Шифры перестановки

Бакундукизе Эжид Принц НФИмд-01-21

21 сентября, 2022, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Изучение алгоритмов шифров перестановки: маршрутное шифрование, шифрование с помощью решеток и таблица Виженера

Выполнение лабораторной работы

Шифры перестановки

Шифр перестано́вки — это метод симметричного шифрования, в котором элементы исходного открытого текста меняют местами. Элементами текста могут быть отдельные символы (самый распространённый случай), пары букв, тройки букв, комбинирование этих случаев и так далее. Как правило, при шифровании и дешифровании шифра простой перестановки используется таблица перестановок:

1	2	3	$\ldots$	n
I_1	I_2	I_3	$\ldots$	I_n

Маршрутное шифрование

Простейшим примеров перестановочного шифра являются так называемые «маршрутные перестановки», использующие некоторую геометрическую фигуру (плоскую или объемную). Шифрование заключается в том, что текст записывается в такую фигуру по некоторой траектории, а выписывается по другой траектории. Шифруемое сообщение в этом случае записывается в прямоугольную таблицу по маршруту: по горизонтали, начиная с верхнего левого угла, поочередно слева направо.

Контрольный пример

```
Введите текст: секретный текст
Введите число n: 3
Введите число m: 3
Введите слово-пароль: пароль
с е к
р е т
н ы й
п а р
а  =  1
п  =  0
р  =  2
ееысрнктй
```

Figure 1: Работа алгоритма маршрутной перестановки

Шифрование с помощью решеток

Решётка Кардано — инструмент кодирования и декодирования, представляющий собой специальную прямоугольную (в частном случае — квадратную) таблицу-карточку, четверть ячеек которой вырезана. Таблица накладывается на носитель, и в вырезанные ячейки вписываются буквы, составляющие сообщение. После переворачивания таблицы вдоль вертикальной оси, процесс вписывания букв повторяется. Затем то же самое происходит после переворачивания вдоль горизонтальной и снова вдоль вертикальной осей.

Контрольный пример

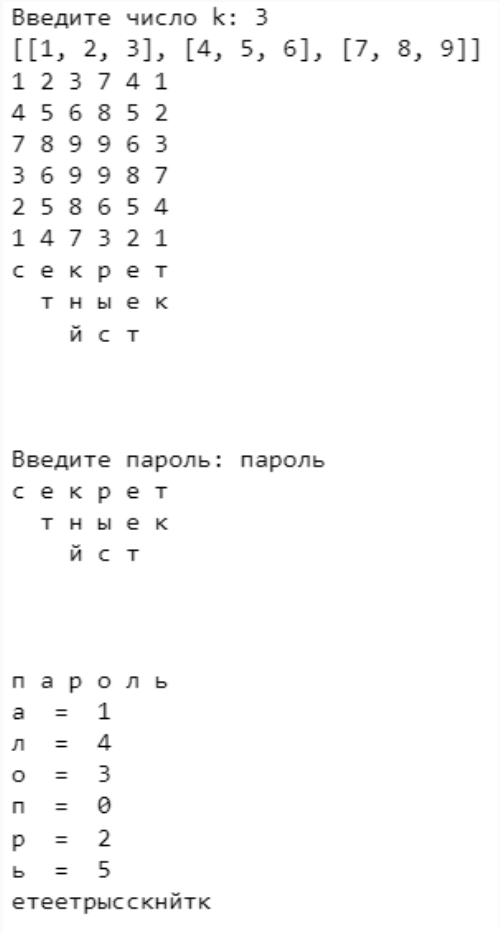
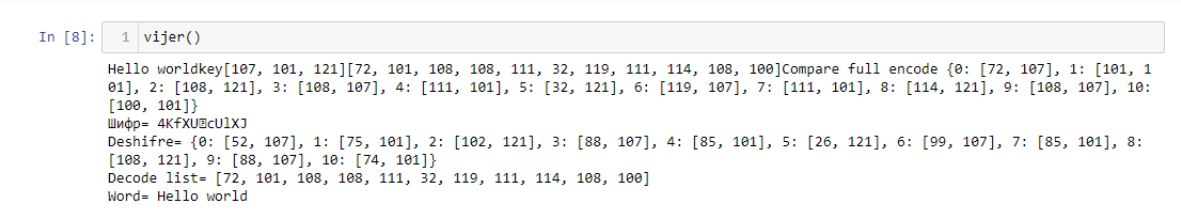


Figure 2: Работа алгоритма решетки

Шифр Виженера

Шифр Виженера — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова. Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.

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

В ходе выполнения данной лабораторной работы мы изучили алгоритмы шифров перестановки: маршрутное шифрование, шифрование с помощью решеток и таблица Виженер. Реализовали данные методы шифрования программно и продемонстрировали результат.