

Алгоритмы маршрутной перестановки, решеток и Виженера

Кейела Патачона

20 ноября, 2021, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Шифры перестановки

Цель лабораторной работы

Изучение алгоритмов маршрутной перестановки, решеток и Виженера

Выполнение лабораторной работы

Шифр маршрутной перестановки

Широкое распространение получили шифры перестановки, использующие некоторую геометрическую фигуру.

Преобразования из этого шифра состоят в том, что в фигуру исходный текст вписывается по ходу одного “маршрута”, а затем по ходу другого выписывается с нее. Такой шифр называют маршрутной перестановкой. Например, можно вписывать исходное сообщение в прямоугольную таблицу, выбрав такой маршрут: по горизонтали, начиная с левого верхнего угла поочередно слева направо и справа налево. Выписывать же сообщение будем по другому маршруту: по вертикали, начиная с верхнего правого угла и двигаясь поочередно сверху вниз и снизу вверх.

Шифр Кардано

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.

В частном случае квадратной таблицы, для получения новых позиций для вписывания букв, можно поворачивать квадрат на четверть оборота.

Чтобы прочитать закодированное сообщение, необходимо наложить решётку Кардано нужное число раз на закодированный текст и прочитать буквы, расположенные в вырезанных ячейках.

Такой способ шифрования сообщения был предложен математиком Джероламо Кардано в 1550 году, за что и получил своё название.

Шифр Виженера

Шифр Виженера (фр. Chiffre de Vigenère) — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова.

Этот метод является простой формой многоалфавитной замены. Шифр Виженера изобретался многократно. Впервые этот метод описал Джован Баттиста Беллазо (итал. Giovan Battista Bellaso) в книге *La cifra del. Sig. Giovan Battista Bellaso* в 1553 году, однако в XIX веке получил имя Блеза Виженера, французского дипломата. Метод прост для понимания и реализации, он является недоступным для простых методов криптоанализа.

Шифр Виженера

В шифре Цезаря каждая буква алфавита сдвигается на несколько строк; например в шифре Цезаря при сдвиге +3, А стало бы D, В стало бы Е и так далее. Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая *tabula recta* или квадрат (таблица) Виженера.

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 1

▼ Задача № 1 Маршрутное шифрование

```
1m 1 # Мы принимаем пароль и текст на шифрование
password = str(input('Введите пароль:'))
my_word = ''.join(str(input("Введите фразу:")).split())

# Длина прямоугольника
n = len(password)
# Дополняем если нужно
if len(my_word)%n != 0:
    my_word += 'a'*(n-len(my_word) % n)

# Отсортируем буквы пароля
password_sort = ''.join(sorted(password))
index_list = []
for i in range (len(password)):
    f_index = password.find(password_sort[i])
    index_list.append(f_index)

# Шифруем наш текст
new_word = ''
for i in index_list:
    for j in range(len(my_word)//n):
        new_word += my_word[j*n+i]

# Выводим отшифрованный текст
print(new_word)

Введите пароль:rudn
Введите фразу:Faculty of physics mathematics and natural sciences
cyhctasnrccaouyshtaabaieaFlfsmteintlesatpiamcdusna
```

Figure 1: Работа алгоритма маршрутной перестановки

Контрольный пример 2

▼ Задача № 2 Шифрование с помощью решеток

```
[ ] import numpy as np
```

```
# We enter to word to encode
word_to_encode = list(''.join(input().split()).upper())
print(word_to_encode)

# WE DEFINE THE VALUE OF K:  $4k*2 = N$ 
if int(np.sqrt(len(word_to_encode)/4)) == np.sqrt(len(word_to_encode)/4):
    k = int(np.sqrt(len(word_to_encode)/4))
else:
    # WE FILL THE EMPTY POSITIONS WITH STARS
    k = int(np.sqrt(len(word_to_encode)/4)) + 1
    word_to_encode += ['*']*(4 * k*2 - len(word_to_encode))
print(word_to_encode)

KEYELA PATATCHONA
['K', 'E', 'Y', 'E', 'L', 'A', 'P', 'A', 'T', 'A', 'T', 'C', 'H', 'O', 'N', 'A']
['K', 'E', 'Y', 'E', 'L', 'A', 'P', 'A', 'T', 'A', 'T', 'C', 'H', 'O', 'N', 'A']
```

```
[ ] # Simple matrix of k * k
k_matrix = np.reshape(np.arange(k*2),(k,k))
print(k_matrix,'\n')

# Complete matrix:
full_matrix = np.concatenate((np.concatenate((k_matrix,np.rot90(k_matrix,-1)),axis=1),
                               np.concatenate((np.rot90(k_matrix,-3),np.rot90(k_matrix,-2))),axis=1
                               ),axis=0)
print(full_matrix)

[[0 1]
 [2 3]]

[[0 1 2 0]
 [2 3 3 1]
 [1 3 3 2]
 [0 2 1 0]]
```

```
full_matrix_id = full_matrix.flatten()
print(full_matrix_id)
slovar = {}
```

Контрольный пример 3

Задача № 3 Таблица Виженера

```
172 ✓
1 slovar = 'абвгдеёжзийклмнопрстуфхцчшщъыьэя'
2 password = str(input('Введите пароль: ')).lower()
3 word = str(input('Введите фразу для шифрования: ')).lower()
4 k = (len(word) % len(password)) # Количество символов которые нужно дополнить
5 password_len = '' + password * (len(word) // len(password)) + password[:k]
6 print(word, password_len, sep='\n')
7 slovar_visinera = []
8 slovar_i = 'абвгдеёжзийклмнопрстуфхцчшщъыьэя'
9 for i in range(len(slovar)):
10     slovar_visinera.append(slovar_i)
11     new = slovar_i[1:] + slovar_i[0]
12     slovar_i = new
13 print("Квадрат виженера:", slovar_visinera)
14 message = ''
15 for i in range(len(word)):
16     f_index1 = slovar.find(word[i])
17     f_index2 = slovar.find(password_len[i])
18     message += slovar_visinera[f_index1][f_index2]
19 print(f'Зашифрованное сообщение: {message}')
```

Введите пароль: рудн
Введите фразу для шифрования: Кейела Патачона
кейела патачона
руднруднруднруд
Квадрат виженера: ['абвгдеёжзийклмнопрстуфхцчшщъыьэя', 'бвгдеёжзийклмнопрстуфхцчшщъыьэя', 'вгдеёжзийклмнопрстуфхцчшщъыьэя', 'гдеёжзийклмнопрстуфхцчшщъыьэя', 'еёжзийклмнопрстуфхцчшщъыьэя', 'ёжзийклмнопрстуфхцчшщъыьэя', 'жзийклмнопрстуфхцчшщъыьэя', 'зийклмнопрстуфхцчшщъыьэя', 'йклмнопрстуфхцчшщъыьэя', 'клмнопрстуфхцчшщъыьэя', 'лмнопрстуфхцчшщъыьэя', 'мнопрстуфхцчшщъыьэя', 'нопрстуфхцчшщъыьэя', 'опрстуфхцчшщъыьэя', 'прстуфхцчшщъыьэя', 'рстуфхцчшщъыьэя', 'стуфхцчшщъыьэя', 'туфхцчшщъыьэя', 'уфхцчшщъыьэя', 'фхцчшщъыьэя', 'хцчшщъыьэя', 'цчшщъыьэя', 'чшщъыьэя', 'шщъыьэя', 'щъыьэя', 'ъыьэя', 'ыьэя', 'эя', 'я']
Зашифрованное сообщение: ынтъуэзрёдеябд

Figure 2: Работа алгоритма Виженера

Выводы

Изучили алгоритмы шифрования с помощью перестановок