Шифры перестановки

Семмар вассим

27 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.

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

```
Entrée [16]: marhsrutshifr()

             Введите текст secretmessage
             Введите число n 4
             Введите число m 3
             Введите слово-пароль code
             s e c r
             e t m e
             s s a g
             c o d e
             c  =  0
             d  =  2
             e  =  3
             o  =  1
             sescmaregets
```

Figure 1: Работа алгоритма маршрутной перестановки

Контрольный пример

```
cardangrille()
```

```
Введите число k 3
[[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
e x a m p s
  l e m s a
    e g e



Введите парольsecret
e x a m p s
  l e m s a
    e g e



s e c r e t
c  =  2
e  =  1
e  =  1
r  =  3
s  =  0
t  =  5
aeexlxlmmgesa
```

Figure 2: Работа алгоритма решетки

Контрольный пример

```
Entrée [20]: vijer()

Data Sciencecipher[99, 105, 112, 104, 101, 114][68, 97, 116, 97, 32, 83, 99,
105, 101, 110, 99, 101]Compare full encode {0: [68, 99], 1: [97, 105], 2: [11
6, 112], 3: [97, 104], 4: [32, 101], 5: [83, 114], 6: [99, 99], 7: [105, 10
5], 8: [101, 112], 9: [110, 104], 10: [99, 101], 11: [101, 114]}
Шифр= (KeJ□FGSVWIX
Deshifre= {0: [40, 99], 1: [75, 105], 2: [101, 112], 3: [74, 104], 4: [6, 10
1], 5: [70, 114], 6: [71, 99], 7: [83, 105], 8: [86, 112], 9: [87, 104], 10:
[73, 101], 11: [88, 114]}
Decode list= [68, 97, 116, 97, 32, 83, 99, 105, 101, 110, 99, 101]
Word= Data Science
```

Figure 3: Работа алгоритма Виженера

Выводы

Результаты выполнения лабораторной работы

Изучили алгоритмы шифрования с помощью перестановок