

Шифры перестановки

Михаил Киронда

18 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.

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

```
print(result)

In [3]: 1 marhsrutshifr()

Введите текст тест
Введите число n 3
Введите число m4
Введите слово-пароль код
т е с
т а а
а а а
а а а
к о д
д = 2
к = 0
о = 1
саааттааеааа
```

Figure 1: Работа алгоритма маршрутной перестановки

Контрольный пример

```
In [9]: 1 candangrille()

Введите число k3
[[1, 2, 3], [4, 5, 6], [7, 8, 9]]
1 2 3 7 4 1
4 5 6 8 5 2
7 8 9 9 6 3
3 6 9 9 8 7
2 5 8 6 5 4
1 4 7 3 2 1
т е с т т е
  е с т с т
    т

Введите паролькод
т е с т т е
  е с т с т
    т

К о д з з з
z = 3
z = 3
z = 3
д = 2
к = 0
о = 1
TTTTTCSSTee
```

Figure 2: Работа алгоритма решетки

Контрольный пример

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

Hello worldkey[107, 101, 121][72, 101, 100, 100, 111, 32, 119, 111, 114, 100, 100]Compare full encode {0: [72, 107], 1: [101, 1
01], 2: [100, 121], 3: [100, 107], 4: [111, 101], 5: [32, 121], 6: [119, 107], 7: [111, 101], 8: [114, 121], 9: [100, 107], 10:
[100, 101]}
Cipher= AKFXUDCUIXJ
Deshiftres={0: [52, 107], 1: [75, 101], 2: [102, 121], 3: [00, 107], 4: [05, 101], 5: [26, 121], 6: [99, 107], 7: [05, 101], 8:
[100, 121], 9: [00, 107], 10: [74, 101]}
Decode list= [72, 101, 100, 100, 111, 32, 119, 111, 114, 100, 100]
Word= Hello world
```

Figure 3: Работа алгоритма Виженера

Выводы

Изучили алгоритмы шифрования с помощью перестановок