# Защита лабораторной работы №2

## Шифры перестановки

Бурдина К. П.

23 сентября 2023

Российский университет дружбы народов, Москва, Россия

# Докладчик


* Бурдина Ксения Павловна
* студентка группы НФИмд-02-23
* студ. билет № 1132236896
* Российский университет дружбы народов
* 1132236896@rudn.ru


# Вводная часть

# Цель выполнения лабораторной работы

- Освоение шифров перестановки - маршрутное шифрование, шифрование с помощью решеток и таблица Виженера
- Программная реализация шифров перестановки

# Теоретические сведения. Маршрутное шифрование

При маршрутном шифровании открытый текст записывают в некоторую геометрическую фигуру по некоторому пути, а затем, выписывая символы по другому пути, получают шифртекст.

| | | | | | |
|---|---|---|---|---|---|
| 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:** Маршрутное шифрование

# Теоретические сведения. Шифрование с помощью решеток

Шифрование с помощью решеток производится путем выбора натурального числа $k$, построения квадрата размерности данного числа и заполняется последовательно числами $1, ..., k^2$. Затем квадрат поворачивают и подставляют рядом. Производят это до построения нового квадрата. Далее вырезаются некоторые клетки, в которые вписывают буквы исходного текста.

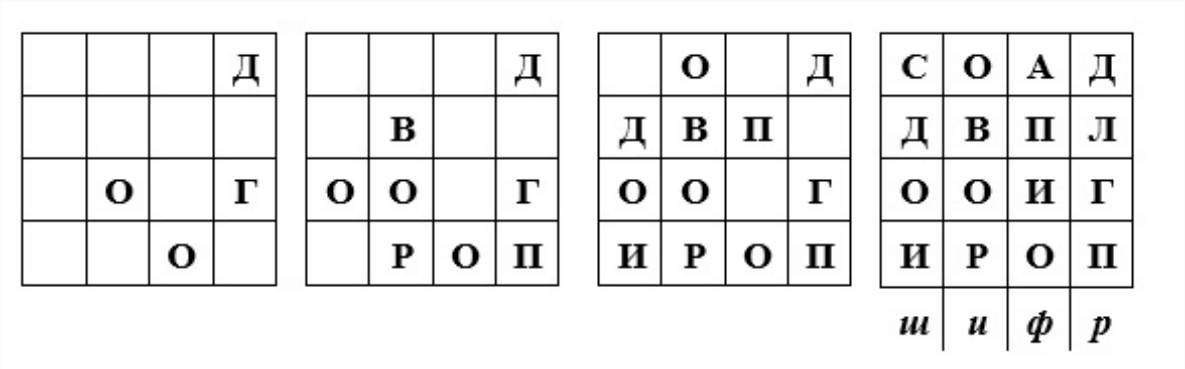


**Figure 2:** Шифрование с помощью решеток

# Теоретические сведения. Таблица Виженера

Схема построения шифра Виженера: в таблицу в строки записываются буквы русского алфавита. При переходе от одной строке к другой происходит циклический сдвиг на одну позицию.

| 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 |

**Figure 3:** Таблица Виженера

# Результат выполнения лабораторной работы

# Результат выполнения лабораторной работы

Постановка задачи:

1. Рализовать маршрутное шифрование
2. Реализовать шифрование с помощью решеток
3. Реализовать таблицу Виженера

# Результат выполнения лабораторной работы. Маршрутное шифрование

Алгоритм поиска зашифрованного текста на основе принципа формирования маршрутного шифрования:

```python
# маршрутное шифрование
def mar(text, key, m, n):
    global rus
    textws = text.replace(' ', '')
    if len(textws)<m*n:
        textws += rus[:m*n-len(textws)]
    t = iter(textws)
    matrix = [[next(t) for y in range(m)] for x in range(n)]
    ps = [rus.index(x) for x in key]
    pss = sorted(ps)
    output = ''
    for letter in pss:
        for x in range(n):
            output += matrix[x][ps.index(letter)]
    return output
```

```python
print(mar('нельзя недооценивать противника', 'пароль', 6, 5))
```

```
еенпнзоатаьовокннеьвлдирияцтиа
```

**Figure 4:** Реализация маршрутного шифрования

# Результат выполнения лабораторной работы. Шифрование с помощью решеток

Алгоритм поиска зашифрованного текста на основе принципа формирования шифрования с помощью решеток:

```
import numpy as np

# шифрование с помощью решеток
k = 2
k2 = [x+1 for x in range(k**2)]
matrix = [[0 for x in range(2*k)] for y in range(2*k)]
matrix = np.array(matrix)
for x in range(k**2):
    c = 0
    for x in range(k):
        for y in range(k):
            matrix[x][y] = k2[c]
            c += 1
    matrix = np.rot90(matrix)
ds = {k: 0 for k in k2}
dss = {1:2, 2:4, 3:3, 4:3}
for x in range(k**2):
    for y in range(k**2):
        ds[matrix[x][y]] += 1
        if ds[matrix[x][y]] != dss[matrix[x][y]]:
```

# Результат выполнения лабораторной работы. Шифрование с помощью решеток

Алгоритм поиска зашифрованного текста на основе принципа формирования шифрования с помощью решеток:

```
text = 'договорподписали'
key = 'шифр'
ct = 0
t = iter(text)
matrixt = [['O' for y in range(k**2)] for x in range(k**2)]
for d in range(4):
    for x in range(k**2):
        for y in range(k**2):
            if matrix[x][y] == 0:
                matrixt[x][y] = text[ct]
                ct += 1
    matrix = np.rot90(matrix, -1)
ps = [rus.index(x) for x in key]
pss = sorted(ps)
output = ''
for letter in pss:
    for x in range(k**2):
        output += matrixt[x][ps.index(letter)]
print(output)
```

```
оворддлгпапиосдои
```



Figure 6: Реализация шифрования с помощью решеток 2

# Результат выполнения лабораторной работы. Таблица Виженера

Алгоритм поиска зашифрованного текста на основе принципа формирования таблицы Виженера:

```
# таблица Виженера
def key_k(m, key):
    key.replace(' ', '')
    m.replace(' ', '')
    key = list(key)
    if len(m) == len(key):
        return(key)
    else:
        for i in range(len(m) - len(key)):
            key.append(key[i%len(key)])
    return(''.join(key))

def vig(m, key):
    ct = []
    m.replace(' ', '')
    for i in range(len(m)):
        x = (ord(m[i]) + ord(key[i])) % 32
        x += ord('A')
        ct.append(chr(x))
    return(''.join(ct))
```

**Figure 7:** Реализация таблицы Виженера

# Выводы

# Выводы

1. Изучили шифры перестановки
2. Реализовали маршрутное шифрование
3. Реализовали шифрование с помощью решеток
4. Реализовали таблицу Виженера