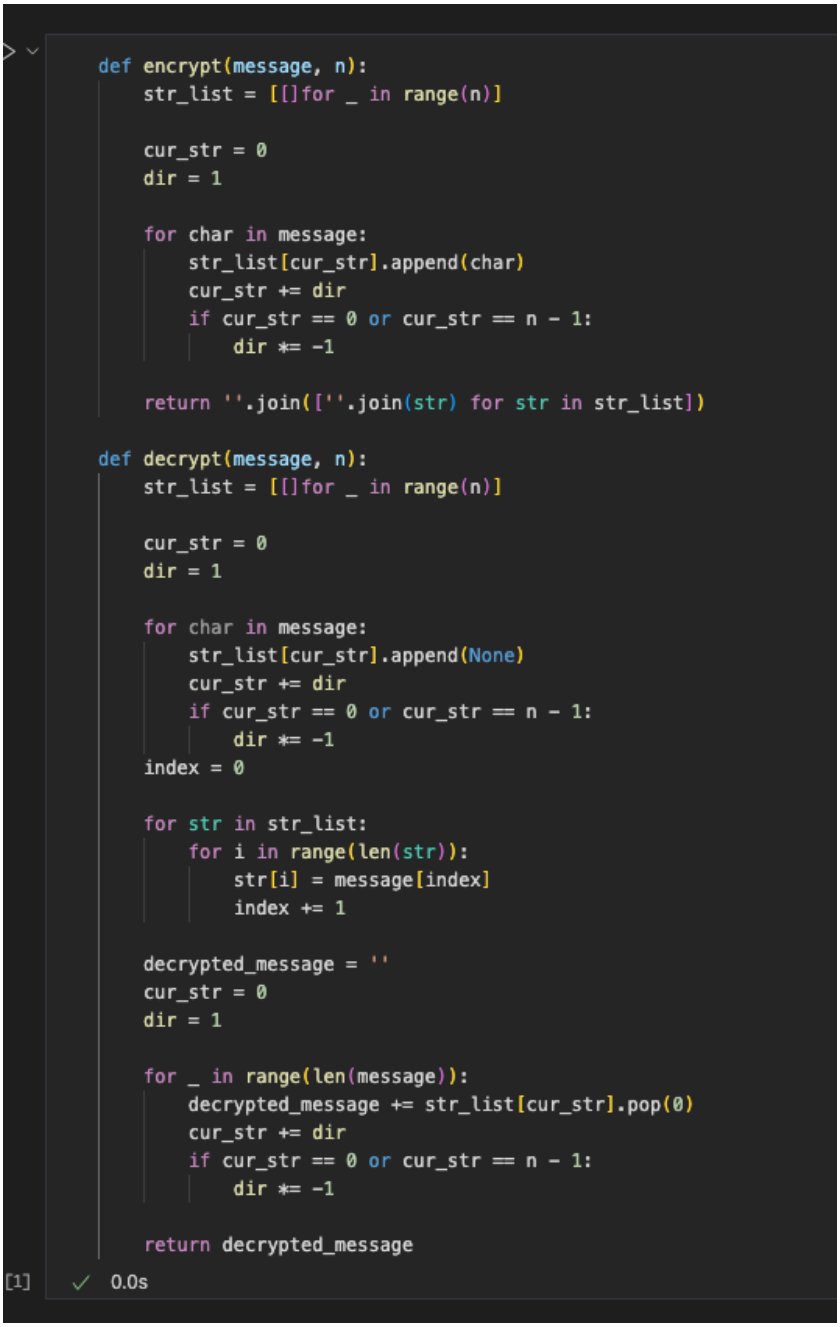
исходного текста по порядку их следования. Когда заполнятся все прорези, решето поворачивается на 90° и вписывание букв продолжается. После третьего поворота все клетки большого квадрата окажутся заполненными. Подобрав подходящий пароль (число букв пароля должно равняться k? и они не должны повторяться), выпишем буквы по столбцам. Очередность столбцов определяется алфавитным порядком букв пароля. Пример. Исходный текст - договор подписали; пароль шифр. С применением вышеуказанной решетки за пять шагов получаем следующую криптограмму. ддад а и ии ” ФР Получившаяся криптограмма: ОВОРДЛГПАПИОСДОИ. Важно отметить, что число k подбирается в соответствии с количеством букв N исходного теста. В идеальном случае k? = N. Если такого равенства достичь невозможно, от можно либо дописать произвольную букву к последнему слову открытого текста, либо убрать е. 3. Таблица Виженера. В 1585 году французский криптограф Блез Виженер опубликовал свой метод шифрования в «Трактате о шифрах». Шифр считался нераскрываемым од 1863 года, когда

австриец Фридрих Казиски взломал его. Открытый текст разбивается на блоки длины п. Ключ представляет собой последовательность из п натуральных чисел: ал,а2, …, ап. Далее в каждом блоке первая буква циклически сдвигается вправо по алфавиту на а, позиций, вторая буква - на аз позиций, последняя - на а, позиций. Для лучшего запоминания в качестве ключа можно взять осмысленное слово, а алфавитные номера входящих в него букв использовать для осуществления сдвигов. Рассмотрим еще одну 10

схему построения шифра Виженера. В нижеприведенной таблице в строчках записаны буквы русского алфавита. При переходе от одной строке к другой происходит циклический сдвиг на одну позицию. Исходный текст: криптография серьезная наука; пароль - математика. Пароль записывается с повторениями над буквами сообщения. ма ик ематикамат ма иафиЯе3НЯНа ГЕХК3 П Ф ⊠bЫ]Я Б 30 ⊠Щ10 Д Е ЕЖ Н М ⊠ 29 ШЩ I Вгоризонтальном алфавите находим букву «к», а в вертикальном - букву «м». На пересечении столбца истроки втаблице расположена буква «ц». Далее переходим кбуквам «р» и«а» соответственно. Витоге получается следующая криптограмма: ЦРЬФЯОХШКФФЯДКЭЬЧПЧАЛНТШЦА. Задания к лабораторной работе Реализовать все рассмотренные шифры программно. 1 ⊠ ⊠E⊠31⁄41⁄4KJMHonPCTyexug⊠⊠bh3l R ^-“-FeXmHHKAMHo=Pc- ox = 1 0 ⊠A E B ⊠A E Z 3 H H K J MH O T P C T y ⊠x ⊠⊠⊠ ⊠ ⊠A E B ⊠A E Z 3 H H K J MH O E P C T y e X I T ⊠⊠ 6⊠21 AEBTHEW3HIKIMHOnPCTyexu y ⊠X⊠⊠5531⊠AEB⊠AEZ3⊠MKJMHOnPCT 2OXTy⊠2⊠⊠ AEBTAE*3HiKJMHOTP P C T Y ⊠X 4 5 5 3 1 ⊠A E B ⊠A E ⊠3 M H K J M H O I ⊠⊠ b N 9 0 % A E B ⊠ A E Z 3 W H K J M H O Ty x ⊠bb3108ABBTAEZ3HHKJMH C TyeX ⊠⊠55319A5BDAEZ3⊠⊠NJM 5 5 3 1 0 ⊠ A B B ⊠ AE ⊠ 3 H M K ⊠ b UI 9 1 9 A B B T ⊠ E X 3 H M K 3HMKH 6551O8AEBT AEZ 3⊠ ⊠⊠⊠⊠10 AbB ⊠E⊠ 293=⊠ iaeaeduxuxouo4nECwHmM: H X o K i o d uO HW U M M ue X a x -Z=AMMW⊠* hnXexHad O HN I M M M ×= =2: JagYt acmr; EIX⊠KLOAUOHN HdGSVBOCl9. nhxexiadI m Xe KIad M n x e K ao d UMMHW Au ^- EE

4 Выполнение лабораторной работы

1. Для начала реализуется алгоритм маршрутного шифрования на языке Python (рис. 4.1).



```python
def encrypt(message, n):
    str_list = [[]for _ in range(n)]

    cur_str = 0
    dir = 1

    for char in message:
        str_list[cur_str].append(char)
        cur_str += dir
        if cur_str == 0 or cur_str == n - 1:
            dir *= -1

    return ''.join([''.join(str) for str in str_list])

def decrypt(message, n):
    str_list = [[]for _ in range(n)]

    cur_str = 0
    dir = 1

    for char in message:
        str_list[cur_str].append(None)
        cur_str += dir
        if cur_str == 0 or cur_str == n - 1:
            dir *= -1
    index = 0

    for str in str_list:
        for i in range(len(str)):
            str[i] = message[index]
            index += 1

    decrypted_message = ''
    cur_str = 0
    dir = 1

    for _ in range(len(message)):
        decrypted_message += str_list[cur_str].pop(0)
        cur_str += dir
        if cur_str == 0 or cur_str == n - 1:
            dir *= -1

    return decrypted_message
```

```
[1]  ✓  0.0s
```

Рис. 4.1: Программная реализация маршрутного шифровани

2. Зашифрованное сообщение выглядит следующим образом (рис. 4.2).

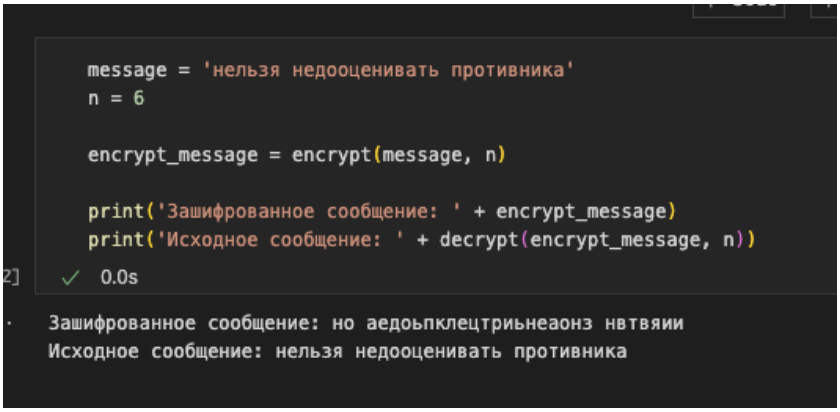
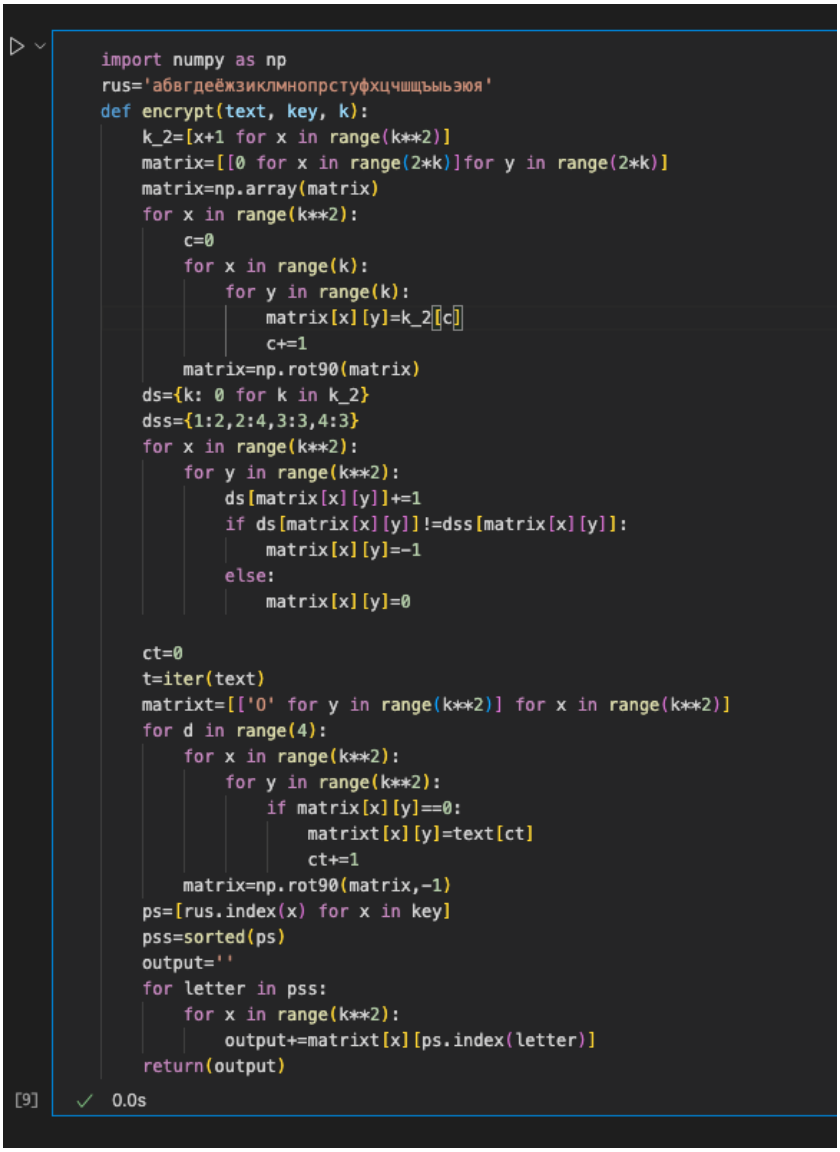


Рис. 4.2: Результат работы программы

3. Затем реализуется алгоритм шифрования с помощью решеток на языке Python (рис. 4.3).



```python
import numpy as np
rus='абвгдеёжзиклмнопрстуфхцчшщъыьэюя'
def encrypt(text, key, k):
    k_2=[x+1 for x in range(k**2)]
    matrix=[[0 for x in range(2*k)]for y in range(2*k)]
    matrix=np.array(matrix)
    for x in range(k**2):
        c=0
        for x in range(k):
            for y in range(k):
                matrix[x][y]=k_2[c]
                c+=1
        matrix=np.rot90(matrix)
    ds={k: 0 for k in k_2}
    dss={1:2,2:4,3:3,4:3}
    for x in range(k**2):
        for y in range(k**2):
            ds[matrix[x][y]]+=1
            if ds[matrix[x][y]]!=dss[matrix[x][y]]:
                matrix[x][y]=-1
            else:
                matrix[x][y]=0

    ct=0
    t=iter(text)
    matrixt=[['O' for y in range(k**2)] for x in range(k**2)]
    for d in range(4):
        for x in range(k**2):
            for y in range(k**2):
                if matrix[x][y]==0:
                    matrixt[x][y]=text[ct]
                    ct+=1
        matrix=np.rot90(matrix,-1)
    ps=[rus.index(x) for x in key]
    pss=sorted(ps)
    output=''
    for letter in pss:
        for x in range(k**2):
            output+=matrixt[x][ps.index(letter)]
    return(output)
```

[9] ✓ 0.0s

Рис. 4.3: Программная реализация шифрования с помощью решеток

4. Зашифрованное сообщение выглядит следующим образом (рис. 4.4).

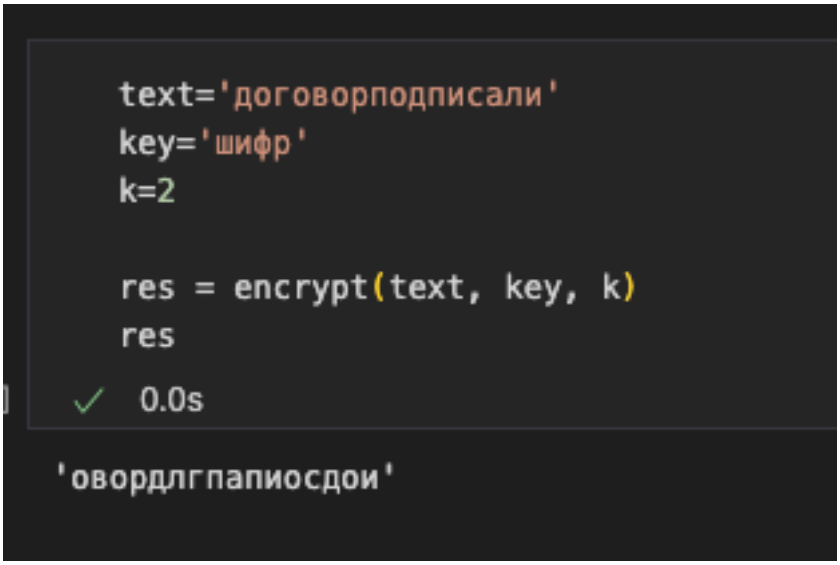


Рис. 4.4: Результат работы программы

5. Затем реализуется алгоритм таблицы Виженера на языке Python (рис. 4.5).

Рис. 4.5: Программная реализация таблицы Виженера

6. Зашифрованное сообщение выглядит следующим образом (рис. 4.6).

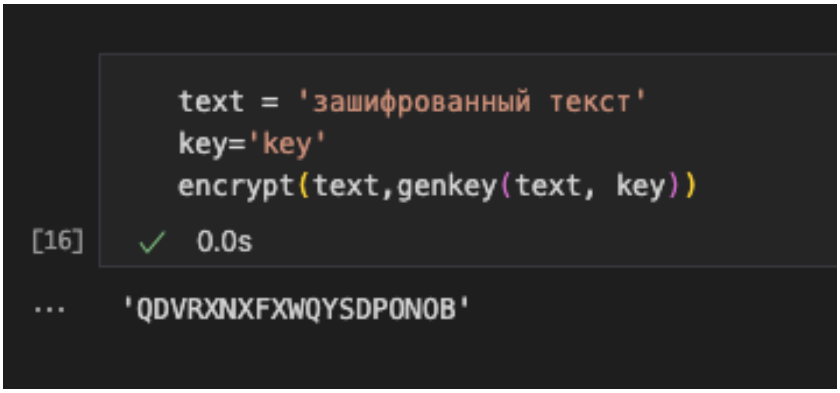


Рис. 4.6: Результат работы программы

5 Выводы

В ходе работы были реализованы алгоритмы шифрования . Реализацция алгоритмов была произведена на языке програмирования Python.