# Лабораторная работа №2

Назарьин Артем. - НПМмд-02-23

27.09.2023

# Шифр перестановок, решеток, таблицы Виженера

# Цель выполнения лабораторной работы

Реализовать шифрование перестановками, шифрование с помощью решеток и таблицы Виженера.

# Выполнение

- Реализую маршрутное шифрование перестановками

```python
#столбцовая перестановка
def stolb_encryption(input_text, key):
    #Удаляем символы-разделители из ключа и переводим его в список символов
    key = [c for c in key if c.isalpha()]
    #Удаляем все символы-разделители из исходного текста
    input_text = ''.join([c for c in input_text if c.isalpha()])
    #Определяем количество столбцов на основе длины ключа
    num_columns = len(key)
    #Вычисляем количество строк в таблице с зашифрованным текстом
    num_rows = len(input_text) // num_columns
    if len(input_text) % num_columns != 0:
        num_rows += 1

    #Заполняем таблицу с шифротекстом пустыми символами
    table = [[''] * num_columns for _ in range(num_rows)]

    #Заполняем таблицу с исходным текстом по столбцам
    index = 0
    for col in range(num_columns):
        for row in range(num_rows):
            if index < len(input_text):
                table[row][col] = input_text[index]
                index += 1

    #Создаем список, содержащий индексы столбцов после перестановки
    column_order = [key.index(c) for c in sorted(key)]
```

**Figure 1:** Маршрутное шифрование, часть 1

# Выполнение

```
    #Создаем список, содержащий индексы столбцов после перестановки
    column_order = [key.index(c) for c in sorted(key)]

    #Шифруем текст, объединяя символы в каждом столбце в порядке перестановки столбцов
    ciphertext = ''
    for col in column_order:
        for row in range(num_rows):
            ciphertext += table[row][col]

    return ciphertext

input_text = 'this message is secret'
key = 'super'
ciphertext = stolb_encryption(input_text, key)
print(ciphertext)
```

```
ssecageiretthismess
```

**Figure 2:** Маршрутное шифрование, часть 2

# Выполнение

- Реализую шифрование с помощью таблицы Виженера. Исходный текст: криптография серьезная наука; пароль – математика. Итоговый результат частично не совпал с примером из задания, поскольку в задании была представлена таблица с неполным алфавитом.

# Выполнение

```
[ ]  #Таблица Виженера
     #шифрование
     def vigenere_encrypt(input_text, key):
         #Преобразуем текст и ключ в верхний регистр
         input_text = input_text.upper()
         key = key.upper()

         #Создаем шифрованный текст
         ciphertext = ''
         for i in range(len(input_text)):
             char = input_text[i]
             if char.isalpha():
                 #вычисляем смещение для текущего символа
                 shift = ord(key[i % len(key)]) - ord('A')
                 #шифруем символ
                 encrypted_char = chr((ord(char) - ord('A') + shift) % 32 + ord('A'))
                 ciphertext += encrypted_char
             else:
                 ciphertext += char

         return ciphertext
```

Figure 3: Шифрование с помощью таблицы Виженера

# Выполнение

```python
#дешифрование
def vigenere_decrypt(ciphertext, key):
    #Преобразуем текст и ключ в верхний регистр
    ciphertext = ciphertext.upper()
    key = key.upper()

    #Создаем дешифрованный текст
    input_text = ""
    for i in range(len(ciphertext)):
        char = ciphertext[i]
        if char.isalpha():
            #Вычисляем смещение для текущего символа
            shift = ord(key[i % len(key)]) - ord('А')
            #Расшифровываем символ
            decrypted_char = chr((ord(char) - ord('А') - shift) % 32 + ord('А'))
            input_text += decrypted_char
        else:
            input_text += char

    return input_text
```

```python
[ ] input_text = 'криптография серьезная наука'
    key = 'математика'

    ciphertext = vigenere_encrypt(input_text, key)
    print('Зашифрованный текст:', ciphertext)

    decrypted_text = vigenere_decrypt(ciphertext, key)
    print('Расшифрованный текст:', decrypted_text)
```

```
Зашифрованный текст: ЦРЪЮЮХШКФФЯ ЦСРОНСНЧЯ ТМУЬИ
Расшифрованный текст: КРИПТОГРАФИЯ СЕРЬЕЗНАЯ НАУКА
```

**Figure 4:** Шифрование с помощью таблицы Виженера

# Выводы

Я реализовал шифрование перестановками и шифрование с помощью таблицы Виженера.