Шифры перестановки

Гаглоев Олег Мелорович

29 сентября, 2024, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Изучение алгоритмов маршрутной перестановки, решеток и Виженера

Выполнение лабораторной работы

Шифр маршрутной перестановки

Данный шифр относится к классу шифров перестановки и характеризуется простотой выполнения операций шифрования/расшифрования. Один из наиболее распространенных способов шифрования/расшифрования задается некоторым прямоугольником (таблицей) и соответствующим правилом его заполнения. Например, открытый текст записывается в таблицу по строкам, а шифртекст получается в результате выписывания столбцов соответствующей таблицы, или наоборот.

Шифр Кардано

Решетка Кардано — это ключ к секретному посланию, как правило, специальная карточка, в которой в определенных местах имеются прорези — ячейки. Чтение зашифрованного послания происходит при наложении на кодированный текст. Данный метод придуман в 16 веке итальянским математиком Джероламо Кардано.

Шифр Виженера

Шифр Виженера — это метод шифровки, в котором используются различные «шифры Цезаря» на основе букв в ключевом слове. В шифре Цезаря каждую букву абзаца необходимо поменять местами с определенным количеством букв, чтобы заменить исходную букву. Например, в латинском алфавите A становится D, B становится E, C становится F. Шифр Виженера построен на методе использования различных шифров Цезаря в различных частях сообщения.

Контрольный пример

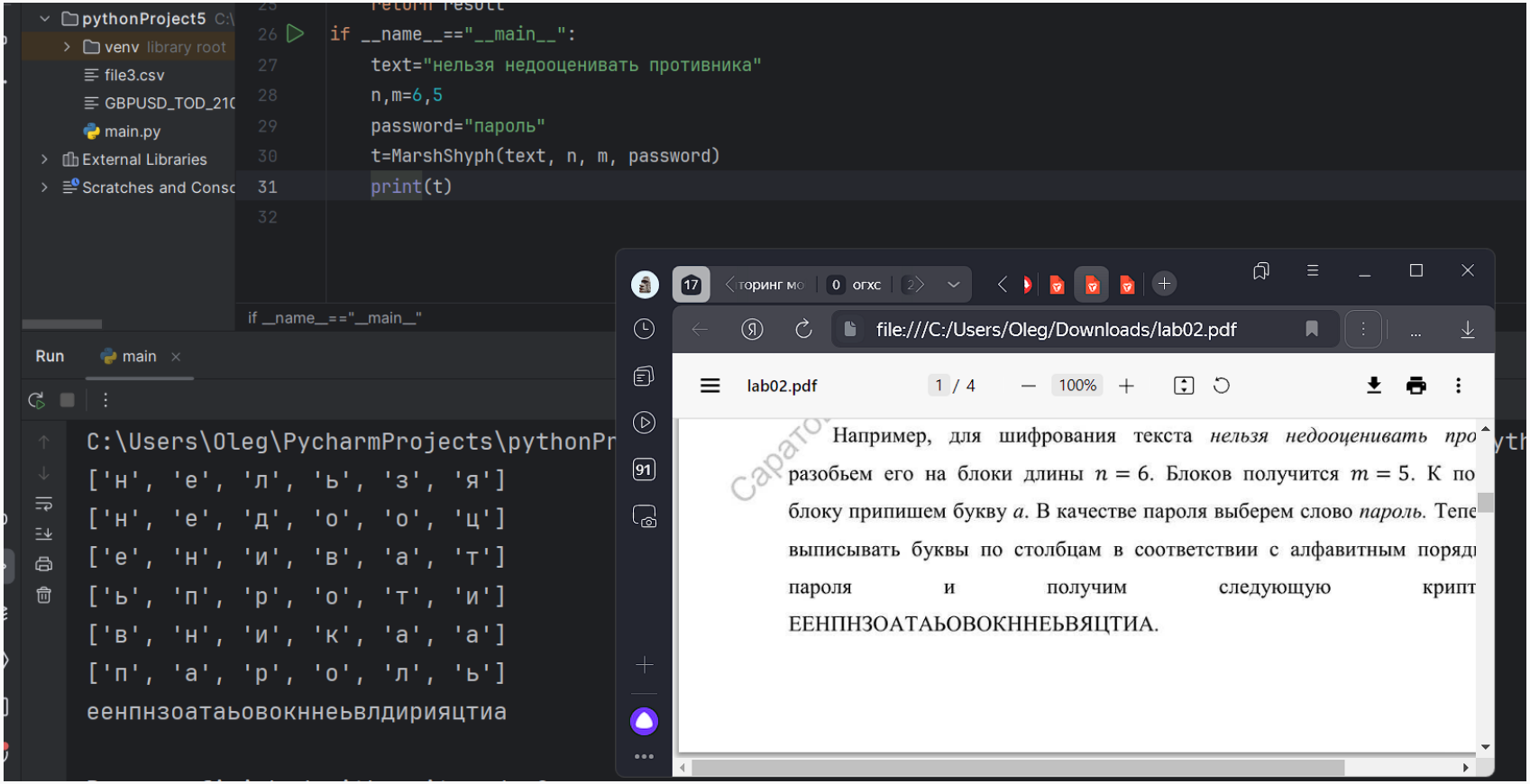

Рис. 1: Работа алгоритма маршрутной перестановки

Контрольный пример

```
In [9]: 1 cardangrille()
```

```
Введите число k3
[[1, 2, 3], [4, 5, 6], [7, 8, 9]]
1 2 3 7 4 1
4 5 6 8 5 2
7 8 9 9 6 3
3 6 9 9 8 7
2 5 8 6 5 4
1 4 7 3 2 1
т е с т т е
  е с т с т
    т



Введите паролькод
т е с т т е
  е с т с т
    т



к о д z z z
z  =  3
z  =  3
z  =  3
д  =  2
к  =  0
о  =  1
тттттссттее
```

Контрольный пример

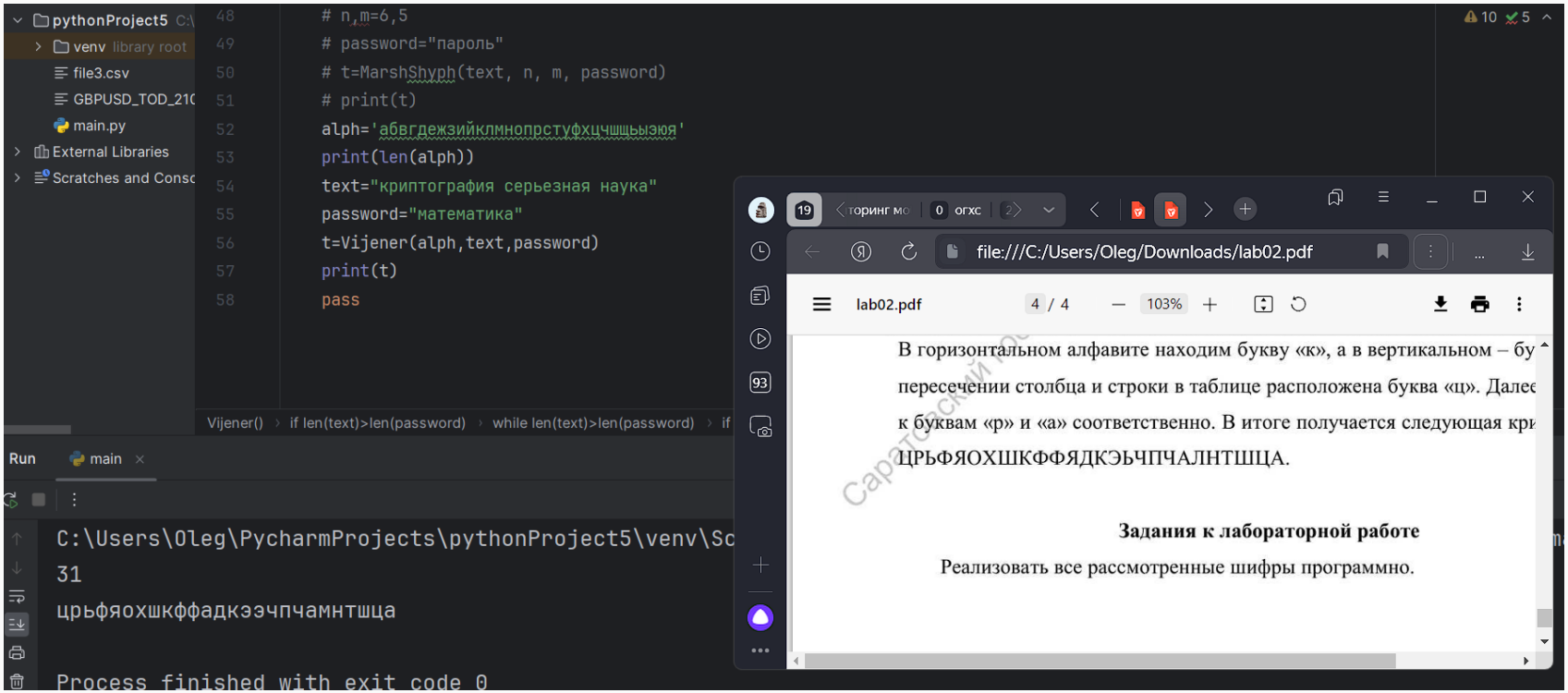

Рис. 3: Работа алгоритма Виженера

Выводы

Результаты выполнения лабораторной работы

Изучили алгоритмы шифрования с помощью перестановок