Шифры перестановки

Никита Венчаков

21 сентября, 2023, 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

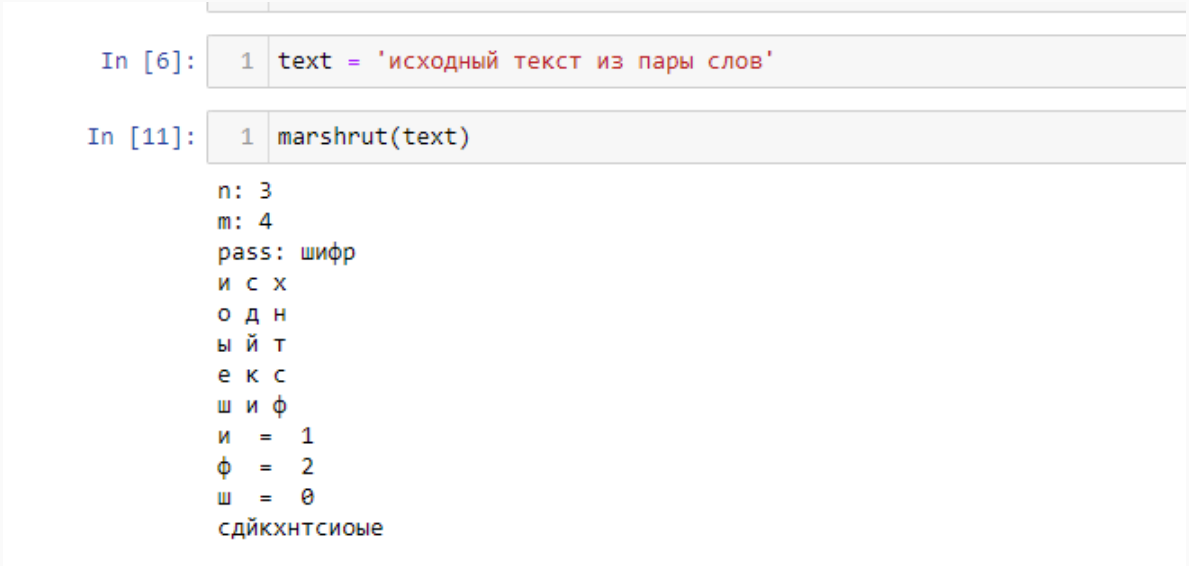
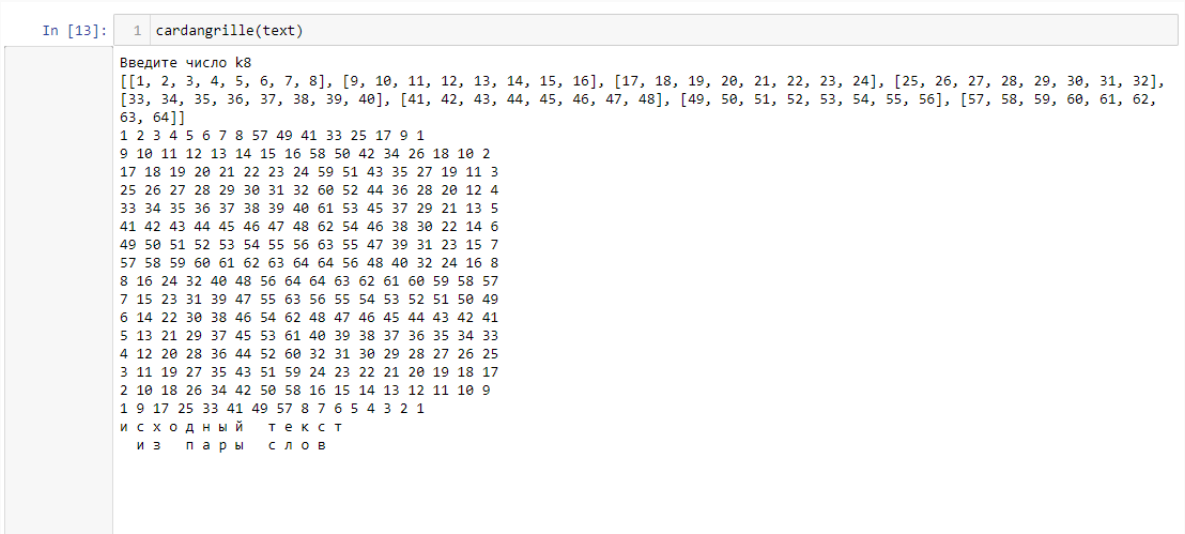


Figure 1: Работа алгоритма маршрутной перестановки

Контрольный пример



```
In [13]: 1 cardangrille(text)

Введите число k8
[[1, 2, 3, 4, 5, 6, 7, 8], [9, 10, 11, 12, 13, 14, 15, 16], [17, 18, 19, 20, 21, 22, 23, 24], [25, 26, 27, 28, 29, 30, 31, 32],
[33, 34, 35, 36, 37, 38, 39, 40], [41, 42, 43, 44, 45, 46, 47, 48], [49, 50, 51, 52, 53, 54, 55, 56], [57, 58, 59, 60, 61, 62,
63, 64]]
1 2 3 4 5 6 7 8 57 49 41 33 25 17 9 1
9 10 11 12 13 14 15 16 58 50 42 34 26 18 10 2
17 18 19 20 21 22 23 24 59 51 43 35 27 19 11 3
25 26 27 28 29 30 31 32 60 52 44 36 28 20 12 4
33 34 35 36 37 38 39 40 61 53 45 37 29 21 13 5
41 42 43 44 45 46 47 48 62 54 46 38 30 22 14 6
49 50 51 52 53 54 55 56 63 55 47 39 31 23 15 7
57 58 59 60 61 62 63 64 64 56 48 40 32 24 16 8
8 16 24 32 40 48 56 64 64 63 62 61 60 59 58 57
7 15 23 31 39 47 55 63 56 55 54 53 52 51 50 49
6 14 22 30 38 46 54 62 48 47 46 45 44 43 42 41
5 13 21 29 37 45 53 61 40 39 38 37 36 35 34 33
4 12 20 28 36 44 52 60 32 31 30 29 28 27 26 25
3 11 19 27 35 43 51 59 24 23 22 21 20 19 18 17
2 10 18 26 34 42 50 58 16 15 14 13 12 11 10 9
1 9 17 25 33 41 49 57 8 7 6 5 4 3 2 1
и с х о д н ы й   т е к с т
  и з   п а р ы   с л о в
```

Figure 2: Работа алгоритма решетки

Контрольный пример

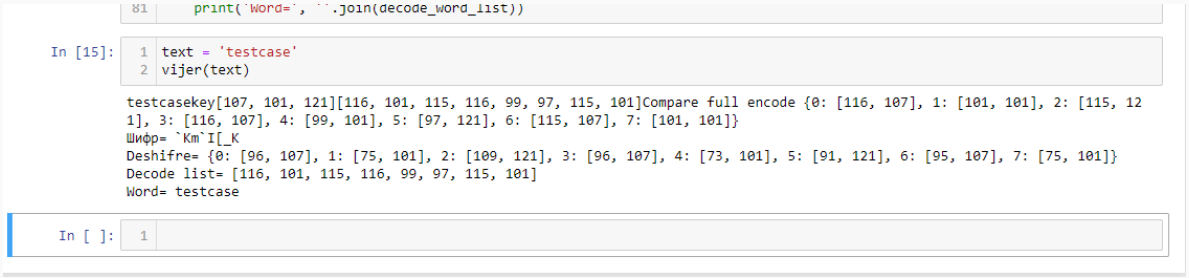


Figure 3: Работа алгоритма Виженера

Выводы

Результаты выполнения лабораторной работы

Изучили алгоритмы шифрования с помощью перестановок