Отчёт по лабораторной работе №2. Шифры перестановки

Дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Леонова Алина Дмитриевна, 1032212306
Группа: НФИмд-01-21
Преподаватель: д-р.ф.-м.н., проф. Кулябов Дмитрий Сергеевич

20 ноября, 2021, Москва

Цель работы

Целью данной работы является ознакомление с шифрами перестановки и их реализация на выбранном языке программирования.

Задание

Реализовать все рассмотренные шифры программно.

Теоретическое введение (промежуточная страница)

Шифры перестановки преобразуют открытый текст в криптограмму путем перестановки его символов. Способ, каким при шифровании переставляются буквы открытого текста, и является ключем шифра.

Маршрутное шифрование

н	е	л	ь	з	я
н	е	д	о	о	ц
е	н	и	в	а	т
ь	п	р	о	т	и
в	н	и	к	а	а
п	а	р	о	л	ь

Figure 1: Пример шифр перестановки (2)

Текст разбивается на блоки равной длины, блоки записываются в виде таблицы, недостающие символы дополняются. Создается ключ-строка, в которой все символы различны. В алфавитном порядке символов ключа выписываются столбцы таблицы.

Маршрутное шифрование

```python
def grid_reading(key, table):
    _key = sorted(key)
    order = [key.index(i) for i in _key]
    print(list(key))
    #print(_key)
    print('Порядок использования столбцов:', order)
    m = table.shape[0]
    res = ''
    for j in order:
        for i in range(m):
            res += table[i][j]
    return res
```

Figure 2: Фрагмент кода программы маршрутного шифрования

Маршрутное шифрование

```
ru:  ['а', 'б', 'в', 'г', 'д', 'е', 'ж', 'з', 'и', 'й', 'к', 'л',
'м', 'н', 'о', 'п', 'р', 'с', 'т', 'у', 'ф', 'х', 'ц', 'ч', 'ш', 'щ',
'ъ', 'ы', 'ь', 'э', 'ю', 'я']
##########################################################################
# 1.
Текст:  Нельзя недооценивать противника
Ключ: пароль
Длина текста: 29
n =  6
m =  5
[['н' 'е' 'л' 'ь' 'з' 'я']
 ['н' 'е' 'д' 'о' 'о' 'ц']
 ['е' 'н' 'и' 'в' 'а' 'т']
 ['ь' 'п' 'р' 'о' 'т' 'и']
 ['в' 'н' 'и' 'к' 'а' 'а']]
['п', 'а', 'р', 'о', 'л', 'ь']
Порядок использования столбцов: [1, 4, 3, 0, 2, 5]
Криптограмма:  еенпнзоатаьовокннеьвлдирияцтиа
--------------------------------------------------
Текст:  Live long and prosper
Ключ: Spock
Длина текста: 18
n =  5
m =  4
[['l' 'i' 'v' 'e' 'l']
 ['o' 'n' 'g' 'a' 'n']
 ['d' 'p' 'r' 'o' 's']
 ['p' 'e' 'r' 'r' 'r']]
['s', 'p', 'o', 'c', 'k']
Порядок использования столбцов: [3, 4, 2, 1, 0]
Криптограмма:  eaorlnsrvgrrinpelodp
##########################################################################
```

Шифрование с помощью решеток

Строка дополняется произвольными одинаковыми символами так, чтобы её длина была квадратом целого четного числа. Взяв корень из длины строки получаем размерность маленького квадрата k. Путем поворота его на 90 градусов вправо и присоединения к исходному квадрату справа получим больший квадрат размерности $2k$.

Шифрование с помощью решеток

Теперь из большого квадрата мы случайным образом удаляем k различных чисел, чтобы получить своего рода “решето”. С помощью решета получаем таблицу с символами, а затем применяем маршрутное шифрование (см. рис. 2).

Шифрование с помощью решеток

```
##################################################################
# 2.
Текст:  договор подписали
Длина текста: 16
Ключ: бьцъ
Квадрат цифр:
 [[1. 2. 3. 1.]
 [3. 4. 4. 2.]
 [2. 4. 4. 3.]
 [1. 3. 2. 1.]]
Сгенерированная схема:
 [[1. 0. 0. 0.]
 [0. 4. 0. 2.]
 [0. 0. 0. 3.]
 [0. 0. 0. 0.]]
Схема из букв:
 [['д' 'с' 'а' 'в']
 ['о' 'о' 'о' 'г']
 ['д' 'л' 'п' 'о']
 ['и' 'р' 'п' 'и']]
['б', 'ь', 'ц', 'ъ']
Порядок использования столбцов: [0, 2, 3, 1]
Криптограмма:  додиаоппвгоисолр
------------------------------------------------------
Текст:  за что мне все эти страдания
Длина текста: 23
Ключ: сохадк
Квадрат цифр:
 [[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.]]
Сгенерированная схема:
 [[1. 2. 0. 0. 0. 0.]
 [0. 0. 0. 0. 0. 0.]
 [0. 0. 0. 9. 6. 3.]
 [0. 0. 0. 0. 0. 0.]
 [0. 5. 8. 0. 0. 4.]
 [0. 0. 7. 0. 0. 0.]]
Схема из букв:
 [['э' 'а' 'я' 'д' 'я' 'с']
 ['а' 'е' 'я' 'н' 'и' 'э']
 ['т' 'и' 'я' 'ч' 'т' 'о']
 ['я' 'я' 'я' 'с' 'я' 'я']
 ['я' 'м' 'н' 'т' 'я' 'е']
 ['я' 'р' 'в' 'а' 'я' 'я']]
['с', 'о', 'х', 'а', 'д', 'к']
Порядок использования столбцов: [3, 4, 5, 1, 0, 2]
Криптограмма:  днчстаяитяяясэояеяаеиямрзатяяяяяянв
##################################################################
```

Шифрование таблицей Виженера

м	а	т	е	м	а	т	и	к	а	м	а	т	е	м	а	т	и	к	а	м	а	т	е	м	а
к	р	и	п	т	о	г	р	а	ф	и	я	с	е	р	ь	е	з	н	а	я	н	а	у	к	а

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я
Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А
В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б
Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В
Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г
Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д
Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е
З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж
И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З
Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й
Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н
П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Ч	Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Ш	Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Щ	Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Ъ	Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Ы	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы
Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э
Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Э	Ю

В горизонтальном алфавите находим букву «к», а в вертикальном – букву «м». На пересечении столбца и строки в таблице расположена буква «ц». Далее переходим к буквам «р» и «а» соответственно. В итоге получается следующая криптограмма:

ЦРЬФЯОХШКФФЯДКЭЬЧПЧАЛНТШЦА.

{#fig:005

Шифрование таблицей Виженера

Создадим таблицу Виженера - таблицу, в начале строки и столбца которой находятся все возможные буквы выбранного алфавита (см. рис. 5).

Ключ повторяется до тех пор, пока его длина не станет равна длине сообщения. На пересечении iтых координат сообщения и ключа по таблице получается символ.

Результат работы шифрования Виженера

```
##########################################################################
Словарь букв ru:  {'а': 0, 'б': 1, 'в': 2, 'г': 3, 'д': 4, 'е': 5,
'ж': 6, 'з': 7, 'и': 8, 'й': 9, 'к': 10, 'л': 11, 'м': 12, 'н': 13,
'о': 14, 'п': 15, 'р': 16, 'с': 17, 'т': 18, 'у': 19, 'ф': 20, 'х':
21, 'ц': 22, 'ч': 23, 'ш': 24, 'щ': 25, 'ъ': 26, 'ы': 27, 'ь': 28,
'э': 29, 'ю': 30, 'я': 31}
# 3.
Таблица Виженера:
 [['а' 'б' 'в' ... 'э' 'ю' 'я']
 ['б' 'в' 'г' ... 'ю' 'я' 'а']
 ['в' 'г' 'д' ... 'я' 'а' 'б']
 ...
 ['э' 'ю' 'я' ... 'ъ' 'ы' 'ь']
 ['ю' 'я' 'а' ... 'ы' 'ь' 'э']
 ['я' 'а' 'б' ... 'ь' 'э' 'ю']]
Текст:  криптография серьезная наука
Длина текста: 26
Ключ: математика
-----
криптографиясерьезнаянаука
математикаматематикаматема
-----
Криптограмма:  цръфюохшкффягкььчпчалнтшца
--------------------------------------------------
Текст:  ты не пройдешь
Длина текста: 12
Ключ: Гендальф
-----
тынепройдешь
гендальфгенд
-----
Криптограмма:  хаъйпыкэзкеа
```

Выводы

Цель лабораторной работы была достигнута, три данные шифра перестановки были изучены и реализованы на языке программирования Python.