Шифры перестановки

Игорь Солодовников

20 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

```
In [6]:  1  text = 'проверка кода'

In [7]:  1  marshrut(text)

n: 3
m: 5
pass: код
п р о
в е р
к а к
о д а
а а а
к о д
д  =  2
к  =  0
о  =  1
оркаапвкоареада
```

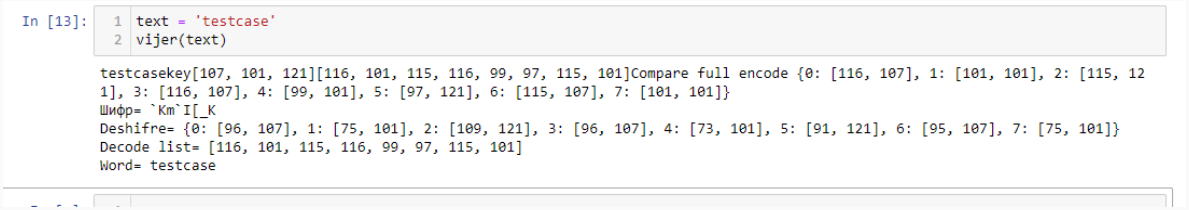
Figure 1: Работа алгоритма маршрутной перестановки

Контрольный пример

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

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
п р о в е р к
  а   к о д
    а




Введите паролькод
п р о в е р к
  а   к о д
    а




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

Figure 2: Работа алгоритма решетки

Контрольный пример



```
In [13]:
1 text = 'testcase'
2 vijer(text)

testcasekey[107, 101, 121][116, 101, 115, 116, 99, 97, 115, 101]Compare full encode {0: [116, 107], 1: [101, 101], 2: [115, 12
1], 3: [116, 107], 4: [99, 101], 5: [97, 121], 6: [115, 107], 7: [101, 101]}
Шифр= `Km`I[_K
Deshifre= {0: [96, 107], 1: [75, 101], 2: [109, 121], 3: [96, 107], 4: [73, 101], 5: [91, 121], 6: [95, 107], 7: [75, 101]}
Decode list= [116, 101, 115, 116, 99, 97, 115, 101]
Word= testcase
```

Figure 3: Работа алгоритма Виженера

Выводы

Результаты выполнения лабораторной работы

Изучили алгоритмы шифрования с помощью перестановок