

Шифры перестановки

Лисягин Евгений Алексеевич

18 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.

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

```
In [5]: 1 | marshrutshifr("безопасность")
```

```
n: 3  
m: 5  
pass: зуб  
б е з  
о п а  
с н о  
с т ь  
а а а  
з у б  
б = 2  
з = 0  
у = 1  
заоьабоссаепнта
```

Figure 1: Работа алгоритма маршрутной перестановки

Контрольный пример

```
In [7]: 1 cardangrille("безопасность")

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
б е з о п а с
н о с т ь

Введите парользуб
б е з о п а с
н о с т ь

з у б з з з з з
z = 3
z = 3
z = 3
z = 3
z = 3
б = 2
з = 0
у = 1
ососососозобен
```

Figure 2: Работа алгоритма решетки

Контрольный пример

```
In [9]: 1 vjfer("security")

securitykey[107, 101, 121][115, 101, 99, 117, 114, 105, 116, 121]Compare full encode {0: [115, 107], 1: [101, 101], 2: [99, 12
1], 3: [117, 107], 4: [114, 101], 5: [105, 121], 6: [116, 107], 7: [121, 101]}
Wdfr= _k]axc-
Deslfrw= {0: [95, 107], 1: [75, 101], 2: [93, 121], 3: [97, 107], 4: [88, 101], 5: [99, 121], 6: [96, 107], 7: [95, 101]}
Decode list= [115, 101, 99, 117, 114, 105, 116, 121]
Word= security
```

Figure 3: Работа алгоритма Виженера

Выводы

Изучили алгоритмы шифрования с помощью перестановок