Информационная безопасность. Лабораторная работа № 2 на тему “Шифры перестановки”

Мухамеджанов Исматулло Иззатуллоевич

RUDN University, Moscow, Russian Federation

Содержание

Содержание

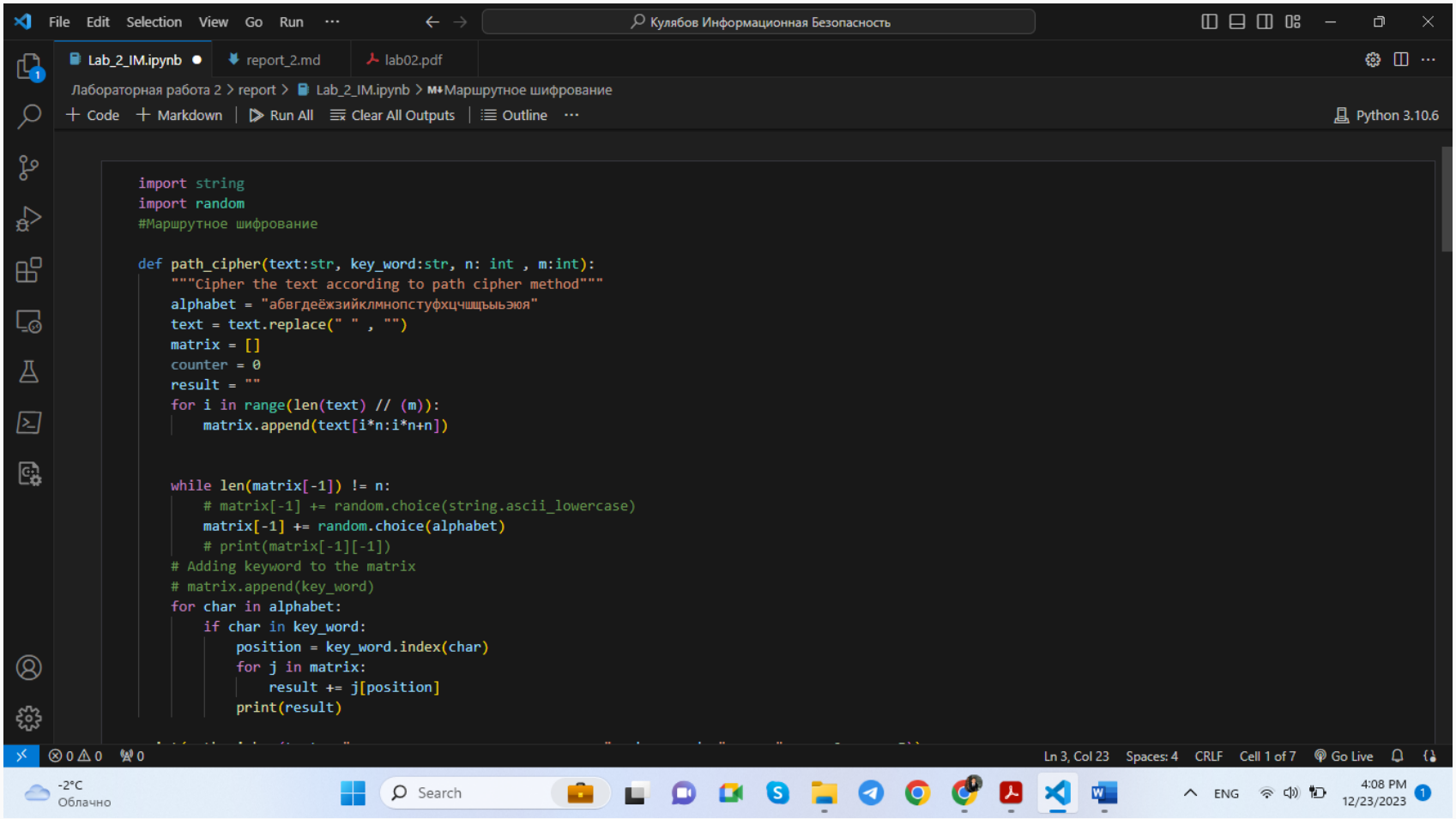
Цели и задачи

Цели и задачи

Освоить на практике применение шифров на основе перестановки

Выполнение

Выполнение



Шифрование с помощью решёток

```
from random import choice, randint
from collections import Counter

text = input("Write the massage: ")
symbols = [chr(x) for x in range(65,91)] # A - Z
symbols += [chr(x) for x in range(97,123)] # a - z
# A - z
while True:
```

Выполнение

```
    text = text.replace(" " , "")
    matrix = []
    counter = 0
    result = ""
    for i in range(len(text) // (m)):
        matrix.append(text[i*n:i*n+n])


    while len(matrix[-1]) != n:
        # matrix[-1] += random.choice(string.ascii_lowercase)
        matrix[-1] += random.choice(alphabet)
        # print(matrix[-1][-1])
    # Adding keyword to the matrix
    # matrix.append(key_word)
    for char in alphabet:
        if char in key_word:
            position = key_word.index(char)
            for j in matrix:
                result += j[position]
            print(result)

print(path_cipher(text = "нельзя недооценивать противника" , key_word= "пароль", n = 6 , m = 5))
```

```
еенпн
еенпнзоата
еенпнзоатаьовок
еенпнзоатаьовокннеьв
еенпнзоатаьовокннеьвяцтил
None
```

Figure 1: Результат маршрутного шифрования

Выполнение

```
keys: [2, 8, 17, 18, 24, 25, 39, 57, 59, 60, 64, 65, 69, 71, 86, 88, 91]

     1   2   3   4   5   6   7   8   9   10
0  | C | д | B | D | V | w | l | o | q | D |
1  | t | M | Q | x | z | T | r | o | j | s |
2  | b | F | B | в | o | P | R | e | d | g |
3  | X | m | L | b | S | Y | J | h | p | z |
4  | n | m | g | C | H | i | j | g | M | q |
5  | B | y | T | T | Q | Y |   | G | п | o |
6  | T | l | p | д | п | c | H | n | и | u |
7  | c | a | r | C | b | H | P | Z | s | w |
8  | O | r | d | r | Q | a | f | л | m | q |
9  | и | Q | g | i | F | k | Q | y | l | z |
```

Figure 2: Результат шифрования с помощью решёток

Выполнение

```python
def encrypt_vegener(plaintext, key):
    key_length = len(key)
    key_as_int = [ord(i) for i in key]
    plaintext_int = [ord(i) for i in plaintext]
    result = ''
    for i in range(len(plaintext_int)):
        value = (plaintext_int[i] + key_as_int[i % key_length]) % 26
        result += chr(value + 65)
    return result

print(f'Result of encryption {encrypt_vegener("cryptography crucial science", "math")} ')
```

✓ 0.0s

```
Result of encryption ADDIRALKYBMRLOWNAUFELEHBCZHX
```

Figure 3: Результат шифрование Виженера

Результаты

Результаты

Освоено на практике применение шифрований методом перестановки, таких как Маршрутное Шифрование Шифрование с помощью решёток Шифрование Виженера

Список литературы

Список литературы

1. Методические материалы курса