

Математические основы защиты информации и информационной безопасности

Роман Сергей Михайлович

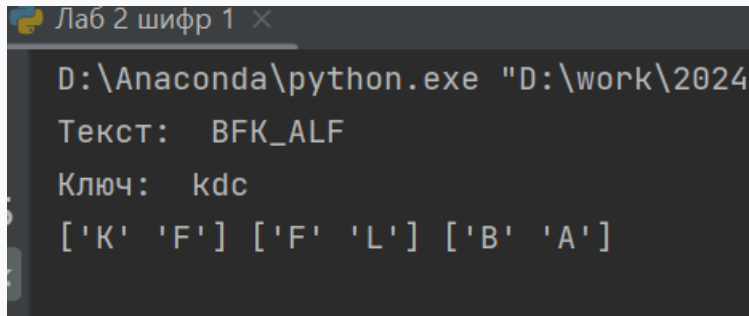
23 Сентября 2025

РУДН, Москва, Россия

Лабораторная работа 2

Маршрутное шифрование

```
Лаб 2 шифр 1.py x Лаб 2 шифр 2.py x Лаб 2 шифр 3.py x
1 import numpy as np
2 translation = {}
3 key = 'kdc'
4 text = "BFK_ALF"
5
6 matr0 = text.split(sep="_")
7 matr = []
8 for i in matr0:
9     matr.append(list(i))
10 matr = np.array(matr)
11
12 j = 0
13 for i in key:
14     translation[i] = str(matr[:,j])
15     j+=1
16
17 answer = dict(sorted(translation.items()))
18 a = answer.values()
19 print(*a)
```

A screenshot of a terminal window with a dark background. The title bar at the top shows a Python logo icon, the text 'Лаб 2 шифр 1', and a close button icon. The terminal displays the following text:

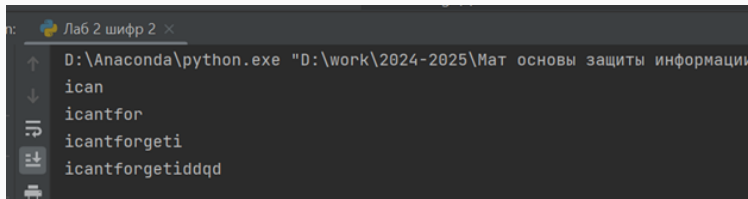
```
D:\Anaconda\python.exe "D:\work\2024  
Текст:  BFK_ALF  
Ключ:   kdc  
['К' 'F'] ['F' 'L'] ['B' 'A']
```

Рис. 2: Вывод программы

Шифрование с помощью решёток

```
Лаб 2 шифр 1.py x Лаб 2 шифр 2.py x Лаб 2 шифр 3.py x
1 def compress(key, val): # similar for itertools.compress
2     key = list(''.join(key)) # make all in one list like ['.....']
3     val = list(''.join(val))
4     return ''.join(v for v, k in zip(val, key) if k == 'X')
5
6 def right_rotate(array):
7     return tuple(map(lambda a: ''.join(reversed(a)), zip(*array)))
8
9 key = ( 'X...',
10        '..X.',
11        'X..X',
12        '....')
13
14 value = ('itdf',
15          'gdce',
16          'aton',
17          'grdi')
```

Рис. 3: Реализация программы

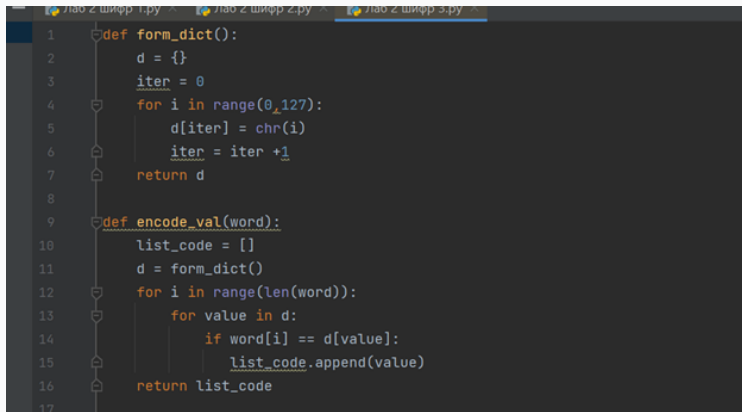


The screenshot shows a terminal window with a dark background. The title bar at the top reads "Лаб 2 шифр 2". The command prompt shows the execution of a Python script: `D:\Anaconda\python.exe "D:\work\2024-2025\Мат основы защиты информации\lab2\shifrir.py"`. The output of the script is displayed on the following lines:

```
ican  
icantfor  
icantforgeti  
icantforgetiddqd
```

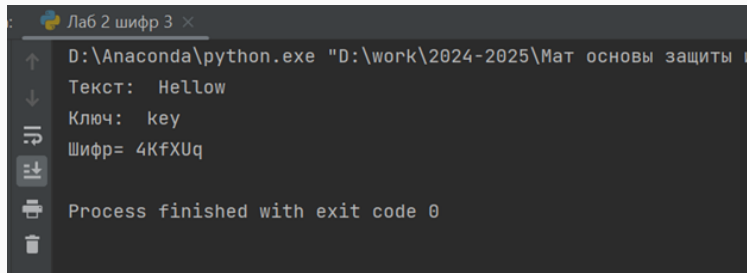
Рис. 4: Реализация программы

Таблица Виженера



```
1 def form_dict():
2     d = {}
3     iter = 0
4     for i in range(0, 27):
5         d[iter] = chr(i)
6         iter = iter + 1
7     return d
8
9 def encode_val(word):
10     list_code = []
11     d = form_dict()
12     for i in range(len(word)):
13         for value in d:
14             if word[i] == d[value]:
15                 list_code.append(value)
16     return list_code
17
```

Рис. 5: Реализация программы

A screenshot of a terminal window with a dark background. The title bar at the top reads "Лаб 2 шифр 3" with a Python logo icon and a close button. The terminal content shows the execution of a Python script using the command "D:\Anaconda\python.exe \"D:\work\2024-2025\Мат основы защиты\"". The output of the script is displayed in three lines: "Текст: Hellow", "Ключ: key", and "Шифр= 4KfXUq". Below the output, a status message states "Process finished with exit code 0". On the left side of the terminal, there is a vertical toolbar containing icons for navigation (up and down arrows), running (a play button), saving (a floppy disk), printing (a printer), and deleting (a trash can).

```
Лаб 2 шифр 3 ×
D:\Anaconda\python.exe "D:\work\2024-2025\Мат основы защиты"
Текст: Hellow
Ключ: key
Шифр= 4KfXUq
Process finished with exit code 0
```

Рис. 6: Вывод программы

- Изучил шифры перестановки.

Реализовал программным путём:

- маршрутное шифрование
- шифрование с помощью решёток
- таблицу Виженера.

Спасибо за внимание!