Шифры перестановки

Тимофей Сергеев

19 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

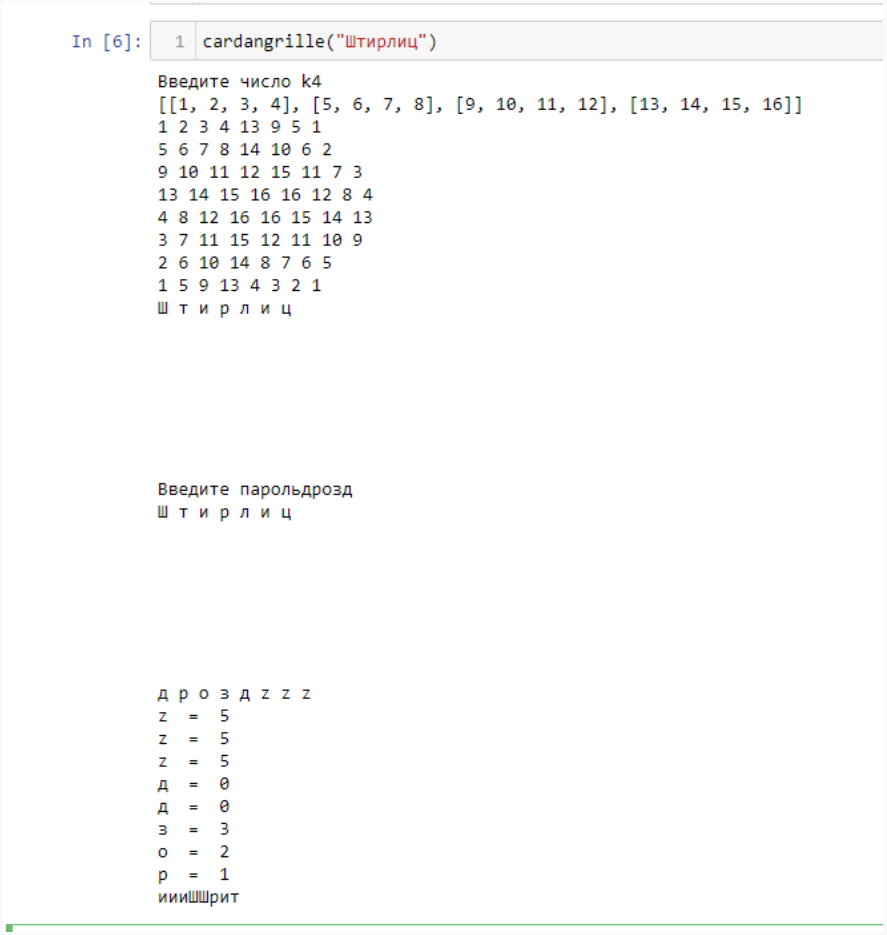
Шифр Виженера — это метод шифровки, в котором используются различные «шифры Цезаря» на основе букв в ключевом слове. В шифре Цезаря каждую букву абзаца необходимо поменять местами с определенным количеством букв, чтобы заменить исходную букву. Например, в латинском алфавите A становится D, B становится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

Контрольный пример

```
            for j in range(len(lists)):
                if j==len(lists)-1:
                    continue
                result += lists[j][lists[len(lists)-1].index(i)]
        print(result)

In [4]: marshrutshifr()

Введите текст: штирлиц
Введите число n 3
Введите число m 4
Введите пароль дрозд
ш т и
р л и
ц а а
а а а
д р о
д  =  0
о  =  2
р  =  1
шрцаииаатлаа
```

Figure 1: Работа алгоритма маршрутной перестановки

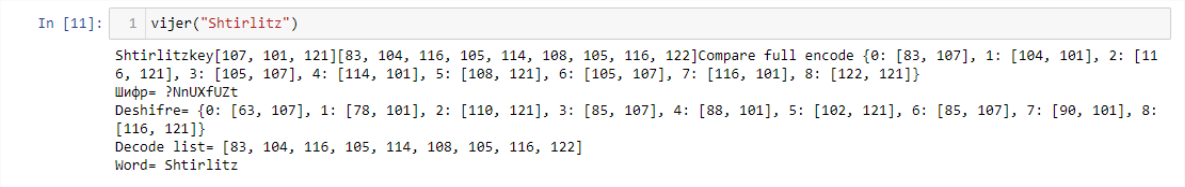
Контрольный пример



```
In [6]: 1 cardangrille("Штирлиц")

Введите число k4
[[1, 2, 3, 4], [5, 6, 7, 8], [9, 10, 11, 12], [13, 14, 15, 16]]
1 2 3 4 13 9 5 1
5 6 7 8 14 10 6 2
9 10 11 12 15 11 7 3
13 14 15 16 16 12 8 4
4 8 12 16 16 15 14 13
3 7 11 15 12 11 10 9
2 6 10 14 8 7 6 5
1 5 9 13 4 3 2 1
Ш т и р л и ц




Введите парольдрозд
Ш т и р л и ц




д р о з д z z z
z = 5
z = 5
z = 5
д = 0
д = 0
з = 3
о = 2
р = 1
ииишШрит
```

Figure 2: Работа алгоритма решетки

Контрольный пример



```
In [11]:  1 vijer("Shtirlitz")

Shtirlitzkey[107, 101, 121][83, 104, 116, 105, 114, 108, 105, 116, 122]Compare full encode {0: [83, 107], 1: [104, 101], 2: [11
6, 121], 3: [105, 107], 4: [114, 101], 5: [108, 121], 6: [105, 107], 7: [116, 101], 8: [122, 121]}
Шифр= ?NnUXfUZt
Deshifre= {0: [63, 107], 1: [78, 101], 2: [110, 121], 3: [85, 107], 4: [88, 101], 5: [102, 121], 6: [85, 107], 7: [90, 101], 8:
[116, 121]}
Decode list= [83, 104, 116, 105, 114, 108, 105, 116, 122]
Word= Shtirlitz
```

Figure 3: Работа алгоритма Виженера

Выводы

Результаты выполнения лабораторной работы

Изучили алгоритмы шифрования с помощью перестановок