Шифры перестановки

Нилой Шоумитра Басак

31 августа, 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  marhsrutshifr()

Input anythingСекретное слово
Введите число n4
Введите число m4
Введите слово-парольдрозд
С е к р
е т н о
е с л о
в о а а
д р о з
д  =  0
з  =  3
о  =  2
р  =  1
Сееврооакнлаетсо
```

Figure 1: Работа алгоритма маршрутной перестановки

Контрольный пример

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

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
д о г о в о р
  п о д п и
    с а л
      и



Введите парольдрозд
д о г о в о р
  п о д п и
    с а л
      и



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

Figure 2: Работа алгоритма решетки

Контрольный пример

```
In [8]:  1  vijer()

Hello worldkey[107, 101, 121][72, 101, 108, 108, 111, 32, 119, 111, 114, 108, 100]Compare full encode {0: [72, 107], 1: [101, 1
01], 2: [108, 121], 3: [108, 107], 4: [111, 101], 5: [32, 121], 6: [119, 107], 7: [111, 101], 8: [114, 121], 9: [108, 107], 10:
[100, 101]}
Шифр= 4KfXU□cUlXJ
Deshifre= {0: [52, 107], 1: [75, 101], 2: [102, 121], 3: [88, 107], 4: [85, 101], 5: [26, 121], 6: [99, 107], 7: [85, 101], 8:
[108, 121], 9: [88, 107], 10: [74, 101]}
Decode list= [72, 101, 108, 108, 111, 32, 119, 111, 114, 108, 100]
Word= Hello world
```

Figure 3: Работа алгоритма Виженера

Выводы

Результаты выполнения лабораторной работы

Изучили алгоритмы шифрования с помощью перестановок