

Лабораторная работа №1

**Математические основы защиты информации и информационной
безопасности**

Колчева Юлия Вячеславовна

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	10
5	Список литературы	11

List of Tables

List of Figures

3.1	Программа реализации шифра Цезаря	7
3.2	Вывод программы	8
3.3	Реализация шифра Атбаш 1	8
3.4	Реализация шифра Атбаш 2	9
3.5	Вывод программы	9

1 Цель работы

Изучить шифр Цезаря и шифр Атбаш, научиться реализации данных шифров программным путём.

2 Задание

1. Реализовать шифр Цезаря с произвольным ключом k
2. Реализовать шифр Атбаш

3 Выполнение лабораторной работы

Так как я не изучала язык Julia на бакалавриате, первую лабораторную работу я реализовала на python. При дальнейшем изучении я перейду на новый язык.

Для реализации шифра Цезаря мной была написана следующая программа:

```
4 def text_func(text):
5     ctext = ''
6     for i in text:
7         ctext_s = translation[i]
8         ctext += ctext_s
9     return(ctext)
10 key = ""
11 translation = {}
12 letters = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
13 text = "LNFKSLD"
14 random.seed(23)
15 for i in letters:
16     key_s = random.choice(string.ascii_letters)
17     translation[i] = key_s
18     key += key_s
19
20
21 print("Текст:", text)
22 print("Ключ:", key)
23 ctext = text_func(text)
24 print('Зашифрованный текст:', ctext)
```

Figure 3.1: Программа реализации шифра Цезаря

В данной программе:

4-9 строки: функция, реализующая “перевод” текста в шифртекст побуквенно

10 строка: создание пустого словаря

11: зададим алфавит, который будем кодировать. Можно использовать юникод,

однако тогда в шифре мы можем получить не только буквы, но и знаки.

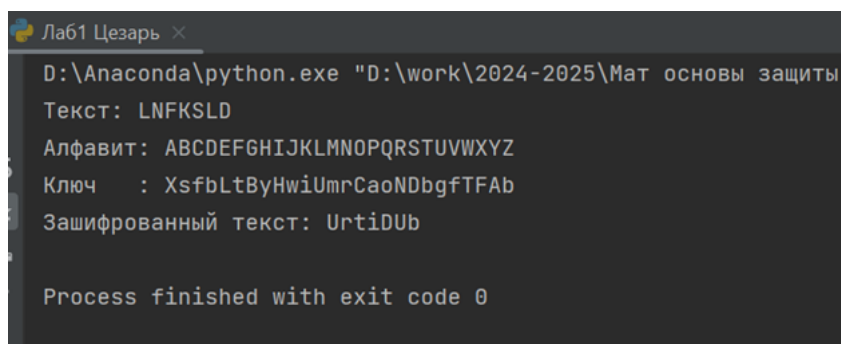
12: текст, который будем кодировать

14: Задаем корень, чтобы ключ каждый запуск оставался одинаковым

15-18: формирование случайного ключа и запись в словарь посимвольное соответствие.

23: запуск функции

Далее представлен результат работы программы



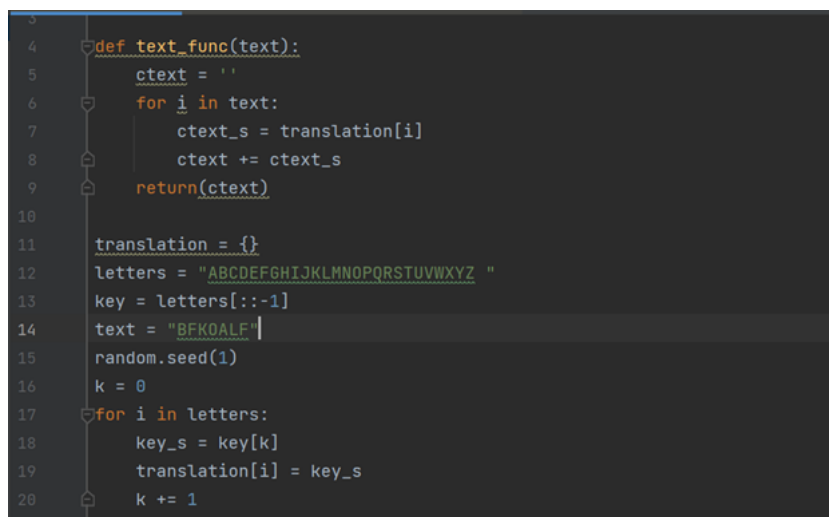
```
Лаба1 Цезарь x
D:\Анаconda\python.exe "D:\work\2024-2025\Мат основы защиты
Текст: LNFKSLD
Алфавит: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ключ : XsfbLtByHwiUmrCaoNDbgfTFAb
Зашифрованный текст: UrtiDUb

Process finished with exit code 0
```

Figure 3.2: Вывод программы

Как видно, программа работает верно

Теперь представим программу реализации шифра Атбаш



```
3
4 def text_func(text):
5     ctext = ''
6     for i in text:
7         ctext_s = translation[i]
8         ctext += ctext_s
9     return(ctext)
10
11 translation = {}
12 letters = "ABCDEFGHIJKLMNOPQRSTUVWXYZ "
13 key = letters[::-1]
14 text = "BFKOALF"
15 random.seed(1)
16 k = 0
17 for i in letters:
18     key_s = key[k]
19     translation[i] = key_s
20     k += 1
```

Figure 3.3: Реализация шифра Атбаш 1


```

21
22     ctext = text_func(text)
23     print("Текст:", text)
24     print("Алфавит:", letters)
25     print("Ключ  :", key)
26     print('Зашифрованный текст:', ctext)

```

Figure 3.4: Реализация шифра Атбаш 2

В данной программе:

4-9 строки: функция, реализующая “перевод” текста в шифртекст побуквенно

11 строка: создание пустого словаря

12: зададим алфавит, который будем кодировать.

13: В данном случае ключом будет являться наш же алфавит в обратном порядке
(с пробелом)

17-20: запись в словарь посимвольное соответствие.

22: запуск функции

Посмотрим на результат работы программы



```

D:\Anaconda\python.exe "D:\work\2024-2025\Мат основы защи
Текст: BFKOALF
Алфавит: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ключ   : ZYXWVUTSRQPONMLKJINGFEDCBA
Зашифрованный текст: ZVQM PV
Process finished with exit code 0

```

Figure 3.5: Вывод программы

Программа работает верно.

4 Выводы

Я изучила шифр Цезаря и шифр Атбаш, научилась реализации данных шифров программным путём.

5 Список литературы

Лабораторная работа №1 Шифры простой замены [Электронный ресурс]. URL:

https://esystem.rudn.ru/pluginfile.php/2368411/mod_folder/content/0/lab01.pdf?forcedownload=1