

Шифры перестановки

Шевляков Илья Николаевич НФИмд-01-21

18 ноября, 2021, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Изучение алгоритмов маршрутной перестановки, решеток и Виженера

Выполнение лабораторной работы

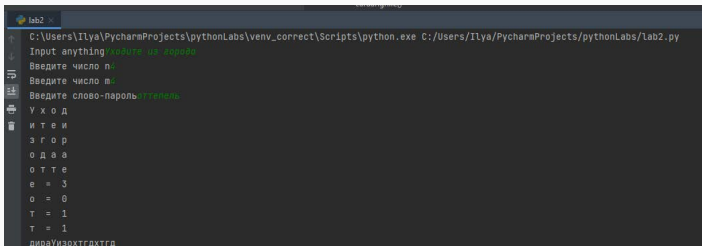
Шифр маршрутной перестановки

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.

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

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 А становится D, В становится Е, С становится F. Шифр Виженера построен на методе использования различных шифров Цезаря в различных частях сообщения.

Контрольный пример



```
lab2
C:\Users\Ilya\PycharmProjects\pythonLabs\venv_correct\Scripts\python.exe C:/Users/Ilya/PycharmProjects/pythonLabs/lab2.py
Input anything/введите из города
Введите число n:4
Введите число m:4
Введите слово-парольоттепель
У х о д
и т е и
з г о р
о д а а
о т т е
е = 3
о = 0
т = 1
т = 1
дираУиэхтгдхтгд
```

Figure 1: Работа алгоритма маршрутной перестановки

Контрольный пример

```
Введите число K:
[[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]]
1 2 3 4 5 21 16 11 6 1
6 7 8 9 10 22 17 12 7 2
11 12 13 14 15 23 18 13 8 3
16 17 18 19 20 24 19 14 9 4
21 22 23 24 25 20 15 10 5
5 10 15 20 25 25 24 23 22 21
4 9 14 19 24 20 19 18 17 16
3 8 13 18 23 15 14 13 12 11
2 7 12 17 22 10 9 8 7 6
1 6 11 16 21 5 4 3 2 1
скрывайте
сб

Введите пароль:
скрывайте
сб

Добро пожаловать
1 - 5
2 - 5
3 - 5
4 - 5
5 - 5
6 - 5
7 - 5
8 - 5
9 - 5
10 - 5
11 - 5
12 - 5
13 - 5
14 - 5
15 - 5
16 - 5
17 - 5
18 - 5
19 - 5
20 - 5
21 - 5
22 - 5
23 - 5
24 - 5
25 - 5
```

Figure 2: Работа алгоритма решетки

Контрольный пример

```
Test sent just [100, 117, 115, 110] [84, 101, 115, 110, 37, 115, 101, 110, 110] compare full encode 0: [84, 100], 1: [101, 117], 2: [115, 115], 3: [110, 110], 4: [37, 100], 5: [115, 117], 6: [101, 115], 7: [110, 110], 8: [110, 110]
Msgs: 2 [alive]
Dehifree 0: [05, 100], 1: [01, 117], 2: [105, 115], 3: [105, 110], 4: [11, 100], 5: [105, 117], 6: [09, 115], 7: [09, 110], 8: [05, 100]
Deconv list: [84, 101, 115, 110, 37, 115, 101, 110, 110]
Word: Test sent
Process finished with exit code 0
```

Figure 3: Работа алгоритма Виженера

Выводы

Изучили алгоритмы шифрования с помощью перестановок