# Отчёт по лабораторной работе №2. Шифры простой замены

#### Цель работы

Реализация алгоритмов маршрутного шифрования, шифрования с помощью решеток, таблицы Виженера с помощью выбранного языка программирования

## Маршрутное шифрование

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.

```
[7]: text = 'Здравствуйте, я Григорий'
newText = text.replace(' ', '').lower()
кеу = 'пароль'
keyLetters = {key[i] : i for i in range (len(key))}
keyLen = len(key)
textLen = len(newText)
m = int(round(textLen/keyLen))
A = np.full((m,keyLen), '')
for i in range(m*keyLen - textLen):
    newText += newText[-1]
tmp_count = 0
for i in range(m):
    for j in range(keyLen):
        A[i][j] = newText[tmp_count]
        tmp_count += 1
print(keyLen, m)
print(np.matrix(A))
6 4
[['s' 'd' 'p' 'a' 'b' 'c']
 ['т' 'в' 'у' 'й' 'т' 'е']
 [',' 'я' 'r' 'p' 'и' 'r']
 ['o' 'p' 'и' 'й' 'й' 'й']]
```

Фрагмент кода программы маршрутного шифрования

# 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.

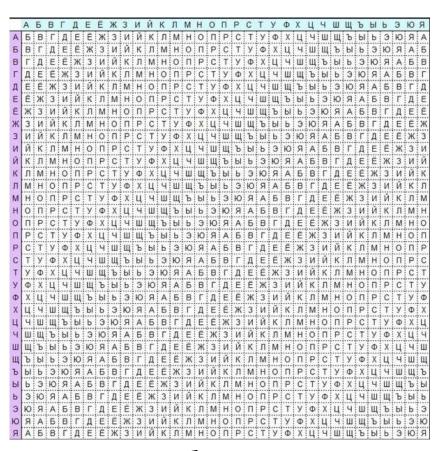
# Шифрование с помощью решеток

```
[46]: print('Bam текст : ', text)
 print('Matrix B:\n', np.matrix(B))
 print('Result matrix\n', np.matrix(answer))
 print('Key = ', key)
 print('Cyphered text = ', ans_text)
 Ваш текст : Здравствуйте я Григорий
 Matrix B:
  [[0. 2. 0. 0. 0. 0.]
  [0. 0. 0. 8. 5. 0.]
  [0. 0. 0. 9. 6. 0.]
  [0. 0. 0. 0. 0. 7.]
  [0. 0. 0. 0. 0. 0.]
  [0. 4. 0. 3. 0. 1.]]
 Result matrix
  [['p' '3' 'u' '*' 'ŭ' '*']
  ['й' '*' '*' 'д' 'р' 'т']
  ['*' '*' '*' 'a' 'B' '*']
  ['e' '*' '*' 's' 'r' 'c']
  ['*' '*' '*' 'p' 'u' '*']
  ['r' 'T' 'o' 'B' '*' 'y']]
 Кеу = лаизьй
 Cyphered text = з****ти****o*т*c*ypй*e*гйрвги**даярв
```

Результат работы программы шифрования 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.

## Шифрование таблицей Виженера



Пример таблицы Виженера

Создадим таблицу Виженера - таблицу, в начале строки и столбца которой находятся все возможные буквы выбранного алфавита. Ключ повторяется до тех пор, пока его длина не станет равна длине сообщения. На пересечении *i*тых координат сообщения и ключа по таблице получается символ.

# Результат работы шифрования Виженера

```
[52]: text = 'Здравствуйте я Григорий'
 newText = text.replace(' ', '').lower()
 key = 'Kapta'
 newKey = key.lower()
 keyLen = len(newKey)
 textLen = len(newText)
 key = newKey
 while len( key) < textLen:
     k = len( key)
     key += key[k-n]
 result = ""
 for i in range(textLen):
     x = letters[ key[i]]
     y = letters[newText[i]]
     result += vignere table[x][y]
 print(result)
 сдатвсдвуутхсгръгоъищ
```

Результат работы шифрования Виженера

#### Выводы

Цель лабораторной работы была достигнута, все три шифра реализованы и работают успешно