# Информационная безопасность. Отчет по лабораторной работе № 2

**Шифры перестановки**

Мухамеджанов Исматулло Иззатуллоевич

# Содержание

# List of Figures

# List of Tables

# 1 Цель работы

Освоить на практике применение шифрование перестановкой [1].

# 2 Указание к работе

Исходные данные. Маршрутное шифрование Шифрование с помощью решёток Таблица Виженера # Выполнение лабораторной работы 1. Маршрутное шифрование.

Данный способ шифрования разработал французский математик Франсуа Виет. Открытый текст записывают в некоторую геометрическую фигуру (обмчно прямоугольник) по некоторому пути, а затем, выписывая символы по другому пути, получают шифртекст. Пусть m и п — целые положительные числа, большие Открытый текст разбивается на блоки равной длины, состоящие из яисла символов, равному произведению ти. Если последний блок получится меньше остальных, то в него следует дописать требуемое количество произвольных символов. Составляется таблиqа размерности ти. Блоки вписывается построчно в таблицу. Криптограмма получается выписыванием букв из таблицы в соответствии с некоторым маршрутом. Ключом такой криптограммы является маршрут и числа m и п. Обычно буквьl выписывают по столбцам, которые упорядочивают согласно паролю: внизу таблицы приписывается слово из п неповторяющихся букв и столбцы нумеруются по алфавитному порядку букв пароля.

Рассмотренный способ шифрования (столбцовая перестановка) в годы первой мировой войны использовала легендарная немецкая шпионка Мата Хари.

2. Шифрование с помощью решеток.

Данный способ шифрования предложил австрийский криптограф Эдуард Флейснер в ISS1 году. Суть этого способа заключается в следующем. Выбирается

натуральное число k > 1, строится квадрат размерности k и построено заполняется числами 1, 2,..., k2. В качестве примера рассмотри квадрат размерности k —— 2.

Повернем его по часовой стрелке на 900 и присоединим к исходному квадрату справа.Проделаем еще дважды такую процедуру и припишем получившиеся квадраты снизу. Получился большой квадрат размерности 2k.

Далее из большого квадрата вырезаются клетки, содержащие числа от 1 до k2. В каждой клетке должно быть только одно число. Получается своего FOdil решето. Шифрование осуществляется следующим образом. Решето накладывается на чистый квадрат 2k X 2k и в прорези вписываются буквы

исходного текста по порядку их следования. Когда заполнятся все прорези, решето поворачивается на 900 и вписывание букв продолжается. После третьего поворота все клетки большого квадрата окажутся заполненными. Подобрав подходящий пароль (число букв пароля должно равняться k2 и они не должны повторяться), выпишем буквы по столбцам. Очередность столбцов определяется алфавитным порядком букв пароля.

3. Шифрование с помощью решеток. В 1585 году французский криптограф Блез Виженер опубликовал свой метод шифрования в «Трактате о шифрах». Шифр считался нераскрываемым до 1863 года, когда австриец Фридрих Казиски взломал его. Открытый текст разбивается на блоки длины п. Ключ представляет собой Следовательность из п натуральных чисел: m, n2, ... , . Дал е в каждом блоке первая буква циклически сдвигается вправо по алфавиту на •1 позиций, вторая букIЗа — на m позиций, последняя — на ntt позицFfй. Для лучшего запоминания в качестве ключа можно взять осмысленное слово, а алфавитные номера входящих в него букв использовать для осуществления сдвигов.

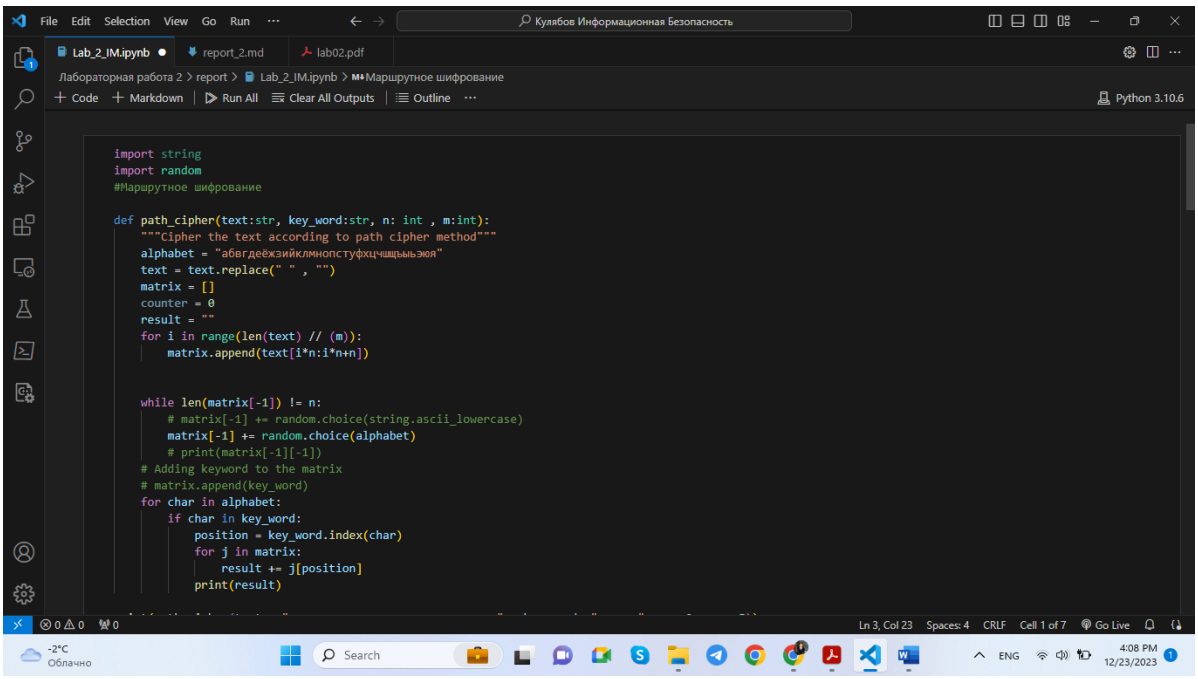


Figure 2.1: Программа (1)

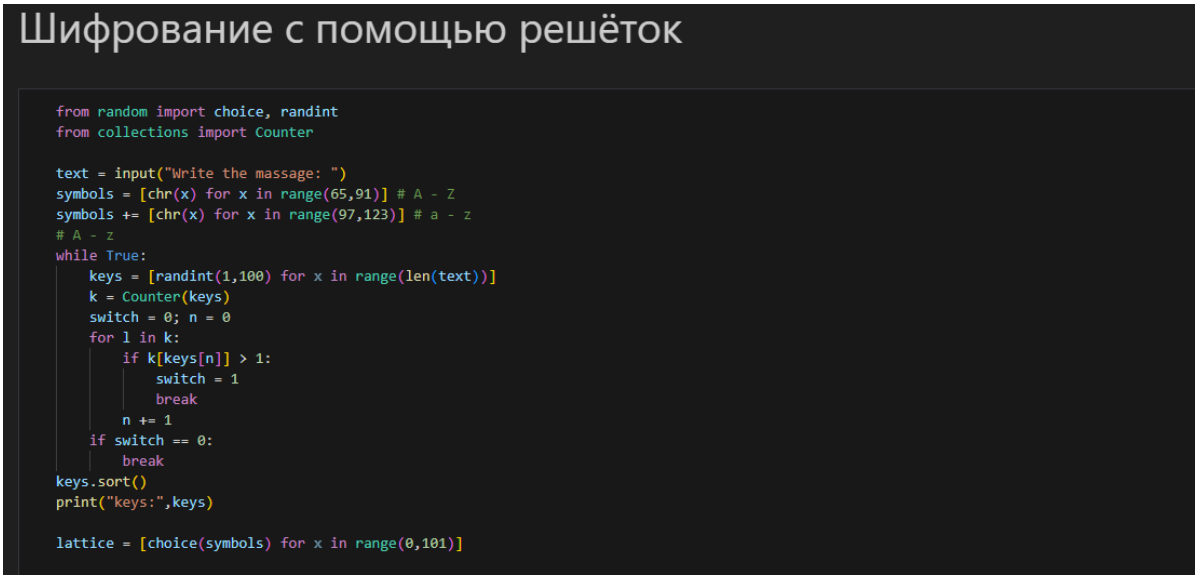


Figure 2.2: Программа (2)

```
lattice = [choice(symbols) for x in range(0,101)]

n = 0
for i in range(len(lattice)):
    if n < len(text):
        if i == keys[n]:
            lattice[i] = text[n]
            n += 1
print()

for j in range(0,11):
    if j == 0:
        print(" ", end = "    ")
    else:
        print(j, end = "   ")
print()

n = 0
for j in range(1,len(lattice)):
    if j == 1:
        print(n, end = "  | "); n += 1
        print(lattice[j], end = " | ")
    elif j % 10 != 0:
        print(lattice[j], end = " | ")
    else:
        print(lattice[j], end = " | ")
        print()
        if n < 10:
            print(n, end = "  | "); n += 1
print()
```

Figure 2.3: Программа (3)

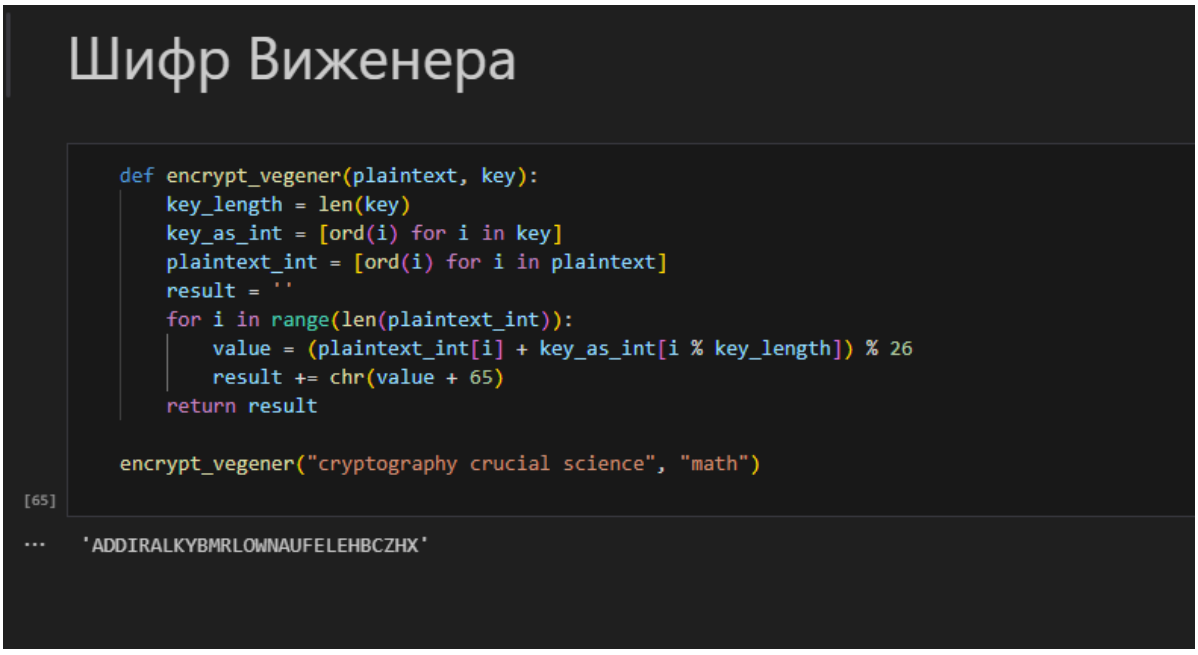


Figure 2.4: Программа (4)

# 3 Выводы

Освоены шифры методом перестановки

# 4 Список литературы

1. Методические материалы курса